Acquisition Directorate
peter.kowalski@ncia.nato.int
Tel: +32 (0)2 707 8221
Fax: +32 (0)2 707 8770

NCIA/ACQ/2016/1646
21 September 2016

To : All Nominated Prospective Bidders

Subject : **INVITATION FOR BID NO. IFB-CO-13810-CS, AMENDMENT NO. 4**

PROVIDE ENTERPRISE NATO PUBLIC-KEY INFRASTRUCTURE (E-NPKI)

Reference(s) :
A. AC/4-D/2261 (1996 Edition)
B. NCI AGENCY IFB-CO-13810-CS issued 20 April 2016
C. NCI AGENCY IFB-CO-13810-CS AMD 1 issued 15 June 2016
D. NCI AGENCY IFB-CO-13810-CS AMD 2 issued 28 July 2016
E. NCI AGENCY IFB-CO-13810-CS AMD 3 issued 31 August 2016

Dear Sir / Madam,

1. The purpose of this Amendment 4 is to:

   a) Revise the IFB Bid Closing Date,

   b) Publish Round 4 of IFB Bidders' questions and NCI Agency answers,

   c) Issue revised IFB documents (Book I + Book II),

2. In accordance with the Procedures for International Competitive Bidding AC/4-D/2261 (1996 Edition), paragraph 10 (d), sub-paragraph (iii) (1), the Book I, Part I, Bidding Instructions, Section 2, General Bidding Information, Para 2.3.1, is hereby revised as follows:

   FROM:

   "*All Bids shall be in the possession of the Purchaser at the address given below in paragraph 2.3.2 before 12:00 hours (Brussels Time) on* ***28 SEPTEMBER 2016*** *at which time and date bidding shall be closed.*

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int

TO:

"*All Bids shall be in the possession of the Purchaser at the address given below in paragraph 2.3.2 before 12:00 hours (Brussels Time) on* ***19 OCTOBER 2016*** *at which time and date bidding shall be closed.*

3. Final NCI Agency answers to all Bidders' further requests for clarification resulting from the clarifications or changes made at IFB Amendment 3 are hereby published with this IFB Amendment 4 as Attachment 1. The period for submission of requests for clarification as stated in IFB Book I, Para 2.6.2 remains closed.

4. Some answers to Bidders' further requests for clarification have necessitated changes to the IFB bidding documents. Revised bidding documents as indicated in Para 1 above are attached to this IFB Amendment 4 as Attachment 2 and replace the original versions in their entirety. Potential Bidders are strongly advised to carefully review these revised bidding documents.

5. With the exception of the revisions mentioned above, all other IFB documents remain unchanged from their original version as issued on 20 April 2016 or as already amended.

6. Prospective Bidders are advised that the NATO NCI Agency reserves the right to cancel this IFB at any time in its entirety and bears no liability for bid preparation costs incurred by firms or any other collateral costs if bid cancellation occurs.

7. The sole NCI Agency point of contact for all information concerning this IFB is Mr. Peter Kowalski, Senior Contracting Officer, who may be reached at Peter.Kowalski@ncia.nato.int or by telephone on +32 (0)2 707 8221.

FOR THE GENERAL MANAGER:

[*Original Signed By*]

Agata Szydelko
Deputy Director of Acquisition

Attachments: IFB Amendment 4

1) IFB Bidders' Questions and Answers at AMD 4

2) Revised Bidding Documents:

a) IFB Book I – Bidding Instructions, Annex A

b) IFB Book II – SSS and SOW Annex A SRS

Distribution List

All Nominated Prospective Bidders 1

NATO Delegations (Attn: Infrastructure Adviser):

Belgium	1
Bulgaria	1
Canada	1
Czech Republic	1
Denmark	1
Estonia	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
The Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1
United Kingdom	1
United States	1

Distribution for information

NATO HQ

NATO Office of Resources
Management and Implementation Branch – Attn: Deputy Branch Chief 1

Director, NATO HQ C3 Staff
Attn: Executive Co-ordinator 1

SACTREPEUR
Attn: Infrastructure Assistant 1

Strategic Commands

ACT

HQ SACT Attn: OF4 J. Maher, OF4 V. Bello	1

SHAPE

Attn: J6 – Cyber Defence Plans and Policy – Mr Paul Atkinson	1
Attn : J6 - Cyber Defence Plans and Policy – Mr Stefano Piermarocchi	1

NCI Agency – NATEXs

Belgium	1
Canada	1
Czech Republic	1
Denmark	1
Germany	1
Greece	1
Hungary	1
Italy	1
The Netherlands	1
Norway	1
Poland	1
Spain	1
Turkey	1
UK	1
USA	1

NCI Agency

ACQ Director of Acquisition – Mr P. Scaruppe	1
ACQ Deputy Director of Acquisition – Ms A. Szydelko	1
ACQ Contract Award Board Administrator - Ms M-L Le Bourlot	1
ACQ Principal Contracting Officer - Ms T. Pezzi	1
ACQ Acquisition Consultant - Ms Sherrie Mendes	1
DIS – Chief CS SL – Mr I. West	1
DIS – CS SL – Mr F. Jordan / Mr G. Hallingstad	1
DIS – Project Manager	1
DIS – Technical Lead	1
ACQ ILS – Mr C. Lucas	1
NLO - Mailbox	1
Legal Office	1
Registry	1

Index No.	IFB Source Document	IFB Paragraph Reference	Bidder's Question	Purchaser's Answer	IFB Package Amended ?	Released @ AMD #
CR#1	Book II Part IV	SOW FINAL	[Bidder requested Purchaser to furnish 86 reference documents from the SOW]	The majority of the reference documents are available on-line or through commercial publication services. The following links can be helpful: www.everyspec.com www.nato.int/docu/standard.htm Wikipedia has a large collection of NATO documents like STANAGS, AQAP's, etc. For documents above NATO UNCLASSIFIED you will need to contact your National authorities (ex. your MoD/DoD and/or your Nations Delegation to NATO) to ask them to provide you with a copy. Note that they can only transmit such documents if you have in place the ability and permissions to receive and store such data. Bidders who can document that all the possibilities described above have been completely exhausted without positive results may contact the Purchaser POC for further direction.	NO	**AMD#1**
CR#2	Book II Part IV	page 111	Would you have a job description of both Site Implementation and Manager ILS Engineer please?	The Labour categories "Site Implementation Manager and ILS Engineer" are not described in the IFB because those roles are not considered to be "Key Personnel" for the project.	NO	**AMD#1**
CR#3	Book I	2.3.1	Please confirm that the Bid Submission Date is 13 July 2016 as per the content of the covering letter and not 1 July 2016 as per paragraph 2.3.1 of the Instructions to Bidders.	It is confirmed that there was a discrepancy in the IFB as issued - the correct initial Bid Closing Date is 13 July 2016. With Amendment 1, and further to a Nation's request, the revised Bid Closing date at AMD 1 is 8 August 2016.	YES	**AMD#1**
CR#4	Book I	3.6.4.10.1	The format for the BRCM in Annex E proposed has separate columns for the Bid Instructions and the various SOW content that need to be traced through to the proposal made by the contractor, which is as per the standard NATO proposal format. However it shows that there should also be traceability between the Bid Instructions and the SOW where appropriate. However this additional traceability between the Bid Instructions and SOW will result in a large amount of white space within the BRCM when printed out because the 326 statements in the Bid Instructions will not easily trace to the ~2000 requirement statements across the SOW. Do we need to demonstrate the traceability between BI and SOW as majority of the SOW statements will either not be traced to a Bid Instruction (as N/A) or many SOW statements will be traced to the same Bid Instruction? Wouldn't it be more efficient to just trace Bid Instructions and SOW requirements to the relevant part of the Contractor's proposal, i.e. BRCM only uses 4 columns; Requirement Reference, Description, Bid Reference, Remarks?	It is not the Purchaser's intention to create unnecessary burden on the Bidders. The proposed BRCM template actually aims at reducing the number of rows in the matrix by combining/tracing appropriately Bidding Instructions and SOW requirements. However, the Purchaser welcomes the Bidder's suggestion and proposal to optimize the BRCM exercise. As a result, Book I Annex E was updated at IFB AMD 1 and replaces the version from the original IFB in its entirety. Further, the Bidders shall deliver the BRCM in an Excel format, according to the template provided by the Purchaser as part of IFB AMD 1.	YES	**AMD#1**

CR#5	Book I	3.6.4.10.1	It is assumed that when populating the BRCM, we should only include the SOW statements that are considered requirements (because they include an appropriate “shall”, or a sub bullet of an appropriate “shall” statement) with the appropriate section headers to provide context, and we can omit the information statements (i.e. non-requirement statements). Is this acceptable?	The Bidders shall refer to the new Book I Annex E (see CR#4). The new Book I Annex E mentions that the "Reference ID" column of the BRCM shall cover: - Bidding Instructions - SOW requirements (covering all "shall' statements of the SOW (including SOW Annexes A, B, and C)	NO	**AMD#1**
CR#6	Book I	Annex E	The BRCM identifies that the SOW requirement references to be used for Annex C should be “SOW Annex B - #”. It is assumed that this is a typo, and should be “SOW Annex C - #”?	Corrected at IFB AMD 1.	YES	**AMD#1**
CR#7	Book I	Annex E	Although there is a requirement to complete the BRCM, NCIA have not expressed a preference for labelling where in the proposal a requirement is answered. Could NCIA confirm that their intention is to rely on the BCRM to identify where requirements are answered, and that it will not be necessary to include the lengthy requirement labels within the proposal volumes themselves?	As mentioned in Book I Annex E, in the BRCM the "Bid Reference" shall be provided in the form "Volume # - Doc # - Section #". The Purchaser confirms that there is no need to include the SOW labels in the proposal volumes themselves.	NO	**AMD#1**
CR#8	Book I	4.4.1.5.1	It is assumed that paragraph 4.4.1.5.1 should refer to paragraph 3.4.3.2 and not paragraph 3.4.4.2 - Please confirm this is the case.	Corrected at IFB AMD 1.	YES	**AMD#1**
CR#9	Book II Part IV	5.5.2.5 & 5.5.7	Paragraphs 5.5.2.5 & 5.5.27 Refer to document REF 2.1.2.10, which appears to be incorrect, should these references be to documents listed in 2.1.3?	This is correct. Corrected in IFB AMD 1.	YES	**AMD#1**
CR#10	Book II Part II	5.5	Please provide the formal definition of "identifiable sub-assemblies" in the context of software.	The existing NATO definition does not exclude software.	NO	**AMD#1**
CR#11	Book II Part IV	Annex A, SRS 3.4.9.5, SRS-2198 & SRS-2199	It is assumed that the 99.5% and 98% availability requirements for the revocation services at sites is calculated per site (i.e. should exceed the availability target per site), and is not the target for the availability of the service at all sites. Is this a correct interpretation?	As stated in SRS-2198 the requirement refers to "the end to end availability of revocation services." (i.e. the ability for an end entity at a site to find at least one available source of revocation data within the system without the requirement for manual intervention.)	NO	**AMD#1**
CR#12	Book II Part IV	Annex A, SRS 4.1.12, SRS-631	It is assumed that the 99.5% availability requirements for E-PKI at sites is calculated per site (i.e. should exceed the availability target per site), and is not the target for the availability of the service at all sites. Is this a correct interpretation?	As stated in SRS-631 the requirement refers to the E-NPKI system availability as a whole. (i.e. when considering all components which are providing geographically diverse backup of each other.) If one CA fails, but the failure does not impact service operations (i.e. the other two sites cover the service without degradation or manual intervention), then there is no impact on system availability. The availability requirement for Registration Authorities is a per site and per domain calculation. New Requirement SRS-2828: Registration Authority services on each domain of each site shall have an availability of 99.5%.	YES	**AMD#1**

CR#13	Book II Part IV	Annex A, SRS SRS-2814	Where no CMS components are in place, the E-NPKI shall provide the full CMS including camera and printing capabilities. Can the Purchaser please define the scope/scale of this requirement by Site?	The scope of CMS is defined in sections 2 through 4 of FIPS201-2 (see SOW Ref 2.2.4.) The CMS shall support all biometric capture requirements of FIPS 201-2 chapter 2, but the vendor is only required to provide hardware to support image capture and printing. See details in CR#15 through CR#18 for information by site.	YES	**AMD#1**
CR#14	Book II Part IV	Annex A, SRS SRS-2014	Integration with existing physical control systems - Can the Purchaser please confirm the number of discrete instances by Site that this activity is required at?	All sites have physical Access control systems. See details in CR#15 through CR#18	NO	**AMD#1**
CR#15	Book II Part IV	Annex A, SRS SRS-2161	Integration with CITI manageID CMS - Can the Purchaser please confirm the number of discrete instances by Site that this activity is required at?	Currently installed at NATO Command Structure sites (SOW Table 7 sites 5 through 40) and NCI Agency The Hague on PBN. (All NCI Agency sites are co-located with NATO Command Structure except NCI Agency The Hague and NCI Agency Brussels)	NO	**AMD#1**
CR#16	Book II Part IV	Annex A, SRS SRS-2722	Entrust IdentityGuard CMS - Can the Purchaser please confirm the number of discrete instances by Site that this activity is required at?	Currently planned for the New NATO HQ in 2016 on PBN and ON (1 site, 2 discrete instances)	NO	**AMD#1**
CR#17	Book II Part IV	Annex A, SRS SRS-2723	Xtec AuthentX Basic enrolment Station CMSs - Can the Purchaser please confirm the number of discrete instances by Site that this activity is required at?	Not currently installed at any sites.	NO	**AMD#1**
CR#18	Book II Part IV	Annex A, SRS SRS-2163	Non FIPS 201 compliant existing CMS implementations - Can the Purchaser please confirm the number of discrete instances by Site that this activity is required at?	For the ON, assume this to be the default for all sites not covered by CR#14 through CR#17.	NO	**AMD#1**
CR#19	Book II Part IV	Annex C Site 14	NATO HQ has no users/devices listed against any network, is this correct?	For this question, the Purchaser assumes that the bidder referred to the NCIS Group HQ, and not NATO HQ for which is addressed under CR#21. The NCIS group HQ is co-located and fully serviced by Site 5 (SHAPE). Therefore user and device quantities are included in the SHAPE numbers. Number of users and devices to be verified during site survey.	NO	**AMD#1**
CR#20	Book II Part IV	SOW 16.7.3.2	With regards to the number of Contractor supplied smart cards this section states that "Where interim NPKI users have RSA only smart cards, certificates shall be loaded onto a Contractor supplied smartcard". However, Annex C does not distinguish between Elliptic Curve smart cards and RSA smart cards. Can this distinction be made to give indicative numbers of Contractor supplied RSA replacement cards?	E-NPKI is an Elliptic Curve cryptographic (ECC) system. All smart cards identified in Annex C are ECC smart cards. Where interim NPKI users have RSA only smart cards, certificates shall be loaded onto a Contractor supplied ECC based smartcard. Updated in IFB AMD 1 .	YES	**AMD#1**

CR#21	Book II Part IV	Annex C Site 1	New NATO HQ has no Card readers or Smart Cards listed against any network, is this correct?	As stated in the table in Book II - Part IV, Pages 192-194 Table 9 - User List; the NNHQ requires certificates to be deployed, but does not require smart cards. The NNHQ has already procured ECC smart cards ((SRS-2824 refers to Safenet SC650 (ON) and Gemalto IDPrime PIV card v2.0 (PBN)) which shall be integrated by the E-NPKI Contractor. The NATO HQ site referenced in Table 9 and the New NATO Headquarters site referenced in Table 10 refer to the same site (NATO HQ will transition to the New NATO HQ prior to the deployment of E-NPKI.)	NO	**AMD#1**
CR#22	Book II Part IV	Annex B 4.1.4	The Purchaser requirement defines integration and complements the NATO tools - Can the Purchaser please confirm the following: Does integration mean - the synchronisation of status and data via regular updates and over available interfaces within the ITSM tooling such as SMTP?	The intention is not to have the contractor duplicate existing ITSM tools. The Contractor shall provide integration and licenses as required for those tools already installed in the purchaser's environment. The following tools are currently in use by the purchaser • BMC Remedy • LanSweeper • BMC Atrium • BMC Atrium Discovery and Dependency Mapping tool (ADDM) • MS System Centre • SNMP • MS SCOM and agents NCI Agency is utilising BMC ITSM (version 7.6, expected to be upgraded to version 8.1 by the end of 2016) toolset for following Service Management and Control capabilities: • Centralized Service Desk (Mons) is using Remedy 7.6 as incident management tool in NS, NR and NU domains. • Atrium 7.6 is the enterprise level CMDB for NS, NR and NU domains. LanSweeper and ADDM is being used for IT asset discovery. • Change Management, Request fulfilment, Problem Management and Knowledge Management is being implemented currently. MS System Centre 2012 is used for the following SMC capabilities: • Event Management and infrastructure availability/performance monitoring. • Software deployment management. The Contractor shall implement interfaces for following SMC functions using the protocols/technologies defined: • Incident and Problem Management: SMTP, Web services with payload format compatible with BMC Remedy 7.6 and 8.1 • Service Asset and Configuration Management: Web services with payload format compatible with BMC Remedy 7.6 and 8.1. Support BMC ADDM asset discovery for infrastructure and software components. • Event Management and monitoring: SNMP, MS SCOM agents. The Contractor shall provide licenses for the following modules/products to compensate the additional usage required to provision E-NPKI services: • Remedy Incident Management concurrent licences: X (# of E-NPKI first line	YES	**AMD#1**
CR#23	Book II Part IV	SOW 6.5.2.1	Can the Purchaser confirm that the components that SDIP 293/1 is applicable to are all keyed certificate generation and storage devices?	SDIP 293/1 is applicable to all certificate generation and storage devices. Status of key load is not relevant.	NO	**AMD#1**

CR#24	Book II Part IV	SOW 6.5.2.1	Can the Purchaser confirm that a device is not considered 'crypto' until its First Operational Key is loaded? Also can the Purchaser confirm what state the device is to be considered to be at and thus handled if a manufactures recommended purge cycle has been performed for : a- transportation to a different location b - Final Disposal	See answer to CR#23, CR#25, and CR#26. See SOW Annex A SRS 3.6.2.1 SRS-774 and SRS-776. As defined in SRS-2650, once operationally keyed, hardware security modules are never deemed to be declassified. Personalized smart cards are not deemed to be suitable for re-use by other persons. Non-personalized tokens (if any) would also be returned to cryptographic inventory. SRS 2651 states that "In the event of media or HSM components under warranty, the failed units shall not require return to the vendor in order to receive warranty replacement." SRS 2652 states that any "Failed component shall be destroyed in accordance with NATO policy."	NO	**AMD#1**
CR#25	Book II Part IV	SOW 7.4.10.2.1	Can the Purchaser confirm who is responsible for the shipment of all components (crypto & non-crypto) to and from the CFSP and the relevant Level 2 maintenance facility?	After initial deliveries to the location specified in the SSS, the Purchaser shall be responsible for the shipment of all components to the relevant Level 2 maintenance facility (assuming acceptance IAW paragraph 21 of the General Conditions). The purchaser shall also assume responsibility for any costs associated with the return of equipment under warranty to the purchasers designated repair/replacement facility. Any subsequent costs for the replacement of a warranty item to the designated delivery location specified by the purchaser shall be the responsibility of the Contractor. Where nationally mandated, crypto/CCI material shall be shipped to the NDA of the appropriate Nation for forwarding to the purchaser specified location at Contractor expense.	NO	**AMD#1**
CR#26	Book II Part IV	SOW 7.4.10.3.2	Can the Purchaser confirm who is responsible for the shipment of all components (crypto & non-crypto) to and from the relevant Level 3 maintenance facility?	On initial purchase, the Contractor shall be responsible for the shipment of all components to the location specified in the SSS. Subsequently the Purchaser shall be responsible for the shipment of all components to any Level 3 maintenance facility (assuming acceptance IAW paragraph 21 of the General Conditions). The purchaser shall also assume responsibility for any costs associated with the return of equipment under warranty to the purchasers designated repair/replacement facility. Any subsequent costs for the replacement of a warranty item to the designated delivery location specified by the purchaser shall be the responsibility of the Contractor. Where nationally mandated, crypto/CCI material shall be shipped to the NDA of the appropriate Nation for forwarding to the purchaser specified location at Contractor's expense.	NO	**AMD#1**
CR#27	Book II Part IV	Annex A, SRS 3.4.9.5, SRS-2198 & SRS-2199 and 4.1.12, SRS-631	It is assumed that the availability target measurement period is calculated over a one year period, i.e. the availability is equal to time service is available over a 1 year period divided by 1 year as percentage. Is this a correct interpretation?	Yes, since the Agreed Service Time (AST) is the same as calendar time (i.e. 100% utilisation) then Operational Availability (Ao) = Uptime / (Uptime + Downtime), where Uptime + Downtime = AST and Downtime includes any form of downtime, whether caused by failures, preventive maintenance, breaks, strikes, refilling, cleaning... whatever.	NO	**AMD#1**
CR#28	Book II Part IV	Annex A, SRS 4.1.1.4.1, SRS-2553	It is assumed that this requirements means that MTTR for each subsystem is not excluded from the Availability calculation, i.e. time to restore service is included as part of the unavailability time. Is this a correct interpretation?	Yes Time to restore service is included as part of the unavailability time. (See CR#27)	NO	**AMD#1**

CR#29	Book II Part IV	Annex B 3.3.5	Can the Purchaser please confirm at which security tiers they expect integration with the NATO ITSM Toolkit for change requests: a - NU/NR b - NS c - Both	Both. See CR#22.	NO	**AMD#1**
CR#30	Book II Part IV	Annex B 3.3.5	Can the Purchaser please confirm at which security tiers they expect integration with the NATO ITSM Toolkit for event transfer and escalation: a - NU/NR b - NS c - Both	Both. See CR#22.	NO	**AMD#1**
CR#31	Book II Part IV	Annex A, SRS SRS-2758	Can the Purchaser please confirm that for the auto-enrolment of Windows Devices, all operational CAs are using Active Directory Certificate Services (ADCS) on Windows Server 2008 R2 or higher?	There is no requirement for the provision of a specific CA in this SRS item. The choice of CA product is the responsibility of the bidder. All CA software shall have a Cryptographic approval from a NATO Nation CIS Security Authority (NCSA). Requirement is for integration of a vendor selected (and NCSA approved) CA product configured to provide an online interface with Microsoft Windows Servers and Workstations.	NO	**AMD#1**
CR#32	Book II Part IV	Annex A, SRS SRS-2758	Can the Purchaser please provide the total number of discreet existing Domain issuing CAs within NATO which must be signed by the E-NPKI solution? Can this be provided per security domain and also confirm these numbers reflect the totality of Domains (this includes each Domain in a Forest independently)?	The total number of authorized Certificate Authorities, their function, and their location is defined in Book II - Part IV Annex C Section 1 Table 7 - List of sites. There is no additional authorization for separate Domain issuing CAs.	NO	**AMD#1**
CR#33	Book II Part IV	Section 2	Please could NCIA supply up to date issues of the documents listed as Applicable Documents at Section 2 of the SOW?	See answer at CR #1.	NO	**AMD#1**

CR#34	Book II Part II	12.1	Is it reasonable that Contractor will indemnify and hold harmless NATO, its servants or agents, against any liability, loss or damage arising out of or in connection of the Supplies and Services under this Contract? Regarding the provisions set out in Article 9, "Intellectual Property Rights Indemnity and Royalties", this is reasonable, but regarding the remainder Tenderer would like to propose the following text: The Contractor shall be held liable for any loss or damage sustained by NATO in connection of the Supplies and Services under the Contract, but only to an amount not exceeding the total amount of what is paid by Purchaser to Contractor in the calendar year before the event occurred. The Contractor will indemnify NATO, its servants or agents against any liability, loss or damage arising out or in connection of the Supplies and Services under this contract regarding the provisions set out in Article 9, "Intellectual Property Rights Indemnity and Royalties". Nevertheless, if the damage or loss is caused by the gross negligence or wilful misconduct of the Contractor or of its personnel or subcontractors, the Contractor shall have unlimited liability for the amount of the damage or loss.	The purchaser in unable to modify the Article as requested. Regarding liabilities, potential Bidders may find it useful to keep in mind the context of the governing Belgian commercial law regarding which damages may need to be covered (i.e. those which are direct and predictable).	NO	**AMD#1**
CR#35	Book II Part III	13.9	With reference to the very last sentence of this article: "The Contractor shall indemnify the Purchaser for damages caused by the Contractor to the Purchaser, its property and staff and arising out of the Contractor's use of the Purchaser Furnished Property", Contractor suggests to add a cap of the liability Contractor mentioned in questions # 1, stated that Contractor is only liable to an amount not exceeding the total amount of what is paid by Purchaser to Contractor in the calendar year before the event occurred. Can Purchaser agree with such change in the liability?	Bidder acceptance of the NCI Agency Contract General Provisions is mandatory and changes may not be considered.	NO	**AMD#1**
CR#36	Book II Part III	40.1	Regarding the following sentence: "The performance of Work under this Contract may be terminated by the Purchaser in accordance with this Clause in whole, or from time to time in part, whenever the Purchaser shall determine that such termination is in the best interest of the Purchaser"". Will Purchaser, when Purchaser intends to terminate the Contract for convenience as stated in this clause, consider to grant the Contractor a hundred-and-eighty (180) days' written notice? Furthermore will Purchaser in the event of such termination for convenience consider to compensate Contractor for non-amortized investments?	Bidder acceptance of the NCI Agency Contract General Provisions is mandatory and changes may not be considered. It is not possible in advance, without all the facts and circumstances being known, to state with certainty how the Purchaser would treat the allocability and/or allowability of any particular contract termination cost(s).	NO	**AMD#1**
CR#37	Book II Part I	SSS	Provide the Microsoft Excel version, please.	The Purchaser does not provide this document at the IFB stage in native Excel format. This is to prevent that a Bidder would improperly use that file as a Bidding Sheet for their price proposal.	NO	**AMD#1**

CR#38	Book I	Annex A	On tab “Delivery per Site” deliverables (e.g. “Letter to Site POC”) are assigned to CLIN’s (this case CLIN 2,3,7-18). However on the tabs related to the CLIN’s the deliverables do not show up consistently. For this example only tab CLIN 2 and CLIN 3 contain a line item for “Letter to Site POC”. A corresponding line item in CLIN7-18 is missing. Why? Are the totals now calculated correctly?	As mentioned in Book I Annex A-2 Section 7.2, the tab "Delivery per site" distinguishes between Technical Services sub-CLIN (highlighted in GREEN), and User Services sub-CLIN (highlighted in YELLOW). The item "Letter to Site POC" is highlighted in GREEN, and therefore is part of the "Technical Services". CLIN7-18 request the delivery of "Site-Specific System Implementation deliverables - Technical Services" according to the "Delivery per site" tab, and "Site-Specific System Implementation deliverables - User Services" according to the "Delivery per site" tab. As a result, all items from the tab "delivery per site" are required for CLIN7-18; there is no mistake in the Bidding Sheets. However, it is the responsibility of the Bidder to ensure all calculations and links are correct when completing the bidding sheets.	NO	**AMD#1**
CR#39	Book I	Annex A	In tabs CLIN 1….19 column E contains the Quantity and column I contains the total Firm Fixed Price. Does the total Firm Fixed Price cell contain the item price for that sub-CLIN or is it the item price multiplied with the number in Quantity? If the first (so it is a price per item) is the total for the CLIN (investment ceiling) calculated correctly? If it is the latter (so the price reflects the total of all the items to be delivered) is the item price not relevant for future use? Also in that case, what is the meaning of “as required” in column E? Does contractor carry the risk for the quantity to be delivered?	The "Total Firm Fixed Price" column contains the item extended price, unit price multiplied with the number in Quantity. There has been an update to the Bidding Sheets and SSS to include the Unit Price requirement. The item price is relevant for future use and the detail is required in the CLIN Breakdown sheets to provide traceability from the details to the unit price and to the Total Firm Fixed Price. In the last question, "as required" is used when providing a quantity is not practical or not possible. Bidders are invited to read the SOW carefully to estimate the relevant quantities. Bidders bear the risk for the quantities to be delivered.	YES	**AMD#1**
CR#40	Book I	Annex A	In tab “CLIN 2” row 80 about CLIN 2.7.16, On-site training is mentioned a quantity “See delivery per site”. Following this reference and looking in tab “Delivery per Site” we find in the column “On-site training” only 1 site: the non production environment Mons. What is the reason for this and why don’t we see the first 6 sites of CLIN 2 in this column?	In the tab "Delivery per Site", the column AS "On-site Training" is traced to all CLINs as appropriate (namely CLINs 2-3, 7-18) The Purchaser invites the Bidders to carefully read the tab "Delivery per Site".	NO	**AMD#1**
CR#41	Book I	Annex A	In tab “CLIN 4” in column E (Quantity) several times the reference to “See delivery per Site” is mentioned. In the tab “Delivery per Site” however we do not see any indication of CLIN 4. Now it looks like all these deliverables in CLIN 4 have a quantity of 0. What is the number of sites to be delivered where the price should be based on?	In CLIN 4, Training Requirement Analysis (TRA) report, and Training Materials refer to the tab "Delivery per site". In the tab "Delivery per site", the columns AQ and AR trace to the TRA report and the Training Materials respectively. In those two columns Bidders can find the relevant CLINs under which the TRA Report and the Training Materials shall be delivered.	NO	**AMD#1**
CR#42	Book I	Annex A	In the tab “Bidding Instructions” is mentioned in row 25 that the Grand total per CLIN should feed into the SSS. Is this “Book II Part I SSS Final”, in which cells do the Grand Total (x) feed into?	The SSS is equivalent to the Detailed CLIN Summary. The Bidders are invited to complete the tab "Detailed CLIN Summary" as if it was the SSS. The cells that should be fed with the Grand Total X are the Total lines for each CLIN. These totals should also align with the CLIN Summary as well.	NO	**AMD#1**

CR#43	Book I	Annex A	In the tab “Site Summary” a break down per site is requested. What needs to be done with row 8 “NON-SITE SPECIFIC” and what is the relation with the CLIN breakdown sheets?	There was an error in line 8, this has been adjusted to reflect the required cells indicated by the yellow highlighting.	YES	**AMD#1**
CR#44	Book I	several	Taking in consideration the information provided in the “1_IFB-CO-13810-CS Book I Instructions to Bidders FINAL” document, point 1.5.5, “The potential Bidders may submit questions in writing not later than 7 days prior to the date of the Conference to the POC” and the information provided in the same document, point 2.6.2, “All questions and requests for clarification shall be forwarded to the Purchaser via email using the Clarification Request Form provided at Annex D of this Book I. Such questions shall be forwarded to the point of contact specified in Section 2.5.1 above and shall arrive not later than twenty eight (28) calendar days prior to the stated "Bid Closing Date”, we are kindly asking you to confirm which is the dead-line for submission of clarification question towards the Purchaser.	Para 1.5.5 refers only to questions that a Bidder would like to be answered at/during the Bidders' Conference. Para 2.5.1 is the global deadline for Clarification Requests.	NO	**AMD#1**
CR#45	Book I	Annex B-12, point b) Section 2.2.4	In order to allow the bidders to create a more competitive technical and financial offer please confirm our understanding that the hardware provided as part of the offer can include individual components such as power supplies, HDD, RAM components etc. that are manufactured outside the boundaries of the NATO participating nations. Also please confirm our understanding that the requirement impose that the company that sell, manufacture and assembly the COTS equipment shall be registered in a Participating Country, even if that company had manufacturing/assembly facilities in Non-Participating Country (for Example Intel processors used in servers are produced by Intel, an American company, but the processors are assembled in Facilities located in China, Malaysia, Vietnam http://www.intel.com/content/www/us/en/architecture-and-technology/global-manufacturing.html)	The IFB requirements prescribed in Book I, Instruction to Bidders, paragraph 2.2.4, Annex B-12, as well as related prospective contract Special and General Provisions derive from standard NATO procedures for international competitive bidding, and as the Purchaser has not been authorised to proceed otherwise, any deviation or qualification from the requirements of the IFB may render a Bid non-compliant.	NO	**AMD#1**
CR#46	Book I	N/A	Related to the presentation of the offer, please confirm if there is a limitation regarding the number of pages of the offer (minimum/maximum number of pages)?	No minimum or maximum is prescribed in the IFB.	NO	**AMD#1**
CR#47	Book I	Section 12	Considering the amount of time between offer submission and contract signature, estimated at around 12 months, please confirm that the security clearance for the key personnel as well as the English certification based on STANAG 6001 can also be presented at contract signature.	See Book I Para 1.4.3. There are no Book I requirements beyond this provision. The IFB Book I, Para 2.10 Bid Validity period of 12 months is not the Purchaser's estimated time between offer submission and contract signature.	NO	**AMD#1**

CR#48	Book I	Section 7.10	Taking in consideration the information provided in the 5_IFB-CO-13810-CS Book II Part II Spec Provs FINAL document, section 7.10 “In the absence of valid security clearances for the Contractor's personnel at contract signature […]”, please confirm our understanding that the security clearance required for the Contractor's personnel at contract signature, are related to the key personnel as defined in 7_IFB-CO-13810-CS Book II Part IV SOW FINAL, section 12.	See change to Book II, Part II, Contract Special Provisions, Article 7, Security, Para 7.10.	Yes	**AMD#1**
CR#49	Book I	Section 2.11.1	Taking in consideration the information provided in the “1_IFB-CO-13810-CS Book I Instructions to Bidders FINAL” document, point 1.5.5, “The Bid Guarantee shall be substantially similar to Annex C as an irrevocable, unqualified and unconditional Standby Letter of Credit (SLC) issued by a Belgian banking institution fully governed by Belgian legislation or issued by a non-Belgian financial institution and confirmed by a Belgian banking institution fully governed by Belgian legislation.” In case the Bid Guarantee is issued by a non-Belgian financial institution, please provide the template letter for confirmation for the Belgian banking institution which will be provided together with the Bid Guarantee.	There is no mandatory template letter for the confirmation referenced. Suggest you take contact with your bank's Trade Credit department for more information on the specifics.	NO	**AMD#1**
CR#50	Book II Part IV	Section 1.6.1.6	Please provide information regarding the other certification authorities deployed by NATO besides the iNPKI.	There are a number of ad hoc Microsoft Certificate Authorities to be removed and replaced by E-NPKI. The numbers are not precise as some of them are currently being migrated to iNPKI (Entrust Version 8.1). The Contractor shall identify the existing CAs during the site survey process.	NO	**AMD#1**
CR#51	Book II Part IV	Section 1.6.1.6	Please detail what “transition” means and which are the services to be performed by the contractor during the transition period.	Details on Service Transition may be found in ITIL documents. See also SOW 5.5.6	NO	**AMD#1**
CR#52	Book II Part IV	Section 2	Please provide the documents from section 2.1 and 2.3.	See answer at CR #1.	NO	**AMD#1**
CR#53	Book II Part IV	Section 4.5.2.1.2.4	Please confirm that "interface" is missing and the requirements should be read " Each interface between the E-NPKI subordinate or superior E-NPKI components shall be documented in a specific annex of the Interface Control Document (ICD). "	This is correct. Corrected in IFB AMD 1.	YES	**AMD#1**
CR#54	Book II Part IV	Section 4.5.2.1.2.5	Please confirm that "interface" is missing and the requirements should be read " Each interface between the E-NPKI and end-entity users and devices shall be documented in a specific annex of the Interface Control Document (ICD). "	This is correct. Corrected in IFB AMD 1.	YES	**AMD#1**

CR#55	Book II Part IV	Section 4.5.3.1.5	The risk assessment methodology should be presented during the design review or also as part of the offer?	The use of the Magerit risk management methodology implemented within PILAR and the associated NATO Template is mandatory. (See SOW REF: 2.1.8.2, and section 11.3.13.) The "Risk Assessment Methodology" referred to in SOW Section 4.5.3.1.5 relates to the methodology the Contractor will use to produce security documents (in particular the Security Risk Assessment (SRA) document). Bidders are invited to describe the "approach to meeting the security accreditation process requirements" under Book I Section 3.6.5.5.4. During project execution, the Contractor will have the opportunity to present and discuss its proposed Risk Assessment Methodology during Security Working Group meetings (see SOW section 11).	NO	**AMD#1**
CR#56	Book II Part IV	Section 6.6.5.3	The certificates are issued by the CA based on certificate request and usually are delivered to the end users. How to deliver certificates at a central location? This can mean more than licensing the CA software to issue the required number of certificates + 10%?	This is a licensing item. i.e. if the vendor's pricing model includes fees for certificates, the additional +10% license strings shall be delivered centrally to be added to the system.	NO	**AMD#1**
CR#57	Book II Part IV	Section 7.1.8	Please clarify if the Contractor manpower allocated for activities related to WORK PACKAGE 5: OPERATION AND MAINTENANCE (O&M) can be freely allocated by the Contractor according project needs or it should be limited to the figures from section 7.1.9.1.	As mentioned in SOW section 7.1.9, the Contractor shall supplement Purchaser's manpower, on the understanding that the Purchaser will provide the resources described in SOW section 7.1.9.1. Therefore the Contractor shall provide additional resources (i.e. on top on Purchaser's provided resources) as needed, depending on the Contractor's proposed solution.	NO	**AMD#1**
CR#58	Book II Part IV	Section 7.1.9	Please confirm that when located in SHAPE and when traveling to other NATO locations the contractor’s manpower will receive from NATO office space and all the required logistic support in order to fulfil their duties.	Office space and associated logistics support will be provided at SHAPE co-located with NATO PKI staff. Associated logistics support will be provided when travelling to other NATO locations.	NO	**AMD#1**
CR#59	Book II Part IV	Section 7.1.9	Please clarify if the manpower required in section 7.1.9.1 must be present permanently in SHAPE site (with the possibility to travel to other NATO locations as required).	The onsite personnel are envisioned to be provided at SHAPE. This does not mean that travel will not be required. Off site support (e.g. offsite helpdesk) are the responsibility of the contractor.	NO	**AMD#1**
CR#60	Book II Part IV	Section 7.2.2.2	What are the standards that will be used by the external Auditor and Vulnerability Assessment teams for which support is required?	Auditors and Vulnerability Assessment teams adopt commercial and government best practices. Contractor Support is required to provide answers to technical questions, or to demonstrate how specific security functionality has been implemented during an audit or testing session. Remarks raised as the result of the Audit / Vulnerability Assessment process shall be taken into account and implemented as appropriate by the Contractor.	NO	**AMD#1**
CR#61	Book II Part IV	Section 7.3.8.2	Please detail which are the E-NPKI internal operations of interest for NCIRC?	All security relevant events. All auditable events as defined in Book II Part 4 Annex A.	NO	**AMD#1**
CR#62	Book II Part IV	Section 7.3.8.2	Please confirm that the input for NCIRC from the Identity and Access Management processes where E-NPKI capability is utilized should be provided by the Identity and Access Management systems and not by E-NPKI.	Responsibility to provide audit information to NCIRC resides with the system which generates the audit information.	NO	**AMD#1**
CR#63	Book II Part IV	Section 7.4.9	Please clarify if the manpower required to perform the integration of third-party applications/systems with E-NPKI (100 man-days per year, starting at PSA) is included in the manpower required in section 7.1.9.1.	As mentioned in CR#57, the Contractor shall supplement Purchaser's manpower. The Contractor's manpower required to the support third-party applications is included in the additional manpower to be provided by the Contractor.	NO	**AMD#1**
CR#64	Book II Part IV	Section 7.5.3.1	Please clarify if the support provided for exercises will be realized on site or remote?	This support is envisioned to be provided from SHAPE. This does not mean that travel will not be required.	NO	**AMD#1**

CR#65	Book II Part IV	Section 11.1.5	Can you please detail what are the security testing NATO plans to undertake?	Security testing is based on commercial and government best practices. The tools used vary over time to adapt to new threat scenarios. Remarks raised as the result of the Security Testing process shall be taken into account and implemented as appropriate by the Contractor.	NO	**AMD#1**
CR#66	Book II Part IV	Section 12	Please confirm that specific E-NPKI project related qualification for key personnel, such as NATO SECRET security clearance and demonstrated spoken and written English, at a minimum of 4343 as defined in STANAG 6001, must be obtained prior to contract signing, and it is not mandatory to be detailed in the submitted offer.	Bidders may, but are not required, to deliver personnel language proficiency or security clearance certificates with their bids. However, Bidders should take good note of the requirements at Book I, Para 1.4.3.	NO	**AMD#1**
CR#67	Book II Part IV	Annex C	In the table 7 provided in Section 1 – List of Sites, there are several sites where there are no Technical Services to be implemented, namely Military Committee (Brussels, Belgium), NATO Communications and Information Systems Group HQ, ACT Staff Element Europe, NATO SOF Headquarters (NSHQ) (Mons, Belgium). Furthermore, these sites don't have users, according to table 10 from SECTION 3 USER LIST. In the same time, these sites are named among those who are defined as PSA milestones. Please clarify those aspects.	Bidders shall distinguish between a geographical location and the NATO organisations that may co-located in the same geographical location. Table 7 lists all NATO organisations AND geographical locations. In some cases, several NATO organisations are co-located in the same geographical site. For example, ACT Staff Element Europe (Mons, Belgium) and NATO SOF Headquarters (NSHQ) (Mons, Belgium) are co-located with SHAPE (Mons, Belgium). Accordingly: - the Registration Authorities to be delivered in Mons are accounted against site 5 (SHAPE) and shall serve all NATO organisations co-located in SHAPE (Mons, Belgium) - all sites co-located in SHAPE (Mons, Belgium) will be included in the PSA milestone With respect to Table 10, for bidding purposes the Bidders shall consider that: - "Military Committee" numbers are subsumed into "New NATO Headquarters" numbers - "NATO Communications and Information Systems Group HQ" numbers are subsumed into "SHAPE" numbers - "ACT Staff Element Europe" numbers are subsumed into "SHAPE" numbers - "NATO SOF Headquarters (NSHQ)" numbers are subsumed into "SHAPE" numbers - "Alternate SOC" numbers are subsumed into "NCIA" numbers Bidders shall note that tables 9 and 10 are estimated quantities. During project execution, the Contractor shall update those estimated quantities (see SOW Annex C Section 3.1.2)	NO	**AMD#1**
CR#68	Book II Part IV	Annex C Section 3	In the tables 9 and 10 provided in Section 3: USER LIST, there are inconsistencies both within each table and between the two tables. Please specify how these inconsistencies should be treated by the bidders.	After careful review, the Purchaser was unable to identify any inconsistencies.	NO	**AMD#1**

CR#69	Book II Part IV	Annex C Section 3	In the tables 9 and 10 provided in Section 3: USER LIST there are three security domains MN (Mission Network), PBN (Protected Business Network) and ON (Operational Network). As stated in chapter 1.3 of the same document, the project shall implement and operate: i. E-NPKI on the Operational Network (ON); ii. E-NPKI on the NATO Enterprise Protected Business Network (PBN); iii. independent offline Root CAs (supporting SSL interception certificates) Moreover, the MN domain is not detailed in the IFB. Please clarify this aspect.	In SOW Annex C Section 3, the numbers associated to MN (Mission Network) are estimated quantities for the 3 NATO Signal Battalions and 18 underlying DCMs. Indeed, when deployed those elements will likely be connected to a Mission Network. It is currently assumed that the E-NPKI Technical Services (CA, RA, OCSP...) to be implemented under this project on ON will support the certificates required for MN. Therefore, for bidding purposes, bidders shall consider that numbers provided in SOW Annex C section 3 (tables 9 and 10) for MN are part of the project scope.	NO	**AMD#1**
CR#70	Book II Part IV	Annex A Section 1.4.1.6	Please confirm that this statement is a descriptive text and not a requirement to implement, even if it contains the term "shall".	As stated in Book II Part IV Annex A Paragraph 1.6 SRS Conventions: To clarify between descriptive text and requirements statements within the SRS, requirements are preceded by a “Requirement ID:” and are included as Blue text. Text in Black is descriptive. Requirement ID: SRS-31 The system requirements, defined in this document, are individually identified by a unique number which shall be used at all times as the specific reference for each.	NO	**AMD#1**
CR#71	Book II Part IV	Annex A SRS-34	Please clarify how will be treated the situations in which major changes of standards and specifications will be involved?	SRS-34 and SRS-36 have been merged to better reflect the requirements. See updated SRS-36 in IFB AMD 1.	YES	**AMD#1**
CR#72	Book II Part IV	Annex A SRS-35	Please clarify how will be treated the situations in which the system will be implemented based on a draft document and, during the operation and maintenance phase, the standard will be ratified with major changes?	SRS-35 has been deleted from SOW Annex A in IFB AMD 1.	YES	**AMD#1**
CR#73	Book II Part IV	Annex A Description between Requirement ID: SRS-2129 and Requirement ID: SRS-2131	Please clarify if the "offline SSL interception Root CAs" SHALL be provided under this project? Please clarify if there are requested 2 offline SSL interception Root CAs, in sites New NATO Headquarter and SHAPE (as per SOW Annex C, table 7) or the SSL interceptions Root CAs shall be supplied additional to the quantities from Annex C in all subordinate CAs?	See CR#32. Notes 1 and 3 of SOW table 7 states "1 for ON, 1 for PBN, and 1 for SSL Interception (alternatively, the CA for SSL interception will be located at JFC Naples instead of New NATO HQ; to be determined during contract execution)" SSL interception Root CAs shall be provided under this project and are included in the total number of CAs.	NO	**AMD#1**
CR#74	Book II Part IV	Annex A Section 3.1.3.3	“The E-NPKI Sponsor works with the E-NPKI CAs and RAs to register devices and shall meet the obligations of subscribers as defined throughout this document. Within this document these IT products are referred to as “devices.”" Please confirm that this statement is a descriptive text and not a requirement to implement, even if it contain the term "shall".	See CR#70 (Descriptive Text)	NO	**AMD#1**

CR#75	Book II Part IV	Annex A SRS-2813	Please detail the integration level required. Please confirm that Purchaser will supply all the information (ex: API, SDK, ICD, etc.) required for integration.	See FIPS 201. See Book II Part IV Annex A Paragraph 3.4.1 through 3.4.4. The Purchaser will only provide (after Contract Award) the database Schema of the existing CMS systems so that the Contractor can define and implement interconnectivity requirements.	NO	**AMD#1**
CR#76	Book II Part IV	Annex A SRS-2814	Please detail the requirements and componence for a "full CMS".	See FIPS 201. See Book II Part IV Annex A Paragraph 3.4.1 through 3.4.4.	NO	**AMD#1**
CR#77	Book II Part IV	Annex A SRS-2014	Please detail the integration level required. Please confirm that Purchaser will supply all the information (ex: API, SDK, ICD, etc.) required for integration.	See CR#75	NO	**AMD#1**
CR#78	Book II Part IV	Annex A SRS-2161	Please detail the integration level required. Please confirm that Purchaser will supply all the information (ex: API, SDK, ICD, etc.) required for integration.	See CR#75	NO	**AMD#1**
CR#79	Book II Part IV	Annex A SRS-2722	Please detail the integration level required. Please confirm that Purchaser will supply all the information (ex: API, SDK, ICD, etc.) required for integration.	See CR#75	NO	**AMD#1**
CR#80	Book II Part IV	Annex A SRS-2723	Please detail the integration level required. Please confirm that Purchaser will supply all the information (ex: API, SDK, ICD, etc.) required for integration.	See CR#75	NO	**AMD#1**
CR#81	Book II Part IV	Annex A SRS-2163	Please detail for all sites the existing CMS implementation	See details in CR#15 through CR#18	NO	**AMD#1**
CR#82	Book II Part IV	Annex A SRS-2644	Please clarify if delivery of racks is in scope of the project and if the E-NPKI system shall use dedicated racks or it is possible to collocate the equipment in existing racks or racks that will be provided by other projects (e.g. ITM)?	During the Site surveys (see SOW section 10), the availability of appropriate existing rack space shall be verified. If rack space meeting the requirements of the SRS is not available, an ECP will be raised.	NO	**AMD#1**
CR#83	Book II Part IV	Annex A Section 3.5.1.3 "Power and Air Conditioning"	- Please confirm that this statement is a descriptive text and not a requirement to implement, even it contain the term "shall". - Please confirm that the power (UPS, Generator, etc.) and air conditioning facilities will be available in sites and are not in scope of this contract.	See CR#70 Descriptive Text to cover the structure of a Certificate Policy. Subject to Contractor verification during site surveys, the power (UPS, Generator, etc.) and air conditioning facilities will be available in sites and are not in scope of this contract.	NO	**AMD#1**
CR#84	Book II Part IV	Annex A SRS-650	Please clarify if it is required a central electronic storage for all sites (1 storage per E-NPKI system) or there are needed storages for each sites to cover 10 years operational data for that site, with no central storage.	Book II Part IV Annex A Paragraph 3.5.5.1 "Types of records archived" does not presume to define the CA and RA deployed by the contractor. If the proposed system is capable of archiving records centrally at the CA, then the disk to disk storage capacity provided by the contractor at the CA meets the requirements for short term backup. Information deemed to be sensitive to the specific site (e.g. clearance records or information synchronised from Physical access control systems) may not be permissible to archive centrally. For this information, the disk to disk and archive capability would be required for the site itself.	NO	**AMD#1**
CR#85	Book II Part IV	Annex A SRS-652	Taking into account the requirement SRS-650 which state 10 years for online storage, please confirm that 30 years period is referring to offline archiving on archive media.	Yes, confirmed.	NO	**AMD#1**

CR#86	Book II Part IV	Annex A SRS-2263	Please confirm that there is required a short term Disk-to-Disk backup solution on site that will backup active operational data, and a long term backup solution (30 years) that will use offsite archive media. Please clarify if it is required a central solution for the entire system, or there are needed independent backup solutions for each site.	See CR#84.	NO	**AMD#1**
CR#87	Book II Part IV	Annex A Section 3.6.5.1 "Specific computer security technical requirements"	Please clarify if IP Cryptographic equipments are in scope of the project.	See CR#70. The referenced paragraphs: "Confidentiality. On the Operational Network (ON), military-grade NATO IP cryptographic equipment (NICE) will provide confidentiality to subscriber data. On the Protected Business Network (PBN), approved IP cryptographic equipment will provide confidentiality to subscriber data. Most of this equipment is PKI enabled." are in black text and without a Requirement ID.	NO	**AMD#1**
CR#88	Book II Part IV	Annex A Section 3.6.5.1 "Specific computer security technical requirements"	Please clarify if BPS equipments are in scope of the project.	BPS equipment is not in scope of the project. During the Site surveys (see SOW section 10), the availability of appropriate existing BPS shall be verified. An ECP will be raised if needed.	NO	**AMD#1**
CR#89	Book II Part IV	Annex A SRS-857	Please clarify if the term "CA servers" refers or not to the OCSP servers, TimeStamp and RA servers as well	SRS 583 states "OCSP responders shall conform to the same technical and security standards as the NPKI CA(s) which it supports." SRS-859 states "The E-NPKI secure time-stamping service shall meet the same system availability requirements as the CA." Therefore SRS 857 applies to OCSP and Timestamp servers. SRS-857 was amended as follows: "All E-NPKI CA servers, OCSP servers, and Timestamp servers shall be protected from attack through any open or general purpose network with which they connected. "	YES	**AMD#1**
CR#90	Book II Part IV	Annex A SRS-761	Please clarify which will be the reference time source and what protocol will be used to get the reference time. Please clarify if a reference time source is available and provided by Purchaser for each security domain.	NTP will be provided by the Purchaser on all domains.	NO	**AMD#1**
CR#91	Book II Part IV	Table 7 "List of sites"	Please clarify where are mentioned 2 RA if one is for PBN and one is for ON. Where is mentioned just 1 RA (e.g. NATO Intelligence Fusion Centre) please clarify which security domain needs to be considered?	Cross Referencing between Tables 7 and 9 of Book II Part IV SOW Annex C provides the following answer (i.e. the other domain has no users or devices as it is not deployed at that site): - NIFC: ON - NAHEMA: PBN - NETMA: PBN - NAPMA: PBN	NO	**AMD#1**

CR#92	Book II Part IV	Sections 9.2.3.8 and 9.2.3.9	Can the Purchaser please clarify what they mean by 'The Purchaser will execute the OAT and that the Contractor shall assist with OAT execution? Does this mean that the Purchaser staff will perform the IV&V function against the agreed contractor test plan? Also please clarify what is meant by 'sampling'.	The purchaser will execute the OAT based on a purchaser based test plan developed in accordance with reference 2.1.6.10. The scope of the purchaser test plan will be based on the requirements defined in the SRS (mostly chapter 3). The test procedure will be based on the details provided by the bidder to meet the requirements of Book 1 section 3.6.5.5.2 and SOW sections 11.3.15.3 and 11.3.15.4. (the detailed information on the steps and procedures required to verify the E-NPKI system compliance with the Certificate Policy and the E-NPKI SRS). The contractor assistance to OAT is to ensure that the verification steps in book 1 section 3.6.5.5.2 are achieved efficiently. The Contractor shall also note the deliverables associated to OAT (see CLIN 2.3). The words "by sampling" have been removed from SOW 9.2.3.8". Book I section 3.6.5.5.1 has been updated to reflect the correct reference to SOW section 11.3.15.	YES	**AMD#1**
CR#93	Book II Part IV	Sections 9.2.3.1	Can the Purchaser please provide the correct link to REF 2.1.6.10. It appears to be unrelated to SOW 9.2.3.1 which states that 'OAT is a requirement mandated in REF 2.1.6.10'	Reference 2.1.6.10 includes testing requirements for cryptographic products. Testing will be based on the requirement defined in the SRS.	NO	**AMD#1**
CR#94	Book II Part IV	Annex A SRS-2127	Can the Purchaser please clarify this SRS requirement. Based upon the tables within Annex C where RA implementations are identified, can the Purchaser please clarify what functions this RA implementation is expected to perform? It is assumed that the only function to be performed by this capability is that defined within SRS 2812. Furthermore can the Purchaser confirm that if there is an existing CMS Equipment set at a location that this contract is to provision suitable certificates to that equipment to satisfy this function?	The assumption is not correct. SRS-2047 states “The E-NPKI Registration Authority integration, workflows, and automation shall allow for the issuance and management of tokens by physical security (Security pass issuance) offices without the requirement for additional manpower for all sites implementing FIPS 201 compliant card management systems.” The Card Management System for each security domain is installed within the Physical Security Pass Office at each site. Additional RA functionality is also required within the Service Kiosk or NCIA CSU to manage issuance of device certificates and to manage certificate profiles for users. All user and device certificate management is foreseen to be implemented via RA functionality at all physical sites including Datacentres. User and sponsor identification including the face to face authentication must be implemented and the authentication evidence must be audited and archived by the E-NPKI system (See SRS-516). To clarify the RA requirements, the following paragraphs will be inserted into Amd1: - Requirement ID: SRS-2825 Within each security domain, E-NPKI RA functionality is divided into two separate functionalities; Token issuance (See SRS 2047) and device certificate issuance (See SRS-2826 - Requirement ID: SRS-2826 Additional RA functionality is required within the Service Kiosk or NCIA CSU to manage issuance of device certificates and to manage certificate profiles for users. - Requirement ID: SRS-2827 The RA components defined in SRS-2047,SRS-2825 and SRS-2826 shall be capable of providing redundancy between them to avoid single points of failure within a site.	YES	**AMD#1**

CR#95	Book II Part IV	Annex A SRS-2013	Can the purchaser confirm that when integration with any of the existing CMS or PACS systems, the only requirement is that of integration and there is no inferred support or maintenance burden for this existing capability.	Yes, confirmed.	NO	**AMD#1**
CR#96	Book II Part IV	Annex A SRS-2163	Can the purchaser please provide a comprehensive list identifying by location: - FIPS 201 ready (Y/N) - Existing Functionality - Equipment suite (make model) - Software Suite (vendor version)?	See CR#14 to CR#18.	NO	**AMD#1**
CR#97	Book II Part IV	Annex A SRS-2164	Can the purchaser confirm that this contract is only responsible for the warranty and maintenance of any additional components provided and all existing components' maintenance and warranty are specifically excluded?	Yes, confirmed.	NO	**AMD#1**
CR#98	Book II Part IV	Annex A SRS-2318	Can the Purchaser confirm that the functions that can be performed remotely (subject to suitable protection) include PED functions?	PED functionality shall be locally implemented and is not permissible to perform remotely.	YES	**AMD#1**
CR#99	Book II Part IV	Annex A SRS-849	This requirement states that key functions (CA/OCSP) must reside on dedicated platforms. Can the Purchaser confirm that as long as these platforms are only used to support key certificate generation services and not peripheral management, administrative or supporting functions it is acceptable to co-host other certificate services on these dedicated hosts (for example, key escrow and timestamp services)?	Yes, confirmed	NO	**AMD#1**
CR#100	Book II Part IV	Annex A SRS-2048	Can the Purchaser please explain how this requirement will be used when balanced against SRS 2021 which requires NONCE interchanges?	It is unclear to the Purchaser how Nonces for OCSP requests relates to RA manpower requirements.	NO	**AMD#1**
CR#101	Book II Part IV	Annex A SRS Section 11.3.13.2	The Contractor shall use the SRA application “PILAR” with NATO profile for producing the E-NPKI Security Risk Assessment. It is assumed, that the NATO PILAR Profile will be made available post-contract award at the same time as the other NATO Security relevant documentation and settings are released, as identified in Annex E Table 2.1 Row NATO Security Settings. Can the Purchaser please confirm that this is the case?	The Purchaser assumes that the question refers to SOW 11.3.13.2, not Annex A SRS 11.3.13.2. The NATO PILAR Profile will be made available to the selected Contractor at Contract Award (CAW), and as needed (updates) during contract execution. PFE list (see SOW Annex E) updated accordingly. The Contractor shall be responsible to procure the PILAR Software license and shall load the NATO PILAR Profile into the PILAR Software.	YES	**AMD#1**
CR#102	Book I	Section 3.4.2	Do subcontractors need to submit any administrative documents, including but not limited to the conflict of interest declaration?	No, all Administrative Package documents/certifications must be submitted and signed only by the (prime) Bidder.	NO	**AMD#2**
CR#103	Book I	Section 3.3	Packaging: Our understanding is that the proposal can be submitted as one parcel (i.e. a box) containing three separately wrapped packages, for the Administration, Price and Technical parts, respectively. Please confirm or clarify our understanding.	Your understanding is correct.	NO	**AMD#2**

CR#104	Book I	Section 3.4.2	Administrative Certificates: Are bidders allowed to reproduce the different Annexes B-x in Word documents so as to easily fill them out?	Yes. It is for his very reason that we issue the Book I in its native MS Word format (.doc).	NO	**AMD#2**
CR#105	Book I	Section 3.6.6.2.1	Our understanding is that the word “Logistics” is missing in “initial Integrated Logistics Support Plan (ILSP)”. Please confirm or clarify our understanding.	Confirmed. Book I updated accordingly.	YES	**AMD#2**
CR#106	Book I	Sections 3.6.4.5.2 and 3.6.4.5.5	Our understanding is that bidders can use CV and references (and other resources) from subcontractors to display the capacity to deliver the contract or to compose their team. Please confirm or clarify our understanding?	The Bidder (i.e. the Prime) needs to identify the resources they propose to use to execute the project - be that organic or subcontracted. With reference to necessary corporate experience or capabilities, this should be interpreted solely in the context of the Bidder as the Prime.	NO	**AMD#2**
CR#107	Book I	Section 3.6.4.6.3.4.6	Could you please specify what form of evidence you require of our ensuring continuity of the team?	Bidders need to determine the form and content of evidence.	NO	**AMD#2**
CR#108	Book II Part IV	Annex A SRS-496	Certificates which give legal authenticity as handwritten signatures, are considered qualified certificates as defined by EU regulation. Please advise if E-NPKI should be capable of issuing certified QC or advanced equivalent.	E-NPKI is not governed by the European Union Electronic Signature Directive. However, for the implementation of its PKI, NATO shall follow the international standards for the technological choices in order to facilitate the interoperability between NATO and nations. For electronic signature issues, NATO shall seek to adhere to the highest technical standards of the European Union Electronic Signature Directive in order to facilitate cross-certification with the NATO member nations.	NO	**AMD#2**
CR#109	Book II Part IV	Accreditation of PKI solution	NATO accreditation processes (NSAB) will be used to evaluate the E-NPKI solution. Please supply further information on the accreditation processes.	SOW section 11 provides details related to the security accreditation process.	NO	**AMD#2**
CR#110	Book II Part IV	Requirement List	Could you share with bidders a Word or Excel version of the tender requirements?	This can be provided upon individual request. See however CR #37 regarding Book II, SSS.	NO	**AMD#2**
CR#111	Book II Part IV	Architecture	Can NCIA provide more specific descriptions on the overall system architecture where the PKI has to be deployed?	Key components of architecture are included in the SRS. Back end infrastructure is to be deployed in datacentres. All physical sites are to have registration authorities.	NO	**AMD#2**
CR#112	Book II Part IV	External Interfaces	Could you please define the external interfaces of the system?	See SRS 1766, 2795, 1216, and **SRS** section 4.9.2	NO	**AMD#2**
CR#113	Book II Part IV	Annex A SRS-2015	FIPS 201 compliance - card mgmt sys / integration 4 other products (Safelayer) + biometric enrolment devices issue	No question provided	NO	**AMD#2**
CR#114	Book II Part IV	Annex A Section 2.2.1 paragraph 3	The paragraph mentions that "E-NPKI will co-exist with…". Could you please clarify this point and define the co-existence?	Interoperability based on Trusted root CA Certificates and cross certification shall be supported. The existence of Microsoft CAs or the Entrust based interim PKI shall not cause or receive interference from the E-NPKI.	NO	**AMD#2**
CR#115	Book II Part IV	Certificate Policies	Could you share the existing certificate policies and relevant documentation?	A CD is now available on request containing NATO applicable documents referenced in the SOW : E-NPKI - Applicable documents, IFB-CO-13810-CS AMD#2 The CD contains some documents at NATO RESTRICTED level, therefore, the “Certificate of Security Obligation” will need to be completed, signed, and returned to the Contracting Officer prior to its issuance.	NO	**AMD#2**
CR#116	Book II Part IV	Migration	Please advise any migration expectations, time frames and any proposed reuse of existing processes	Migration activities are documented in the SOW Section 5 System Implementation	NO	**AMD#2**
CR#117	Book II Part IV	Annex A SRS-2032	The requirement refers to "external dierctory service": what is intended by "external" in this context?	The directory service is provided by the NEDS project.	NO	**AMD#2**

CR#118	Book II Part IV	Annex A SRS-555	Body of evidence related to NR signatures will be the control over the signing key, contained within a Secure Cryptographic Device. Requirement for brute force protection with therefore be within scope of FIPS201 or FIPS 140-2. Please clarify this requirement.	Cryptographic devices shall be shown to be immune to offline brute force attacks. I.e. the cryptographic keys shall not be available in either plain text or encrypted form. State information shall be maintained regarding the number of failed login attempts even if power is removed from the cryptographic device between authentication attempts.	NO	**AMD#2**
CR#119	Book II Part IV	Archiving	Does an archiving system exist for documents in the scope of this contract? If so, could you please describe the solution?	The bidder shall deliver a digital archiving system to provide for the storage of artefacts. Book II SOW Annex A (SRS) was updated appropriately at AMD3. See chapter 3.5.5.	YES	**AMD#3**
CR#120	Book II Part IV	Archiving	What is the data retention period for the archive?	See SRS 652	NO	**AMD#2**
CR#121	Book II Part IV	Section 7.1.9.1.2.5	Our understanding is that the requirement should read "to FSA + 5 Years" instead of 4 years. Please confirm or clarify our understanding.	Correct. SOW updated accordingly.	YES	**AMD#2**
CR#122	Book I	Section 3.6.5.5.2	What could it be a satisfying level on granularity related to validating the system's compliance against the SRS? The starting basis may be a traceability matrix of covering SRS (which, further on may provide potential input for SRA). This choice may be to premature to be applied/proposed (at a bid level). Another approach for fulfill this topic (at bid level) may be a short-story descriprion of chosen technical and functional testing methods.	See CR#92 and CR#123	NO	**AMD#2**
CR#123	Book I	Section 3.6.5.5.2	Is there any system's compliance standard followed by NATO for proper validation against SRS (in general)?	When checking compliance against the SRS, the Purchaser will use a combination of methods including for example test and demonstration. The bidder will propose the methods in the Requirements Traceability Matrix (RTM).	NO	**AMD#2**
CR#124	Book I	Section 3.6.5.5.2	Neither document IFB or SOW mentions Stress Testing needs. Should this topic be taken into account in our proposal? Are there any requirements/constraints related to it?	Performance criteria for critical interfaces are defined. It is for the contractor to demonstrate that the performance criteria are met. Stress Testing is one method of demonstrating compliance with the performance criteria.	NO	**AMD#2**
CR#125	Book II Part IV	Section 9.1.6.4	Test support tools: does this fall under the responsibility of the contractor? Are there any client proposals/constrains in terms of what Testing support tools must be used?	The availability of "test support tools" will be checked at the Test Readiness Review (TRR). Test support tools fall under the responsibility of the Contractor, unless specifically agreed with the Purchaser during project execution.	NO	**AMD#2**
CR#126	Book II Part IV	Section 9.1.6.5	Is Test Data Creation under Testing team exclusively? Or, do we have an input from the client?	Getting to a final test data set will require coordination between the Contractor and the Purchaser during project execution. The Purchaser expects the Contractor to propose an approach as well as test data for discussion with the Purchaser.	NO	**AMD#2**
CR#127	Book II Part IV	Section 9.1.6.5	Are Use Cases provided by the client?	Use cases are not currently planned to be provided by the Purchaser.	NO	**AMD#2**
CR#128	Book II Part IV	Section 9.1.6.10	Are there any reference standards followed by NATO for the FCA (Functional Configuration Audit) process?	The FCA shall be conducted in accordance with the Configuration Management Plan (CMP) to be agreed between the Contractor and the Purchaser. See SOW 15.6.5.	NO	**AMD#2**
CR#129	Book II Part IV	Section 11.4.3.3	Could you provide more detail and constraints/requirements concerning Performance Testing?	See CR#124	NO	**AMD#2**

CR#130	Book II Part IV	Section 4.9	« As part of this work package, the Contractor shall conduct site surveys at all the sites related to the PSA milestone" However in Annex A Bidding Sheets, two sites (NATO Communications and Information Systems Group HQ, ACT Staff Element Europe) are related to PSA milestone while the site survey is under CLIN3 (instead of expected CLIN2) Could you clarify?	This is correct. The site surveys at the 2 sites (NATO Communications and Information Systems Group HQ, ACT Staff Element Europe) are part of CLIN 2. Corrected in IFB AMD2.	YES	**AMD#2**
CR#131	Book II Part IV	Section 2	A long list of reference documents is provided in the SOW. Can NATO make those available to bidders, at least those that NATO is at liberty of sharing with the industry?	See answer at CR #115	NO	**AMD#2**
CR#132	Book II Part IV	Section 4.4	Do all requested functions/interfaces of the Contractor's solution need to be available for the Operational acceptance test (OAT)? Is it possible to provide subsets of functions/interfaces at a later time in the project schedule which shall be fixed in the contract (e.g. at BLAT)?	See CR#92 Please refer to SOW 9.2.3, and in particular to 9.2.3.8 and 9.2.3.11, for the scope of the OAT testing. Physical Access Control CMS functional integration tests with existing purchaser CMS systems are out of scope of OAT as there is not enough time for the contractor to complete this integration before OAT.	NO	**AMD#3**
CR#133	Book II Part IV	Section 4.4	Integration with NEDS, CMS systems and PAC can only be provided in NATO environment. Shall these integrations be provided and tested at BLAT or during site installation?	Full integration needs to be demonstrated during BLAT as mentioned in Book II Part IV 9.2.4.9, this will be performed on customer premise as stated in SOW 4.1.7.3.	NO	**AMD#2**
CR#134	Book II Part IV	Section 5.5.1.1	"delivery and installation of any E-NPKI elements": Is contractor responsible for the deployment/installation of user desktop hardware and software (e.g. card readers, drivers, smart card middleware)?	Yes the contractor is responsible for the delivery and installation of all E-NPKI elements. The ITM project includes Card readers integrated within several components. The bidder shall identify duplication of elements during the site survey process and delete these duplications of hardware components from their design.	NO	**AMD#2**
CR#135	Book II Part IV	Section 5.5.1.1	Contractor has to provide the HSM hardware for E-NPKI. Does the contract include maintenance and field service for the HSMs?	The bidder is responsible for the maintenance and field service of HSM under the Warranty as per SOW 6.9. The activity will be part of the O&M activities once the warranty period is over.	NO	**AMD#2**
CR#136	Book II Part IV	Section 5.5.1.1	Are the CA, RA, OSCP, TSP, CA/RA database server and storage hardware components part of the deliverables or are they provided by NATO infrastructure services?	To allow for the calculation of best value, bidders shall provide prices for all hardware components, also including hardware for systems proposed for virtualization. For components not requiring dedicated Hardware (Either dedicated Servers or Hardware Security Modules,) NATO will determine in conjunction with the successful bidder, the appropriate components to be provided as Infrastructure as a Service (IAAS) by the ITM project.	NO	**AMD#2**
CR#137	Book II Part IV	Section 5.5.1.1	Does the contract include maintenance and field service for the hardware components listed in the question before?	All components delivered under this contract will fall under the O&M conditions of this contract.	NO	**AMD#2**
CR#138	Book II Part IV	Section 5.5.6	iNPKI and other Certificate Authorities provide capabilities which shall be replaced by E-NPKI. Which other CA systems besides iNPKI have to be replaced?	See CR#50	NO	**AMD#2**

CR#139	Book II Part IV	Section 5.5.6	Which applications and devices currently rely on iNPKI?	The characteristics of the integration activities are described under SRS 4.10. See CR#181 for a rough breakdown of device certificates currently deployed. There are large number of devices which rely on certificates to support their management interface. The contractor is responsible to identify applications and version during site surveys.	NO	**AMD#2**
CR#140	Book II Part IV	Section 5.5.6	Existing CA certificates which will be needed for CRL signing and existing OCSP certificates from iNPKI and other Certificate Authorities shall not be migrated. Is this correct?	yes this is correct.	NO	**AMD#2**
CR#141	Book II Part IV	Annex A SRS-2790	Which Offline Request/Response interface for issuance of SSL interception proxy certificates shall be supported by the SSL interception offline Root CA? E.g. import/export of files containing PKCS#10/7 request/response structures (base64 encoded)?	Yes. See SRS 4.9.2.3, SRS-2752 to SRS-2757 applying to all CAs.	NO	**AMD#2**
CR#142	Book II Part IV	Annex A SRS-503	Is it Purchaser's intention that the authentication of certificate requests via pre-shared secrets is based on a one-time pre-shared secret which is only valid for one request? Or may the same pre-shared secret be used several times as long as the face-to-face registration of subscriber or sponsor has not expired?	Pre-shared secrets are one of many possible mechanisms which may be used for authentication. Where a pre-shared secret is used it shall only be used once, for a single transaction.	NO	**AMD#3**
CR#143	Book II Part IV	Annex A SRS-503	Does a sponsor need to register each single device within his responsibility separately? If not, is it allowed to authenticate multiple device or application certificate requests via the same pre-shared secret of the sponsor?	Batch processing for a group of certificate requests is permitted (see srs-531), however credential issuance is still an individual activity. Application workflows require completion during the issuance process. No data is omitted.	NO	**AMD#2**
CR#144	Book II Part IV	Annex A SRS-2746	Are devices and applications (e.g. Web Services) which are requiring certificates stored in NEDS to verify certificate attributes? Or is in that case the content of a certificate request (e.g. IP adresses of VPN devices) issued by an authenticated sponsor seen as a valid source?	E-NPKI shall query NEDS for availably of information to be used as certificate attributes. In situation where attribute information is not available, E-NPKI shall be able to generate it.	NO	**AMD#3**
CR#145	Book II Part IV	Annex A SRS-578	Cross certificates are normally issued by the Root, which is not provided by this project. Is this requirement applicable to subordinate CAs?	Cross Certification is implemented at the Root CA level. Subordinate CAs shall not implement Cross Certification E-NPKI shall support path discovery, and path validation including cross certificates. SRS-2464 updated See also CR#439.	YES	**AMD#2**
CR#146	Book II Part IV	Annex A SRS-2335	Cross certificates are normally issued by the Root, which is not provided by this project. Is this requirement applicable to subordinate Cas?	see CR#145	NO	**AMD#3**
CR#147	Book II Part IV	Annex A SRS-2464	Cross certificates are normally issued by the Root, which is not provided by this project. Is this requirement applicable to subordinate CAs?	see CR#145	YES	**AMD#2**
CR#148	Book II Part IV	Annex A SRS-2086	Expired certificates shall remain in the CRL. Which validity model shall be used for end entity certificates: The PKIX (RFC 5280) validity model or the model according to signature laws ?	As stated in SRS-2469 "E-NPKI CAs shall issue X.509 version two (2) CRLs in accordance with the RFC3280 and RFC5280 Certificate and CRL Profile" CRL will perpetually contain revoked certificates which is not in violation of RFC5280. This is required to support NATO applications.	NO	**AMD#3**

CR#149	Book II Part IV	Annex A SRS-579	Can you please provide an estimation of the quantity structure of OCSP requests addressed to one OCSP server?	The total community size envision for the system is defined in SOW Annex C. The bidder needs to estimate the value in order to justify its design. The solution shall be capable of providing an OCSP response for all E-NPKI CAs.	NO	**AMD#2**
CR#150	Book II Part IV	Annex A	Can you please provide an estimation of the quantity structure of time stamp requests addressed to one TSP server?	The total community size envision for the system is defined in SOW Annex C. The bidder needs to estimate the value in order to justify its design. The solution shall be capable of providing a timestamp response for any client request.	NO	**AMD#2**
CR#151	Book II Part IV	Annex A SRS-2814	Shall the own CMS be FIPS-201 compliant? If yes, is a FIPS-201 certification required?	CMS solution provided for the PBN shall be FIPS-201 certified. Also, all CMS components provided for ON and PBN shall be approved by a NATO Nation National Communications Security Authority for the security level they will operate at.	NO	**AMD#3**
CR#152	Book II Part IV	Annex A SRS-2814	Besides the PIV-(I) cards, shall the own CMS also issue smart cards which are not enabled for physical access and/or contain other certifcate profiles ?	PIV compliant smart cards shall use the PIV-(C) profile. All smartcards to be issued via a CMS. See SRS-2837 in AMD#2 Smartcards on the ON are not to be enabled for Physical access. See SRS-2838 in Amd#2 See SRS-2801 and SRS-771 for additional requirements. See also CR#177 regarding the use of PIV-(C).	YES	**AMD#2**
CR#153	Book II Part IV	Annex A SRS-2014	Which certificate enrolment protocols are supported by the three existing CMS systems for communication with the CA?	Those are not identified, as SRS-2163 mentions, the bidder needs to integrate and therefore identify the certificate enrolment protocols if different from the one required as part of the SRS. There are multiple interfaces supported by each CMS, the appropriate interface can only be determined in cooperation between CMS vendor and CA vendor.	NO	**AMD#2**
CR#154	Book II Part IV	Annex A SRS-2014	Do the existing CMS systems support the transferal of pre-shared secrets (which have been issued by the E-NPKI RA during subscriber registration) to the E-NPKI CA during enrolment?	See CR#153	NO	**AMD#2**
CR#155	Book II Part IV	Annex A SRS-2127	The CMS register subscriber identification data during initial card issuance. This is also the task of the E-NPKI RA. Is it intended that registration shall be devided in a way that the RA registers and validates part of the user data (e.g. subscribers signed agreement) and CMS registers another part (e.g. biometric data)?	The bidder shall describe his solution to respond to the requirements. As stated in 3.1.3.2, the purchaser does not enforce such design decision.	NO	**AMD#2**
CR#156	Book II Part IV	Annex A SRS-2814	Has the contractor to provide all necessary hardware components required for the “full own CMS”, e.g. workstation, screen, data base, card printer, fingerprint scanner, camera and so on? If yes, is maintenance of this equipment required during contract duration?	Yes. See CR#13 and CR#204 The bidder is responsible for the maintenance under the Warranty as per SOW 6.9. The maintenance activity will be part of the O&M activities once the warranty period is over.	NO	**AMD#2**
CR#157	Book II Part IV	Annex A SRS-2814	How many installations of own CMS systems have to be provided?	See CR#13 and CR#14	NO	**AMD#3**
CR#158	Book II Part IV	Annex A SRS-2736	The E-NPKI shall be capable of direct database connectivity to external PAC systems via an ODBC compliant interface. Which PAC systems have to be supported?	See CR#13	NO	**AMD#2**

CR#159	Book II Part IV	Annex A SRS-1766	Does not mention EST (contrary to SRS-2807). Is it required to provide both EST and CMP?	yes, both EST and CMP shall be supported. SRS-2736 was updated in AMD#2.	YES	**AMD#2**
CR#160	Book II Part IV	Annex A SRS-2807	Which end entitiy certificates shall be managed via EST? Only facilities and back end devices and applications like web services?	It is not defined. SRS-2807 requires the PKI solution in order to include EST to maximize compatibility.	NO	**AMD#2**
CR#161	Book II Part IV	Annex A SRS-2620	Which end entitiy certificates shall be managed via CMP? Only facilities and back end devices and applications like web services?	see CR#160	NO	**AMD#2**
CR#162	Book II Part IV	Annex A SRS-2807	Are EST and CMP client applications already alvailable in NATO environment?	Current CMP client is specific to iNPKI vendor. NATO does not have an independent CMP application available. EST Client is not yet implemented.	NO	**AMD#2**
CR#163	Book II Part IV	Annex A SRS-2807	Is an ESTclient software required as part of the E-NPKI deliverables?	no EST client is required	NO	**AMD#3**
CR#164	Book II Part IV	Annex A SRS-2620	Is a CMPclient software required as part of the E-NPKI deliverables?	yes, the E-NPKI software client shall implement CMP to meet the requirement SRS-845.	NO	**AMD#3**
CR#165	Book II Part IV	Annex A SRS-2744	Is there a NATO specification for a certificate management WebService already available? If yes, please provide us with the specification.	There are no such specification. Annex A: SRS 4.6.2.1.1 describes the requirements to be followed.	NO	**AMD#2**
CR#166	Book II Part IV	Annex A SRS-2744	Is there a NATO certificate management Web Service client implementation already available?	There are no such client application. Annex A: SRS 4.6.2.1.1 describes the requirements to be followed.	NO	**AMD#2**
CR#167	Book II Part IV	Annex A SRS-2744	Shall a Web Service specification be provided as a E-NPKI deliverable (including initial identification via pre-shared secret?	The purchaser is expecting the contractor to provide a web server interface to support protocols such as SCEP or EST between the CA and the end user devices.	NO	**AMD#3**
CR#168	Book II Part IV	Annex A SRS-2744	Is a Web Service client library to be provided as E-NPKI deliverable?	If the solution includes API interfaces, the Contractor shall provide the API documentation.	NO	**AMD#3**
CR#169	Book II Part IV	Annex A SRS-1839	One example for file exchange could be export and import of PKCS#10/7 structures (base64) for SSL applications. Can you please give other examples of file exchange?	See CR#141	NO	**AMD#2**
CR#170	Book II Part IV	Annex A SRS-771	Is Contractor responsible for the deployment of smart card middleware or any other client software?	See CR #134	NO	**AMD#2**
CR#171	Book II Part IV	Annex A SRS-520	Which types of organization/group certificates shall be issued? Please describe the mechanism for identification/registration in case of group certificates, and the intended enrolment interface.	It is not intended to create group certificates based on sharing private keys. SRS-520 declares the subscriber identity shall be verified in order to authorized the issue of certificates on behalf of an organisation or a group. Certificates shall contain unique key material and shall use other extensions (E.g. subject alternate name) to express group/organization membership. The bidder shall describe how the validation will be implemented.	NO	**AMD#2**
CR#172	Book II Part IV	Annex C Section 1	Does 1 item in the “technical services” colomns always mean Primary+Backup System of CA or RA or OCSP?	For CA, the quantity identified for each site relate to the number of domains on which the CA is to be installed for that site. CA are distributed across datacentres to provide geographically separated redundancy and backup. The choice of implementation within a domain at a site is for the bidder to design. For RA, SRS-2828 specifies the availability requirement within a site. For OCSP, the same remark as for CA is applicable.	NO	**AMD#2**
CR#173	Book II Part IV	Annex C Section 1	How many Time Stamp Servers (TSP) have to be set up in which locations?	See CR#296.	Yes	**AMD#2**

CR#174	Book II Part IV	Annex C Section 1	Which site RA shall be connected to which CA productive site?	Certificate Authorities shall provide redundancy for each other for all CA services (automated failover) within a security domain. Registration authorities, OCSP, Timestamp need to automatically connect to another CA or repository in the event of maintenance, failure, etc. at one CA or repository. See also CR#12	NO	**AMD#2**
CR#175	Book II Part IV	Annex C Section 1	3 of the listed sites shall have only one RA (e.g. NAHEMA). Shall this belong to ON or PBN?	See CR#91	NO	**AMD#2**
CR#176	Book II Part IV	Annex C Section 3	There are sites which shall not be provided with Smart Cards and Readers, but with User Identities (e.g. NATO HQ). Are there User Identities in any of the sites which will be provided with Software Certificates instead of or besides the certificates stored on Smart Cards?	The E-NPKI scope does not include software certificates for persons as all persons will require smartcards for physical and logical access control. See CR#21 for clarification.	NO	**AMD#2**
CR#177	Book II Part IV	Annex C Section 3	Shall all Smart Cards which have to be provided be PIV-(I) compliant and shall all issued smart Cards be used for physical access in PAC systems?	PIV-(C) is only mandatory for the PBN smartcard. Only the PBN smartcard shall be used for physical access control. SRS-2014 updated to reference PBN. See SRS-2801 regarding orthogonal smart card selection between security domains.	YES	**AMD#2**
CR#178	Book II Part IV	Annex C Section 3	If one user has two user identities on two smart cards (one for ON, one for PBN), shall both cards/identities provide physical access in PAC systems?	Only the PBN smartcard shall be used for physical access control.	NO	**AMD#2**
CR#179	Book II Part IV	Section 11	Exactly which software components require prior certification and at what level (Common Criteria)?	The examples provided in **Book I** Annex B 16 provide non-exhaustive guidance regarding cryptographic certification requirements.	NO	**AMD#2**
CR#180	Book I	Section 1.1.2	For the current system: what is the vendor and what are the product names of the components of the IOC?	See slides from Bidders conference for details. Entrust Authority 8.1, Entrust IdentityGuard version 11, Safenet Luna PCI (multiple models) Oberthur IAS ECC Smartcards (RSA only) Gemalto ID Prime PIV 2.0 Smartcards, Safenet SC650 Smartcards.	NO	**AMD#2**
CR#181	Book I	Section 1.1.2	For the current system: what is the scale of deployment of CAs and RAs and at what locations?	As a snapshot, Today there are approximately 5000 users with smart cards, and 3500 devices. Prior to PSA this number is planned to grow to around 15000 users and 10,000 devices. There are currently Registration Authorities deployed in 5 sites across 3 countries in Europe. Prior to PSA there are expected to be Registration Authorities deployed in 10 sites across 7 countries (globally disbursed) (Mons-BE, Lago Patria-IT, Northwood-UK, Norfolk-US, Izmir-TU, Sigonella-IT, Hague-NL, Geilenkirchen-DE, Brussels-BE, Brunssum-NL)	NO	**AMD#2**
CR#182	Book I	Section 1.1.2	For the current system: what are the types of certificates with reference to the list in section 4.10 of Book II, part IV, SOW, Annex A - SRS?	The requirements as stated are sufficient to complete the integration based on commercially available information. The ability to integrate the CA with a wide range of commercial software is a component of the best value criteria in this IFB.	NO	**AMD#2**
CR#183	Book II Part II	Section 13.2	What does it mean "a reasonable time" in the sentence "the replacement personnel shall be in place within a reasonable time" and who determines and defines "a reasonable time"?	Reasonable time in the Purchaser's estimation depending on all the facts and circumstances.	NO	**AMD#2**
CR#184	Book II Part II	Sections 13.2, 13.3, 13.4	Is it possible at the time of the appointment of the Key Personnel to obtain acceptance of the Employer for deputies of the Key Personnel, who in time could substitute the Key Personnel?	Such a scenario would likely be favourably considered by the Purchaser.	NO	**AMD#2**

CR#185	Book II Part II	Section 14.1	Could you confirm that the statement “The working language of the Project Team is English” means also that any interviews in all sites covered by the implementation can take place in English, and all documents in all sites covered by the implementation will be available in English?	Confirmed.	NO	**AMD#2**
CR#186	Book II Part II	Section 14.1	Please confirm that all training (including training in all sites covered by the implementation) can be conducted in English.	Confirmed.	NO	**AMD#2**
CR#187	Book II Part II	Section 23.5	Please confirm that possible change of location, ("change the Stated destination") 30 days earlier than planned supply, may only refer to the location defined in the "LIST OF SITES" (IFB-CO-13810-CS), and if the change will apply to locations outside of this list, the Contractor will be able to benefit with the clause of this Contract entitled "Changes"?	Correct. Keep in mind that an assertion for under the Changes provisions does not necessarily obligate the Purchaser to grant the contractual relief requested.	NO	**AMD#2**
CR#188	Book II Part II	Sections 23.7, 23.8	Is the possibility to postpone by 90 days of delivery / start of work at a given location also means the possibility to changes in the cost of the project and the project schedule?	Para 23.8 forecloses the Contractor's right to submit claims for delays in the Para 23.7 notification as long as the delay does not exceed 90 days. After 90 days, the right to claim is no longer foreclosed.	NO	**AMD#2**
CR#189	Book II Part II	Sections 23.7, 23.8	Is the possibility to postpone by 90 days of delivery / start of work at a given location also means the possibility to postpone the Final System Acceptance (FSA)?	Considering all the facts and circumstances, a Contractor's delay in the achievement of a defined milestone event as a result of a Para 23.8 delay could possibly be considered as an excusable delay within the context of the Liquidated Damages clause.	NO	**AMD#2**
CR#190	Book II Part II & IV	Part II Sections 23.7, 23.8 Part IV section 5.4.4	Is the possibility of moving the commencement of work by 90 days makes it necessary to re-run Site Verification Survey (if such a test took place earlier)?	As mentioned in SOW section 5.4.4: - site verification surveys will be performed if required (i.e. there's no guarantee that they will be needed) - the actual visit of the sites subject to the Site Verification Survey is left to Contractor’s appreciation As s result, the potential re-run of site verification surveys should not be of nature to impact the project costs.	NO	**AMD#2**
CR#191	Book II Part II	Section 25.1	Will the full list of "purchaser Furnished Equipment" PFE be available for the Contractor at the time of bid evaluation?	For bidding purposes, the list of PFE is fixed. SOW Annex E as well as Book I Section 3.6.4.9.5 were updated at IFB AMD#2.	YES (AMD 2)	**AMD#3**
CR#192	Book II Part II	Section 25.1	Is it possible to reduce the valuation of Contractor's bid by taking into account the content of "purchaser Furnished Equipment" PFE at the time of the tender?	The PFE list has been defined by the Purchaser and therefore, there will be no possibility to reduce the valuation of the Contractor’s bid at the time of the tender. Therefore, your Bid cost shall not include prices for PFEs. The value of any proposed PFEs will be excluded from the calculation of the Price Score. See also CR#290.	NO	**AMD#3**
CR#193	Book I	Section 2.11.1	In reference to 2.11.1. the bidder need to confirm the bid guarantee document by the Belgian banking institution, if the document has been issued by a non-Belgian institution. Is it possible to receive from the Purchaser a list of appropriate and acceptable Belgian banking institutions, which can be requested by bidder to obtain the required confirmation.	The Purchaser does not maintain such a list. Any bank or financial institution legally licensed by the Belgian authorities may issue such a confirmation.	NO	**AMD#2**
CR#194			Is the contracting authority registered as a VAT payer?	No, as the Purchaser is exempt from all VAT obligations under the Ottawa Agreement (See Book II, General Provisions, Clause 26).	NO	**AMD#2**

CR#195	Book II Part IV	Sections 12.2.5, 12.3.1.5,12.4.1.5, 15.5.1.5	Referring to the requirements for language skills specified by the Purchaser in Section 12 Labour Categories points 12.2.5, 12.3.1.5,12.4.1.5, 15.5.1.5 - is it sufficient, if the Contractor declare in written statement that the key personnel assigned to the contract has the required knowledge of English (as described in Language Proficiency levels of STANAG 6001 4343)?	The Purchaser always reserves the right to demand the Contractor to submit the appropriate language proficiency certificate. If the Purchaser exercises this right a mere written statement will not be sufficient. See as well CR #66.	NO	**AMD#2**
CR#196	Book II Part IV	Sections 12.2.5, 12.3.1.5,12.4.1.5, 15.5.1.5	If a certificate is required, will any of the certificates below be treated as equivalent to STANAG 6001 (4343)? • First Certificate in English • Business English Certificate Vantage • Higher TOLES • Certificate in Advanced English • Business English Certificate Higher • ICFE • ILEC • TOEIC (exam result min. 805 points) • IELTS (exam result min. 6.5 points) • Certificate of Proficiency in English • Advanced TOLES	It is the Bidder's responsibility to research STANAG 6001 (4343) to determine which (or if any) of the certificates listed can be used to fulfil the contract requirements, to include the relevant STANAG.	NO	**AMD#2**
CR#197	Book II Part IV	Annex A SRS-2795	Does it mean that E-NPKI should work with NEDS which uses LDAP forwarding (passing request to other LDAP server in case of lack data on the first server) or E-NPKI should forward information received from NEDS to any other service ?	E-NPKI shall support LDAP forwarding, meaning in this case that it must understand redirection request to another LDAP directory.	NO	**AMD#2**
CR#198	Book II Part IV	Annex A SRS-501	Does Distinguished Name should be unique through whole history of E-NPKI or it should concerns only active (non-deleted) subscribers?	yes it should be unique through the whole history of E-NPKI.	NO	**AMD#2**
CR#199	Book II Part IV	Annex A SRS-502	Is it a procedural requirement or the technical one?	It is a procedural requirement.	NO	**AMD#2**
CR#200	Book II Part IV	Annex A SRS-2016	What is the source of information concerning organizational affiliation of trusted role personnel, in context of verification of affiliation. NEDS?	This will be addressed during site surveys.	NO	**AMD#2**
CR#201	Book II Part IV	Annex A SRS-2014, 2161, 2723	Does it mean that E-NPKI should be integrated with that systems during implementation phase (PSA and FSA) or this integration should be proved during OAT/BLAT?	See CR#132. All functional requirement must be demonstrated prior to completion of BLAT.	NO	**AMD#2**
CR#202	Book II Part IV	Annex A SRS-2015	This requirement greatly reduce the competition because FIPS-201 is not used in Europe and for European companies is difficult to have proved integration with CMS conforming to FIPS-201. We suggest withdraw this requirement and require this integration in the implementation phase.	Support for FIPS-201 is mandatory due to the results of previous International Competitive Bidding process involving all 28 NATO Nations. Regarding SRS 2015, the wording is changed at IFB AMD#2 . **The E-NPKI shall demonstrate a proven track record for integration with multiple vendors Physical Access Control (PACS) Card Management Systems (CMS) including Biometrics, without requiring custom modifications to the E-NPKI Certification Authorities.**	YES	**AMD#2**
CR#203	Book II Part IV	Annex A SRS-512	Does it mean that is expected that E-NPKI will contain subscribers' biometric data stored in E-NPKI database?	E-NPKI shall support the writing of biometric data captured by the CMS, onto the FIPS-201 chip.	NO	**AMD#2**

CR#204	Book II Part IV	Annex A SRS-517	What does it mean “evidence” in context of verification of subscriber information? Is it expected either to store scanned ID document and photo made by camera to prove visual identification or provide a checkbox that confirm such verification?	The bidder shall scan and electronically store documents and photos , see SRS-2019 and SRS-509	NO	**AMD#2**
CR#205	Book II Part IV	Annex A SRS-2152	In case of generating keys on behalf of the applicant, the keys should be generated only by CA or RA is also permitted to do so?	The purchaser assume the bidder is referring to SRS-710, key generation is intended to be implemented on either end entity token or within the HSM of the CA. Generating keys within the RA would require an HSM to be installed in every RA.	NO	**AMD#2**
CR#206	Book II Part IV	Annex A SRS-531	How to reconcile the requirement of signing agreements by subscribers (SRS-538) and digitally storing its (SRS-2626) and bulk applications? Does it mean that either all data gathered in certificate application workflow should be put in a batch or some data for such process can be omitted?	See CR# 143	NO	**AMD#2**
CR#207	Book II Part IV	Annex A SRS-2630	Regarding that E-NPKI will operate also in a SECRET domain, can we assume that network at the security level SECRET connecting such sites is provided and encryption is expected only for a separation of concerns?	The ON environment includes high grade cryptographic backbone providing cryptograph approved for the protection of Secret information. On the ON, E-NPKI will provide need to know separation.	NO	**AMD#2**
CR#208	Book II Part IV	Annex A SRS-447	Is it a procedural requirement or the technical one?	It is a combination of both, see CR#144	NO	**AMD#3**
CR#209	Book II Part IV	Annex A SRS-2060	Does distribution to the new distinguished name mean distribution of old certificates to a new LDAP node?	yes	NO	**AMD#2**
CR#210	Book II Part IV	Annex A SRS-2645	Can it be a paper log?	No. See SRS-602.	NO	**AMD#2**
CR#211	Book II Part IV	Annex A SRS-837	The SRS-837 requirement states that Common Criteria certificate is required for CA and RA software, but Annex B-16 states that approval for cryptographic product issued by National CIS Security Authority is sufficient. Can you confirm that the approval can be delivered instead of certificates?	Requirement ID: SRS-837 The E-NPKI CA and RA systems shall be certified compliant to the CIMC Protection Profile Security Level 3 or equivalent. (Common Criteria certificate shall also be delivered to demonstrate conformance) Requirement ID: SRS-838 CA and RA certification and approval shall be performed by a NATO Nation CIS Authority for the security relevant elements of the E-NPKI CA and RA. (Annex B-16 refers to these certificates) Requirement ID: SRS-840 The selection and use of other Common Criteria Protection Profiles, which have been certified by a NATO National Security Authority (NSA) shall be utilised where appropriate. (The confirmation statement that the alternate Common Criteria Protection Profile is equivalent to the CIMC PP shall be delivered.)	NO	**AMD#2**
CR#212	Book I	Annex B-16	Could you clarify what is the date of delivery certificates/approval letter to the Purchaser and relate it to any point in the bidding process?	The Purchaser is aware that a few Nations will not, in accordance with their standard practice, provide approval certificates/letters directly to Bidders. It is with this situation in mind that the Annex B-16 certificate is written to allow the delivery ‘prior to the conclusion of the bid evaluation’. On the other hand, most Nations will provide approval certificates/letters to their industry. If the certificates/letters are available to Bidder’s as part of normal national practice, those Bidders are fully expected to include copies of all necessary approval certificates along with their bids.	NO	**AMD#2**
CR#213	Book II Part IV	Annex A SRS-1471	Does E-NPKI either have to provide security gateway between domain or E-NPKI should prepare data in the format acceptable by existing gateways?	The provision of security gateway between domains is not in scope of project.	NO	**AMD#3**

CR#214	Book II Part IV	Annex A SRS-1086	SRS-1086 states that 500 simultaneous session between RA and a single CA is required, and SRS-2101 requires only 100 simultaneous connection between RA and CA. Could you clarify what is the proper requirement?	Requirement is clear as written : SRS-1086 the minimum is for 500 concurrent **sessions** on each CA server **including RAs and end entities**. And as mentioned by SRS-2101 a minimum of 100 simultaneous **RAs connections** per CA.	NO	**AMD#2**
CR#215	Book II Part IV	Annex A SRS-2758	What is “Windows Device” ? Does it concern auto-enrolment of windows stations and domain controllers?	yes, additional devices such as phones would be connected via a MDM. Please note that Blackberry Enterprise was added to SRS-2769	yes	**AMD#2**
CR#216	Book II Part IV	Annex A SRS-2758	Auto-enrolment of window station/server works only with Microsoft CA. Is it acceptable to install on the windows station/server a dedicated service to perform this function?	See CR#31 Auto-enrolment of Windows servers is not limited to a Microsoft CA. The use of plugin or client software specific to the CA is permitted.	NO	**AMD#2**
CR#217	Book II Part IV	Section 1.6.1.5.2	Please confirm, that points from 1.6.1.5.3 to 1.6.1.5.5 are related to 1.6.1.5.2 as a sub-requirements of this point.	Confirmed and corrected in AMD#2	Yes	**AMD#2**
CR#218	Book II Part IV	Sections 5.5.4.2.2, 5.5.4.3.2, 5.5.4.4.2	Please confirm, that localized version means a version translated to the national language.	No. "Localized" versions does not mean translation to the national language. Rather, it means adaptations to specific local considerations.	NO	**AMD#2**
CR#219	Book II Part IV	Section 5.5.6.9	Documentation says “…(see 10.1.8.1.11 and 10.1.8.1.12)…”, but there is no such point in this document. Please confirm which point this statement relates to.	Correct. Those references were incorrect and have been updated to 10.4.1.11 and 10.4.1.12 respectively in the IFB AMD#3.	NO	**AMD#3**
CR#220	Book II Part IV	Section 6.6.1	Documentation says “…The Contractor shall provide a fully detailed and priced Recommended Spare Parts List (RSPL)…”. Please clarify if this spare parts should be delivered by Contractor without any additional costs, or it will be purchased.	The Contractor shall deliver spare parts (SOW 6.6.3 and 6.6.4) at no additional cost to the Purchaser.	NO	**AMD#2**
CR#221	Book II Part IV	Section 7.3.3.2	Please clarify if the physical access control systems in NATO sites are standardized and uses the same mechanisms (egg. Mifare), or during the implementation process Contractor will have to integrate with different types of interfaces, databases, or software that operates in this sites	See SRS-2838 and SRS-2824 updated in AMD#2. The bidder shall assume that all NATO PACS system are using Mifare DESFire.	NO	**AMD#3**
CR#222	Book II Part IV	Section 16.8.5.3	Please clarify if Contractor will be operating on this systems (egg. have access to administrative accounts, to import new certificates into device or system) or will just prepare tools and mechanisms to use by the current system’s administrator	The bidder will liaise with the system administrators in order to import certificates.	NO	**AMD#2**
CR#223	Book II Part IV	Annex A SRS-2015	“The E-NPKI shall demonstrate a proven track record for integration with multiple vendors FIPS-201 Card Management systems without requiring custom modifications to the E-NPKI Certification Authorities.” Please clarify if declaration of integration with existing CMS systems without additional cost to NATO is enough? (similar to SRS 2163) If NOT, how many and which CMS systems should be examined by us and when we have to submit „proven track record of integration” with these systems?	See CR#202 SRS-2015 is requesting proven track record. It is up to the bidder to provide any deemed relevant information.	NO	**AMD#2**

CR#224	Book II Part IV	Annex A SRS-2164, 2165, 2166, 2038	Regarding SRSs: 2164, 2165, 2166 and 2038 – Purchaser require E-NPKI to support the existing FIPS 201 compliant biometric equipment (scanning devices, readers and smart cards). Some functionalities are implemented in middleware delivered by manufacturers. In case of lack of appropriate middleware (e.g. not supporting some versions of operating systems) there is possibility to make such a software by a Contractor. However it requires to obtain detailed information from manufacturers and standard procedure is to sign the NDA. What's going to be when manufacturer doesn't agree to submit this information?	In case existing FIPS 201 compliant biometric equipment integration with the bidder's solution are not allowing to fulfil all functional requirements from the SOW, it is the bidder's responsibility to provide an alternative solution/hardware.	NO	**AMD#3**
CR#225	Book II Part IV	Annex A SRS-2273 & 2620	Regarding SRS-2273, SRS-2620: Documentation says in SRS-2273 that: ”E-NPKI CAs shall be able to issue CRLs signed by the old CA private key until the expiry of all end entity certificates signed by the old CA private key.” But in SRS-2620 it says: “The E-NPKI shall implement PKIX Certificate Management Protocol (CMP) defined in RFC4210.” CRL production is one of the mandatory PKI management function. According to the RFC 4210 to change the key of the CA, the CA operator generates a new key pair; creates „oldwithnew”, „newwithold” and „newwithnew” self signed CA certificates; next publish them in the repository and/or sending special „CAKeyUpdAnn” message to EE. After that the old CA private key is no longer required – CRL's are signed using new key, even the old one is not expired. It means that SRS 2273 and 2620 are conflicting. Please clarify, which of this two requirement should be implemented in the system.	SRS-2773 and SRS-2620 are mandatory for compatibility reasons. The reality of awareness in PKI enabled appliances is that today, most of these appliances do not correctly perform path validation including the "newwithold" signed certificate. This means that as soon as the CA Certificate is updated, all appliances experience immediate path validation errors and required redeployment. Most of these appliances use only TLS which does not rely upon the LDAP repository for Certificate lookup.	NO	**AMD#2**
CR#226	Book II Part IV	Annex A SRS-2388, 724, 2800, 2324, 2333, 2467, 2469, 453, 454, 2478, 492, 2616, 493, 724	Regarding SRS 2388, 724, 2800, 2324, 2333, 2467, 2469, 453, 454, 2478, 492, 2616, 493, 724, : “The E-NPKI subscriber certificates (Subscribers and Devices) shall correctly process the extensions identified in the PKIX certificate and CRL profile (RFC3280 and RFC 5280.)” It must be noted that RFC 5280 obsoleted RFC 3280. In case of extensions there are some differences, egg: - RFC 5280 recommends marking the policy mappings extension as critical; RFC 3280 required that the policy mappings extension be marked as non-critical (similar considers policy constraints extension); - RFC 3280 specified the holdInstructionCode CRL entry extension; this information was removed from RFC 5280 – should we support it? - RFC 5280 doesn't track the criticality of the „certificate policies” extensions in a chain of certificates. Please clarify, if we should implement RFC 5280, and if it will be differences between this two standards Purchaser will require that system will comply with RFC 5280.	Policy mappings: shall be supported HoldInstructionCode: shall be disabled Certificate Policies extension shall be supported SRS-2273 and SRS-2620 are overlapping, but they are not conflicting.	NO	**AMD#3**

CR#227	General		The IFB documentation makes clear those "basic" sites (where funds are already confirmed) and also those sites which are "options" (i.e. those for which funding has not, as yet, been confirmed). CLIN 19 indicates the desire, by NATO, to have the E-NPKI solution also implemented at the optional sites, but CLIN 19 is not included in the total project budget summary. For the avoidance of doubt, would you therefore please confirm whether further funding for these (optional) sites will be made available to the successful Contractor, or whether it is NATO's position that these are already included in the stated total project budget.	CLIN 19 is an Option CLIN to be executed for any additional sites which are not included in the ceiling values. At this point, there is no guarantee that CLIN will executed.	No	**AMD#2**
CR#228	General		Our understanding, from the IFB documentation, is that there are 14 Certification Authorities, 126 Registration Authorities and 9 OSCPs. Please confirm that these planning/sizing assumptions of ours are correct.	yes, as stated in Book II Part VI, 1.1.5, this is the type and quantity of technical service required as per Table 7.	NO	**AMD#2**
CR#229	General		The HQ Allied Joint Force Command Naples is shown as having 2 CAs, 2 RAs and 2 OCSPs. Please confirm on which network(s) these services will reside.	Each technical service need to be deployed on both PBN and ON for HQ Allied Joint Force Command Naples . In addition , see CR#73	NO	**AMD#2**
CR#230	General		The current I-NPKI solution will employ equipment that may be appropriate to our solution and could therefore, if made available, assist in our ability to cut costs. Please indicate if this is possible and, if so, on what terms would NATO seek to make such equipment available.	The current iNPKI equipment will continue to function in parallel (as an RSA-based system) along with the E-NPKI solution until all legacy devices are migrated or withdrawn from service. For bidding purposes, Bidders shall consider that no iNPKI equipment will be available for reuse by E-NPKI.	NO	**AMD#3**
CR#231	General		Can we please have access to the formal I-NPKI design pack, together with a list of all equipment (including specifications) that make up the current system?	The iNPKI Architecture is described in the slides for the bidders conference. Current quantities of users and devices provided in CR#181	NO	**AMD#2**
CR#232	General		Clearly, the E-NPKI solution will need to enable the (remote) Registration Authorities to connect to one of the 3 primary sites that contain the Certification Authorities. Does NATO have a preference for how this site to site connectivity should be undertaken, by the Contractor?	The bidder should propose a design based on its own recommendation paying close attention to the availability and automated failover requirements.	NO	**AMD#2**
CR#233	General		The documentation indicates that the Contractor will integrate to existing Card management Systems (CMS) and supply certificates to elliptic encryption capable Smart Cards. The Contractor must also supply new cards where they are not capable of elliptic encryption. Within the User list Smart Cards only are stated, but this information does not include the type of Smart Card e.g. site access vs IT access. Please therefore confirm the quantities and variations of Smart Cards.	For physical access control cards (on the PBN only) the cards shall also support Mifare desfire. See SRS-2824 and SRS-2838 as updated in AMD#2. See also CR#20.	Yes	**AMD#2**

CR#234	Book II Part IV	Section 5.5.6.12	We note that the Contractor will deploy E-NPKI certificates onto existing Purchaser's smartcards that support elliptic curve algorithms and that this will be without the requirement to replace the existing cards. Please therefore provide details of the numbers/whereabouts of those smart cards that do support elliptic curve algorithms, together with a breakdown of the numbers/whereabouts of other cards (e.g. RSA). Please also provide the specification of the Smart Cards currently in use within the I-NPKI system.	Quantities of existing RSA smartcards (all from iNPKI) is irrelevant as those cards shall be replaced by Elliptic Curve smartcards provided by the E-NPKI project. For bidding purposes, the Bidders shall consider the estimated quantities of smartcards in Tables 9 & 10. Estimated quantity of existing Elliptic Curve Smartcards is 2,200 for ON and 1,600 for PBN (see SOW table 10, New NATO Headquarters). The types of existing Elliptic curve smartcards are identified in SRS 4.9.2.4. See also CR#20.	NO	**AMD#3**
CR#235	Book II Part IV	Section 5.5.6.12	We note that, in those circumstances where no CMS components are in place, the E-NPKI Contractor will be required to provide "the full CMS including camera and printing capabilities". Please provide details of those sites to which this will apply (i.e. where no CMS components are currently in place).	See CR#13	NO	**AMD#2**
CR#236	Book II Part IV	Section 1.4.4.4	Are we correct that only the initial installation is to be performed by the Contractor; i.e. in line with the three level maintenance model, and that all subsequent installations will be performed by the Purchasers level 1 and 2 staff?	The installation of the full scope of the E-NPKI IFB is the responsibility of the Contractor. Any subsequent reinstallations due to Level 1, 2, or 3 maintenance activities may require contractor support as defined in SOW section 7.4.10	NO	**AMD#3**
CR#237	Book II Part IV	Sections 6.3.2.4, 6.3.2.5, 6.3.2.6, 6.3.2.7	Are the terms CBT and CAT intended to be used synonymously? Please also confirm whether these are expected to be standalone electronic training packages, or is all training (including delta training for updates), to be instructor led?	CBT and CAT can be considered to be synonymous for the purpose of this contract. These are expected to be self led stand alone products. Paragraphs updated to CBT in AMD#2	YES	**AMD#2**
CR#238	Book II Part IV	ANNEX B Section 3.3.5, 7.1.9 (in particular 7.1.9.1)	Please confirm whether the manpower requirements specified in section 7.1.9.1 cover both onsite and offsite support (including Helpdesk) or do they specifically relate to the onsite support element (only)?	SOW section 7.1.9.1 relates to onsite Purchaser's manpower.	NO	**AMD#2**
CR#239	Book II Part IV	ANNEX B Section 3.3.7	"During normal working days, the Contractor shall provide Hardware, Software and technical resolutions within four hours of notification of failure by the Purchaser." Please confirm if the four hour resolution time relates to all sites or just the sites with an onsite presence?	All sites.	NO	**AMD#2**
CR#240	Book II Part IV	Section 7.4.10	We note that all level 1 and 2 maintenance will be performed by Purchaser personnel, who may ask for support from the Contractor (whilst level 3 maintenance will be provided by the Contractor). We have assumed that any request for assistance for level 1 and 2 will come from a central Purchaser point (SHAPE?) and will not take place until staff at the requesting sites have performed standard procedures, prior to calling the helpdesk? Is this correct?	Assistance requests will come through NATO Centralized Service Desk (not physically bound to a specific location) following standard procedures. Service desk tickets are used to track all issues or service disruptions.	NO	**AMD#3**
CR#241	Book II Part IV	Section 7.4.10.3.2	Will equipment requiring level 3 maintenance be shipped to Mons, by the Purchaser; in particular where equipment needs to be rendered unclassified or is it the Contractor's responsibility to collect it from site?	Transportation after initial delivery will be the responsibility of the Purchaser, who will ship IAW the established procedures. The Contractor will be responsible for the return of any equipment to the Purchaser after Warranty repair.	NO	**AMD#2**

CR#242	Book II Part IV	Annex B Sections 3.3.5.2 & 3.3.11	Are we correct in interpreting the term “response” as being an appropriate engineer / technician contacting the originator of the incident / service request via phone / e-mail?	yes	NO	**AMD#2**
CR#243	Book II Part IV	Annex B Section 3.3.5.2	Are we correct in assuming that the helpdesk / service desk is the single point of contact and that the 1 hour response time is for any call / e-mail received, regardless of incident priority?	yes	NO	**AMD#2**
CR#244	Book II Part IV	Annex C Section 1.1.6	What requirements, if any, apply to those sites that don’t have any apparent technical services to be deployed (e.g. RA, CA, OCSP) but which nonetheless form part of either PSA or FSA milestones (e.g. Site ID 14 NATO Communications and Information Systems Group HQ @ Mons?)	See Q#29. See CR#67.	NO	**AMD#2**
CR#245	Book II Part IV	Section 3.9.2.4	Please provide a draft Terms of Reference for the Security Working Group, in order to assist us with our estimation of resource requirements.	There's currently no Terms of Reference of the Security Working Group (SWG). SOW Section 11.2 (in particular 11.2.7) should be sufficient for the Bidder to estimate resource requirements.	NO	**AMD#2**
CR#246	Book II Part IV	Section 3.1	Please provide details of the IV&V Contractor, together with the process for Validation.	SOW section 3.10 provide more details about the IV&V Contractor.	NO	**AMD#2**
CR#247	Book II Part IV	Section 4.1.2	Please provide details of the NATO Security accreditation process, together with the requirements, resource and timescale estimates for accreditation.	Sufficient details related to the Security Accreditation Process are already part of the SOW (section 11).	NO	**AMD#2**
CR#248	Book II Part IV	Section 6.3.4.7	The SOW refers to the use of MS Office Professional, Portable Document Format (PDF) and Visio. Does NATO have a preferred version number for these? E.g. 2013	Office 2013 is the preferred format. No preference for PDF.	NO	**AMD#3**
CR#249	Book II Part IV	Section 11.1	We note the requirement for E-NPKI to be accredited to NSAB. Please provide details of the requirements and the process needed to achieve NSAB accreditation.	Sufficient details related to the Security Accreditation Process are already part of the SOW (section 11).	NO	**AMD#2**
CR#250	Book II Part IV	Section 11.3.13.2 & 3	Please provide a briefing document on PILAR, which will be used to conduct Risk Assessments for EPKI for the 3 domains.	For bidding purposes, the bidders shall note that versions of the PILAR tool (commercial and trial) as well as guidance/documentation are available at www.ar-tools.com. The Purchaser plans to provide a more complete User Guide to the selected Contractor, after contract award.	NO	**AMD#2**
CR#251	Book II Part IV	Section 14.1	We note that QA&C must be in line with AQAP. What is NATO’s view on the use, by Contractors, of ISO9001/2700x for QA&C, as this is closely aligned with AQAP?	This is acceptable	NO	**AMD#2**
CR#252	Book II Part IV	Annex A	Please describe how the namespace works - will NEDS be federated, enabling publishing to one common namespace across all CAs, or is CRL publishing on a per-CA basis?	NEDS covers the entire namespace for E-NPKI and will therefore replicate information between sites. The model for CRL publishing is for the bidder to provide taking careful note of the redundancy and automated failover requirements.	NO	**AMD#2**
CR#253	Book II Part IV	Annex A Section 3.3.1.1	Are there any restrictions on Storage Area Networks (SANs), in respect (for example) of wildcards for web servers?	We suppose the bidder means Subject Alternate Name instead of Storage Area Network. Subject Alternate Name shall be supported, however application requiring wild card certificates will require NATO PKI Management Authority (NPMA) approval.	NO	**AMD#2**

CR#254	Book II Part IV	Annex A Section 3.3.2.1	Will Certificate Management Protocol (CMP) be initiated over HTTP or HTTPS? The standard specifies HTTP not HTTPS. SRS-834 requires session cryptography, but what SSL certificate will be used as the ENPKI root cert will not be trusted at the time of request?	We assume the bidder is making reference to RFC6712 [CMPtrans] mentioned in CR#260, and particularly to : "For direct interaction between two entities, where a reliable transport protocol like TCP is available, HTTP SHOULD be utilized for conveying CMP messages." But RFC6712 also states : “CMP provides inbuilt integrity protection and authentication. The information communicated unencrypted in CMP messages does not contain sensitive information endangering the security of the PKI when intercepted. However, it might be possible for an eavesdropper to utilize the available information to gather confidential technical or business critical information. Therefore, users of the HTTP transfer for CMP might want to consider using HTTP over TLS according to [RFC2818] or virtual private networks created, for example, by utilizing Internet Protocol Security according to [RFC4301]. Compliant implementations MUST support TLS with the option to authenticate both server and client.” SRS-834 (which is in section 3.6.5.1) does not prescribe the transport protocol, but establishing cryptographic sessions shall be part of the design of each bidder's cryptographic implementation.	NO	**AMD#3**
CR#255	Book II Part IV	Annex A SRS-2155 & 2157	Please advise whether this applies to the renewal of tier 2 CAs, or just to subscriber certificates.	Both SRS-2155 and SRS-2157 applies to all requests.	NO	**AMD#2**
CR#256	Book II Part IV	Annex A SRS-2013	Please advise what IdM interfaces are available? What information is expected to be provided by IdM?	See SRS section "4.9.2.1 LDAP / LDAP over SSL" See SRS section "4.6.3.2.2.1 Directory services" and "4.9.1 Information Products" See SRS-1216 "ODBC database interfaces for the connection to external PACS systems"	NO	**AMD#2**
CR#257	Book II Part IV	Annex A SRS-2813, 4, 2014, 2161, 2722 ,2723 ,2163	Please advise which versions of each CMS are used and at which sites. Also, what capability does each site have to operate the CMS in question? What is the Contractor expected to provide in respect of both operating the capability and training?	See CR#15 through CR#18.	NO	**AMD#2**
CR#258	Book II Part IV	Annex A SRS-2626	Please advise what form of signature is valid, as a strong electronic signature by PKI cannot be done until after the certificate is issued. Will NATO require this as “wet ink on paper”, implying the need for scanning/archiving, or electronic signature by checking box (“EULA-style”) only?	Policy permits the use of the newly issued credential to digitally sign the electronic subscriber agreement in order to eliminate the need to scan additional paper records. Added to SRS section 3.4.1	yes	**AMD#2**
CR#259	Book II Part IV	Annex A SRS-2626	“Simple Certificate Enrolment Service” is not a recognised interface protocol. Please confirm that this, in fact, refers to SCEP as defined in http://www.ietf.org/id/draft-gutmann-scep-02.txt (as per SRS-2768)	SRS-1766 not SRS-2626 Yes, the "Simple Certificate Enrolment Service" mechanism mentioned in SRS-1766 refers to SCEP as mentioned in SRS-2768	YES	**AMD#2**

CR#260	Book II Part IV	Annex A SRS-691	RFC4610 is not as described. Please confirm RFC4210, as amended by RFC6712, is what is actually required.	The reference to RFC4610 is incorrect; it should be RFC 4210. SRS-691 has been amended accordingly at AMD#3.	YES	**AMD#3**
CR#261	Book II Part IV	Annex A SRS-858	Please confirm that this requirement is limited to tier 2 Certification Authorities, or should it also be considered to cover Tier 3 Registration Authorities, as well?	Provision of Boundary protection devices are not in scope. See CR#88. Some CMS systems for PACS are segregated behind Boundary protection devices.	NO	**AMD#2**
CR#262	Book II Part III	Section 6.2	Please detail the applicable laws and regulations for compliance?	It is the Bidder's responsibility to ascertain and comply with all applicable laws and regulations. The Purchaser cannot provide all references as requested.	NO	**AMD#2**
CR#263	Book II Part IV	Annex A Section 3.6.6.1 SRS-858	One of the system development control requirements requires equipment (hardware and software) to be procured in a fashion to reduce the likelihood that a component has been tampered with. Can the Contractor assume that this requirement only applies to active components that are procured and does not apply to non-active components within the solution?	The Bidder is kindly requested to define what he considers to be active and non-active components	NO	**AMD#2**
CR#264	Book II Part IV	SoW section 5.5.2.8 Annex A section 3.5.1.3	The IFB indicates that the Purchaser is responsible for providing the power facilities that are required to power up and operate the installed E-NPKI equipment across the various sites, but it has not clarified whether this power is filtered and uninterrupted. Can the Purchaser confirm that the power provided at the various sites where racks are likely to be is filtered and uninterrupted, so the Contractor can exclude provision of dedicated UPS's to clean and protect the power?	Yes. Note that the descriptive text does not have an SRS- Requirement number allocated against it.	NO	**AMD#2**
CR#265	Book II Part IV	Annex A SRS-2278, 661, 759	Requirements SRS-2278 and SRS-661 indicate that the Contractor should not assume that services that it relies upon are 100% available, but SRS-759 potentially seems to conflict this as measurements of availability shall not include failures from factors that are external to E-NPKI. Can the Purchaser confirm that Requirements SRS-2278 and SRS-661 are included so that the Contractor delivers a solution that has been architected so it can cope with failures of external services, but SRS-759 has been included so that the measured unavailability excludes failures as a result external service failures?	yes this is correct. SRS-2278 and SRS-661 are included to design a resilient service. SRS-759 is directed at the measurement of the E-NPKI service availability.		**AMD#2**
CR#266	Book II Part IV	Annex A SRS-758, 2253	Requirement SRS-2553 indicates that MTTR values from each subsystem shall not reduce the required system or subsystem availability, but SRS-758 indicates that non-availability time includes time to repair. Has the Purchaser included requirement SRS-2553 to ensure that the Contractor cannot exclude planned maintenance and repair times down times from the availability calculation?	yes. See CR#27	NO	**AMD#2**

CR#267	Book II Parts I and II	Schedule of Supplies and Services & Clause 21 of Part II	In light of the fact that there are no service credit figures within the IFB, please could the Purchaser confirm whether the Liquidated Damages detailed within Clause 21 of the Contract Special Provisions shall also apply to CLIN 5.0 (Operations and Maintenance (Option)), including sub-CLIN's 5.1, 5.2, 5.3, 5.4, 5.5 and 5.6?	The Purchaser cannot waive the application of Liquidated Damages for any portion (CLIN) of the foreseen contract effort. Situations could be reasonably foreseen whereby the simple accrual of service credits against an SLA would not adequately protect the Purchaser's interests. An example of this would be a Contractor's complete failure to provide any services.	NO	**AMD#2**
CR#268	Book II Part II and IV	Part II Clause 4 Part IV Section 7.1.6	It is noted that the Purchaser may exercise the Options up to 5 years from Final System Acceptance (FSA) – Can the Purchaser confirm that irrespective of the time where the options are exercised this programme will cease no later than FSA + 5 years?	The contract will only be fully concluded and closed when all duties and obligations under the contract are determined to be complete, and when both parties have signed a mutual release of all claims. Accordingly, the Purchaser cannot make the confirmation as requested in the question.	No	**AMD#3**
CR#269	Book I	Annex A (Bidding Sheets) CLIN 2.5.1	The CLIN numbering appears incorrect for the Security Working Group (SWG) CLIN. Can the Purchaser confirm the below CLIN numbering to be correct? 2.5.1.1 Documentation to support SWG meetings 2.5.1.2 SWG meetings 2.5.1.3 SWG meetings minutes	Corrected at IFB AMD2.	YES	**AMD#2**
CR#270	Book I	Annex A (Bidding Sheets) CLIN 2.7.9	The delivery form is identified as HW/SW for CLIN 2.7.9. Can the Purchaser confirm if the correct delivery form should be identified as HW / SW / Labour?	Corrected at IFB AMD2.	YES	**AMD#2**
CR#271	Book I	Annex A (Bidding Sheets) CLIN 2.8.7	The delivery form is identified as Electronic for CLIN 2.8.7. Can the Purchaser confirm if the correct delivery form should be identified as HW / SW as identified for the same item under CLIN 3.5.6?	Corrected at IFB AMD2.	YES	**AMD#2**
CR#272	Book I	Annex A (Bidding Sheets) CLIN 3.2	The description reads "Site Surveys for FSA sites" for CLIN 3.2. Can the Purchaser confirm if the description should read "Site Surveys for PSA and FSA sites"?	CLIN 3.2 only relates to site surveys for FSA sites. Site surveys for PSA sites are covered under CLIN 2.9	NO	**AMD#2**
CR#273	Book I	Annex A (Bidding Sheets) CLIN 4.2.3	The delivery form is identified as Electronic for CLIN 4.2.3. Can the Purchaser confirm if the correct delivery form for the Training Materials should be identified as Electronic / HW / SW / Labour to include the delivery of the Training System or can the Purchaser confirm under which CLIN the Training System is to be delivered?	CLIN 4.2.3 covers the preparation of training materials for all the sites. Their effective delivery to the sites is covered under the "Delivery per site" spreadsheet. For clarity purposes, CLINs 2.7.16, 3.3.2.23, and 3.3.2.24 were added in IFB AMD#2. CLINs 2.7.16 and 2.7.17 were renamed 2.7.17 and 2.7.18 respectively. Besides: - as mentioned under SOW 6.4.11, the Contractor shall provide all other facilities, services and equipment (including servers and workstations for students and teachers, network equipment, all required SW, etc.…) necessary to carry out the On-Site Training activities. - the delivery of non-production environments - Reference System and Testbeds - is covered under CLIN 2 and 3.	YES	**AMD#2**

CR#274	Book I & Book II Part IV	Book I Annex A (Bidding Sheets) CLIN 4.2.3 Book II Part IV section 6.4.11	The delivery form is identified as Electronic for CLIN 4.2.3.3. Can the Purchaser confirm if the correct delivery form for the CBT should be identified as HW / SW to accommodate the requirement for the Contractor to provide all other facilities, services and equipment necessary to carry out the On-Site Training activities as per SOW 6.4.11?	The delivery form "Electronic" for CLIN 4.2.3.3 is correct. It does not prevent the Contractor from considering that SW would be more appropriate. See CR#283.	NO	**AMD#2**
CR#275	Book I	Annex A (Bidding Sheets) CLIN 19.3.1	The CLIN numbering appears incorrect for the Site-Specific System Implementation deliverables - Technical Services CLIN. Can the Purchaser confirm the below CLIN numbering to be correct? 19.3.1.1 Certificate Authorities (CA) 19.3.1.2 Registration Authorities (RA) 19.3.1.3 Online Certificate Status Protocol (OCSP) 19.3.1.4 Timestamp	Confirmed to be correct. Also, note that in 19.2, the correct sub-CLINs are as follows: 19.2.1 Site-Specific System Engineering deliverables (if required) 19.2.1.1 Certification Practice Statement (CPS) 19.2.1.2 Security Risk Assessment (SRA) 19.2.1.3 System Security Requirement Statement (SSRS) 19.2.1.4 CA 19.2.1.5 RA 19.2.1.6 OCSP 19.2.1.7 Timestamp These changes have been updated in the bidding sheets.	Yes	**AMD#2**
CR#276	Book I	Annex A (Bidding Sheets) CLIN 6 Subj to Inv Ceiling – 6.3 System Implementation CLIN 19 Not in Ceilings – 19.3 System Implementation	The System Implementation under CLIN 6.3 is limited to the below two sub-CLINS without dedicated CLINS for Hardware and Software respectively. 6.3.1 Site-Specific System Implementation deliverables - Technical Services 6.3.2 Site-Specific System Implementation deliverables - User Services Can the Purchaser confirm if the System Implementation for CLIN 6.3 (and potentially for the other optional sites from CLIN 7 to CLIN 18) should be aligned with the high level breakdown of the Additional Sites in CLIN 19.3 as seen below? 19.3.1 Site-Specific System Implementation deliverables - Technical Services 19.3.2 Hardware 19.3.3 Software 19.3.4 Site-Specific System Implementation deliverables - User Services	The current breakdown of CLIN 6.3 is aligned with the high level breakdown of the additional sites in CLIN 19.3 (i.e. "Site-Specific System Implementation deliverables - Technical Services" and "Site-Specific System Implementation deliverables - User Services"). The Bidding Sheets and the SSS were updated at AMD3 to: - reflect the correct delivery form i.e. "HW / SW / Labour / Electronic", for all option CLINs 6 thru 18. - reflect the correct "Delivery Form" (i.e. Labour) for CLIN 19.3.1. The details for each applicable sub-CLIN (e.g. CLIN 6.3.1) should be provided in the CLIN Price Breakdown sheets to detail all necessary deliverables (e.g. Hardware, Software, labour). Please reference the Bidding Instruction tab of the Bidding Sheets.	YES	**AMD#3**
CR#277	Book II Part II	Clause 18	It is noted that the Purchaser intends to make one single payment for sub-CLIN 5.1, 5.2, 5.3, 5.4, 5.5 and 5.6 – Please could the Purchaser confirm whether this payment will be made in advance or arrears of the support being provided under these sub-CLINs, or whether the Purchaser would consider multiple payments per sub-CLIN through the course of the period of performance for each sub-CLIN, e.g. quarterly?	See changes in Contract Special Provisions, “Schedule of Payments”.	Yes	**AMD#3**

CR#278	Book I	Annex A (Bidding Sheets) CLINs 8, 9, 19	Please confirm that CLIN's 8,9 and 19 details should not be recorded on the "Detailed CLIN Summary" sheet as their cells are greyed out. They therefore should not form part of the total on row 533 labelled "Grand Total Firm Fixed"	Confirmed, these CLINs are not part of the ceiling values and will not be evaluated as part of the Best Value Competition.	No	**AMD#2**
CR#279	Book I	Annex A (Bidding Sheets)	Optional CLIN's "Detailed CLIN Summary" – please confirm if the "Site-Specific System Implementation deliverables - User Services" row should have a highlighted yellow cell in the "Investment" column on all relevant Optional CLIN's (currently Investment and O&M are both grey cells, and there is a yellow cell for the total only)	For all Option CLINs the Site-Specific ILS deliverables (if required). User Services only. Should be highlighted yellow in the Investment column. The only Option CLINs not highlighted in yellow for the referenced sub-CLIN are 8,9 and 19 as they are not part of the ceiling values nor will they be evaluated as part of the Best Value Competition.	No	**AMD#2**
CR#280	Book I	Annex A (Bidding Sheets)	Site Summary – please confirm if "Non-Site Specific" price totals should be recorded on row 8. Please confirm if the "Total" at row 7 should just be for site-specific prices below, or whether it should also include the non-site specific and record a Grand Total price?	The bidding sheets were updated in Amendment #1 to reflect the requirement of the non-site specific costs as part of this summary and should be summed in the Total Prices for each CLIN.	No	**AMD#2**
CR#281	Book II Part IV	Sections 6.4.1, 6.4.2, 6.4.3	Can the Purchaser confirm that the development of the training programme specified in 6.4.1 will commence with a Training Requirements Analysis (TRA), as specified in 6.4.3, which is expected to identify the need for a Training Needs Analysis (TNA) which will then identify the training which must be delivered and whether it is available off the shelf or will need to be developed by the Contractor?	The TRA to TNA process is described in the ACT DIR 75-2 (E&T Directive), and the Contractor is correct that the TRA will determine a need for a TNA. As stated in CR#282 there is overlap between the reference documents. 75-2 states "Gaps identified on Education and Individual Training (E&IT) in the Training Requirements Analyses (TRA) will be defined through the Training Needs Analysis (TNA) process". For simplicity, the Contractor shall supply a TNA (and associated TNA report) which will identify any knowledge gaps. The IFB was amended to replace the Training Requirement Analysis by a Training Needs Analysis.	YES	**AMD#2**
CR#282	Book II Part IV	Section 6.4.1	The Applicable Documents section of the SOW calls up the BI-SC D 75-7 Education and Individual Training Directive but this is not referenced from within the SOW or SRS. As this has content overlap with ACT Directive 75-10, and forms part of a suite of documents (BI-SC 75-2 and BI-SC 75-3) could NCIA please confirm which is the appropriate applicable documentation?	It is true that there is content overlap in the referenced Directives, which can lead to some confusion. The requirement is for the Contractor to perform a TNA. The process for this is described in the ACT Directive 75-10 which the Contractor can consider as the definitive document for this purpose. The IFB was amended to replace the Training Requirement Analysis by a Training Needs Analysis.	YES	**AMD#2**
CR#283	Book II Part IV	Section 6.3.2.4	Could the Purchase please describe the mechanism by which the CBT is to be distributed and made available to users? A Learning Management System (LMS) would allow training content to be delivered as an online service, hosted in a secure environment, maintaining the information at an unclassified level, in order to ensure back to back release control with software and training updates for the lifecycle of the product, while allowing the purchaser the ability to make its own updates to the CBT package. However, it is not clear from the requirement whether the Purchaser has an existing LMS on which the CBT should be hosted, whether the Contractor should host a system specific to E-NPKI or whether the CBT is to be distributed by some other means, such as via DVD.	The Purchaser has no intent to distribute the CBT via a LMS platform. Therefore the provision of an LMS platform shall not be included in the bids. The Contractor may supply the CBT in DVD format or other equivalent means.	NO	**AMD#2**
CR#284	Book II Part IV	Annex A SRS-287 & 288	Can the Purchaser confirm that these requirements identify the need for an SCVP service?	Please confirm the SRS number as neither SRS-287 nor SRS-288 exist in the IFB. SCVP is not referenced within the IFB.	NO	**AMD#2**

CR#285	General		Can the Purchaser confirm if there is a requirement to provide administrative consoles and peripherals for the NATO and the Contractors O&M Staff or are all operational workstations provided by NATO to support the centralised functions?	Full management of the E-NPKI system is required within the scope of the IFB including any separate management consoles or peripherals required by the bidder's solution. See CR#136	NO	**AMD#3**
CR#286	Book II Part IV	Section 1.6.4	Given the statements on NCIRC within this section and the requirement to deploy NCIRC agents - Can the Purchaser confirm that NCIRC will be performing all Security Event and Incident Monitoring activities and for E-NPKI and there is no requirement for the Contractor to maintain a discrete security monitoring posture within the scope of this contract.	No, see SRS-601. The E-NPKI trusted roles are responsible for the incident monitoring of the E-NPKI systems. The NCIRC is only consolidating part of the security events. See also CR#22	NO	**AMD#2**
CR#287	Book II Part IV	Annex A Section 3.5.1.4, SRS-2647	The water exposure requirement requires all CA equipment to be mounted into 19" racks at least 1.2m above the floor, but it is unclear what floor level it is referring to. Can the Purchaser clarify whether the floor level is either: a) The floor that the rack is mounted upon (so there is a large amount of rack space that is not used) b) The real floor of the room that the rack is mounted in, i.e. any suspended floor uses up some of the 1.2m space c) The floor is the local ground plane of the building that the CA equipment is installed in.	Response b is the correct interpretation.	NO	**AMD#3**
CR#288	Book II Part IV	Sections 6.6.5.1, 6.6.5.3, Annex C	In light of the fact the Purchaser states in numerous sections of the IFB that the quantities detailed in Annex C of the SOW are estimates, please could the Purchaser confirm when the estimates for the data contained within Annex C of the SOW were produced, and the age of the data upon which these estimates were based?	Data contained in SOW Annex C were collected in 2Q15.	NO	**AMD#2**
CR#289	Book II Part I	Schedule of Supplies and Services CLIN 4.2.3.3	Can the Purchaser confirm whether they are supplying a platform to host the CBT or does the Contractor need to include this in their offer? Can the Purchaser confirm from which security domains the CBT must be accessible, if Contractor provided?	The Contractor is not required to provide a platform to host the CBT. Therefore the Bidders shall not include the provision of such a platform in their offer. See also CR#283	NO	**AMD#2**
CR#290	Book II Part IV	Annex E	Can the purchaser please clarify the following: 1. The Contractor can include any product within the additional PFE to be proposed by the bidder rows as they apply to any identified NATO enterprise agreement (for example under the MS EA, the contractor could include MSSQL, MS Exchange, MS SharePoint Server, Enterprise CALs etc. as valid PFE) 2. For additional rows added as PFE in this table, can the purchaser confirm if the contractor should include the cost of these licenses within the relevant CLINs or preclude these prices based on them being PFE?	See CR#191. For bidding purposes, the list of PFE is fixed (SOW Annex E); no additional PFE can be added. Bidders shall follow instruction of Book I 3.6.4.9.5 in particular. Any additional Software that may be needed as part of a Bidder's solution shall be included in the Bidder's bid (including prices as part of the Bidding Sheets). Bidders should take good note of Clause 25 in Book II Part II concerning Software.	YES (AMD 2)	**AMD#3**
CR#291	Book II Part IV	Section 7.1.9.1	Requirement 7.1.9.1 states that "The Purchaser will provide the following manpower for O&M activities …". Please confirm that this is a type which should read "The Contractor shall provide …"	SOW 7.1.9.1 is correctly phrased. "SHALL" requirements are only applicable to the Contractor (see SOW 1.8.5)	**NO**	**AMD#2**

CR#292	Book I	Section 3.6.4.6.3.5	Please confirm if a high level description of the engineering process in PMP is enough, in order to avoid redundancy with Volume 2	Confirmed. The initial PMP shall demonstrate that the Bidder has understood the engineering process imposed in SOW Section 4 and describe how he will support the cycle of design reviews and approvals.	**NO**	**AMD#2**
CR#293	Book I	Section 3.6.4.8.1	Please clarify if PMS should be integral part of initial PMP	The initial PMS shall be delivered in Microsoft Project format as part of Volume 1. See Book I section 3.6.4.8.2 and SOW 3.4.2.3. The Bidders shall also deliver a pdf version is included in Volume 1, potentially as an annex to the initial PMP. Book I updated accordingly.	**YES**	**AMD#2**
CR#294	Book II Part IV	Sections 13.15.1.4, 13.15.1.5	Please clarify if a high level description of the engineering & system implementation activities in PMP is enough, in order to avoid redundancy with Volume 2	Confirmed.	**NO**	**AMD#2**
CR#295	Book II Part IV	Annex A SRS-860	Is NATO's intention that successful bidder shall deliver the same number of Timestamping servers as the number of Tier 2 production Certification Authorities (i.e. for PBN and ON domains)? If yes, is it expected that they will be installed in the same location as CAs? If not, what number of Timestamping servers successful bidder shall deliver and what will be their locations?	See CR#150 and CR# 297	NO	**AMD#2**
CR#296	Book II Part IV	Annex A SRS-860	Does NATO require the successful bidder to deliver Timestamping servers also for non-production environments (i.e. testbed and reference system environments)? If yes, then how many Timestamping servers should be delivered for each non-production environment?	The Timestamping service is to be delivered to the same non-production locations as OCSP and CAs. See also CR#136,173, and 279.	YES	**AMD#2**
CR#297	Book II Part IV	Annex A SRS-860	Does NATO require the successful bidder to deliver Timestamping servers on dedicated hardware platforms as it is in case of CAs and OCSP servers (see requirement SRS-849)?	See CR#136 Timestamping servers do not require separation from the OCSP servers. However, the requirement to use a Hardware Security Module may not be compatible with the use of virtualization (to be determined by the bidder.)	NO	**AMD#2**
CR#298	Book II Part IV	Annex A SRS-2090	In case when successful bidder will be providing Timestamping servers also for testbed and reference system environments, is this this high performance requirement also valid for testbed and reference Timestamping servers? If not, what performance is expected from Timestamping servers installed in testbed and reference system environments? Is this required for non-functional testing?	For bidding purposes, the Bidders shall consider that the same performance specifications apply to the non-production environments. Further discussion will take place during pre-award discussions.	NO	**AMD#3**
CR#299	Book II Part IV	Annex A SRS-2100	Is this high performance requirement also valid for HSMs that will be installed in testbed and reference system environments? If not, what performance is expected from HSMs installed in testbed and reference system environments? Is this required for non-functional testing?	For bidding purposes, the Bidders shall consider that the same performance specifications apply to the non-production environments. Further discussion will take place during pre-award discussions.	NO	**AMD#3**
CR#300	Book II Part IV	Annex A SRS-732	SRS-732 requires an approval to all software to be used by NATO. Is this approval required before bidding on the project, or can it be requested and achieved after?	See CR#212	NO	**AMD#2**

CR#301	Book II Part IV	Annex A SRS-2163	On Requirement SRS-2163, our understanding is that the current 3 CMS products need to be adapted to the new E-NPKI needs. However, the bidder on this tender will need to negotiate with those 3 parties on the necessary changes. How can we know beforehand the required changes, so we can make a cost estimate? What is the impact on this on the new E-NPKI CMS?	The requirement SRS-2163 request the bidder to interface and integrate the 3 CMS products with his proposed PKI. The integration need to meet the same requirements applicable to the bidder's CMS implementation. These 3 CMS system are known to fully integrate with multiple COTS PKI systems. The Purchaser understands that the bidder might not have previously integrated these CMS whit his proposed PKI solution. But it is for the bidder to estimate the cost impact of such integration.	NO	**AMD#3**
CR#302	Book II Part IV	Section 6.3.2.4	Does NCIA have an LMS (Learning Management System) which is needed for viewing webinars and videos?	The Purchaser has no intent to distribute the CBT via a LMS platform.	**NO**	**AMD#2**
CR#303	Book II Part IV	Annex A SRS-2166	Please clarify which are the existing biometric scanning equipment.	Biometric scanning equipment is connected directly to the PACS CMS environment, writing of the FIPS-201 compliant biometric information to the FIPS-201 card is required by the E-NPKI.	NO	**AMD#2**
CR#304	Book II Part IV	Annex A	Since middleware from different card manufacturers, in a single desktop machine, tend to generate collisions in the hardware access, what is the current strategy of NATO to manage or avoid this situation? Or is the E-NPKI strategy to have a single provider of smartcards/middleware? In any case, what is the strategy to support legacy cards and the new cards, given the middleware conflicts? Is it, for example, by having a physical segregation - using PIV cards only on some NATO locations, and using other smartcards in the other locations?	Resolving middleware collisions is the responsibility of the bidder's design. The E-NPKI deployment strategy is to drive for standardization by using the fewest number of smartcards type possible. The requirement exists to have non interoperable smartcard solutions deployed between PBN and ON (See SRS-2801 and SRS-771)	NO	**AMD#3**
CR#305	Book II Part IV	Annex A	Does the current existing middleware in NATO have PKCS#11 libraries available?	FIPS-201 compliant cards do not use PKCS#11 libraries.	NO	**AMD#3**
CR#306	Book II Part IV	Annex A	Although ECDSA algorithms are mentioned throughout the tender, it is not clear to us where ECDSA is required. Can you please elaborate in more detail the use cases where ECDSA is to be used (at CA level, end user certificates, device certificates)?	see CR#20	NO	**AMD#2**
CR#307	Book II Part IV	Annex A	Will the existing personalized PIV cards be supported with their current middleware and CMS products? How are they to be supported on the E-NPKI? Only on a usage point of view, or it must be possible to personalize those smartcards with the new CMS?	The existing personalized PIV cards are integrated with a logical access control CMS integrated with the i-NPKI and also a physical access control (PACS) CMS (See slide from bidders conference). The SRS requires E-NPKI integration with the existing PACS CMS. Personalization of the PBN smartcard is responsibility of the existing PACS CMS.	NO	**AMD#2**
CR#308	Book II Part IV	Annex A	When can bidders expect to see the Certificate Policy (CertP) for E-NKI to be published?	See CR#115	NO	**AMD#2**
CR#309	Book II Part IV	Annex A Page 17 - 2.2.3 SSL Interception proxy certificates	Will these certificates need to be present on both the PBN and ON?	SSL Interception certificates are only for the PBN.	YES	**AMD#2**
CR#310	Book I	Section 3.6.1.1	Please clarify if Section 8 of SOW to be addressed in Volume 1, should cover only the Project Management perspective; while Volume 2 should still include the technical approach in Section 8 of SOW	SOW section 8 focuses on the implementation at optional sites. The Purchaser does not expect any technical specifies for the implementation at those sites in comparison to the sites being part of the basic contract. Therefore, as part of Volume 1, the Bid shall explain the Bidder's approach to implementing optional sites (see Book I 3.6.4.9.3.1)	**NO**	**AMD#2**

CR#311	Book I	Section 3.6.4	Please clarify if Volume 1 should be one document covering all the requirements, or multiple documents; if case of multiple documents, please clarify what should be these documents, and the structure for each of them	Volume 1 is expected to include multiple documents. Book I section 3.6.4 provides details on the Purchaser's expectations. Accordingly, the Purchaser recommends volume 1 includes the following individual documents: Executive summary, Table of Content, initial PMP, initial WBS, initial Risk Log, initial PMS, BRCM. Other information such as Bidder's qualification and Key personnel can be part of the "main body" of Volume 1.	**NO**	**AMD#2**
CR#312	Book I	Section 3.6.5.2.1.3	Please confirm that initial PBS submitted in Volume 2, as part of SDS, should refer to technical products, only	The PBS to be delivered under contract execution shall cover all types of products (management products and specialist products) - see SOW 3.4.1.3. However, for bidding purposes, the Purchaser confirm that the PBS can focus on specialist products. Book I 3.6.5.2.1.3 was updated accordingly.	**YES**	**AMD#2**
CR#313	Book I	Sections 3.6.4.6.3.1 & 3.6.4.6.3.3	The initial PMP structure mentioned in section 13 refer to fewer areas than those required for, in other sections of the RFP documentations. Just to give some examples, Issue Management, Configuration Management, Quality and Project Controls are not included in section 13; still, we have point 3.6.4.6.3.3 asking for project controls in initial PMP. Please clarify what areas should be addressed in initial PMP.	SOW Section 13 was updated to reflect the need to address "Project Controls" and "Issue Management" in the PMP. Therefore, those two areas shall be covered by the initial PMP. Configuration Management and Quality Assurance shall be covered by the initial CMP and initial QAP respectively. See Book I sections 3.6.6.5 and 3.6.6.4.	**YES**	**AMD#2**
CR#314	Book II Part IV	Section 4.9	The section states "as part of this work package, the Contractor shall conduct site surveys at all the sites related to the PSA milestone", however in Annex A Bidding Sheets, two sites (NATO Communications and Information Systems Group HQ, ACT Staff Element Europe) are related to PSA milestone while the site survey is under CLIN3 (instead of expected CLIN2). Could you please clarify?	Corrected at IFB AMD#2. See CR#130.	**YES**	**AMD#2**
CR#315	General		Could you give bidders an indication of the size of the enrolment staff?	Maximum Enrolment staff at a large site is less than 4 persons who have additional assigned duties to perform. Small sites will only have 2 persons who are assigned enrolment duties as "additional assigned duties"	NO	**AMD#2**
CR#316	Book II Part IV		Could you clarify where the NEDS is located?	The NEDS is currently installed on the NS domain, with 2 NEDS nodes: one node is located in SHAPE, the other is located in Lago Patria. The proliferation of NEDS is planned to be executed prior to E-NPKI implementation. As a result, eventually NEDS nodes will be located in SHAPE, Lago Patria, and New NATO HQ on both ON and PBN. The NEDS nodes serve the NATO Enterprise.	**NO**	**AMD#2**
CR#317	Book II Part IV	SoW 12.1.3 & 12.1.4 SRS-2659	Our understanding of requirement SRS 2659 is that CTS security clearance is required for onsite users with System Admin privileges and that other users may have a NATO SECRET clearance. Please confirm or clarify our understanding.	SRS-2659, SOW 12.1.3 and 12.1.4 have been aligned in AMD#2 Onsite E-NPKI contractor personnel shall hold at least a COSMIC TOP SECRET Security Clearance if they require Administrative access to systems, or access to CA or OCSP systems	**YES**	**AMD#2**
CR#318	Book I	Annex A	"Training materials" and "onsite training" are allocated to CLIN3 (for non-optional sites). However, those two items cannot be found in the CLIN3 tab; instead only "onsite training" is found under CLIN2 (item 2.7.16). Could you clarify?	See CR#273.	**YES**	**AMD#2**

CR#319	Book I	2.1.1.5	Albania, Croatia and France are NATO members but not part of the Participating Country list. Is there any restrictions to using nationals (key personnel and/or installation resources) of these 3 countries?	No restrictions on individuals (i.e. bona fide employees of a firm otherwise eligible) apply, but all security as well as the requirements noted at Book I, Para 2.2. are fully applicable.	NO	**AMD#2**
CR#320	Book I	2.1.1.5 And Annex B	Is the list of "participating NATO member countries" (Book I Instructions to Bidders - Annex B-12) referring to the list of "Participating countries" (Book I Instructions to Bidders - 2.1.1.5)?	Yes.	NO	**AMD#2**
CR#321	Book II Part IV	6.5.3.3	Can NATO please specify which format should be used to deliver MDS to each site?	The format will be provided in due time after contract award. The MDS is normally an Excel spreadsheet. SOW section 6.5.3.1 provides details on information contained in the MDS.	NO	**AMD#2**
CR#322	Book II Part IV	Annex B 2.1.7	"The SLA proposed by the Contractor shall be aligned with the SLA between NCI Agency and the end users". Can NATO please include the SLA between NCI Agency and the end users as a reference document to this IFB?	The SLA between NCIA and its final customer is not yet available as it will partially depend on the SLA between NCIA and the E-NPKI Contractor.	NO	**AMD#2**
CR#323	Book II Part IV	6.3.4.1	"The manuals, exclusive of covers, shall be produced on the best grade white bond or lithographic paper. All paper used for drawings and calibration curves etc. shall be of a quality and thickness that will permit repeated folding and opening without tearing and cracking at the folds." The last part of this requirement - All paper used for drawings and calibration curves etc. shall be of a quality and thickness that will permit repeated folding and opening without tearing and cracking at the folds. - is not exact and can lead to a difference in interpretation. Can NATO please state the exact quality of the paper required for printing drawings and calibration curves etc., on?	The Purchaser believes the requirement as stated in the IFB to be sufficiently clear for bidding purposes. Clarification can be provided if necessary after contract award.	NO	**AMD#2**
CR#324	Book I	1.3.1	Can NATO please confirm the exact milestone for the Transfer of Ownership from the Contractor to NATO?	See Book II, Part III, Contract General Provisions, Clause 24, Ownership and Title.	NO	**AMD#2**
CR#325	Book II Part IV	6.3.4.11	Can NATO confirm that the requirement to update Manuals would solely be as a result of a change to the Contractor provided solution?	Yes	NO	**AMD#2**
CR#326	Book II Part IV	9.2.4.12	Can NATO please confirm that the product baseline in this context relates only to the Contractor supplied components?	The product baseline is described in SOW 15.3.3. The requirement is to perform regression testing of the product baseline , which is including all hardware and software configuration items (CIs) and interfaced external system (NEDS,CMS...). This shall ensure that the changes made by the E-NPKI Contractor do not affect the operational CIS.	NO	**AMD#3**
CR#327	Book II Part IV	7.2.2	Can NATO please clearly define the activities to be run by the Contractor and the activities run by the Purchaser (or its 3rd parties) during and post audits and vulnerability assessment tasks? During vulnerability assessment, who shall be responsible for definition and coordination of remediate plans?	Remediation activities after a Vulnerability Assessment (or disaster recovery exercise) (performed on the reference environment) shall be addressed by the Contractor. Remediation activities after an Audit (performed on the operational system) shall be addressed cooperatively by the Contractor and the Purchaser. The delineation between roles is based on the Purchaser holding the CA and RA operational trusted roles. During vulnerability assessment, the contractor shall be responsible for definition and coordination of remediation plans.	NO	**AMD#3**
CR#328	Book II Part IV	6.3.2.7	Can NATO please quantify the number of changes and developments to be delivered to the Training packages for the two years following the FSA?	Changes to the Training Package will only be expected if the Contractor changes the baseline HW/SW	NO	**AMD#2**

CR#329	Book II Part IV	6.3.2.7	Can NATO please specify which changes and developments need to be delivered to the Training packages for the two years following the FSA?	Changes to the Training Package will only be expected if the Contractor changes the baseline HW/SW	NO	**AMD#2**
CR#330	Book II Part IV	6.3.3.12	Can NATO please specify who will custody the disaster recovery kits? In case NATO will custody these kits, can NATO please specify how these kits will be made to the contractor?	Disaster recovery kits will be held by Purchaser staff on each Site. The Disaster Recovery Plan and procedures shall detail procedures related to the kit management.	**NO**	**AMD#3**
CR#331	Book II Part IV	6.3.3.12	Can NATO please clarify if the Contractor is required to provide a soft copy of all developed manuals to every site or only centrally to the core team? Can NATO please specify the medium on which these copies need to be provided as well as the number of copies required.	One soft copy and a minimum of one paper copy of each custom manual shall be delivered at each delivery site. The Core Team shall also be provided with one soft copy. The soft copy shall be delivered on a USB stick or CD. The Contractor shall also deliver as many copies as needed to meet the training requirements. See also CR#337	NO	**AMD#3**
CR#332	Book II Part IV	6.3.3.20	"If changes to previously delivered documents have been made, the contractor shall deliver change pages, replacement drawings/schematic diagrams etc. as appropriate." Regarding this requirement; can NATO please clarify if the Contractor is responsible to cater for this requirement during the installation phase only (till FSA) or is the contractor required to cater for this requirement throughout the optional ILS years as well? In case the contractor is required to cater for this requirement trough the optional ILS years, can NATO please clearly specify the number of changes the contractor is required to cater for on a yearly basis?	The latter. The contractor is required to cater for this requirement throughout the contract execution, including during optional O&M years as well.	NO	**AMD#2**
CR#333	Book II Part IV	6.3.3.20	Can NATO please define what's the leadtime is to update the existing documentation after a change is accepted?	There no pre-defined leadtime as it depends on the document, the changes, and overall E-NPKI service delivery context. Rather, it will be discussed and agreed as and when needed between the Purchaser and the Contractor.	NO	**AMD#3**
CR#334	Book II Part IV	6.3.4.10.2	How long will it take the Purchaser to review a draft copy of the documents submitted and submit the Contractor with recommended changes, corrections and/or additions?	See in particular SOW 3.9.4	**NO**	**AMD#2**
CR#335	Book II Part IV	6.4.11	Can the Purchaser please confirm NATO can handle the storage of the equipments required to provide On-Site Training before the training is scheduled, till such time the training is provided by the contractor?	Confirmed: NATO will be responsible for the storage and custody	NO	**AMD#2**
CR#336	Book II Part IV	6.4.11	Can NATO please confirm the rooms being used for On-Site Training will remain booked and available for the Contractor between training sessions (if not happening in consecutive days) with Contractor's equipment inside? Can NATO please confirm these rooms are locked between sessions?	Confirmed: NATO will be responsible to ensure space availability and the custody of the training equipment	NO	**AMD#2**
CR#337	Book II Part IV	6.4.13.8.1	Can NATO please specify if the Contractor is required to provide a copy of the Student Manual, and other relevant training materials to each student? In such case should this be provided as a soft copy or paper copy, or both? In case there's a requirement for providing the materials as a soft copy, can NATO please specify the medium on which the soft copy needs to be provided?	Training manuals should be provided in both Hard and Soft Copies for each student. The Soft copy shall be provided on a USB stick device or CD. See also CR#331.	NO	**AMD#3**

CR#338	Book II Part IV	6.4.10	Can NATO please confirm the Contractor will be allowed to provide all On-Site Training sessions on one particular site in consecutive days?	Confirmed	NO	**AMD#2**
CR#339	Book II Part IV	6.5.4.1	Can NATO please confirm the Purchaser accepts the responsibility for storage and custody of deliverables shipped to sites until their installation or use?	Confirmed: NATO will be responsible for the storage and custody	NO	**AMD#2**
CR#340	Book II Part IV	6.5.8.1	Can NATO please confirm, the Purchaser accepts to receive deliverables shipped to sites, acknowledge the number of individual boxes and communicate these information's to Contractors PM Office?	Confirmed: NATO will be responsible for the storage and custody	NO	**AMD#2**
CR#341	Book II Part IV	6.6.5	Can NATO please confirm, the Purchaser accepts the responsibility for the storage and custody of spare parts and consumables shipped to sites and central locations until their installation or use?	Confirmed: NATO will be responsible for the storage and custody	NO	**AMD#3**
CR#342	Book II Part IV	6.6.5.1 6.6.5.3	Can NATO please explain in which scenarios the spare parts and consumables (20% for smartcards and 10% for certificates) delivered to the central location will be used? Can NATO please clarify if the Contractor is responsible to replenish the used spare parts and consumable coming from this stock of 20% for smartcards and 10% for certificates? In case the contractor is required to replenish, can NATO please confirm the costs for replacing the used items will be covered under ECP principle?	Spare parts will be used for any repairs which may occur, and consumables will be used as required. See SOW 7.1.2 and 7.4.8, the Contractor shall be responsible to replace spare parts and consumables (before and after warranty), under WP5 (Fix Firm Price).	NO	**AMD#3**
CR#343	Book II Part IV	6.6.5.1 6.6.5.3	Can NATO please confirm, the Purchaser will manage and fund the shipping of the spare parts and consumables delivered by the Contractor to the Purchaser to its central locations (20% for smartcards and 10% for certificates) to the remote sites, in case these elements are needed there?	NATO will be responsible for any shipments of spares and consumables after the initial deliveries by the Contractor. The bidder shall note that the critical spare parts are to be delivered to the relevant sites (see SOW 6.6.3). The bidder shall also note SOW 7.4.8.	NO	**AMD#3**
CR#344	Book II Part IV	6.7.3	Can NATO please confirm, the Purchaser will provide standard Tools and Test Equipment as part of the RTTL? Can NATO please specify which Tools and Test Equipment will be provided as part of the RTTL?	As mentioned in SOW 6.7.2, the RTTL covers only the "Standard" Tools and Test Equipment which are likely to be available at NATO sites. Standard Tools and Test Equipment being available at NATO sites will be provided by NATO. Standard Tools and Test Equipment not being available at NATO sites may be purchased from the RTTL. The Purchaser is not in position to provide the Standard Tools and Test Equipment available at NATO sites that will be available at E-NPKI implementation. The Contractor shall deliver "Special to Type" tools and/or test equipment (see SOW 6.7.3 and CLINs 2.7.10 & 3.3.2.3).	NO	**AMD#3**
CR#345	Book II Part IV	7.3.8.2	Can NATO please specify if the Contractor is required to provide the installation and configuration of NCIRC-agents as part of the FFP budget for investment?	Yes, the installation, configuration and coordination with NCIRC is part of the FFP. For clarification purposes, SOW 1.6.4 was updated accordingly at AMD3. See also SOW 7.3.8.2.	YES	**AMD#3**
CR#346	Book II Part IV	7.4.10.3.2	"Level 3 maintenance is expected to be minimal and will be performed on an ad-hoc basis." Can NATO please describe the framework that should be used for level 3 maintenance? Can NATO please specify the term 'minimal' both qualitatively and quantitavely?	The Contractor will be responsible to execute level 3 maintenance tasks as required. They shall be costed accordingly in their Firm Fixed Price bid.	NO	**AMD#3**

CR#347	Book II Part IV	7.4.10.3.2	From the way this requirement is written - should the Contractor understand that Level 3 maintenance can be billed in a case-by-case basis once the content is properly defined?	See CR#346	NO	**AMD#3**
CR#348	Book II Part IV	7.5.2.3	Can NATO please define how many specialized training sessions the Contractor is required to organize to cover all CA staff?	No - this is the reason for the TNA requirement and the provision of a Training Plan and Training program. See SOW 6.4. SOW 6.4.10 updated at AMD3.	YES	**AMD#3**
CR#349	Book II Part IV	7.5.2.4	Can NATO please specify if the annual test of the disaster recovery plan is happening every year in the same period, and in which period of the year this needs to happen?	The period will be defined during contract execution.	NO	**AMD#3**
CR#350	Book II Part IV	7.5.3.2	Can NATO please clearly specify the Contractor's responsibilities during Exercises? Can NATO please specify the expected level of support by the Contractor; in skillset, allocation of people and duration? Are there any specific tasks to be provided by the Contractor?	Application Integration and troubleshooting clarified in Amd#2 section7.5.3.2	YES	**AMD#2**
CR#351	Book II Part IV	7.5	The non-production environment is delivered to provide support on training, exercises and support testing. A number of scheduled activities will happen every year in this environment as Disaster Recovery testing (at least once per year), Exercise testing (estimated 4 per year) or Business Continuity testing (at least once per year). Can NATO please clearly specify the annual agenda for these activities on the Non-production environment ?	This will be defined during contract execution in coordination with the Contractor.	NO	**AMD#2**
CR#352	Book II Part IV	Annex B 2.5.2.4.2.1	Can NATO please define the NATO normal working hours for all countries sin scope?	This may vary amongst the different countries and individual locations between 38 - 40 hrs. per week. A comprehensive list for each country and location is not available. Bidders are reminded that all prices are FFP and are not subject to change and are advised to take prudent assumptions in their bids to account for any variations.	**NO**	**AMD#2**
CR#353	Book II Part IV	Annex B 2.5.4.4	Can NATO please clarify is next to the validation that all KPI are met, are there any other acceptance criteria before pronouncing FSA successful? Can NATO please lists all other criteria that need to be met, if any, before announcing successful FSA?	See SOW section 16.	**NO**	**AMD#2**
CR#354	Book II Part IV	Annex B 3.2	Can NATO please specify the volumetric in terms of change requests, to be taken into account as a baseline for inclusion in the FFP for this IFB?	Change management covers : 1- Contractor requested changes. 2- Changes required to meet the performance, security, or availability of the E-NPKI system. 3- Software updates. 4- NATO requested changes. Category 1,2,3 shall be handled at no cost for NATO as part of the FFP. Category 4 not falling under other categories will be subject to ECP.	**NO**	**AMD#3**
CR#355	Book II Part IV	Annex B 3.2.4.3.1 3.2.4.3.2	Can NATO please specify if there are regular change windows which can be used for delivery of new releases? Can NATO please specify these windows?	There is currently no change windows defined at NATO Enterprise level. Change windows will be defined and agreed as part of the release management process defined in SOW 3.2.4.2		**AMD#3**

CR#356	Book II Part IV	Annex B 3.3.13	"The Contractor shall include measures to protect the confidentiality and integrity of the information transferred between the Help Desk and NATO, and shall identify and authenticate the users in accordance with NATO Security Policy". a) Can NATO please provide this policy? b) Can NATO please specify which measures are to be take specifically related to Phone conversations between NATO and the Contractor Help Desk? c) Can NATO please specify which measures are to be take specifically related to e-mail exchanges between NATO and the Contractor Help Desk? d) Can NATO please specify which measures are to be take specifically related to the usage of any on-line tools?	The NATO Security policy is part of the CD under 2.1.6.1 , see CR#115 The required measures depend on the level of information being exchanged, and will need to meet the NATO Security policy minimum requirements. Details will be discussed during pre-award discussions.	NO	**AMD#3**
CR#357	Book II Part IV	Annex B 4	Can NATO please provide volumetrics around the number of agents that are expected to manage the solution? How many agents need to be able to administer the project at the same time? Is this number flat or variable (day/night shifts)?	See CR#22. The number of agents required is dependent on the contractor design. Remedy Incident Management licensing is based on the number of concurrent licenses. Number of licenses is the sum of contractor staff on site to support E-NPKI plus 3 additional licenses for Purchaser E-NPKI staff.	NO	**AMD#2**
CR#358	Book II Part IV	Annex B 5	Can NATO please specify what type of BMC license are required to be provided - Named user or Concurrent?	See CR#357	NO	**AMD#3**
CR#359	Book II Part IV	7.4.10.3.2	Can NATO please clarify if the Contractor shall be responsible for sanitisation of broken hardware modules (removal of memory, disks, ...) or will the Purchaser manage this?	The Purchaser will handle the task of sanitation or destruction of broken hardware (memory) modules. SOW 7.4.10.3.2 and 7.4.10.3.3 were updated accordingly.	YES	**AMD#3**
CR#360	Annex A	Detailed CLIN Summary	The structure of the bidding sheets doesn't allow to put in Investment pricing for the sub-CLINs called "Site-Specific System Implementation deliverables - User Services". Can NATO please confirm that this sub-CLIN does not need to be priced as a separate element?	Confirmed.	NO	**AMD#2**
CR#361	Annex A	Detailed CLIN Summary	Can NATO please confirm that CLIN 19 does not need to be priced out in detail given the fact that all cells are grey out in tab "Detailed CLIN Summary"	On the "Detailed CLIN Summary" CLIN 19 does not need to be priced. However, in the CLIN 19 Pricing Sheet and Breakdown Sheets are required and indicated in yellow.	NO	**AMD#2**
CR#362	Annex A	Delivery per site	Can NATO please explain the correlation between on one hand the Site-specific deliverables in the top row of the table and the different CLINs mentioned on a per site basis? As an example the same Site-specific deliverable "Site Survey Report" has a link to CLIN 2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18.	The Delivery Per Site tab is intended for the Bidder as a guide as related to the SOW in order to reference what is included through the SOW to each CLIN or sub-CLIN line of the CLIN Pricing Sheets. For example, a "Site Survey Report" shall be delivered under all the CLINs mentioned in the "Delivery per Site" table (i.e. CLINs 2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18.)	NO	**AMD#3**
CR#363	Annex A	Delivery per site	Can NATO please explain the usage and correct interpretation of the delivery per site tab in the Bidding Sheets?	See CR#362.	NO	**AMD#3**
CR#364	Annex A	NA	Can NATO please explain the reason for the difference in level of details required in the Bidding Sheets for the mandatory sites compared to the Groups of optional sites? For the mandatory ones all the information need to go into 1 tab while for the optional groups there are 4 tabs per group to complete. Can you please confirm this is the correct level of documentation required?	This is the correct level of documentation required. This is due to the allocation of costs to the Investment Ceiling and O&M Ceilings for the Options.	NO	**AMD#3**

CR#365	Annex A	Delivery per site	Can NATO please explain why for some sites (as an example NATO Force Structure) there is the mentioning of the word "Exceptional" in column M Technical Services?	The wording "Exceptional" reflects the fact that the implementation of Technical Services at some sites has been "exceptionally" authorised by the NATO Nations. For bidding purposes, bidders shall consider the wording "YES (Exceptional)" as equivalent to "YES"	**NO**	**AMD#2**
CR#366	Book II Part IV	1.3.1	Can NATO confirm operate in this context, i.e. Is the E-NKPI going to be NONO (NATO owned, NATO operated or NOCO NATO owned, Contractor operated)?	NONO, with contractor staff augmentation to support the Purchaser. (see SOW 7.1.5, 7.1.9 and 7.1.10 in particular).	NO	**AMD#2**
CR#367	Book II Part IV	6.6.5.3	Can NATO please confirm the requirement? Certificates have DN that identify the certificate subject. Therefore, whilst the e-NPKI have the capacity to issue an additional 10% of certificates, it isn't possible to deliver additional certificates to a central location.	See CR#56	NO	**AMD#2**
CR#368	Book II Part IV	10.4.1.13	At the Bidders Conference on 17 June, we were advised that the Contractor is expected to leverage the existing ITSM tools and not duplicate these, but that this might require additional licences. Is the sourcing of these licences a Contractor responsibility?	Yes, the sourcing of the additional licenses is the responsibility of the Contractor. Bidders shall include the cost of those additional licenses in their bid. See also CR#22.	NO	**AMD#2**
CR#369	Book I	Multiple	Several existing PKI infrastructures are mentioned in the IFB documents (see IFB reference). Can you please confirm they're all referring to the same unique existing PKI solution currently used by NATO? In case they're disparate platforms, can you please provide further detail to each individual platform as well as to the way they work together?	see CR#50	NO	**AMD#2**
CR#370	Book II Part IV	Annex B 3.3.9.1	"The Help Desk shall be responsible to receive and record all calls from NCI Agency." Does this requirement refer to voice record calls or tracking calls, or both?	Voice recording is not required. SOW Annex B 3.3.9.1 updated accordingly at AMD#3	YES	**AMD#3**
CR#371	Book II Part IV	Annex B 4	Could the requirement for 24X7 support be provided by a round the clock shift presence using NATO existing tooling and not have any specifically provided tooling?	The offsite components of the Contractor's Help Desk shall be available to the Purchaser on a 24/7 basis for first line support accessible via telephone and email/web (see SOW Annex B section 3.3.5). Purchaser has 24/7 shift presence already. For support activities which require contractor support, the offsite helpdesk shall also be available 24/7 to ensure availability targets for the system are met.	NO	**AMD#3**
CR#372	Book II Part IV	Annex B 4	Can NATO please confirm the correct interpretation of this requirement is to configure the existing NATO ITM toolset to support PKI as opposed to implement a separate new toolset just for PKI?	Yes, the requirement is for the bidder to provide concurrent access and agent licenses as required and to configure the existing NATO ITSM toolset to support PKI.	NO	**AMD#2**
CR#373	Book II Part IV	Annex B 4	Can NATO please specify what the exact toolset and capability in place will be for the Contractor to use or the PKI project?	See CR#22	NO	**AMD#2**
CR#374	Book II Part IV	Annex B 4	Can NATO please confirm the version of the BMC stack and modules they are running?.	See CR#22. Further information will only be available after contract award.	NO	**AMD#3**

CR#375	Book II Part IV	Annex B Section 4	Can NATO please clarify if any further additional integration is planned between ITSM tools and other Nato tools/systems, and how this would impact the Contractor? Can NATO please confirm if the contractor will be allowed to recover any required support at that time as an ECP to the contract?	The integration with current ITSM tools shall be included in the E-NPKI cost (Firm Fixed Price). Further additional integration between future ITSM tools and other NATO tools/systems will be assessed on a case by case basis with regard to their potential impact on E-NPKI.	NO	**AMD#3**
CR#376	Book II Part IV	SRS-602	Can NATO please specify the type of logs, the quantity and EPS required to be delivered under the FFP of the IFB?	The first 5 items relate to information under direct control of the CA system and trusted role operators: · physical access logs **to the CA / OCSP / Timestamp systems;** · system configuration changes and maintenance; **to the E-NPKI system hardware, operating system, and all installed software on the E-NPKI** · personnel changes **for E-NPKI personnel including RA Operators; (This item can be met through the Trusted role subscriber agreements in electronic format.)** · discrepancy and compromise reports; **for all E-NPKI components including tokens.** · Records of the destruction of media containing key material, activation data, or personal subscriber information. The remaining log items shall be delivered directly by those systems. and not by the E-NPKI CA (and will be deleted from the SRS-602 (· Security relevant logs from the Directory · DN changes made by entities other than the E-NPKI CA or RA Officers · Firewall and IDS Logs)	YES	**AMD#2**
CR#377	Book II Part IV	SRS-2644	The E-NPKI Contractor shall implement physical access control mechanisms, while SOW 2.1.6.3 (AC/35 – D/2001 –REV2) describes access control mechanisms which should be implemented depending on the necessity. Can NATO please define exactly which mechanisms are to be foreseen by the contractor, as part of the deliverables under the FFP of the IFB, on top of the existing access control mechanisms which are already in place and thus out of scope for this IFB? Or can NATO confirm the existing access control mechanism (outside the scope of this IFB) are sufficient and the contractor is therefore not required to include any additional ones in his response?	Similar to the CR#82, the availability of appropriate physical access control mechanisms shall be verified during site surveys. If physical access control mechanisms are not adequate, an ECP may be raised.	NO	**AMD#3**
CR#378	Book II Part IV	9.2.4.12	Can NATO please confirm the Bidders interpretation of this requirements as follows: The test to be conducted by the Contractor shall be limited to the software installed by the contractor.	SOW 9.2.4.12 refers to the execution of regression tests on the updated product baseline. As such, the scope of those tests is the product baseline.	NO	**AMD#2**
CR#379	Book II Part IV	9.2.4	Can NATO please confirm that any directed change in software outside the control of the contractor and impacting the delivered solution will lead to an ECP that will be raised to make the deployed solution again appropriate configured to cater for the changed software.	The Purchaser does not understand the wording "any directed change in software outside the control of the contractor". The Bidder is invited to explain and, if possible, to associate the question to more specific requirement(s).	**NO**	**AMD#2**
CR#380	Book II Part IV	5.5.6.2	Can NATO please confirm that the contractor is not responsible for making new applications elliptic curve ready?	Any software application not provided by the vendor as part of this contract, and not elliptic curve ready, is not the responsibility of the bidder to make elliptic curve ready.	NO	**AMD#2**

CR#381	Book II Part IV	5.5.2.4	"The Contractor shall solve all integration and interface problems that may occur during the E-NPKI installation. In particular, the contractor shall provide and install all miscellaneous equipment (for example shelves, mounting brackets, power filters, signal filters, cables, installation kits) to enable the connection of E-NPKI elements to the existing infrastructure at a site." Given the fact that this IFB will result in a Firm Fixed Price contract and the timing (post contract signature) of the Site Surveys during which the inventory of these 'miscellaneous equipment' can be made, it's impossible for the contractor to quantify the amount of necessary equipment and man-hours to cater for this requirement and include it in the FFP for this IFB. We kindly request NATO to redraw this requirement from the IFB or rephrase it in such a way that the deliverables of this requirement is covered under the ECP process.	The Purchaser is not able to modify this requirement. Although the cost of miscellaneous equipment is expected to be negligible compared to the overall contract value, Bidders are advised to be prudent to include a factor in their FFP's to account for variations experienced during installations.	NO	**AMD#2**
CR#382	Book II Part IV	9.2.3.10	"The duration of the OAT will normally not take more than one week, exclusive of any preparation time. However, the Contractor shall note that OAT will be repeated as many times as needed, to the Purchaser's satisfaction. Between two OAT sessions, the Contractor shall make the necessary modifications as required by the Purchaser, at no additional cost to the Purchaser." This is an open ended requirement that can't be covered under a Firm Fixed Price, especially because the requirement does not specify clearly the reasons why NATO would require a repetition of the OAT Testing. It's contractors interpretation that NATO will only require a repetition in case a clear non compliancy or non-achievement of pre-defined testing acceptance criteria is detected during the testing. Please confirm this is the correct interpretation.	yes, NATO will only require a repetition in case a clear non compliancy or non-achievement of pre-defined testing acceptance criteria.	NO	**AMD#2**
CR#383	Book II Part IV	9.2.5.4	"The Contractor shall ensure that each Site Activation Test results in a "PASS". If any test on any of the E-NPKI components at any site does not result in a "PASS", the Contractor shall correct the cause of the test failure and shall repeat the test until obtaining a "PASS" result, at no cost to the Purchaser." It's the contractors interpretation that the repetition of the test to obtain a PASS is only required on the site where the test failed and not on all sites. Please confirm this is the correct interpretation.	yes	NO	**AMD#2**

CR#384	Book II Part IV	11.4.5	"Two Software Security and Technical Tests sessions are foreseen, each of duration of 5 (five) working days. However, the test sessions shall be repeated until the software successfully completes the tests for listing on the AFPL for the networks on which the E-NPKI components are to be deployed. The Contractor shall support the Software Security and Technical Tests sessions by preparing and delivering the appropriate documentation as required by the Purchaser. Software Security and Technical tests will normally be performed after BLAT testing, although the two test sessions may overlap." The timing of these test (and whether or not they are done simultaneously with other planned tests) is crucial when it comes to planning and staffing correctly according to the needs of the project. Can NATO please confirm: a) the Two Software Security and Technical Tests sessions will be conducted after the BLAT tests? b) any change in the planning requiring additional resources will be covered via an ECP? c) Any further repetition beyond the initially scheduled two sessions requiring support from the contractor will be covered via ECP.	A) The planning of the BLAT and Software Security and Technical Tests sessions will be done in coordination between the Purchaser and the Contractor during contract execution, with the objective to optimize schedule and resources on both sides. B) as mentioned under A) above, the planning will be set up such as to optimize schedule and resources on both sides. However, neither the Purchaser nor the Bidder can guarantee at this stage that the planning won't need adjustments once established, especially as a result of the test session(s), potentially due to issues/defects identified on the item under test. Those adjustments may diminish or increase the number or duration of the test sessions. The Purchaser expects that the risk associated to these adjustments be included in the (firm-fixed-price) contract. C) See B).	NO	**AMD#2**
CR#385	Book II Part IV	11.4.6	"Two NCI Agency IV&V Service Line test sessions are foreseen, for total of 30 working days. However, the test sessions shall be repeated until the software successfully completes the tests for listing on the AFPL for the networks on which the E-NPKI components are to be deployed. The Contractor shall support the NCI Agency IV&V Service Line test sessions by preparing and delivering the appropriate documentation as required by the Purchaser. IV&V testing will normally be performed after BLAT testing, although the two test sessions may overlap." The timing of these test (and whether or not they are done simultaneously with other planned tests) is crucial when it comes to planning and staffing correctly according to the needs of the project. Can NATO please confirm: a) the Two NCI Agency IV&V Service Line test sessions will be conducted after the BLAT tests? b) any change in the planning requiring additional resources will be covered via an ECP? c) Any further repetition beyond the initially scheduled two sessions requiring support from the contractor will be covered via ECP.	A) The planning of the BLAT and IV&V SL test session will be done in coordination between the Purchaser and the Contractor during contract execution, with the objective to optimize schedule and resources on both sides. B) as mentioned under A) above, the planning will be set up such as to optimize schedule and resources on both sides. However, neither the Purchaser nor the Bidder can guarantee at this stage that the planning won't need adjustments once established, especially as a result of the test session(s), potentially due to issues/defects identified on the item under test. Those adjustments may diminish or increase the number or duration of the test sessions. The Purchaser expects that the risk associated to these adjustments be included in the (firm-fixed-price) contract. C) See B).	NO	**AMD#2**
CR#386	Book II Part IV	9.2.4.12	"The Contractor shall execute any regression tests on the updated product baseline as required by the Purchaser." It's the Contractors interpretation that regression testing will only be required on specific developed software and not on COTS elements in the solution. Can NATO please confirm this is the correct interpretation?	See CR#378	NO	**AMD#2**

CR#387	Book II Part IV	3.2.4.3.2.2	"The Contractor shall plan and perform regression testing – on the E-NPKI Reference System – before deploying maintenance releases in the operational environment." It's the Contractors interpretation that regression testing will only be required on specific developed software and not on COTS elements in the solution. a) Can NATO please confirm this is the correct interpretation? b) In case regression testing is required/asked for by NATO during maintenance operations and/or restoration of service the time needed to complete the testing should be excluded from the SLA calculations. Can NATO please confirm this will be the case.	a) See CR#378 b) SOW Annex B section 3.2.4.3.2.2 addresses the need for regression testing in the context of "Maintenance releases". When an emergency maintenance release is required to fix issues affecting the SLA, the time needed to execute the regression tests will be included in the SLA calculations.	NO	**AMD#3**
CR#388	Book II Part IV	SOW 15.7.1	"The various baselines referred to above shall be established by the Contractor using automated tools where appropriate." Can NATO please be specific about the necessity of automation tools - please define what "appropriate" means in this context? What are the exact requirements for the delivery of these tools?	The Bidder is expected to use a software tool for the maintenance of the CM database. Due to the requirements specified in Section 15 of the SOW, it is clear that this tool should be designed to manage a CM database and a simple spreadsheet would not suffice. It is in this context that appropriate is used.	NO	**AMD#3**
CR#389	Book II Part IV	SOW 15.7.5	"All baselined documents created under this contract shall be maintained by the Contractor in the CSA database using the software tools to allow efficient update, automated tracking of changes through all affected CIs and baseline documents, and continued automated maintenance and printing of these documents, including tables, figures, and readings." It's unclear to the contractor if the software tools and CSA Database are deliverables of the contract or CFI to the contractor. Can NATO please clarify. It's equally unclear what "continued automated maintenance" means in this context. Can NATO please specify what is meant with this term. Finally it's unclear if the equipment for printing the documentation is a deliverable of the contract or CFI to the contractor. Can NATO please clarify.	The Contractor shall use software tools to maintain the CM database (CMDB) during contract execution (i.e. until FSA and any potential Follow-on support period beyond). The software tools shall be sophisticated enough to track changes for all affected CI's and documents, which is what "continued automated maintenance" means in this context. The software tools are not a deliverable, nor are any printing equipment for the documentation. However, the Bidder shall note that the CSA database(i.e. CMDB) is a deliverable (see CLIN 4.3.1) and shall be compatible (i.e. importable and updatable) with the ITSM tools requirements in SOW Annex B. A simple spreadsheet for the CSA database will not suffice.	NO	**AMD#3**
CR#390	Book II Part IV	SOW 1.6.1.5.5	"Secure remote access by deployed users to email and other Automated Information System (AIS) services." Can NATO please be specific about which systems are covered under "other Automated Information System (AIS) services", by means of an exhaustive list. Are these systems to be provided under this contract?	This CR is linked to 1.6.1.5.2.3 due to a renumbering in a previous AMD. AIS services include but are not limited to emails, web portals and standards office applications. These systems are existing services and shall be supported by E-NPKI.	NO	**AMD#3**

CR#391	Book II Part IV	Annex B Section 1.2.7.1	"ITSM Tools Requirements. In this section all the minimum requirements for the Tools necessary to support the SLA Management are presented." It's the contractor's interpretation that the IFB contains ALL requirements to be delivered by the proposed solution and not only "the minimum requirements " - this implies that NATO might request post contract to deliver/cover other requirements, over and beyond the requirements listed in this IFB. Can NATO please confirm the IFB contains ALL requirements to be delivered by the solution? And in case other requirements would be requested post contract these will be covered under the ECP process?	The Purchaser confirms that the IFB contains all requirements identified at this stage. The wording "In this section all the minimum requirements for the Tools necessary to support the SLA Management are presented" is related to the possibility that the ITSM tools that shall be provided by the Contractor could potentially do more (as it would be case for COTS products). The acceptance of the ITSM tools will be based on the compliance with contractual requirements.	NO	**AMD#2**
CR#392	Book II Part IV	Annex B Section 2.1.2	"NCI Agency will provide services to the final Customers, based on Service Level Agreements (SLAs)." It's the contractors interpretation that this SLA NCI Agency will offer its final customers will have to be supported by the SLA the Contractor is offering the NCI Agency as part of the bid submission. In order for the Contractor to come up with a fitting design and associated SLA, capable of supporting the internal NCI Agency's SLA to its customers the contractor requests to include the internal NCI Agency SLA as part of the supporting documentation of this IFB. Can NATO please accommodate this request?	See CR#322. Further, as mentioned in SOW Annex B section 2.1.6, the Contractor shall propose the E-NPKI SLA with NCI Agency. See also CLINs 2.8.3, 3.5.2, 5.1.7, 5.2.7.	NO	**AMD#2**
CR#393	Book II Part IV	Annex B Section 2.1.5	"The Contractor shall be responsible to provide the E-NPKI services as per an E-NPKI Service Level Agreement (SLA) to be agreed with NCI Agency." It's the contractor's interpretation that an SLA needs to be proposed as part of the bid submission and that the apparent winner will be selected based on the submitted bids without further negotiations with the Contractor. Can NATO please explain when the dialogue on the topic of the SLA will take place? And in case this dialogue is to be done post contract award how any change to the designs (and associated cost impacts thereof) deriving from these discussions will be covered? Can NATO please confirm this will be covered under the ECP process?	As mentioned in Book I section 3.6.6.6.1, the Bidder shall provide a draft SLA with NCI Agency according to SOW Annex B and confirm in his Bid that he shall enter into a SLA agreement to provide the specified services. As any other documents provided in the bid, the draft SLA will be evaluated by the Purchaser according to pre-defined evaluation criteria. The dialogue over the SLA will happen after Contract Award in the context of the delivery of the associated CLINs (see CR#392)	NO	**AMD#2**
CR#394	Book II Part IV	Annex B Section 2.1.7	"The SLA proposed by the Contractor shall be aligned with the SLA between NCI Agency and the end users." In order for the Contractor to come up with a fitting design and associated SLA, aligned to the internal NCI Agency's SLA to its customers the contractor requests to include the internal NCI Agency SLA as part of the supporting documentation of this IFB. Can NATO please accommodate this request?	See CR#322.	NO	**AMD#2**

CR#395	Book II Part IV	Annex B Section 2.1.10	"The SLA between the Contractor and NCI Agency may require other SLAs and/or OLAs (Organisation Level Agreements) to be in force (for example between E-NPKI and NEDS). The Contractor shall propose, and more generally, contribute to the establishment of those SLAs / OLAs." This requirement can quickly become a significant cost driver. In order for the contractor to accommodate for this requirement under the Firm Fixed Price for the Investment part the contractor requires clarification from NATO as to the extent of these other SLA's and/or OLA's. Can NATO please provide an exhaustive list of SLA's and/or OLA's the Contractor is requested to contribute to. Can NATO please specify the level of effort and engagement that is required from the Contractor in relation to this requirement?	The requirement is for the contractor to contribute to the OLA/SLAs for services/system integrated with, interfaced with, or supported by E-NPKI which are listed in the SOW. This may require a substantial effort, and bidders are advised to take a prudent approach by including a factor in their price offer to account for this effort within their Firm Fixed Price.	NO	**AMD#3**
CR#396	Book II Part IV	Annex B Section 2.2.4	"The Contractor shall consider the following list of services to develop the E-NPKI Service Catalogue and SLA (the list is a minimum list of Services; additional Services and/or different groupings which shall be subject to Purchaser approval)." It's the contractor's interpretation that the IFB contains ALL requirements to be delivered by the proposed solution and not only "the minimum list " - this implies that NATO might request post contract to deliver/cover other services, over and beyond the original set listed in this IFB. Can NATO please confirm the IFB contains ALL requirements to be delivered by the solution? And in case other requirements would be requested post contract these will be covered under the ECP process?	The wording "minimum" has been introduced to highlight the fact that the Contractor may propose different groupings of services and/or additional services. In other words, depending on the technical solution, the catalogue of services proposed by the Purchaser may have to be adapted, while ensuring that the "minimum" list of services is addressed. Services that would differ completely from the minimum list and would not be proposed by the Contractor as part of his service offering to the Purchaser would be addressed as an ECP, is required by the Purchaser.	NO	**AMD#2**
CR#397	Book II Part IV	Annex B Section 4.1.7.5	"Produce different types of report, in particular Performance Reports on demand and periodically according to the SLA." Can NATO please specify which reports are requested and define which information will need to be provided in each report?	No. The Purchaser cannot be more specific on the reports at this stage.	NO	**AMD#2**
CR#398	Book II Part IV	10.4.1.3	"Identification of the migration requirements from existing Certificate Authorities (in particular iNPKI) to E-NPKI. In particular, identification of the number of iNPKI users and devices to be migrated to E-NPKI." Given the fact that the Site Survey identifying the exact volumes of users and devices to be migrated is to be executed post contract signature the Contractor assumes that any deviation in volumes between the ones stated in the IFB (and baseline for FFP) and the ones identified during site survey will be covered under the ECP process. Can NATO please confirm.	Confirmed. However, the Bidders shall include in their FFP bid the considerations of footnote 4 in SOW Annex C section 3 related to the number of certificate per user and per device.	NO	**AMD#2**
CR#399	Book II Part IV	2.3.1	NPKI Reference Architecture AC/322-D(2004)0018, is not included in the IF package - can NATO please provide a copy of this document?	See CR#115	NO	**AMD#2**

CR#400	Book II Part IV	2.3.2	NPKI Security Accreditation Plan (SAP), is not included in the IF package - can NATO please provide a copy of this document?	See CR#115	NO	**AMD#2**
CR#401	Book II Part IV	2.3.3	E-NPKI System Description (to accompany SAP), is not included in the IF package - can NATO please provide a copy of this document?	See CR#115	NO	**AMD#2**
CR#402	Book II Part IV	2.3.4	NATO Public Key Infrastructure (PKI) Concept of Operations (AC/322-D/0081), is not included in the IF package - can NATO please provide a copy of this document?	See CR#115	NO	**AMD#2**
CR#403	Book II Part IV	2.3.5	NATO Policy for the Implementation of a Public Key Infrastructure (PKI) for NATO CIS (AC/322-D(2003)0032), is not included in the IF package - can NATO please provide a copy of this document?	Document reference corrected to C-M(2003)32 with the same title. See CR#115	YES	**AMD#2**
CR#404	Book II Part IV	2.3.6	Directive for the Implementation of the NATO Public Key Infrastructure (PKI) AC/322-D(2003)028 (INV)	See CR#115	NO	**AMD#2**
CR#405	Book II Part IV	2.3.7	NATO Public Key Infrastructure (PKI) Certificate Policy AC/322-D(2004)0024-REV2, AC/322-D(2004)0024-REV2-ADD1 and AC/322-D(2004)0024-REV2-ADD2, is not included in the IF package - can NATO please provide a copy of this document?	See CR#115	NO	**AMD#2**
CR#406	Book II Part IV	2.3.8	NATO Directive for NATO Public Key Infrastructure (PKI) Interoperability with Nations AC/322-D(2005)0025-REV1, is not included in the IF package - can NATO please provide a copy of this document?	See CR#115	NO	**AMD#2**
CR#407	Book II Part IV	2.3.9	Statement of Technical Characteristics of the NPKI AC/322-N(2008)0004, is not included in the IF package - can NATO please provide a copy of this document?	See CR#115	NO	**AMD#2**
CR#408	CR#1	CR#1	In relation to NATO response (CR1) to the request for delivering the 86 applicable documents - the contractor cannot accept NATO's initial answer to go look for these documents on public available websites. In this scenario it's impossible to know for sure the contractor is selecting the exact version of the supporting documentation NATO is working with. Also for some of these documents (PKI Architectural documents) these are not available on publicly available websites. The contract requests NATO to either compile a CD with all listed applicable documents and put this at the disposal of the bidders or list for each document an exact link to the applicable document.	A CD is now available on request with all NATO applicable documents referenced in the SOW : E-NPKI - Applicable documents, IFB-CO-13810-CS AMD#2 See CR#115	NO	**AMD#2**

CR#409	Book II Part IV	1.3.1	"1.3.1 This project shall: 1.3.1.1 Implement and operate E-NPKI on the Operational Network (ON) which operates up to NATO Secret level. 1.3.1.3 Implement and operate independent offline Root CAs (supporting SSL interception certificates) which operate up to NATO RESTRICTED". This generic shall requirement specifies that the project shall implement and operate an PKI solution; it does not specify who's responsible for the "operation" part of this requirement. Can NATO please clarify if it's the contractors responsibility to operate the deployed solution. And if so, to what extend and during which timeframe?	Operation and Maintenance requirements are defined in SOW section 7.	NO	**AMD#2**
CR#410	Book II Part IV	Annex A Figure 3	Can NATO please confirm the bidders interpretation that the BPD firewalls are PFE to the Contractor?	See CR#88	NO	**AMD#2**
CR#411	Book II Part IV	SRS-660	Can NATO please confirm the exact locations of the NATO Data Centres?	See Book II Part IV Annex C : List of sites.	NO	**AMD#2**
CR#412	Book II Part IV	SRS-1164	The contractor understands that the compute component should be virtualized as much as possible, but does it means that running an Operating System (like Windows) directly on the hardware is not allowed?	Running dedicated hardware is not forbidden, but it should be avoided unless it has an impact on the security or operation of the E-NPKI system. See CR#136	NO	**AMD#2**
CR#413	Book II Part IV	SRS-1745	Can NATO please confirm the Purchaser will provide the DC infrastructure/environment that will host the virtual machines as a PFE element to the Contractor? And that therefore the contractor only has to define the resources / specifications of the virtual machines? If this is correct, can NATO also please specifies what the SLA will be it that will be provided on this environment?	See CR#136	NO	**AMD#3**
CR#414	Book II Part IV	SRS-486	Can NATO please confirm if the E-NPKI has to be capable to issue Qualified Certificates (QCs)?	See CR#108	NO	**AMD#3**
CR#415	Book II Part IV	SRS-2606	The ARL's will be signed by the Root CA, which is offline. Can NATO please confirm that there will be a manual element to the publication of ARL's?	yes	NO	**AMD#2**
CR#416	Book II Part IV	SRS-2184	Can NATO please provide a list of the sites that do not have a full and fully operational CMS in place? Can NATO please provide an overview list of the deployed CMS elements on a per site basis?	See CR#15 through CR#18.	NO	**AMD#3**
CR#417	Book II Part IV	SOW 9.2.4.12	Can NATO please confirm that the product baseline in this context relates only to the Contractor supplied components?	See CR#326		**AMD#3**
CR#418	Book II Part IV	SRS-486	Will the E-NPKI be required to issue Qualified Certificates (QCs)?	See CR#486	NO	**AMD#2**
CR#419	Book II Part IV	SRS-2606	ARLs will be signed by the Root CA, which is offline. Will NATO confirm that there will be manual element to the publication of ARLs?	See CR#415	NO	**AMD#2**
CR#420	Book II Part IV	SRS-2184	Can NATO confirm which sites do not have CMS components in place?	See CR#15 through CR#18.	NO	**AMD#3**

CR#421	Book II Part IV	SRS-2790	At the Bidders Conference on 17 June, we were advised that the Root CAs were outside the scope of the Contractors E-NPKI solution. Can you please confirm this is not the case for the Root CAs for SSL interception and that these are in scope of the Contractor's solution?	Yes, the Root CAs dedicated for SSL interception are part of the scope of the E-NPKI IFB.	NO	**AMD#2**
CR#422	Book II Part IV	SRS-2659	This requirement isn't consistent with paragraphs 12.1.3 and 12.14 of the SOW that states personnel working on site require NATO SECRET Security Clearance and it is only personnel with System Administrator privileges that require CRS. Can NATO please confirm which is correct?	See CR#317, SRS-2659 is amended in AMD2	NO	**AMD#2**
CR#423	Book II Part IV	SRS-2101	This requirement looks to be at odds with SRS-1086, which states that the 'E-NPKI shall support 500 concurrent active sessions on a single CA Server.' Can NATO please confirm the relationship between these two requirements?	see CR#214	NO	**AMD#2**
CR#424	Book II Part IV	SRS-2734	Can NATO confirm that this requirement doesn't apply to CA software as SRS-1095 states 'E-NPKI CAS shall perform a database query search returning 5000 results within 5 seconds.'?	Both requirements apply to CA software : SRS-1095 applies to CAs performing internal database lookup. SRS-2734 applies to CAs performing directory searches.	NO	**AMD#2**
CR#425	Book II Part IV	SRS-1174	Is this 10% growth in subscriber numbers factored into requirement SRS-2095 which states that 'E-NPKI Cas shall be scaled to handle 200,000 subscribers and devices without requiring modifications.'?	The number 200000 in SRS-2095 shall be changed to **250,000 users and devices.** The subscriber and device numbers identified in Table 9 of the SOW Annex C scaled for 10% growth per year over 5 years totals 200,000 This is too tight of a scaling margin to be appropriate. SRS-2098 updated to the same requirement	YES	**AMD#2**
CR#426	Book II Part IV	SRS-1232	Can NATO confirm that an authorised subscriber in this context is an E-NPKI admin?	Yes.	NO	**AMD#2**
CR#427	Book II Part IV	SRS-1234	Can NATO confirm that an authorised subscriber in this context is an E-NPKI admin?	Yes.	NO	**AMD#2**
CR#428	Book II Part IV	6.3.2.4 6.3.2.5 6.3.2.6 6.3.2.7 6.3.2.8	SOW paragraphs 6.3.2.4 and 6.3.2.5 refer to a Computer-Based Training (CBT) course and package, but paras 6.3.2.6 to 6.3.2.8 refer to a Computer Aided Training (CAT) package. As CAT is not defined in the glossary and elsewhere in the IFB, can the Purchaser confirm that they meant CBT under paragraphs 6.3.2.6 to 6.3.2.8 and not something different?	Confirmed. SOW section 6.3.2.6 thru 6.3.2.8 updated at IFB AMD#2.	YES	**AMD#2**
CR#429	Book II Part IV	6.3.2.7	SOW paragraph 6.3.2.7 requires the CAT package to include licences that cover updates for the next 2 years at no additional cost to NATO, but it is not clear when the 2 years start. Can the Purchaser clarify when these 2 years will start from; EDC, PSA, FSA or end of the Warranty Period?	The requirement is for 1 year from FSA. SOW 6.3.2.7 was updated accordingly at AMD3.	YES	**AMD#3**

CR#430	BookI	Annex E	The updated Annex E, indicates that the BRCM template already contains the vast majority of BIs (Bidding Instructions) that require proposal traceability, but emphasises it is the Bidders' sole responsibility to ensure all BIs are properly addressed and complete in the BRCM. In reviewing the pre-populated template against the BI sections that require proposal traceability (i.e. sections 3.6.4, 3.6.5 and 3.6.6) it appears that the Purchaser has omitted the “shall” statements in the BI that introduce a set of bulleted requirements from the required traceability (e.g. BI-3.6.4.7.3 that precedes BI-3.6.4.7.3.1 to BI-3.6.4.7.3.3 and BI-3.6.5.2.1.5 that precedes BI-3.6.5.2.1.5.1 to BI-3.6.5.2.1.5.9). Can the Purchaser confirm that this is deliberate and therefore demonstrates an acceptable and compliant approach that can be adopted elsewhere when generating the BRCM, or should the Bidder populate the traceability to these introduction requirement statements for completeness?	Yes, it is deliberate and acceptable when the set of bullets is covering the whole scope of the shall statement.	NO	**AMD#2**
CR#431	Book II Part IV	2.2.1	The SOW identifies that an applicable document is "ISO/IEC 9126: Information Technology – Software Product Evaluation – Quality characteristics and guidelines for their use", but ISO/IEC 9126 is a standard associated with "Software engineering -- Product quality" and the ISO standard associated with "IT - Software Product Evaluation" is ISO/IEC 14598. It is also noted that both of these standards are now withdrawn and revised by later standards; ISO/IEC 9126 is revised by ISO/IEC 25010:2011 "Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models", and ISO/IEC 14598 is revised by ISO/IEC 25040:2011 "Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Evaluation process". Can the Purchaser confirm the standard that they consider applicable to E-NPKI.	The IFB will be corrected to referenced ISO/IEC 25010:2011 and 25040:2011	YES	**AMD#2**
CR#432	Book II Part IV	Annex A, SRS General Smart Card Issuance	For ON can you please provide the following clarifications for the production of smart cards: 1 - Does the ON Smartcard capture process require the collection and encoding of any biometric data, e.g. facial image 2 - Does the ON smartcard production process require the card to have any visible personalisation details, e.g. Site, User Name, Picture etc.	1) Yes, see SRS-2814. To allow for the calculation of best value, bidders shall provide prices for all hardware components. NATO will determine in conjunction with the successful bidder, the appropriate components to be provided as Infrastructure as a Service (IAAS) by the ITM project. Photograph shall be taken unless site provides replication of photograph from PACS CMS to ON. 2) Yes the card shall be personalized including but not limited to a picture. Design to be agreed with the System Accreditor. See SRS-2833 and SRS-2834 in AMD#2	YES	**AMD#2**
CR#433	Book II Part IV	Annex A, SRS General Smart Card Issuance	Can the purchaser confirm if all smartcards are required to be FIPS 201 compliant or only those cards used within PBN.	See CR#177 and CR#152	YES	**AMD#2**

CR#434	Book II Part IV	CR LOG 1 - 101 AMD 1 FINAL CR#2	In CR#2 it was confirmed that the "Site Implementation Manager and ILS Engineer" are not described in the IFB because those roles are not considered to be "Key Personnel" for the project. However in SOW paragraph 12.5.1 and 12.5.1.4 the "Service Delivery Manager" is being identified as "Field Engineer" and "System Delivery Manager" respectively. Can the Purchaser further clarify the "Service Delivery Manager" role as the requested profile is still unclear.	SOW 12.5.1 associated the Service Delivery Manager profile with a Field Engineer profile for which requirements are provided. Further it must be noted that SOW 12.5.1.4 relates to the required security clearance for this profile.	NO	**AMD#2**
CR#435	Book II Part IV	CR LOG 1 - 101 AMD 1 FINAL CR#9	Equal to CR#9, paragraph 10.4.1.8 & 10.4.1.9 incorrectly refer to REF 2.1.2.10 instead of the documents listed in 2.1.3.	Corrected at IFB AMD2.	YES	**AMD#2**
CR#436	Book II Part IV	Annex A SRS-2098	Can the Purchaser please explain how this requirement will be used when balanced against SRS 2021 which requires NONCE interchanges.	SRS-2022 states that the use of Nonces by client software shall be configurable. The final choice between the two will be based on the results of the security risk assessment. IFB updated to provide performance requirements for OCSP responses including nonces.	YES	**AMD#2**
CR#437	Book II Part IV	Annex A SRS-2751	Can you please confirm if this reference to PIV relates to PIV as a technological standard (PIV-C) - which is our current understanding. If not, does it refer to the use of PIV in the context of asserting the appropriate Federal Bridge PKI OIDs (PIV/PIV-I). If it is the latter, can you please confirm who is responsible for the modification of the CP and maintaining the Federal Bridge cross- certification requirements.	Yes, PIV Reference refers to PIV-(C). See CR#177	YES	**AMD#2**
CR#438	Book II Part IV	Annex A SRS-2166	Can you please provide a list of the fielded equipment you expect the CMS to be capable of supporting with no further modification - Thus allowing us to confirm compliance without caveat.	See CR#303. The exact list will only be available as a result from the site surveys.	NO	**AMD#3**
CR#439	Book II Part IV	Annex A SRS-2080 SRS-2094	Can the Purchaser please clarify against which of these scenarios the requirements refer: - the support of PD-VAL through cross certificates by the internal Relying Parties (i.e. at the end-entity level within NATO) - the support of PD-VAL through cross certificates by the external Relying Parties (i.e. at the end-entity level outside NATO) - the support of PD-VAL through cross certificates by the PKI itself (i.e. making sure all attributes the Relying Parties require to perform PD-VAL is available, such as the AIA values).	Bidder is presumed to be referring to SRS-2074 and not SRS-2094 which does not exist. The requirement refers to the support of PD-VAL through cross certificates by the internal Relying Parties (i.e. at the end-entity level within NATO, all clients shall process all certificate extensions relevant to cross certification as identified in SRS 2075 through SRS-2079 inclusive) and the support of PD-VAL through cross certificates by the PKI itself (i.e. making sure all attributes the Relying Parties require to perform PD-VAL is available, such as the AIA values).	NO	**AMD#2**

CR#440	Book II Part IV	SOW NATO Provided Infrastructure Environment	Can the Purchaser please confirm how they expect this delivery to integrate with NATO Provided Infrastructure and the scope of provision? Specifically please could the Purchaser address if this service is expected to be delivered as a self-contained capability in all aspects or if the Purchaser anticipates this capability to be integrated into an NATO Provided environment (Contractor Provided - delivered by this contract / NATO Provided - made available to the Contractor by NATO as Purchaser Furnished Equipment) This clarification covers all delivered reference, testing, training and operational environments: AD Domain - Discrete or integrated into an existing NATO AD environment Physical Host Computing Platforms - Contractor Provided or NATO Provided Virtual Machine Environment - Contractor Provided or NATO Provided VME - Library Stores - Contractor Provided or NATO Provided Database Services - Contractor Provided or NATO Provided Mail Service (Users) - Discrete or clients of an existing NATO Mail Service Mail Service (Services) - Discrete or clients of an existing NATO Mail Service Trusted Role Workstations @ NIAC CSU - Contractor Provided or NATO Provided Remote RA Workstations - Contractor Provided or NATO Provided Workstations for new instances of CMS - Contractor Provided or NATO Provided Business Software & Licencing (OA etc) - Contractor Provided or NATO Provided	For bidding purposes, bidders shall provide prices for all components. To address the specific items in the question: -For IaaS integration see CR#136 -Boundary protection devices services are PFE see CR#88 and CR#261. -For Interfaces requirement see SRS 4.6.3. -For workstation, similar to CR#136 the bidder is requested to include all elements in his proposal, and additional discussion will take place after contract award. -DHCP,NTP, Office printing services are made available by NATO on the PBN and ON. Other mentioned services are linked to the bidder design proposal. The bidder shall include in his design proposal, all required components and services which are not part of the PFE list in SOW Annex E, and not mentioned as out of scope in the mentioned CR#88 and CR#261. NATO will determine in conjunction with the successful bidder if these components shall be provided by the Bidder or as PFE.	NO	**AMD#3**
CR#441	Book II Part IV	4.4.1	SOW para 4.1 General describes how the Contractor will provision ITSM tooling. Amendment 1 to the IFB states that the Contractor will use the NATO instance of Remedy can you confirm who will implement the development work for the ITSM integration i.e. The NATO team or the Contractor's team?	See CR#372, implementation is the responsibility of the bidder.	NO	**AMD#2**
CR#442	Book II Part IV	Annex A SRS-1471	This requirement appears to preclude the use of any active content within a web service (e.g. Active-X and Java are not supported in the latest versions of some identified browsers). Can the Purchaser please confirm that this was the intent of this SRS or was the intention that any web service with active content could be supported in at least two browsers?	Concerns regarding support of active content within browsers is not relevant to this requirement. See SRS-1165 for browser support requirements.	NO	**AMD#3**

CR#443	Book II Part IV	Annex A SRS-2735	This requirement infers that you expect the Contractor to exercise control over the Subscribers' software cryptographic module. Is that indeed the case? Or is this requirement only to be exercised if the proposed solution has a dependency on the installation of a non-native client-side software cryptographic module?	Yes, the SRS applies to any bidder supplied client software cryptographic module required to support the E-NPKI implementation scope. The bidder shall provide a non-native client if the native client does not support all the requirements in the IFB.	NO	**AMD#3**
CR#444	Book II Part IV	Annex A SRS-1896	Can the Purchaser please elaborate what they mean by 'integrated with Bi-SC AIS Collaborative Services'?	SRS-1896 and 1897 were updated at AMD3 ("Collaborative" was changed to "Collaboration"). Collaboration Services are ad hoc tools to enable users to work together. For example, text-based chat, VoIP, Portal collaboration…	YES	**AMD#3**
CR#445	Book II Part IV	CR LOG 1 - 101 AMD 1 FINAL CR#92	The response to CR#92 states that "The Purchaser will execute the OAT based on a purchaser based test plan". This contradicts requirement 9.2.3.7 which states that the Contractor has to provide the System Test Documentation Package (which includes the OAT Test Plan and dry run results) at least 20 working days before the planned OAT start date. Could NCIA please clarify who is to produce the OAT Test Plan and if it is the Purchaser, can it be confirmed that the Plan will it be available sufficiently in advance of the scheduled start of the OAT testing that the Contractor can dry run the test and provide the results of this dry run to the Purchaser 20 working days prior to the start of that formal testing?	There was a typo in CR#92. The first portion of the Purchaser's answer to CR#92 should read: "The purchaser will execute the OAT based on a ~~purchaser based~~ **Contractor-provided** test plan developed in accordance with reference 2.1.6.10. The scope of the ~~purchaser~~ test plan will be based on the requirements defined in the SRS (mostly chapter 3). The test procedure will be based on the details provided by the bidder to meet the requirements of Book 1 section 3.6.5.5.2 and SOW sections 11.3.15.3 and 11.3.15.4. (the detailed information on the steps and procedures required to verify the E-NPKI system compliance with the Certificate Policy and the E-NPKI SRS). The contractor assistance to OAT is to ensure that the verification steps in book 1 section 3.6.5.5.2 are achieved efficiently. The Contractor shall also note the deliverables associated to OAT (see CLIN 2.3). " The remainder of CR#92 is unchanged.	NO	**AMD#3**
CR#446	Book I	Annex A	Is the scope for pricing sheet CLIN 4 (work package ILS) with regard to quantities only the basic sites (52 sites) or the total number of sites (72 sites)?	CLINs 4.1, 4.2.2, and 4.3 are not site-specific. Therefore, the price for all sites (basic and option) shall be allocated to those sub-CLINs. For CLINs 4.2.1 and 4.2.3, see CR#447.		**AMD#3**
CR#447	Book I	Annex A	Are site specific deliverables "TRA report" and "Training Materials (Instructor's guide, Student Manual, CBT)" for the optional sites priced in CLIN 6-18 or in CLIN 4?	The development of the Training Materials shall be priced under CLIN 4, while the delivery and site-specific tailoring of those Materials shall be priced under option CLINs 6 thru 18. The development of any TNA report (and not "TRA" report) template shall be priced against CLIN 4; while the delivery of the site-specific TNA reports shall be priced under CLINs 2 & 3 and option CLINs 6 thru 18.	NO	**AMD#3**
CR#448	Book I	Annex A	Detailed CLIN Summary: should the cells for the Site-Specific System Implementation deliverables - User Services (e.g.D248, D266 etc) be yellow?	No.	NO	**AMD#2**

CR#449	Book I	Annex A	We understand that CLIN 8 and CLIN 9 are optional and not part of the Ceiling amounts. But we also understand that NATO wants to receive pricing information regarding these work packages. Therefore shouldn't the cells (line 278 and lower) of the TAB "Detailed CLIN Summary" be yellow?	As CLINs 8 and 9 are not part of the ceiling, they are not required in the "Detailed CLIN Summary" tab and therefore are not indicated in yellow. The required pricing information is indicated in the CLIN 8 and CLIN 9 Pricing Sheets and Breakdown Sheets in yellow.	NO	**AMD#2**
CR#450	Book II Part IV	13.14.1.4	SOW: "The detailed implementation sequence of Technical Services and User services. The sequence shall carefully consider and adapt to the ITM implementation sequence in order to minimize the impacts on both projects". The duration time of the ITM project (waves 1, 2, 3 and 4 as mentioned in 01_IFB-CO-13703-ITM) is 5 years. The EDC for ITM is undefined yet. The time lines for E-NPKI are much shorter. The 3rd data centre will be available in ITM wave 3. This conflicts with the E-NPKI time lines for PSA. Clarify please. A considerable number of sites will ITM migrate in for example ITM waves 3 and 4. This conflicts with the E-NPKI time lines for FSA. Clarify please.	ITM and E-NPKI project schedules will be under regular scrutiny to ensure coherence (technically and programmatically). The E-NPKI project may come to implement ahead of ITM at some sites; in such a case E-NPKI will be deployed on existing underlying infrastructure at those sites.		**AMD#3**
CR#451	Book II Part IV	1.4.4.4	Provide system implementation services. Does the "execute installation/deployment" requirement apply to the card readers as well?	The "execute installation/deployment" apply to all equipment (Hardware and Software) delivered under the E-NPKI project.	NO	**AMD#3**
CR#452	Book I	3.6.5.3.6	SOW: "For bidding purposes only, the Bidder shall assume that all elements of its design must be provided in full at the implementation stage and that no hardware, software or business processes exist on site in a reusable form". Does this assumption refer to the card readers as well?.	Yes.	NO	**AMD#3**
CR#453	Book I	Annex B-16	The Certificate B-16 states: I hereby certify that (name of Company) has secured approval letters and/or certificates for all cryptographic Hardware and Software included within this bid and have coordinated with the National CIS Security Authorities of a participating NATO Nation to ensure that these approval letters and/or certificates will be delivered to the Purchaser prior to conclusion of the bid evaluation. Is there a timeline (mentioned) for the conclusion of the bid evaluation? When exactly do you expect the required approval letters / certificates? It would be very helpful to know a latest possible date for the certification.	See answer at CR#212	No	**AMD#3**

CR#454	Book II Part IV		2. In the document "1_IFB-CO-13810-CS CR LOG 1 - 101 AMD 1 FINAL.pdf" links are provided, in order to get the 86 documents referenced in the IFB (SOW). Unfortunately we cannot access these links and Wikipedia.org has not shown really helpful in terms of special STANAGS and AQAPs. Is there any other possibility to access these documents?	See answer at CR#115	No	**AMD#3**
CR#455	Book I	Annex A Bidding Sheets AMD 1 FINAL	We noticed that there are some errors in the Bidding sheets (2A_IFB CO-13810-CS Book I Annex A Bidding Sheets AMD 1 FINAL.xls) The errors are the following: Sheet "CLIN 2" – cells B37, B38 & B39 Current values/references are: • 2.5.2.1 • 2.5.2.2 • 2.5.2.3 Correct values/reference should be: • 2.5.1.1 • 2.5.1.2 • 2.5.1.3 Can NCIA amend and send an updated version of the Bidding sheets (2A_IFB CO-13810-CS Book I Annex A Bidding Sheets AMD 1 FINAL.xls) ?	Corrected at IFB AMD2. See CR#269	YES	**AMD#2**
CR#456	Book I	3.6.4.9.5.1	Please confirm whether the Contractor shall submit a list of PFE for all sites (including both Basic and Optional Sites) as part of its bid submission? If so please confirm whether you require the Contractor to submit one PFE table for the Basic Sites and one PFE table for the Optional Sites?	The Bidder shall submit a list of PFE for all sites (including both Basic and Optional Sites). Book I section 3.6.4.9.5 was amended accordingly at AMD3.	YES	**AMD#3**
CR#457	Book II Part IV	SOW 11.3.7 SOW 11.3.8 SOW 11.3.9	These requirements need us to be compliant with REF 2.3.2 - NPKI Security Accreditation Plan (SAP) and its acompanying document 2.3.3 E-NPKI System Description (to accompany SAP). Can the Purchaser provide us with these documents or provide a date at which these documents shall be made available to the Contractor. Note - It has not been possible to source these through our National Delegation.	See CR#115	NO	**AMD#2**
CR#458	Book II Part IV	CR#22	Can the Purchaser please clarify the purpose of LanSweeper and ADDM as there is potentially significant overlap between the capability of these tools?	ADDM and Lansweeper are used by various NATO operational teams. They might rely on either Lansweeper or ADDM for asset discoveries. Therefore it is required for the E-NPKI to support both tools as mentioned in CR#22.	NO	**AMD#3**

CR#459	Book II Part IV	SOW Annex B 3.3.3 & CR#22	This requirement states that the Contractor shall implement a Help Desk technical support capability to assist with E-NPKI product use, advice, configuration, tuning, troubleshooting issues etc. CR#22 states that "the Contractor will use NATOs instance of Remedy and the Contractor will implement interfaces and workflow for Incident Management and Help Desk services". Can the Purchaser please confirm that the Contractor provided licences shall be used to allow our helpdesk staff to act as a resolver group within the NATO helpdesk service?	Yes, see CR#372, but there might be some additional licenses required to fulfil the SLA support (see CR#391.)	NO	**AMD#3**
CR#460	Book II Part IV	SOW 5.5.4.4.4 SOW 9.2.4.6	Can the Purchaser please confirm that the following understanding is correct for responsibility in the performance of testing as it applies to both Technical (TVP) and Security (STVP): OAT - Purchaser to perform Contractor to support both BLAT - Contractor to perform TVP with Purchaser witnessing, Purchaser to perform STVP with Contractor support. PSA - Contractor to perform TVP with Purchaser witnessing, Purchaser to perform STVP with Contractor support. Site Acceptance - Contractor to Perform TVP Annual Security Vulnerability Testing (if required?) - Purchaser with contractor support.	The Contractor-proposed simplification of TVP and STVP does not accurately reflect the IFB requirements. In particular: - OAT will be executed by the Purchaser based on the Contractor-provided OAT Test plan (see CR#445) - BLAT: see SOW 9.2.4. - Site activation tests: see SOW 5.5.3.4 - PSA is a milestone. See 16.7 - Vulnerability assessments: see SOW 7.2.2	NO	**AMD#3**
CR#461	Book I	3.6.4.6.1	According to the Instructions for Bidders the Contractor has to deliver an initial version of the Work Breakdown structure (WBS) with the proposal but in the SOW no management document WBS is expected, "only" a Product Breakdown Structure (PBS) and a Product Flow Diagram (PFD) as basis for the PMS. Can you please clarify?	An initial WBS is required to be delivered as part of the bid (in Volume 1) to demonstrate that the Bidder understands and addresses all necessary activities (see Book I 3.6.4.6.4). The WBS document is not planned to be maintained during contract execution.	NO	**AMD#3**
CR#462	Book I	SSS/BS	Under column Delivery Form only electronic formats are listed. Under which column shall the HW / SW items be listed, where shall the labour rates be listed?	The HW/SW details shall be listed in the CLIN Detail Pricing Sheets under sections 1. Materials to include unit costs and 2. Material Overhead to include all rates and factors applied to the Materials. Labour Rates shall be listed in section 3. Labour and section 5. Subcontract Labour in the CLIN Detail Pricing Sheets. Bidders shall also note that other delivery form than "Electronic" are mentioned in the SSS and Bidding Sheets; for example "labour", "Paper", "HW/SW".		**AMD#3**
CR#463	Book II Part IV	SRS-2163	Is the assumption correct that this requirement is related to requirements SRS-2161, -2722, -2723 only?	Yes, SRS-2163 relates to the CMS system mentioned in SRS-2723, SRS-2722 and SRS-2161.	NO	**AMD#3**
CR#464	Book II Part IV	SOW 5.5.6	Is the assumption correct that it will not be necessary to take over archived key material and certificates from the Interim PKI system to provide recovery functionality to new E-NPKI smartcards?	Yes this is correct, there is no plan to migrate iNPKI material to the E-NPKI.	NO	**AMD#2**

CR#465	Book II Part IV	SOW 5.5.6.12	Does the user have the access rights to delete existing certificates and key objects on his existing smartcard?	The E-NPKI system has the permission to delete existing certificate on user smartcard. The system shall not rely on user to preform this activity, even if such permission is given to users.	NO	**AMD#3**
CR#466	Book II Part IV	SOW 5.5.6	How do the current (interim) cards fulfil SRS-2801?	See CR#304. The I-NPKI implements orthogonal smartcard and drivers between different security domains.	NO	**AMD#3**
CR#467	Book II Part IV	SOW 7.5.3	Please specify details on necessary support activities for exercises.	see CR#350	NO	**AMD#3**
CR#468	Book II Part IV	SOW 5.4.1	Is there a list of equipment, for which TEMPEST-related requirements have been identified? If yes, please provide.	Tempest scope requirement is fully described in the InfoSec Technical and Implementation Directive on Emission AC/32-D(2007)0036 referenced SOW 2.1.6.11. The list of equipment is dependant on the bidder's proposal, and will have to be reviewed after contract award.	NO	**AMD#3**
CR#469	Book II Part IV	SOW 3.9.1.1	In SOW - 3.9.1.1 it is documented that the Project Status Report has to be send on the third working day of a month. According to the information in 2A_IFB CO-13810-CS Book I Annex A Bidding Sheets AMD 1 FINAL.xls the PSR has to be delivered 3 days after corresponding Project Review Meeting (PRM). Does this mean that the PRM has to be done on the last working day of the previous month?	SSS and Bidding Sheet were updated at AMD#3 so as to reflect the SOW requirements. Project Status Reports (PSR) shall be delivered monthly, on the 3rd working day of the month.	YES	**AMD#3**
CR#470	Book II Part IV	Annex E	We assume that for PFE SW licenses the responsibility for O&M (patches, updates) is with the purchaser. Please confirm.	For PFE software, the Purchaser will make patches and updates available to the Contractor. The contractor shall be responsible for the implementation on the E-NPKI system.	NO	**AMD#3**
CR#471	Book II Part IV	SOW 3.4.1 and IFB 3.6.5.2.1.3	Is the Project Breakdown Structure, which is requested in the Bidding Instructions as part of the SDS (Specialist product), and the Project Breakdown Structure, which is requested in the SOW as a Management Product, the same document and has to fulfil all requirements mentioned in Bidding Instructions and SOW for the PBS?	As per Book I 3.6.5.2.1.3, an initial PBS (focusing on Specialist Products only) is requested to be delivered as part of Volume 2. The initial PBS shall fulfil the requirements of SOW 3.4.1, except for the fact that for bidding purposes it shall focus on Specialist Products only.	NO	**AMD#3**
CR#472	Book II Part IV	Annex E 1.1.1	We assume that systems running on the PFE software VMWare implemented by NATO have an availability of normally 99.5% per server; totally up to 99.99%. Please confirm.	The E-NPKI project is aiming at hosting its services in the ITM provided infrastructure. However the purchaser cannot confirm ITM will be ready to provide IaaS in all locations E-NPKI systems will deploy. As mentioned in CR#450, the E-NPKI project will move ahead either through rescheduling activities to match the ITM schedule, or by installing onto existing underlying infrastructure prior to ITM roll out. The bidder is requested to provide all prices for all hardware as mentioned in CR#136 and CR#440. NATO will determine in conjunction with the successful bidder, the appropriate components to be provided as Infrastructure as a Service (IAAS) by the ITM project. As for availability, the bidder is requested to calculate it based on its design proposal.	NO	**AMD#3**

CR#473	Book II Part IV	SRS-2659	Section 12.1.4 states that only "contractor personnel, who need System Administrator privileges, when working on NATO SECRET systems, shall be required to hold a valid NATO CTS clearance". SRS-2659 states that "Onsite E-NPKI contractor personnel shall hold at least a COSMIC TOP SECRET Security Clearance". Please confirm that "Onsite" means in this context "personnel who needs system administrator privileges"	See CR#317 for clarification	NO	**AMD#2**
CR#474	Book II Part IV	SRS-2604	Can we expect that the protocol to publish certificates will be LDAP or LDAPS, when/where NEDS is not available?	Yes, if NEDS is not available, LDAP or LDAPS will be used. SRS-2604 updated at AMD#3.	YES	**AMD#3**
CR#475	Book II Part IV	SRS-2614 SRS-2635	Please clarify the conflict between the two requirements: "CAs shall publish certificates to NEDS immediately after they are signed" and "CA shall not publish the certificate, or otherwise make it available unless all of the required workflow activities have been completed". Is one of the required workflow activities the activation of the token by the subscriber? (SRS-2674)	No token will be issued without the subscriber being physically present. See also CR#258 for the signature of the agreement as part of the workflow.	NO	**AMD#3**
CR#476	Book II Part IV	SRS-2157	"The E-NPKI workflow shall enforce the generation of key pairs in the presence of the subscriber or sponsor as appropriate." - Please confirm that presence in this context mean that the generation of the signature and authentication keys (encryption keys generated by CA) are part of the workflow and keys shall be generated on time.	See CR#475. - Subscriber will be physically present when generation of the personal certificate is being performed. - Sponsors will be physically present when generation of a device/service certificate is being performed.	NO	**AMD#3**
CR#477	Book II Part IV	SRS-2758	Please confirm that the validation workflow is an automatic process and there is no manual user interaction needed. Please explain which information in the auto-enrolment needs to be validated.	a) The workflow will contain manual interactions. b) In case of enrolment of windows devices, confirmation of sponsor and validation of the identity of the new device.	NO	**AMD#3**

CR#478	Book II Part IV	SRS-2098	"E-NPKI OCSP service shall be capable of precomputing hashes for 200,000 subscribers and devices (average 3 certificates per subscriber or device) within 15 minutes." The precomputing of hashes requires that no nonce value in the OCSP request is used. For security reasons a nonce value should be considered (e.g. to avoid replay attacks). Therefore two questions: 1. Shall the responses precomputed due to performance reasons? 2. Or shall this mean that 200.000 signatures (OCSP responses) shall be generated in 15 minutes?	See CR#425, SRS-2098 was updated to 250 000 signatures. The system shall be capable to pre-compute (generate) all the signatures hashes every 15min.	NO	**AMD#3**
CR#479	Book II Part IV	SRS-849	"E-NPKI CAs and OCSP servers shall have dedicated hardware platforms." SRS-1164, 2597, 1745, 1746 require to define the virtual infrastructure resources needed for E-NPKI. Does this SRS mean that only the HSM must be delivered in a dedicated hardware platform? Or shall the CA, OCSP also be delivered on dedicated HW platforms (and therefore no virtualisation for these components shall be used)?	Hardware for all components shall be dedicated to E-NPKI functionalities and not mixed with non-E-NPKI systems. See CR#136. CA and OCSP components shall not be virtualized on hardware platforms shared with other components ; but CA and OCSP could be virtualized on their own hardware platform. Hardware shall be dedicated for CA and OCSP functions. See also CR#136.		**AMD#3**
CR#480	Book II Part IV	SRS-1741	"E-NPKI shall support the following environment configuration for the server components: Operating System: Microsoft Windows Server 2012 and later." Does the request apply to all core components CA/RA/CM and the additional integration parts (OCSP/Timestamp etc.)? Does the request exclude any method of virtualisation for the integration parts, as far as the required performance is achieved? Are there any other operating systems allowed to operate the E-NPKI products (OCSP, Timestamp, RA, etc.)? Like Red Hat / SUSE Linux, etc.?	SRS-1741 is requesting to deploy all services on Windows operating systems due to several constraints like manpower, integration, security and/or maintenance. For virtualization, see CR#136.	NO	**AMD#3**

CR#481	Book II Part IV	SOW 16.6.10 SOW 16.6.11	SOW - 16.6.10 defines that all tests must have execution status PASSED to get BLAT milestone approval. The following section SOW - 16.6.11 highlights that it is sufficient to have an action plan for failures with severity “Moderate”, “Minor” and “Cosmetic”. Is our understanding correct, that tests with execution status FAILED resulting only from failures with severity “Moderate”, “Minor” and “Cosmetic and an agreed action plan do not impact BLAT milestone acceptance? Same question for PSA (SOW - 16.7.12 and 16.7.13) and Site activation (SOW 16.8.10 and 16.8.11)	The Purchaser confirms that: - SOW 16.6.11 will apply to BLAT milestone - SOW 16.7.13 will apply to PSA milestone - SOW 16.8.11 will apply to Site Activation milestone The fact that a test is PASS or FAIL may not be in direct relation to the severity of the failure identified, hence the distinction between the outcome of a test ("PASS" or "FAIL"), and the severity of the failure. Example: during a test a "cosmetic" failure may be identified albeit not in direct relation to the test case under execution; in such a case the test will get a status "PASS", and a "cosmetic" failure will be logged. The same principle applies for all milestones.	NO	**AMD#3**
CR#482	Book II Part IV	SRS-2164 SRS2038	Do these requirements refer to the actual NIST standards: • NIST 800-73-4 – Interfaces for Personal Identity Verification, Part 1 -3 and • NIST 800-76-2 – Biometric Specifications for Personal Identity Verification, including MoC / OCC fingerprints in ISO/IEC 19794-2:2011 Standard	SRS-2164 and SRS-2038 require interoperability with FIPS 201. As mentioned n the FIPS 201-2 document: "The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73 [SP 800-73]" "The requirements for collection and formatting of biometric information are specified in Special Publication 800-76 [SP 800-76]" Therefore the two requirements are related to the NIST document mentioned.	NO	**AMD#3**
CR#483	Book II Part IV	SRS-2824	Is the assumption correct, that this requirements is only valid for personalizing/rekeying the existing smartcards and the contractor do not have to deliver a appropriate Card API for usage of the cards in the user´s client / application environment?	The contractor will not be required to provide a Card API for existing smartcard where CMS are already in place and will be integrated by the Contractor.	NO	**AMD#3**
CR#484	Book II Part IV	SRS-2100 SRS-2099	Must the requirement for handling 2000 ECDSA 384 signatures per second be fulfilled by a single HSM or can also a cluster of HSMs be used to fulfil this requirement?	No design constraints from the Purchaser regarding this topic. The Bidders are free to propose any appropriate solution.	NO	**AMD#3**
CR#485	Book II Part IV	SRS-699	"NATO Enterprise systems shall store the ENPKI Root CA certificate such that unauthorised alteration or replacement is readily detectable and preventable (i.e. does not succeed in replacing the existing Root CA certificate)." Please confirm that the contractor is only responsible for secure write access to those NATO Enterprise Systems that are part of the E-NPKI respectively components that are delivered and configured by the contractor.	No. SRS-699 applies to E-NPKI systems deployed by the contractor, and in particular to: - Operating Systems (Servers and workstations e.g. via GPO) - Applications identified in SRS chapter 4.10 for E-NPKI Integration	NO	**AMD#3**
CR#486	Book II Part IV	SRS-650	Please confirm that the storage capacity for this information is provided and held by the NATO.	As mentioned in CR#440, for bidding purposes bidders shall provide prices for all hardware components, also including hardware for systems proposed for virtualization and storage.	NO	**AMD#3**

CR#487	Book II Part IV	SRS-857 SRS-858	Please confirm that network segmentation, firewalls and other equipment to fulfil these requirements are PFE.	For PFE Firewall, see CR#88. Bidder is requested to define what they mean by "other equipment" to further respond to the question..	NO	**AMD#2**
CR#488	Book II Part IV	SRS-2463	According to RFC 5280 some attributes must be encoded as PrintableString (e.g. Country). Please confirm: As not otherwise stated in RFC 5280, the components of the DN shall be in the form of an X.501 UTF8String.	Yes the statement "As not otherwise stated in RFC 5280, the components of the DN shall be in the form of an X.501 UTF8String." is correct. SRS-2463 is updated as part of AMD#3	YES	**AMD#3**
CR#489	Book II Part IV	SRS-2224	Please confirm: The contractor has to collect and encrypt all necessary data needed to restore an E-NPKI-System, put this backup, e.g. on the local file share of the corresponding server, and the NATO is responsible for transferring this backup to an off-site location for archiving.	See CR #136. Backup mechanism shall be provided by the bidder as part of the proposal. Detailed backup processes will be discussed after contract award.	NO	**AMD#3**
CR#490	Book II Part IV	SSS	The Delivery Date of the CLIN 3.1.1 is documented as PSD + 1 month. Please explain the milestone PSD.	PSD stands for "Performance Start Date". SOW Annex D was updated accordingly at AMD3.	YES	**AMD#3**
CR#491	Book II Part IV	SRS-2279	The E-NPKI components in the data centre shall be integrated with NATO Service Management Centre (SMC). Is our assumption correct that the E-NPKI components shall deliver status information via SNMPv3 to SMC, which is acting as the central service monitoring system?	SRS-2279 does not limit the scope of the integration with SMC to SNMPv3 and monitoring.	NO	**AMD#3**
CR#492	Book II Part IV	Annex A 4.6.2.1	Requirements for Web-Services are listed in SOW Annex A e.g. in chapter 4.4.1.1 (security requirements) and chapter 4.6.2.1 (interface requirements). It is not specified which functionalities these web services shall provide. Please explain in more detail.	Functionalities are described throughout the SRS document. For example some functionalities are provided in SRS-2742 : user provisioning, CSR approvals, key recovery, certificate revocation, and password resets.	NO	**AMD#3**
CR#493	Book II Part IV	SRS-2524 SRS-509 SRS-516	Please confirm that the capture of written notification and electronically record the ID means to scan a document on the RA client and bind this document to the subscriber or sponsor registration information. If not, please describe an applicable method.	SRS-2524 is not related, we assume the bidder meant SRS-2624 Yes, the example provided is one way of meeting the requirements SRS-2624,SRS-509 and SRS-516.	NO	**AMD#3**
CR#494	Book II Part IV	SRS-486	Please explain the "equivalent level of legal authenticity" as a handwritten signature.	Equivalency to handwritten signatures is established based on a collection of technical and procedural mechanisms defined within NATO Policy and this IFB. The top level document in NATO policy defining equivalency is SOW reference 2.3.5 which is further expanded by SOW reference 2.3.6 and the remaining documents in section 2 of the SOW.	NO	**AMD#3**

CR#495	Book II Part IV	SRS-1193	In CLIN 19 the contractor has to provide prices for software licences for CAs, RAs, TSPs, OCSP, certificates. Please explain in detail the licence scope of SRS-1193 that should not underlie limitations.	Additional items that might be procured under CLIN 19 are not related to SRS-1193. NATO is a dynamic organisation with multiple network domains that may expend or shrink as required. The movement of the user base (users or device quantities) from one network domain to another domain as described in SRS-1193 shall not lead to additional licences costs if the total quantity of software and/or licences does not increase. E-NPKI services shall be available to relying parties of Federated infrastructures. Access to OCSP, timestamp and other E-NPKI services by those Federated identities, shall not result in additional costs for NATO. See also CR#539 SRS section 4.1.7 amended at AMD3.	YES	**AMD#3**
CR#496	Book II Part IV	SOW 2.1.8	Can you assist in providing information on where I may obtain or send me the following templated (if not restricted) 2.1.8 NATO Templates • 2.1.8.1 Interface Control Document template • 2.1.8.2 Security Risk Assessment (SRA) Report (PILAR) Template • 2.1.8.3 Security Test and Verification Plan (STVP) Template for Secure Automated Information System (AIS) • 2.1.8.4 System Interconnection Security Requirements Statement (SISRS) Template • 2.1.8.5 Site Security Compliance Statement (SSCS) Template	See CR#115	NO	**AMD#2**
CR#497	Book II Part IV	SRS-629	• What is the absolute minimum bandwidth available between E-NPKI services and the E-NPKI End-entities and for how long of a timeframe can this be experienced? • How many minimum bandwidth timeframes should the E-NPKI services be expected to operate on without interruption of services within a 24 hours period?	GSM data (9.6 kbps) is the minimum bandwidth envisioned for E-NPKI. Duration and recurrence of bandwidth in this sense is irrelevant as E-NPKI shall be able to support devices with limited bandwidth.	NO	**AMD#3**
CR#498	Book II Part IV	SRS-630	• What is the absolute maximum latency between E-NPKI services and the E-NPKI End-entities and for how long of a timeframe can this be experienced? • How many minimum bandwidth timeframes should the E-NPKI services be expected to operate on without interruption of services within a 24 hours period?	2 satellite hops in each direction shall be supported. (Round trip delay of 4 seconds). Duration and recurrence of latency in this sense is irrelevant as E-NPKI shall be able to support devices deployed across SATCOM infrastructures.	NO	**AMD#3**

CR#499	Book II Part IV	SRS-1090	Your response to 4 questions is requested: • What are the lowest specifications of the reference system or hardware when performing the test? • What are the lowest specifications for a workstation for measuring the performance? • What is the minimal wide area network connectivity when performing the test? • What is the maximum latency when performing the test over a WAN?	1 - The performance specifications of the production environment apply to non-production environments (including the reference environment). 2 - See requirements under SRS-1742 3 - As stated in SRS-1090 the performances need to be demonstrated with a bandwidth of maximum 1000Kb/sec. 4 - As stated in SRS-1090, the performances need to be demonstrated with a latency of minimum 500ms.	NO	**AMD#3**
CR#500	Book II Part IV	SRS-1741	With reference to the requirement for Windows Server 2012 and later. We assume that other operating systems as contained in the NCIA-NATO Secret-Approved Fielded Product List are also allowed for the E-NPKI server components. Is our assumption correct?	See CR#480	YES	**AMD#3**
CR#501	Book II Part IV	SRS-834	The E-NPKI solution will be part of the current network infrastructure of the NATO and E-NPKI elements are to be protected by boundary protection devices from the general purpose network. Is it implied that the E-NPKI is an isolated solution or does it make use of readily available infrastructure components like network components, firewall, storage and virtualized environments. In the latter case which components can be utilized and which are to be provided by the solution provider?	See CR#88 and CR#136	NO	**AMD#3**
CR#502	Book II Part IV	SRS-1753	Can we assume that server deployment package (virtual appliance or installation package) will only be installed on existing infrastructure components (servers who will interact with E-NPKI) or should we also consider the configuration of E-NPKI infrastructure components as part of the provided solution (servers who will be part of the E-NPKI) as a server deployment package?	See CR#136	NO	**AMD#3**
CR#503	Book II Part IV	SoW 2.1	In the SOW, section 2, applicable documents are mentioned which form the basis for the proposal by purchaser. The links already provided by NATO do not allow access to find these documents ourselves: • 2.1.6.13 Guidelines for the Security Approval or Security Accreditation of CIS (AC/35-D/1021-REV3) • 2.1.6.14 Guidelines for Security Risk Assessment and Risk Management of CIS (AC/35-D/1017 –REV2) • 2.1.8.2 Security Risk Assessment (SRA) Report (PILAR) Template • 2.3.2 NPKI Security Accreditation Plan (SAP) • 2.3.7 NATO Public Key Infrastructure (PKI) Certificate Policy AC/322-D(2004)0024-REV2, • AC/322-D(2004)0024-REV2-ADD1 and AC/322-D(2004)0024-REV2-ADD1	See CR#115	NO	**AMD#2**
CR#504	Book II Part IV	Annex A 4.10	Section 4.10 addresses the integration with existing systems and applications. Please confirm that all integration requirements in section 4.10 apply to ITM-migrated sites only.	No, E-NPKI integration applies to all sites of NATO Enterprise described in ANNEX C SECTION 1, whether ITM is deployed or not.	NO	**AMD#3**

CR#505	Book II Part IV	SRS-2038	"Support for writing Biometric data objects to smart cards shall be in accordance with FIPS 201 in all cases where FIPS 201 Smart cards are in use". Please provide an example of the purpose of a case where other than FIPS 201 Smart cards, that must be supported by E-NPKI, could contain Biometric data objects.	Writing biometric data to smartcard is only envisioned for FIPS 201 smartcards.	NO	**AMD#3**
CR#506	Book II Part IV	Annex A	Question Withdrawn	Question withdrawn	NO	**AMD#3**
CR#507	Book II Part IV	SRS-2831	SOW: "The scope of CMS is defined in sections 2 through 4 of FIPS201-2 (See Ref 2.2.4.) The CMS shall support all biometric capture requirements of FIPS 201-2 chapter 2, but the vendor is only required to provide hardware to support image capture and printing. See details in CR#15 through CR#18 for information by site". Please confirm that for the use of (MFP) printers the badge, as produced by the CMS at the PBN level (as indicated on slide 38 of the Bidders Conference), will do on the ON level as well.	If the bidder is asking if dedicated MFP need to be provided on the ON, the response is yes. Existing PBN MFP will not be shared with the ON.	NO	**AMD#3**
CR#508	Book II Part IV	SRS-2831	Please provide an example of a LACS for Users at the ON level.	Smartcard authentication, document signatures are some of the examples. All requirements are included in the SRS document.	NO	**AMD#3**
CR#509	Book II Part IV	AnnexA	SOW: "Support for writing Biometric data objects to smart cards shall be in accordance with FIPS 201 in all cases where FIPS 201 Smart cards are in use". Please confirm that for cards, produced on the right hand column (IT Helpdesk / Kiosk) on slide 38 from the Bidders Conference, any biometric-related SRS requirement will not apply.	Due to requirement to have backup capabilities between pass office and IT Helpdesk, biometrics requirement also apply to IT Helpdesk/Kiosk deployments.	NO	**AMD#3**

CR#510	Book II Part IV	SOW 11 SOW 16 SOW 5.5.4	In SoW section 11 the Security Accreditation Process is explained. The timelines of the Accreditation Process reflected section 16 (see picture on 142). Formal approval of accreditation must be realised at SDR prior to Software Approval Testing and next formal approval at BLAT. This is basis for massive roll out to other sites in the various member states. The before mentioned process and approvals demonstrates and proof that NATO HQ that the E-NKPI is accepted and used as the standard solution to all sites at all NATO member states. In SoW 5.5.4 the local SAA and the local approval is explained. Questions are: 1. Is the certification/accreditation process and (multiple) approvals by NATO HQ (in Belgium) binding to all individual NATO member states? 2. Are there NATO member states where additional national certifications, tests or processes by national (security) bodies are required due to national laws and/or regulations? If so, which NATO member states and what extra certification/accreditations? 3. Are certificates related to cryptographic hardware/software components (see Annex B-16) of by the National Security Agency in country X recognised by all other NATO member-states? 4. What is the scope and acceptance criteria for a local SAA to (dis-)approve in addition to what is already tested, accredited and approved by NATO HQ?	1 - Security Accreditation Authority (SAA) for E-NPKI is NATO CIS Security Accreditation Board (NSAB), not NATO HQ. Lead NATO SAA is NATO Office of Security. 2 - The system is being installed on NATO owned CIS. NATO rules apply. 3 - Yes this project will recognize a cryptographic approval from any of the 25 participating NATO Nations. 4 - The criteria for approval by the local SAA are based on NATO policies. The fact that each local SAA need to approve the system is due to location specific environmental aspects and physical security.	NO	**AMD#3**
CR#511	Book II Part IV	Annex A 16.7.3.1 16.8.5.1 CR#20	Can the purchaser please clarify these requirements and the related CR as they apply to Annex C. Using the number of declared users per site in Annex C, there appears to be circa a third of the sites that have approximately 50 users. The requirements 16.7.3.1 and 16.8.5.1 specifies that site completion must include 50 new users per site, thereby doubling the existing registered users. Can the Purchaser please confirm that this requirement will be applied to all sites?	In case there are less than 50 possible new users onsite, all new users shall be activated.	NO	**AMD#3**
CR#512	Book II Part IV	3.3.2.4 12.5.1 12.5.1.4 CR#2	In CR#2 it was confirmed that the "Site Implementation Manager and ILS Engineer" are not described in the IFB because those roles are not considered to be "Key Personnel" for the project. However in SOW paragraph 3.3.2.4 contractor key personnel for this project lists the “Service Delivery Manager”. Also in SOW paragraphs 12.5.1 and 12.5.1.4 the "Service Delivery Manager" is being identified as "Field Engineer" and "System Delivery Manager" respectively. Can the Purchaser further clarify the "Service Delivery Manager" role as the requested profile is still unclear.	See CR#434. SOW is clear on the requested profiles.	NO	**AMD#3**

CR#513	Book II Part IV	SOW 12	Could the Purchaser please confirm that an ITIL Expert certificate is acceptable as a substitute for the ITIL Intermediate certificate required for the Technical Lead and Service Delivery Manager?	Having an ITIL Expert Certificate does not necessarily mean having the required intermediate certificates (i.e. Service Transition Certificate and Service Operations Certificate for the Service Delivery Manager; and Service Design Certificate for the Technical Lead). As part of the Bid Evaluation process, the Purchaser will evaluate the certificates provided with the Bids. The non availability of requested certificates may impact negatively the technical score.	NO	**AMD#3**
CR#514	Book I	Annex E CR#4	CR#4 clarified, that the BRCM shall be provided in Excel format and Book I Annex E was amended accordingly. But Annex E also contains the former requirement of the original IFB, that "One copy of the duly completed BRCM shall be included in …" Please clarify if beside of the Excel Format the BRCM shall also be provided as a printout.	Please note the changes at AMD 3 concerning the contents of bids (hard and soft copies). No hard copy printout of the BRCM will be necessary.	YES	**AMD#3**
CR#515	Book I	Annex E CR#4	Please clarify, if the provision of project deliverables and content, which are defined in Book II (SOW , SRS) but which are not explicit required in Book I as part of the proposal, will result in a better technical evaluation of the proposal, if they are provided in the bid phase as part of the proposal.	Book I is explicitly requesting documents, which will be evaluated, and for which the level of detail is important. Any additional document provided as part of the bid package and not explicitly required in Book I will only be evaluated if they support and are explicitly cross-referenced to the proposal deliverables called for in the Book I. The Purchaser cannot make any predictions or representations regarding the submission of such materials with regards to the scoring of the proposal.	NO	**AMD#3**
CR#516	Book I	Annex E CR#4	With CR#4, Book I Annex E was replaced in its entirely and the column "Compliance statement" with different possible entries were introduced in the BRCM. Those entries are defined on the one hand in Book I Annex E and on the other hand in the sheet "list" in the Excel file "2B_IFB CO-13810-CS Book I Annex E BRCM AMD 1 FINAL.xlsx". The definitions in the two sources allows different interpretations (e.g. for "Partial"). Please clarify which definitions are valid or harmonize them.	The definition in Book I Annex E is the guidance to be followed : - "Compliance statement": the way and extent the Bid covers and complies with the section/requirement under consideration, using the following classifications: o "Provided/Detailed": The bidder states providing a document or details at the mentioned reference. Such a classification is expected for all BIs and the majority of the SOW and SRS requirements. o "Partial": The bidder states fulfilling the requirement but only describes part of it. Such a classification is expected for a small number of SOW and SRS requirements. o "Deviation proposed": The bidder states tacking and describing an alternative approach to fulfil the section/requirement under consideration. Such a classification is expected for a very limited amount of SOW and/or SRS requirements. o "Not detailed": The bidder states fulfilling the requirement, but does not detail/justify how. It is expected that some requirements from the SOW or SRS cannot be justified/detailed at the bidding stage. Book I Annex E BCRM was updated accordingly in AMD#3.	YES	**AMD#3**

CR#517	Book I	Annex E CR#4	With CR#4, Book I Annex E was replaced in its entirely and the column “Compliance statement“ with different possible entries were introduced in the BRCM. Regarding the fulfillment of the requirements of Book I it is reasonable, that bidder’s proposals shall meet all instructions and requirements for compliance and that it is useful to disclose deviations of the prepared proposal documents in Annex E. Regarding the fulfillment of the requirements of the SOW (or SRS), we assume, that the detailed fulfillment is part of the project execution and is not part of the proposal documents. Nevertheless some “Initial” plans and documents shall and will be provided with the proposal as required with Book I. Furthermore statements of commitment to meet the requirements shall and will be made in the proposal documents as required with Book I (e.g. according to Book I, para 3.6.4.9.1, 3.6.4.9.2, 3.6.4.9.4, 3.6.5.2.2 and 3.6.6.6.1). But a comparison of the different possible entries for the column “Compliance statement“ in Annex E causes the assumption, that purchaser expects that detailed documents and project deliverables as fulfillment of “the majority of the SOW and SRS requirements” shall be already delivered as part of the proposal. Please clarify, if a requirement of SOW or SRS can be assessed as “Provided/…”, when “Book I” requires no further details in the proposal documents and the bidders proposal include a statement (specific or in general), that the requirement will be met during project execution.	If a bidder does not provide details/justification on how the requirement is fulfilled, he should select the category "Not detailed" even when "Book I" does not specifically request further details as part of the bidding stage.	NO	**AMD#3**
CR#518	Book II	Part I SSS, CR#37 CR#42	With CR#37 Purchaser denied the provision of the SSS in native Excel format to prevent that a Bidder would improperly use that file as a Bidding Sheet for their price proposal. But the SSS is also the groundwork for WBS and PMS. To minimize transcription errors and in conjunction with Purchaser's intention not to create unnecessary burden on the Bidder, it is helpful to have the information in Excel format. In the Bidding Sheets the information regarding the SSS and its columns seems to be distributed over several detailed CLIN sheets. With CR#42 Purchaser already stated that “The SSS is equivalent to the Detailed CLIN Summary” in the Bidding Sheets. Please clarify, if the detailed information distributed over several CLIN sheets in the Bidding Sheets are also equivalent to the SSS.	The native Excel version of the Book II SSS will be provided with AMD 3. However, all potential Bidders are once again strongly cautioned NOT to use the Book II model SSS to as the Bidding Sheet. Price Proposals shall only be constructed and submitted using the Book I final IFB version of the Bidding Sheet. The Purchaser makes no representations or guarantees regarding the Book II SSS vs. the Book I Bidding Sheets.	No	**AMD#3**

CR#519	Book I	3.2.4	Book I stated, that “Each Volume shall be in a separate binder or file for ease of segregation and handling…”. Due to technical issues in the case of big file sizes and because some Volumes will contain different file Formats (e.g. pdf/MS Word + MS Excel + MS Project), do you as the purchaser accept the provision of the Volumes regarding the softcopy (CD-ROM or DVD) in specific folders named after each volume, which contains more than one file or subfolders named after “Initial xy Plan” resp. named after headings of “Book I”?	The Purchaser would consider this proposed structure to be administratively compliant.	No	**AMD#3**
CR#520	Book I Book II	3.6.5.2.1.3 SOW 3.4.1.3	In “Book I”, purchaser requires an Initial Product Breakdown Structure (PBS) for the proposal as part of the Initial System Design Specification. For the project execution, SOW splits the products defined in the PBS, in management products (assigned to Project Management activities according to SOW section 3) and specialist products. Due to the requirement of “Book I” to assign the Initial PBS to the Initial SDS, we assume, that the Initial PBS for proposal purposes must only contain the specialist products which are linked to the Initial SDS and the system design. Is this assumption correct?	See CR#312	NO	**AMD#3**
CR#521	Book I Book II	3.6.5.3.3 SOW 13.14	In conjunction with the SOW, the System Implementation Plan (SPS) during project execution shall contain a site-specific design for each site with detailed installation, activation and migration plans as well as checklists. “Book I” requires that the Initial SIP for proposal purposes shall cover the entire implementation scope (SOW Annex C), in terms of sites and quantities of end-entities. This requirement of Book I in combination with SOW means from our perspective word-for-word, that 72 site specifc plans shall be delivered with the proposal, although most of the necessary site specific information are not known because their determination is part of the site surveys during project execution. Does purchaser accept for proposal purposes one generic site planning which contains e.g. the approach to make it concrete for the individual sites and/or metrics to define the expected effort of the different activities at the sites?	The Purchaser understands that site-specific details can't be provided at the bidding stage. The initial SIP shall be a single document covering the Bidders' approach for the entire project scope; and shall include at least one generic site-specific annex which demonstrates how the implementation at each site will be tackled. Site-specific implementation details will be determined during project execution.	NO	**AMD#3**

CR#522	Book I Book II	3.6.4.9.5 Book II Annex E	In conjunction with “Book I” bidders shall update the tables contained in “Book II SOW Annex E” and insert additional Purchaser Furnished Equipment as required. Considering the tables in SOW Annex E, Section 1 and 2, the PFE comprises Software, Property, Services and Documentation. NCIA requested in former NATO IFBs in their proposals three tables from bidders, which specifies Assumptions, Constraints and Obligations necessary to provide the proposed technical solution. We assume that the tables in Book II SOW Annex E express the same intention of purchaser and shall cover all project necessities (Assumptions, Constraints and Obligations) . Is this assumption correct or shall we hand in additional tables?	See CR#191. Bidders are no longer required to provide additional tables covering "Assumptions", "Constraints", and "Obligations".	YES (AMD 2)	**AMD#3**
CR#523	Book II Part IV	3.6.4.5.4	“Book I” requires that bidder provide with the proposal a description of individual skills and experience in relation to the project of all project team members and Subject Matter Experts (SMEs) foreseen to support the project team. Because in the Bid Phase the subsidiary team staff members in person are not known, we assume that this requirement is focused on Key Personnel, which has to be listed by name in Annex B-13 and for which CVs as well as their certificates shall be provided. Is this assumption correct?	Book I 3.6.4.5.4 relates to the individual skills and experience of all project team members and Subject Matter Experts (SME), not only Key Personnel. It is therefore advantageous for Bidders to provide as much information as possible concerning skills and experience, for both Key Personnel as well as implementation SME's.	NO	**AMD#3**
CR#524	Book I Book II	3.6.4.5.5 SOW 12 CR#66	“Book I” requires that bidder provide with the proposal supporting certification documentation (e.g. Prince 2 certificates) of each proposed Key Personnel, that meet or exceed the requirements in SOW Section 12. The combination of certificates for some Key Personnel is very exceptional. Does purchaser accept with no reduction in the technical evaluation, that single certificates will be acquired until EDC, when a respective commitment will be provided by bidder in the proposal?	The Purchaser will evaluate all the bids against the same criteria. The absence - from the bid - of required certificates could impact negatively the technical score.		**AMD#3**
CR#525	Book I	Annex A, Bidding Sheets	When opening “2A_IFB CO-13810-CS Book I Annex A Bidding Sheets AMD 1 FINAL.xlsx” with Excel 2007 an error message appear that unreadeble content was found in the file. After choosing the option recovery, a message appear that a named area was deleted in “/xl/workbook.xml-Part”. To prevent missing information please provide a Excel file without this issue resp. a Excel file which can be opened with Excel 2007 without a error message	The Bidder is instructed to contact the Purchaser POC via email on this compatibility issue.	No	**AMD#3**
CR#526	Book II	SOW 9.1.6.1 Book II, SSS	SOW para 9.1.6.1 stated „System Test Documentation Package delivered and approved by the Purchaser. This includes in particular: up-to-date test plan, up-to-date test procedures, up-to-date RTM.“ The SSS also refer to a RTM. Please clarify what RTM stands for.	RTM stands for "Requirements Traceability Matrix". SOW Section 4.5.2.1, 4.5.2.1.4, 13.8, and Annex D amended at IFB AMD3.	YES	**AMD#3**

CR#527	Book II Part IV	SOW Annex C	Especially the tables in Annex C Section 3 are important for internal calculation and it should be prevented that errors due to manual transmission causes incorrect calculations. Purchaser is kindly requested to provide the bidder with the tables in Annex C in Excel format.	The authoritative versions of those tables are the ones from the IFB (SOW Annex C). As a matter of courtesy, the tables in Excel format will be published at the same time as AMD3.	NO	**AMD#3**
CR#528	Book II Part IV	SOW Annex E	Purchaser is kindly requested to provide the bidder with the tables in “Book II SoW Annex E (PFE)” in Excel format so that they can be used as template for the proposal.	As a matter of courtesy, the PFE tables in Excel format will be published at the same time as AMD3.	NO	**AMD#3**
CR#529	Book II Part IV	SOW 10.4.3	Please clarify if site specific requirements, which have a cost impact and lead to an Engineering Change Proposal with formal contract amendment will increase the project budget.	Any ECP will become contractually applicable once confirmed by a contract amendment. Note that the cost impact may be positive, negative, or neutral.	NO	**AMD#3**
CR#530	Book II Part IV	SOW 10.4.1.3 SOW Annex C section 3	Please confirm, that an increase of the number of E-NPKI users and devices at the commissioned sites, which have a cost impact, will also result in a formal contract amendment to increase the project budget during volume verification in project phase.	Any required change to the contract will go through the ECP evaluation process (technical and contractual) and will become applicable only when confirmed by a contract amendment. See CR#529.	NO	**AMD#3**
CR#531	Book I Book II	Book I, para 3.6.5.3.4 Book II, SOW, para 13.14.2 13.14.1.5.4 13.14.1.5.5 13.14.1.5.6 13.14.1.5.7	The SIP shall include detailed information about installation, migration and activation of E-NPKI for each site and provide these plans with different Annexes specific for each site. Since the necessary site information are not known to bidder during offer phase and this information shall be evaluated e.g. during Site Survey, we assume that one generic Annex to the SIP, which demonstrates in which detail the implementation for each site will be planned, is sufficient for the proposal. Please confirm.	See CR#521.	NO	**AMD#3**
CR#532	Book II	SOW 3.10.2, 3.10.2.4 3.10.2.5 3.10.3 3.10.3.2 3.10.3.4	We assume that the required rights of Purchaser’s IV&V Contractor and/or the NCI Agency IV&V Service Line comprise technical activities and participations in context of E-NPKI project and do not comprise business subjects in context of E-NPKI project. Is this assumption correct?	The SOW (section 10.2 in particular) describes the activities related to IV&V.	NO	**AMD#3**
CR#533	Book II	SOW Annex A Figure 2 and slides 96 and 46 of NATO presentation at Bidders conference	Figure 2 gives the impression that each subordinate CA should have a local backup-CA at the same location and security domain (in analogy to the Root CA). Slide 46 of the NATO presentation at the Bidders conference states that “Certificate Authorities shall provide redundancy for each other for all CA services (automated failover) within a security domain”. Slide 96 says that the total number of CAs is 14 including backup CAs. But 14 is already the number of primary CAs plus ref/test CAs. We conclude that NATO does NOT require local backup-CA systems, but instead requires failover between the primary CAs within the same security domain in the three datacenters. Is this correct ? If not, do you require local backup CAs as well as failover between the three datacenter locations within the same domain?	The purchaser's requirement is to deploy 14 CA services. The purchaser does not constrain the bidder's design of an individual CA presence at a site. E-NPKI will be deployed across 2 security domains. A security domain does not equate to a single site. Figure 2 (updated at AMD3) refers to subordinate CAs within each domain, not each site. No mention is made regarding local backup or clustering. Within a single domain at a site, the contractor is to define the components (for example clustering or backup if required) to meet the performance and availability requirements for that CA. It is for the bidder to determine what software and hardware composition is required for a CA . See CR#12 and CR#84 Figure 2 was updated at AMD3	YES	**AMD#3**

CR#534	Book II	SOW Annex A Figure 2 and slides 96 and 46 of NATO presentation at Bidders conference	If our conclusion from the previous question is correct, this mechanism will not work for the SSL Root CAs for signing SSL Interception proxy certificates. These Root CAs are offline and therefore cannot provide backup for each other. Does NATO require local backup-Root CAs for each of these two offline Root CAs?	The Offline CAs will require a different strategy to meet the requirements. It is up to the bidder to propose a design demonstrating meeting requirements including availability and SLA. See CR#12 and CR#84 and CR#533	NO	**AMD#3**
CR#535	Book II	SOW 5.5.1.1	Contractor is not required to provide consumables for existing CMS systems (e.g. ink for the printers). Please confirm. If not, please provide a detailed list of the existing CMS installations together with technical information about the attached printers.	The contractor is not required to provide consumable for existing CMS systems.	NO	**AMD#3**
CR#536	Book II	SOW Annex A SRS-2611	For securing the communication between E-NPKI components and NATO components, certificates are needed. Shall these certificates be provided by the same subordinate CAs, which issues End-Entity certificates or shall they be issued by separate E-NPKI subordinate CAs?	The E-NPKI service is based on distributed system. It is therefore expected that NATO system will not be bound to a single subordinate CA. This imply that any subordinate CA can sign any NATO system certificate requests.	NO	**AMD#3**
CR#537	Book II	SOW 6.6.5	Contractor shall deliver consumables (i.e. smartcards and associated printer consumables, and certificates), at a central location to be defined by the Purchaser, on top of the estimated quantities mentioned in ANNEX C SECTION 3 ." Shall Contractor also deliver smartcard readers on top of the estimated quantities mentioned in ANNEX C SECTION 3?	Smartcard readers are not considered as consumables. See also CR#220.	NO	**AMD#3**
CR#538	Book II	SOW 12.1.4	Is a valid NATO CTS clearance required for contractor personnel doing initial system installations and integrations in the SECRET domain during the site implementation?	See CR#317	NO	**AMD#3**
CR#539	Book II	SOW Annex A SRS-1174	"E-NPKI shall be dimensioned and configured to scale in performance to support a 10% increase in subscribers and devices per year at each site and a 30% growth in data a year for 10 years without degradation of performance." A 10% increase in subscribers per year implies a 10% increase in smartcards and smartcard readers per year. Are these additional cards and readers reflected in the user lists? If not, shall those additional parts be provided in the BASIC contract for the first five years of operation?	The 10% increase per year in number of certificates and 20% per year in smartcard consumables are to be included in the bidders O&M submission for the 5 years O&M. Assumption regarding card readers is not correct. The bidder shall include the 30% annual growth in data for 10 years as part of their Firm Fixed Price offer.	NO	**AMD#3**
CR#540	Book II Part IV	SOW 16.7.3.2	Does migration of interim-PKI users mean that user registration data from interim-PKI has to be migrated to E-NPKI? If not, does migration mean that subscribers and sponsors need to register at the E-NPKI before requesting E-NPKI certificates?	a - There is no intent to manually re-enter existing information, and existing information will need to be migrated from the existing systems to the E-NPKI. This will include LDIF exports; other information can be read from the directory using LDAP/LDAPS/ODBC. b - Yes, subscribers will need to register to capture identification information.	NO	**AMD#3**

CR#541	Book II Part IV	SOW Annex A SRS-XXX	Is there a need for any differences between certificate profiles of user identities in PBN (PAC and LAC) and in ON (LAC only) from your point of view? Both shall be requested by FIPS-201 compliant CMS systems.	The certificate profiles for FIPS 201 cards is not identical to the certificate profile for non FIPS 201. Certificate profile will be closely related, but some specific characteristics will differ depending on the smartcards.	NO	**AMD#3**
CR#542		Slides 38, 42 and 43 of NATO presentation at Bidders conference	Slide 38 illustrates that besides existing FIPS-201 compliant CMS systems, also existing non-FIPS compliant CMS systems shall be integrated with E-NPKI. Slides 42 and 43 contain illustrations from NATO projects which seem to describe integration with both types of CMS with the iNPKI. Please provide an explanation of the workflows and mechanisms of integration with the CMS systems.	Integration and associated workflows are specific to the individual pairing of the products involved. For such reason, bidders are requested to propose their own workflow and integration mechanism, without relying on existing one.	NO	**AMD#3**
CR#543	Book II Part IV	SOW 7.5.3.2	Is the contractor required to provide any smartcards or smartcard readers for the exercises? If yes, are the numbers contained in SOW Annex C Section 3?	For bidding purposes, the Bidders shall use quantities in SOW Tables 9 and 10. Smartcards and smartcard readers for exercises are covered in those tables.	NO	**AMD#3**
CR#544	Book II Part IV	SOW Annex C Section 3	Shall the ECC smartcards for PBN provide a dual card interface (ISO7816 and ISO1443)? Shall the ECC smartcards for ON provide a dual card interface (ISO7816 and ISO1443) or ISO7816 only?	For PBN, dual card interface, however the wireless interface is used by the Mifare DESFIRE chip. For ON, only ISO7816. See SRS-2838 and SRS-2824 updated in AMD2. See CR#152	NO	**AMD#3**
CR#545	Book II Part IV	SOW Annex C Section 2.1	Is it required to provide 4 CAs in the Reference System, together with 1 RA and 2 OCSP instances. Shall these be configured to simulate two data centers each with ON and PBN CA? If not, please explain which constellations shall be provided in the reference System.	4 CA are required : - 3 for the Simulation of 3 Datacentre on a single security domain. - 1 for the offline SSL interception CA.	NO	**AMD#3**
CR#546	Book II Part IV	SOW Annex C Section 2.1	Shall the reference system also provide a CMS?	yes, to match the CMS provided by the contractor for the ON environment.	NO	**AMD#3**
CR#547	Book II Part IV	SOW Annex C Section 2.1	Is it required to provide 2 CAs in the NATO Testbed, together with 7 RA and 1 OCSP instances. Shall the Testbed be installed during Workpackage 3 (System implementation)?	See SOW, Table 8. Location for RAs to support training requirements are also identified in SOW Table 8. The testbed will be installed under WP3 (see "Delivery per site" tab of the Bidding sheets).	NO	**AMD#3**
CR#548	Book II Part IV	SOW Annex C Section 2.1	Shall the Testbed provide a CMS? If yes: in which location?	yes, Mons (Belgium)	NO	**AMD#3**
CR#549	Book II Part IV	SOW Annex C Section 2.1	Shall the Testbed provide HSMs for CA key operations or may HSMs be replaced by Software Key Stores? If not, may these HSMs provide lower capacities than required for the production environments (this means lower costs)?	See CR#299	NO	**AMD#3**

CR#550	Book II Part IV	SOW 3.5.3.2 SOW 3.5.3.3	Regarding conducting risk management during the project, the SOW determines, that likelihood and impact of a risk shall be assessed in three stages (high, medium, low). Our company conducts risk management according to PMBoK® and PRINCE2 and supports this by tools, management training and experts. This established risk management applies more and detailed stages: 11 for the probability (=likelihood) and 4 for the severity (=impact). With this granularity a configurable 11*4 metric is build up to rate the risk as high, medium or low as required by the SOW. We evaluate a 3*3 metric as not meaningful for a balanced risk assessment. Does purchaser also accept a risk management with an assessment of likelihood and impact of risks in more than 3 stages?	The bidders are advised that their approach to risk management will be evaluated and scored as part of the technical evaluation. Any deviation from the IFB requirements may or may not impact negatively the technical score in this area.	NO	**AMD#3**
CR#551	Book I	Annex B-12 (b)	Please clarify if e.g. RAM-Storagemodules, Hard Drive Disks or CPUs, which will be spare parts during operation and maintenance, are also sub-assemblies, which shall be manufactured or assembled by a firm from and within a participating NATO member country.	The Purchaser considers a sub-assembly to be a portion of an assembly consisting of two or more parts that can be provisioned and replaced as an entity. It is the Bidders responsibility to determine if the equipment in question meets the eligibility requirements of the IFB.	NO	**AMD#3**
CR#552	Book I	Annex B-12 (b)	Please clarify if sub-assemblies can include integrated circuits or SMD (e.g. resistors, transistors, microcontroller), which are manufactured by a firm within a country, which is not NATO member.	See CR#551	NO	**AMD#3**
CR#553	Book II Part IV	SOW 6.3.4.5 SOW 6.3.4.6	Book I para 6.3.4.5 requires Manuals in order to replace or perform maintenance. Book I para 6.3.4.6 requires the provision of a substitution, if the Original Equipment Manufacturer Manuals do not exist, or are inadequate in detail, and we assume that this substituting manual has same objective: Support of replacement or maintenance. Therefore we assume that the level of detail of substituting manuals shall support replacement and maintenance and shall not support detailed engineering understanding of the functionality of all components, units and sub-units (e.g. microprocessors). As a result of this assumption substituting manuals must not have in all cases the level of detail as it is specified in Book I para 6.3.4.6. Are these assumptions correct?	The assumptions are correct.	NO	**AMD#3**
CR#554	Book II Part IV	SOWAnnex C, sec 1	Please clarify if a “Additional Site” (WP 19) might also be at a country which is an operational theatre.	CLIN#19 may also apply to operational theatre sites. See also CR#227.	NO	**AMD#3**

CR#555	Book II Part IV	CR#22, SOW Annex B 4.1.2 4.1.3 4.1.4 4.1.5	CR#22 clarified, that purchaser's "intention is not to have the contractor duplicate existing ITSM tools. The Contractor shall provide integration and licenses as required for those tools already installed in the purchaser's environment" and SOW Annex B para 4.1.2 was amended accordingly. Due to the requirements in SOW Annex B para 4.1.3 and 4.1.4 we assume, that additional instances of the ITSM tools shall be installed, operated and maintained at customers premises/environments. Please clarify, if Purchaser will provide the contractor the manuals, documentation, configurations and customizings of the ITSM Tools currently in use by NATO, so that the identical tools with the same or adjusted configuration and customizings (e.g. datamodels, workflows, dashboards, KPIs, …) as well as interfaces can be operated by customer on its premises with own commercial licences.	The Purchaser is unable to make a firm commitment at this stage on the specific topic raised. This would likely be a discussion point during pre-award discussions (post source-selection) or at the kick-off meeting (post contract award) or later during project execution.	NO	**AMD#3**
CR#556	Book II Part IV	SOW 1.6.2.4	We assume that NEDS is not completely implemented on the Operational Network and Protected Business Network. If this assumption is correct please clarify if NEDS will be completely implemented on the Operational Network and Protected Business Network when starting the E-NPKI implementation with Work Package 3.	NEDS is already operational on ON and the PBN deployment is planned to be completed end of 2017. E-NPKI WP3 is planned to start mid-2018 and should therefore not conflict with NEDS availability. Both project schedules will be under regular scrutiny during contract execution to ensure coherence.	NO	**AMD#3**
CR#557	Book II Part IV	SOW 1.6.3.1	We assume that IEG is not completely implemented at this time. If this assumption is correct please clarify if IEG will be completely implemented when starting the E-NPKI implementation with Work Package 3.	The E-NPKI deployment is not dependent upon the availability of the IEG.	NO	**AMD#3**
CR#558	Book II Part IV	SOW 4.5.3.1.10	In respect of the prospective Firm Fixed Price Contract please clarify the intention and the required level of detail regarding the "Cost considerations", which shall be included in the Design Reviews.	SOW 4.5.3.1.10 is to be understood as any cost elements that the Contractor would need to consider as the design stage. For example, the design activities may have identified change requests (for example further to the site surveys) for which the cost factor must be considered.	NO	**AMD#3**
CR#559	Book II Part IV	SOW 4.1.6	Regarding the integration of the E-NPKI System with other NATO systems we assume that the responsibility of the E-NPKI contractor comprises the activities necessary on the E-NPKI system and the close collaboration with other contractors of NATO or NATO staff, which are responsible for the "other NATO systems", but not comprises any changes of the other NATO systems. Is this assumption correct?	The E-NPKI Contractor shall be responsible for the integration of the E-NPKI system with other systems and applications (see in particular SOW 1.6, SOW 4.1.6, SOW 5.5.6, SRS section 4.10, SRS-2813, SRS-2814, SRS-2831). This includes adaptations of the E-NPKI system as well as coordination with external systems and applications. The E-NPKI Contractor shall not be responsible to make changes to external systems identified in SOW 1.6. But the E-NPKI Contractor shall be responsible to make changes to other external systems identified in the IFB.	NO	**AMD#3**
CR#560		Terms and Condititions	Terms and Condititions provide that liabilities are unlimited; could NCIA set a limitation to the repair of direct damages and to a reasonable amount, according to a rule that you determine?	See answer at CR#34. The Bidder may find it useful to acquaint themselves with the treatment of this topic under the governing Belgian commercial law.	NO	**AMD#3**

CR#561		Audit rights	Concerning audit rights, our understanding is that NATO/NCIA have the right to audit “books, records, documents and other supporting data” that is related to the scope of the contract and supplied services. Please confirm or clarify our understanding.	With reference to Contract General Provision 40.14, your stated understanding is correct. The normal business practice of the NCI Agency is that any necessary audits are most frequently conducted by national audit authorities. Please note as well General Provision 28 – “Right of Access, Examination of Records”.	NO	**AMD#3**
CR#562		License T&C	Terms and Conditiitions: Can NATO/NCIA introduce license terms and conditions on the third party’s rights or existing contractor’s rights as well?	The contract General Provisions contain terms for contractor background. As already stated in the General Provisions, for Third Parties the Purchaser can accept terms from companies, but the Bidder (Prime contractor) has a duty to negotiate terms (in subcontracts) that are in-line with the prime contract. For contractor background IPR, Bidders are to ensure that they license such background IPR to the NCI Agency in line with the contract requirements, in particular the provision on Contractor Background IPR.	NO	**AMD#3**
CR#563		Instructions, Annex E, BRCM	It is unclear why the matrix requires instructions to be split according to the annex containing the relevant requirements (Annex A, B or C). Could you please clarify logic for filling in the matrix? Also, can you confirm each numbered line/paragraph must appear in the matrix, even when it's a mere heading?	The "Reference document" column is used to filter the requirements by documents. Mere headings are not required in the matrix. See CR#4 and CR#530	NO	**AMD#3**
CR#564		SOW 9.3.6.3.5	Can NCIA provide the ICD referenced in the requirement?	As stated in 4.5.2.1.2.8, the bidder shall develop the ICD in accordance with section 13.17. The template is provided on the CD under 2.1.8.1 (see CR#115)	NO	**AMD#3**
CR#565	Book I	IFB 3.6.5.5.3.1 initial SRA	Our undestanding is that bidders are required to provide a description of and confirmation that the proposed solution is compliant to the security requirements (SOW Section 11 and Annex A SRS) and NOT to provide an initial SRA, which will only be performed after contract award and using the PILAR tool to which the new contractor will be given access following contract signature.	Assumption is not correct. Initial Security Risk Assessment is required to be provided in Bid response as per Book I 3.6.5.5.3. However, the use of PILAR is not mandatory at Bid response. The quality and completeness of the Initial Security Risk Assessment will be assessed during the technical evaluation (see Book I 4.5.3.1.1.3) . See also CR#101.	NO	**AMD#3**
CR#566	Book II Part IV	SOW 6.4.3	The section reads "… The data for this shall be otained….": Could you specify to which word "this" refers: is it the training requirements analysis (in which case, how should we understand "the data for the TRA shall show the mapping between the results of the TRA?") or the Traning program?	During site surveys it would be expected that the Bidder would interview staff to be trained, to ascertain their skill levels. Such data would then be used as input to the TNA, to identify the gap between the current knowledge of the staff, and the level required to operate/maintain the Bidders solution (gap analysis). The TNA would be the basis for the training program. TRA replaced by TNA at AMD2.	NO	**AMD#3**
CR#567		Bi-SC 75-7	References are made to several annexes, which are listed in the table of content of Bi-SC 75-7, but are not included in the file we could find on the Internet. Could we be provided with those?	The document is included on the CD (2.1.7.2). See CR#115	NO	**AMD#3**
CR#568		Bi-SC 75-7, p. 2-5	Reference is made to http://www.e-nato.net/ - but the link does not seem to work. Could we be provided with access to it?	Access cannot be provided. The link was deprecated, therefore bidders shall not consider this link	NO	**AMD#3**
CR#569	Book I	Instructions to Bidders 3.6.4.6.3.1	Can the Purchaser confirm the reference should read 13.15 and not 13.?	Correct. Book I 3.6.4.6.3.1 updated according at AMD3.	YES	**AMD#3**

CR#570	Book I Book II Part IV	Instructions to Bidders 3.6.4.6.4 SOW 3.4	The Instruction to bidders is requesting a WBS while the SoW makes no reference to such requirement nor is it included in the PMP structure in 13.15. Can the purchaser confirm a WBS is required and in which section of the PMP it should be placed?	See CR#461.	NO	**AMD#3**
CR#571	Book II Part IV	SOW 6.5.2.1 CR#23	Can the purchaser confirm the answer on CR includes the tokens (smartcards) as these are considered a storage device for the certificate? Can the Purchaser further confirm that, based on the answer, any backup media like tape drives or hard disks (or any other generic storage media) involved in the storage of certificates is to be considered as items identified under SDIP293/1 and therefore have to be transported under crypto logistics precautions, even though these could be plain COTS items normally not affected by SDIP293/1 until first use?	1 - As CR#23 mentions "the document SDIP 293/1 is applicable to all keyed certificate generation and storage devices." 2 - See point 517 of the SDIP 293/1 and additional mentioned references. Publically available COTS like tapes, hard drive, smartcards are only considered to be basic crypto equipment until configuration/keying/use is started. They shall follow NATO classification based transport precautions. These items will be considered Controlled cryptographic item (CCI) when configuration/keying/use is started, and shall follow the SDIP 293/1	NO	**AMD#3**
CR#572	Book II Part IV	SOW 3.9.3.5	Can the Purchaser confirm that the reach service, if provided to the bidder, will be free of charge to the bidder?	The provision of a REACH Capability, and associated costs, will be discussed after the source selection decision is complete. For bidding purposes it is not necessary to factor in any costs for provision of REACH services.	NO	**AMD#3**
CR#573	Book I	2.16.1	Does NCI Agency consider CMMI Level 3 certification to be an equivalent QA/QC regime to AQAP 2110 and ISO 9001:2008?	CMMI is appraised but not certified. The bidder may follow the CMMI practices but there is no CMMI certification . ISO certification is requested in the Bidding instructions and therefore CMMI appraisal do not meet the certification requirement. However AQAP 2011 is not related to CMMI and ISO certification.	NO	**AMD#3**
CR#574	Book I	Annex B-16	To satisfy the requirement for B-16 our response will have to be in the form of a letter from our NCSA. To help prevent misunderstanding for all parties, can NCIA please provide the key aspects and scope that will be needed in the NCSA response for compliancy?	See answer at CR#212. The NCSA shall provide substantially the same information as is called for on the Annex B-16 Certificate. The Purchaser will work directly with the NCSA to obtain confirmations in the event that existing national practices prohibit confirmation data to be transmitted via the Bidder. Equipment for the PBN shall be approved to provide confidentiality, integrity, and authentication security services for the protection of information up to and including NATO Restricted. Equipment for the ON shall be approved to provide integrity, authentication and need to know security services for the protection of information up to and including NATO Secret. The accredited NATO Secret ON environment includes separate encryption and security services.	NO	**AMD#3**

CR#575	Book I	Annex A	The 2B_IFB CO-13810-CS Book I Annex A Bidding Sheets AMD 2 FINAL.xlsx has been amended with the following additional sub-CLIN numbers: CLIN 2 : Added on Row 82 -> 2.7.18 - Site installation and Activation checklist CLIN 3 : Added on Rows 44 -> 3.3.2.23 - Training Materials CLIN 3 : Added on Rows 45 -> 3.3.2.24 - On-site training However the "Detailed CLIN Summary" tab does not contain those additional sub-CLIN numbers. Will NCIA add the missing sub-CLIN references into the "Detailed CLIN Summary" table and send a new amended Bidding sheets file?	Yes, the "Detailed CLIN Summary" tab was updated accordingly at AMD3.	YES	**AMD#3**
CR#576		CR#136	In which CLINs do we need to show Hardware (server, SAN, Load Balancer, Client PC, …) components?	Bidders shall refer to the "DELIVERY FORM" column in the CLIN Pricing Sheets for HW/SW/Labour allocations for each sub-CLIN element. The details of each item of Hardware shall be shown in the CLIN Price Breakdown Sheets in the Materials Section 1.	NO	**AMD#3**
CR#577		CR#136	Will the NCI Agency issue a new set of bidding sheets showing separate CLINs for Hardware?	No	No	**AMD#3**
CR#578		CR#67	Several PSA sites do not have an own RA, so the RA of an agency in the same location will be used. Is it correct that in these cases the coordination with one POC will be sufficient and the Contractor needs to do only one training, one testing, etc.?	Purchaser and Contractor shall constantly seek optimization during contract execution. Combination of training, testing, and of any other activities at a site will be welcome by the Purchaser, and will be aligned with the site points of contact.	NO	**AMD#3**
CR#579		CR#156	Is it accepted to consolidate the clients for registration and personalisation into one workplace?	Yes	NO	**AMD#3**
CR#580		CR#136, CR#88, CR#410	Can you please confirm that load balancer, SAN-storage, NAS for back-up solution, blade enclosure are PFE? If NOT, please clarify the relation to ITM.	See CR#440 and CR#450.	NO	**AMD#3**
CR#581	Book II	SRS-2828	SRS-2828 requests an availability of 99.5%, which requires a fully redundant system. In the document "Statement of Technical Characteristics of the NPKI AC/322-N(2008)0004", issued with the CD, the requirement is to switch to another location under certain circumstances. What are these circumstances?	The document AC322 N(2008) 0004 is mentioning : "The MTTR may be achieved via hardware redundancy, available spares, or logically from another NPKI site in certain circumstances." The bidder needs to justify his design and how he will achieve the requested service availability. And the point 7.8 of the AC322 N(2008)0004 is mentioning that the MTTR may be achieved by the implementing the mentioned mechanisms. See CR#27 for availability calculation	NO	**AMD#3**

CR#582	Book I	Bidders Instructions Annex A-2	Instructions for the Preparation of Bidding Sheets states that additional columns and sheets be inserted in the Bidding Sheets for a multi-currency bid. The excel file of Bidding Sheets only allows for one currency to be selected on the tab called Bidding Sheets Cover. Is this an error?	"If multiple currencies are included in the price offer, the following sheets shall be duplicated and not modified for each currency bid: 1) CLIN Summary Sheet, 2) Detailed CLIN Summary Sheet, 3) Site Summary Sheet and 4) Detailed CLIN Pricing Breakdown Sheets. In addition, for each additional currency, the Bidders shall add two columns ("Unit Price", and "Total Firm Fixed Price) in the CLIN X Pricing Sheets and change the currency in the header of the columns as necessary. Each Detailed CLIN Pricing Breakdown Sheet shall correspond to the CLIN X Pricing Sheet currency columns as appropriate." Book I Annex A-2 Section 5 was amended accordingly at AMD3.	YES	**AMD#3**
CR#583	Book I	Bidders Instructions Annex A-2	If one file is to be used for a multi-currency bid, is it acceptable for a bidder to insert a pricing summary sheet for the avoidance of any doubt over total price?	see CR#582	YES	**AMD#3**
CR#584	Book I	Bidders Instructions Annex A-2	For the avoidance of confusion, for a multi-currency bid, can a bidder submit completed Bidding Sheets per currency? If this is acceptable can the bidder also submit a pricing summary sheet for the avoidance of any doubt over total price?	see CR#582	YES	**AMD#3**
CR#585	Book I	Bidders Instructions Annex A-2	Where should the bidder insert its risk cost estimates in the Bidder Sheets?	Bidders shall include any risk in their bid price (Firm Fixed Price).	NO	**AMD#3**
CR#586	Book II	CR#11 SRS-460 SRS-2206	CR#11 refers to SRS-2198 which describes that the end to end availability of revocation services must be 99.5%. The answer states also that this refers to “the ability for an end entity at a site to find at least one available source of revocation data”. This leads to the availability of less than 99.5% for the revocation service within each data center. For the OCSP (as part of the revocation service) the requirements SRS-460 and SRS-2206 require an availability of 99.5% for each OCSP server. Please clarify if SRS-460 and SRS-2206 refer to each single OCSP server in a data center or for the whole OCSP service in one security domain (across all three data centers) as answered in CR#11.	The contractor shall meet a minimum of 99.5% availability within the datacentre as well as an end to end minimum availability of 99.5%.	NO	**AMD#3**
CR#587	Book II	SRS-592	SRS-592 reads : A minimum of two trusted roles shall be implemented and enforced within the E-NPKI RAs; Auditor and Operator requirement, but this is not in line with Figure 4 of the SRS file, E-NPKI Technical services, where at RA level, an Officer and an Auditor are presented. Should we understand this in line with SRS-2235 (If not implemented as a separate role, the functions of the E-NPKI Operator role shall be combined with a compatible role to be agreed by the System) and assume that the Operator role is carried out by the E-NPKI RA Officer?	SRS-592 was corrected at AMD#3 as follows: "A minimum of two trusted roles shall be implemented and enforced within the E-NPKI RAs; Auditor and Officer." This does not exclude a potential RA Operator role which responsibility is described in SRS 1.4.1.13.	YES	**AMD#3**

CR#588	Book I	Security Accreditation, Instructions to bidders 3.6.5.5.1.2	Description of how SRS requirements are implemented in the system. Could you clarify the scope of this requirement and how it relates to Security Accreditation. Confirm that requirement refers to Security Accreditation and in particular CPS strictly.	Yes, the requirement 3.6.5.5.1.2 applies to the Certification Practices Statements. The scope is defined in SOW 11.3.15.2.	NO	**AMD#3**
CR#589	Book I	Cryptographic equipment, 2B_IFB CO-13810-CS Book I Annex A Bidding Sheets	Could you clarify the delivery form for cryptographic equipment, shouldn't it be « HW » rather than « Electronic »? (the latter would apply to documentation, but not equipment)	Bidding sheets and SSS were corrected at AMD#3 as follows: "Hardware, Electronic"	YES	**AMD#3**
CR#590	Book II Part IV	SOW 13.7.1.1.2	Will the purchaser accept the NAF views in the SDS created in Visio format for the IFB response?	NAF provided in Visio format are acceptable for the IFB response. The Bidders shall note SOW 13.7.1.1.2.	NO	**AMD#3**
CR#591	Book II Part IV	SOW 1.6.2.4	1.6.2.4 states that NEDS will be installed on the PBN and ON networks. Question: Is the NEDS data between PBN and ON synchronized?	As mentioned in SRS-484, PBN and ON are separate infrastructures. For bidding purposes, Bidders shall assume that the NEDS will be available on both PBN and ON. The potential replication of NEDS data - from PBN to ON only (through a diode) - is irrelevant at this stage.	NO	**AMD#3**
CR#592	Book II Part IV	SOW 1.6.5.1 and 1.6.2.4	Can the purchaser confirm availability of a cross-domain data transfer solution under that E-NPKI will be allowed to use, should the bidders proposed design require the cross-domain functionality?	The E-NPKI project is aiming at hosting its services in the ITM provided infrastructure. However the purchaser cannot confirm ITM will be ready to provide IaaS in all locations E-NPKI systems will deploy. In addition, the purchaser cannot guarantee any cross domain data solution will be available where the E-NPKI system will be deployed, nor that such cross domain data transfer would be made available to the E-NPKI project. The bidder is requested to provide all prices for all hardware as mentioned in CR#136 and CR#440. NATO will determine in conjunction with the successful bidder, the appropriate components to be provided as Infrastructure as a Service (IAAS) by the ITM project. See also CR#592	NO	**AMD#3**
CR#593	Book II Part IV	Annex A3.10.2	SRS 2013 states E-NPKI RAs shall be capable of processing 200 new enrolment requests per day. Please clarify if this is expected from each RA at each of the sites? If answer to the above question is 200 for each RA, then for sites that have 2 RA's this will mean that site can process 400 enrollments per day. For an 8 hours working day, it is expected that each enrolment will be completed within approximately 2 minutes and 30 seconds. Given the workflow, and other activities to validate subscriber data, scan documents, collect biometrics (facial image, fingerprint) etc. purchaser is requested to provide realistic number for enrolments per day? Also please provide metrics about the time it takes to enroll one individual in the iNPKI system today. If the purchaser is not providing updated number for enrolments per day, please clearly define the scope for each enrolment.	The purchaser suppose the clarification request is for SRS-2103 and not SRS-2013. The requirement SRS-2103 is updated at AMD3. The value is changed from 200 to 100 new enrolment requests per day. The time for biometric captures is not included in the enrolment time as this is normally performed by the Physical Access Control Systems.	YES	**AMD#3**

CR#594	SRS, General question covering several requirements	SRS, General question covering several requirements	Following in-depth technical discussions with CA/RA vendors, it appears that the products in NIAPC do not fully meet some of N-PKI requirements. In those (rare) occurences, would it be acceptable to propose a deviation?	The NIAPC product list does not guarantee that a product will meet the E-NPKI requirements as it is meant for security accreditation purpose. The purchaser understands that some deviations to requirements may occur. As part of the Bid Evaluation process, the purchaser will review the technical proposal and deviations. The Purchaser will evaluate all the bids against the same criteria's, and deviations may impact negatively the evaluation and its associated score.	NO	**AMD#3**
CR#595	Book II Part IV	SOW-5.5.4.2.1, SOW-5.5.4.2.2 & SOW-5.5.4.2.3	The SoW requires the Contractor to undertake amendments of the SecOPs to comply with or take account of local security instructions. This requires an intimate knowledge of the local security instructions in place at each of the deployment sites or the reliance on the Purchaser to provide the information. Previous project approaches with NATO transferred the modification of "baseline" SecOPs to local NATO personnel which would be a non-compliant approach. Need to agree an arguably compliant approach whilst minimising Contractor to cost/schedule impacts.	The localised version of the SecOPs is under the responsibility of the Contractor. The Contractor shall liaise with local security accreditation authorities for the development and approval of the localised version of the SecOPs.	NO	**AMD#4**
CR#596	Book II Part IV	SOW-5.5.4.3.1, SOW-5.5.4.3.2 & SOW-5.5.4.3.3	The SoW requires the Contractor to undertake amendments of the SecOPs to comply with or take account of local security instructions. This requires an intimate knowledge of the local security instructions in place at each of the deployment sites or the reliance on the Purchaser to provide the information. Previous project approaches with NATO transferred the modification of "baseline" SecOPs to local NATO personnel which would be a non-compliant approach. Need to agree an arguably compliant approach whilst minimising Contractor to cost/schedule impacts.	Requirements SOW 5.5.4.3.1, SOW 5.5.4.3.2 and SOW 5.5.4.3.3 relate to SCCS, not SecOPs. The localised version of the SSCS is under the responsibility of the Contractor. The Contractor shall liaise with local security accreditation authorities for the development and approval of the localised version of the SSCS.	NO	**AMD#4**
CR#597	Book II Part IV	SOW-5.5.4.4.1, SOW-5.5.4.4.2 & SOW-5.5.4.4.3	The SoW requires the Contractor to undertake amendments of the SecOPs to comply with or take account of local security instructions. This requires an intimate knowledge of the local security instructions in place at each of the deployment sites or the reliance on the Purchaser to provide the information. Previous project approaches with NATO transferred the modification of "baseline" SecOPs to local NATO personnel which would be a non-compliant approach. Need to agree an arguably compliant approach whilst minimising Contractor to cost/schedule impacts.	Requirements SOW 5.5.4.4.1 , SOW 5.5.4.4.2 and SOW 5.5.4.4.3 relate to STVP, not SecOPs. The localised version of the STVP is under the responsibility of the Contractor. The Contractor shall liaise with local security accreditation authorities for the development and approval of the localised version of the STVP.	NO	**AMD#4**

CR#598	Book II Part IV	SRS-2644 (Orig) SRS-2839 (AMD 2)	These requirements both cover physical access control mechanisms for racks containing E-NPKI equipment, to be implemented by the Contractor. As the Purchaser has advised that it will be their responsibility to provide racks (CR#83 confirms), and the server rooms are also provided as PFF, can the Purchaser please review this requirement?	See CR#82 and CR#377. If additional racks were required, they will be provided through an amendment to the contract (ECP). Therefore the racks shall not be priced in the Firm Fixed Price offer. However, it is the responsibility of the Contractor to comply with SRS-2644 and SRS-2839 by providing logical and physical access control mechanisms as required. Therefore, the Bidders shall include in their Firm Fixed Price a provision for the furnishing and installation of additional security mechanisms, as necessary, to protect the racks and E-NPKI systems according to SRS-2644 and SRS-2839. Within the server rooms, the contractor shall further limit access control granularity to ensure only appropriate E-NPKI staff have access to the E-NPKI systems (E-NPKI systems shall be isolated in dedicated racks).	NO	**AMD#4**
CR#599	Book II Part IV	SRS-2644 (Orig) SRS-2839 (AMD 2)	These requirements both cover physical access control mechanisms for racks containing E-NPKI equipment, to be implemented by the Contractor. As the Purchaser has advised that it will be their responsibility to provide racks (CR#83 confirms), and the server rooms are also provided as PFF, can the Purchaser please review this requirement?	See CR#598	NO	**AMD#4**
CR#600	Book II Part IV	SRS-1757	What is the [CONFIGURATION TOOL] or tools to be interfaced to?	Requirement SRS-1757 is deleted due to duplication with SOW 15.7	YES	**AMD#4**

CR#601	Book II Part IV	SRS -834 SRS-857 SRS-858 SRS-2320 CR88 CR440 CR501 CR261 CR487	1. The purchaser is kindly requested to further clarify the BPD or BPS. CR88 clearly states that any BPD is out of scope. The bidder assumes therefore that any BPD devices that are currently part of its design to comply with SRS-834 & SRS-857 & 8 will be considered as PFE or out of scope. Please confirm that the mentioned BPD of SRS-834 is explicitly out of scope and shall not be included by the bidder as it request to be included in the requirement?. 2. CR440 is requesting to include pricing for "all components" yet pointing back to CR88 for out of scope BPD. Please confirm "all components" are not meant to include the BPD. 3. The bidder further assumes, that the host-based firewall of req SRS-2320 that will run on dedicated HW platforms (although some shared through virtualization) for the CA, RA and OCSP and timestamping service could be the built in WFAS (windows firewall, or any other software FW, if such a solution is chosen) and as such will be PFE as part of the windows server licensing. 4. Based on 3. The bidder would like to request the PFE list to be updated with the FIrewalls, or have confirmed that these items will become PFE as part of the windows license in order to avoid any confusion. 5. It is the bidders understanding that the purchaser is not expecting to have any network or HW based firewall priced in the proposed solution. The purchaser is kindly requested to confirm our assumptions and elaborate where necessary.	1+2: CR#88 clarifies that infrastructure BPD Firewalls are not to be included in the Firm Fixed Price offer. Therefore hardware and software costs for the BPD mentioned in SRS-834 are out of scope of the Firm Fixed Price. 3: As per CR#191 and CR#290, the PFE list is fixed. WFAS would be deemed as an acceptable solution for Windows based components and would then be covered under the PFE list. Any other Host based firewall solution is the responsibility of the Bidder and shall be included in the Firm Fixed Price offer. 4: As per CR#191 and CR#290, the PFE list is fixed. Any component not being part of the list shall be included in the Firm Fixed Price offer. 5: Yes, CR#88 already clarifies that infrastructure BPD Firewalls are not to be included in the Firm Fixed Price offer.	NO	**AMD#4**
CR#602	Book II Part IV	SRS-2805 SRS-1741 CR480	Can the purchaser kindly confirm no other operating system than Microsoft is allowed on any of the server environments for the E-NPKI system & solution in its totallity?, including i.e. any mangement functions, databases, proxys, load balancers or logging functions that could be running on a linux based server OS solution.	SRS-2805, SRS-1741 and CR#480 apply to E-NPKI services. E-NPKI components shall run on servers running - only - Windows operating system. COTS infrastructure components may be provided as appliances based on other kernels than Windows. However, COTS Software installed on servers shall be provided only on Windows OS servers.	NO	**AMD#4**

CR#603	Book II Part IV	CR450 CR472 CR136	1. The purchaser is requesting to have pricing included for all HW components but is stating that the solution will either be installed on the ITM IaaS or existing underlaying infrastructure per site, but also wants to include the pricing for all components regardless for bid evaluation purposes. Based on the clarification responses recieved it is therefore the bidders assumption that all cost should be included for infrastructure at time of bidding and then at award a decision will be taken as to whether or not these elements are removed from the PKI bidders proposed deliveries due to ITM for example, please confirm? 2. Please confirm, if for all HW components mentioned in point 1. all associated O&M cost should be included accordingly, in order to make the availability requirements, which would include dedicated spares, spares onsite and HW and software / Firmware support contracts for the components in question as part of the O&M clins.	1 - The bidder shall include in their Firm Fix Price offer all infrastructure hardware components required to deliver the E-NPKI services as per CR#440 and CR#450. Should a contract adjustment be necessary, either during pre-award discussions or after contract award, on the basis of the actual situation with regards to infrastructure, the detailed costs provided with the price offer in the CLIN Price Breakdown Sheets shall be used as the basis to adjust the contract price as necessary. It is for this reason that it is essential that Bidders shall provide full detail for all equipment and components in the CLIN Price Breakdown Sheets. 2 - yes, O&M costs for all infrastructure components shall be included as part of the O&M CLINs, and detailed in the CLIN Price Breakdown Sheets, for the same reason and purpose as described in 1 above. 3 - For clarification, the Book I Bidding Instructions, Book I Annex A Bidding Sheets and SSS have been updated (highlighted in purple) to address the pricing of the Warranty of any hardware or software.	NO	**AMD#4**
CR#604	Book II Part IV	CR451 SOW-1.4.4.4 16.8.5.1&2	With the card readers and the reference to "all equipment" the bidder would like to have clarified how this requirements sits in relation to the installation milestones of 16.8.5.1&2. It has been the bidder's assumption that the onsite installation activities would be limited to the migration of INPKI users, and 50 new users. The answer to the clarification CR451 now would suggest that bidder needs to install the card reader on each users and component individual system which would be nearly impossible as the purchaser's users and assets are not permanently onsite. THIs would force the bidder to stay for extended periods on sites in order to achieve the conclusion of the installation services, where bidder previously assumed that the onsite staff would take further new users onto the E-NPKI system after the initial 50 by the bidder. The purchaser is kindly requested their expectation of the bidders scope for onsite deployment of end user equipment, such as the card reader.	The contractor is responsible for the installation and configuration of all components (including card readers) for the new users and iNPKI users as mentioned in SOW 16.7.3.1&2 and SOW 16.8.5.1&2.	NO	**AMD#4**
CR#605	Book II Part IV	CR344 SOW 6.7.2 CLIN 3.3.2.16	Based on the answer of the clarification it is the bidders understanding that the RTTL as mentioned in Clin 3.3.2.16 will be priced for the creation of the list by itself, which then can then be activated for any item on the list under change management and that the complete list of spares and associated cost should not be included. It is the bidder's assumption that the cost for the tools is not to be included at bidding submission.	See CR#344. Spares are not considered as Standard Tools and Test Equipment, and therefore shall not be included in the RTTL. The cost of the RTTL items is requested to be provided with the technical (not price) offer, and should be excluded from the total bid price and cost ceiling calculations.	NO	**AMD#4**

CR#606	Book II Part IV	CR586 SRS-2189	The answer to the clarification questions creates the suggestion that the datacenter revocation service availability needs to be 99.5 which would be conflicting with req. SRS-2189 which calls for a availability of the services of 99.99%. Can the purchaser please confirm the availability of datacenters revocations services inclusive of OCSP and CRL should be 99.99% and how this differs form the answer in CR586.	The IFB takes into consideration that total availability of revocation information decreases as relying parties are located further from the datacentres or over less reliable links. OCSP availability requirements shall be understood as follows : - From within any Datacentre, the TOTAL end to end availability of any revocation information (CRL or OCSP) shall have 99.99% availability as per SRS-2189. - When a site is connected to datacentres via a dual redundant link, the availability of any revocation information (CRL or OCSP) shall be 99.5% as per SRS-2198. - When a site is connected to datacentres with a non-redundant link, the availability of any revocation information (CRL or OCSP) shall be 98% as per SRS-2199. - Each individual OCSP server component shall have at least 99.5% availability as per SRS-460.	NO	**AMD#4**
CR#607	Book II Part IV	Requirement ID: SRS-2161-2-3	Are bidders allowed to use other CMS providers or is it mandatory to stick to the listed ones (namely CITI, Entrust, XTEC)?	The purchaser assumes the bidder is referring to SRS-2161, SRS-2722 and SRS-2723. Accordingly, E-NPKI shall integrate with the CMS products referred to in SRS-2161, SRS-2722 and SRS-2723. Should this integration effort require additional components, the Contractor shall provide those components within the firm-fixed price of the contract. At sites where no FIPS-201 CMS exists at the time of E-NPKI implementation, the Contractor shall provide a CMS. In such a case, the Contractor is allowed to procure and implement any type (i.e. not limited to the types of CMS mentioned in SRS-2161, SRS-2722 and SRS-2723) of FIPS-201 CMS.	NO	**AMD#4**
CR#608	Book II Part IV	SOW 5.5.6	Could you please define the scope of the migration in terms of certified end-entities (e.g. physical user, functional users, routers, webservers, code signing, etc.)? Which of those end-entities need to be migrated?	See CR#139	NO	**AMD#4**

CR#609	Book II Part IV	SOW 6.4.1	What are the already existing mechanisms for DRP? How do you expect NPKI to integrate within those? Could DRP drills be organised in production environments?	1 - The current DRP mechanisms for the I-NPKI include, but are not limited to: - Daily electronic and physical backups, onsite and offsite to a backup location. - Recovery testing of the backups on the Testbed environment. - Switching system mode from Master to Slave between Main and Backup sites. 2 - A DRP was developed specifically for I-NPKI and is not part of a NATO wide DRP. The E-NPKI Contractor shall develop and implement a similar DRP for E-NPKI (see SOW 6.3.3 in particular). 3 - DRP drills on the production environment may be planned, based on approval following operational risk analysis. Frequent DRP drills are generally executed on the Testbed environment. SOW 6.4.1 relates to training: training activities for DRP shall not be performed on the production environment.	NO	**AMD#4**
CR#610	Book II Part IV	SOW 6.4.11	May we use the reference system as back-end for training and reachable in all sites requiring training?	The Bidders shall distinguish between two types of trainings: 1. On-site training which will be performed during implementation activities. 2. Recurring training which will be performed during operation & maintenance phases. Training activities (on-site or recurring) shall NOT be performed on the reference environment. On-site training activities will be performed on two possible environments: 1. Contractor-provided equipment (see SOW 6.4.11), especially if the Testbed is not available 2. Testbed. The bidders shall note that the Testbed is planned to be implemented between PSA and FSA (see SOW Annex C Section 1). Therefore, the Testbed will NOT be available for training activities before PSA. Recurring training activities will be performed on the Testbed (see SOW 7.5.2 in particular). The Training Plan shall define which environment will be used for which training.	NO	**AMD#4**

NATO Communications and Information Agency
Agence OTAN d'information et de communication

Provide Enterprise NATO Public-Key Infrastructure (E-NPKI)

AMD 4 TO IFB-CO-13810-CS

BOOK I

INSTRUCTIONS TO BIDDERS

TABLE OF CONTENTS

1 INTRODUCTION 4
1.1 Purpose and Scope 4
1.2 Overview of the Prospective Contract 5
1.3 Governing Rules, Eligibility, and Exclusion Provisions 5
1.4 Security 6
1.5 Bidders Conference 7
1.6 Documentation 8
2 GENERAL BIDDING INFORMATION 9
2.1 Definitions 9
2.2 Eligibility and Origin of Equipment and Services 10
2.3 Bid Delivery and Bid Closing 10
2.4 Requests for Extension of Bid Closing Date 11
2.5 Purchaser's Point of Contact 12
2.6 Request for IFB Clarifications 12
2.7 Requests for Waivers and Deviations 13
2.8 Amendment of the Invitation for Bid 14
2.9 Modification and Withdrawal of Bids 14
2.10 Bid Validity 15
2.11 Bid Guarantee 15
2.12 Cancellation of Invitation for Bid 17
2.13 Electronic Transmission of Information and Data 17
2.14 Supplemental Agreements 17
2.15 Notice of Limitations on Use of Intellectual Property Delivered to the Purchaser 18
2.16 Mandatory Quality Assurance and Quality Control Standards 18
3 BID PREPARATION INSTRUCTIONS 20
3.1 General 20
3.2 Bid Package Content 20
3.3 Package Marking 21
3.4 Administrative Documentation Package 21
3.5 Price Quotation 23
3.6 Technical Proposal Package 27
4 BID EVALUATION AND CONTRACT AWARD 39
4.1 General 39
4.2 Best Value Award Approach and Bid Evaluation Factors 40
4.3 Evaluation Procedure 41
4.4 Evaluation Step 1 - Administrative Compliance 42
4.5 Evaluation Step 2 - Technical Evaluation 43
4.6 Evaluation Step 3 - Price Evaluation 45
4.7 Evaluation Step 4 – Calculation of Best Value Scores 47
Annex A Bidding Sheets 1
Annex B Prescribed Administrative Forms and Certificates 1
Annex C Bid Guarantee - Standby Letter of Credit 1

Annex D **Clarification Request Form** **1**

Annex E **Bid-Requirements Cross Reference Matrix (BRCM)** **1**

1 INTRODUCTION

1.1 Purpose and Scope

1.1.1 The E-NPKI project is intended to provide the Alliance with a set of security services enabling confidentiality, integrity, authentication, and non-repudiation. It will provide the key and information management functions to other CIS (Communication and Information System) security services by means of lifecycle certificate management.

1.1.2 E-NPKI will eventually replace the Interim-NPKI system currently in use within NATO.

1.1.3 The E-NPKI infrastructure will be made up of several components/services: certificate authorities, registration authorities, revocation services, end entity support (tokens, clients, etc.), security and audit tools, software etc...

1.1.4 The E-NPKI project scope spans across the NATO Enterprise, and thus will enable the provision of E-NPKI Services to the sites as listed in Book II SOW Annex C.

1.1.5 The Services to be provided by the E-NPKI include (see details in Book II SOW Annex B):

1.1.5.1 Business Services: CA Service, RA Service, Certificate Status Validation Service, End-Entity Service;

1.1.5.2 Support Services: Configuration Management Service, Change Management Service, Incident / Problem Management Service.

1.1.6 The E-NPKI will be implemented on two (2) security domains (separate networks):

1.1.6.1 ON (Operational Network): up to NATO SECRET,

1.1.6.2 PBN (Protected Business Network); combining both NATO RESTRICTED and NATO UNCLASSIFIED.

1.1.7 The list of End-Entities (or “User List”) is provided in Book II SOW Annex C.

1.1.8 The E-NPKI project scope will include:

1.1.8.1 Project management;

1.1.8.2 Requirements Analysis, System Engineering/Design, Testing, Site Surveys;

1.1.8.3 Security accreditation;

1.1.8.4 Site implementation (i.e. E-NPKI components deployment), including transition from Interim-PKI to E-NPKI;

1.1.8.5 Integrated Logistics Support (ILS), including Training;

1.1.8.6 Operational Support (Hardware, Software, Manpower) from PSA to 5 years after FSA; as contract options.

1.1.9 The E-NPKI components will be divided into 2 blocks:

1.1.9.1 Technical Services i.e. back-end components (e.g. Certificate Authorities, Registration Authorities, Online Certificate Status Protocol (OCSP) servers), and;

1.1.9.2 User Services i.e. front-end components (see “User List” in Book II SOW Annex C).

1.2 Overview of the Prospective Contract

1.2.1 The Prospective Contract (Book II) requires the selected Contractor to deliver the E-NPKI capability and associated services. The Contractor shall perform all activities required as per Book II Part IV (Statement of Work – SOW) and shall deliver the associated deliverables as per Book II Part I (Schedule of Supplies and Services – SSS). The Contractor’s work encompass the activities described in Section 1.1.8 above). Final System Acceptance (FSA) for the main implementation contract is scheduled for 132 Weeks after Effective Date of Contract (EDC), with follow-on Operation and Maintenance support Options.

1.2.2 The Contract will be governed by Book II, Part II (General Provisions), and Part III (Contract Special Provisions - CSP).

1.3 Governing Rules, Eligibility, and Exclusion Provisions

1.3.1 This solicitation is an International Invitation for Bid (IFB) and is issued in accordance with the procedures for International Competitive Bidding set forth in the NATO document AC/4-D/2261 (1996 Edition).

1.3.2 Pursuant to these procedures, bidding is restricted to companies from participating NATO member nations (see Para 2.1.1.5) for which a Declaration of Eligibility has been issued by their respective government authorities.

1.3.3 Best Value Evaluation Method

1.3.3.1 The evaluation method to be used in the selection of the successful Bidder under this solicitation shall follow the Best Value Procedures set forth in AC/4-D(2008)0002-REV1 dated 27 April 2009 and AC/4(2008)0002-REV2 dated 15 July 2015.

1.3.3.2 The bid evaluation criteria and the detailed evaluation procedures are described in Section 4.

1.3.4 This Invitation for Bid will not be the subject of a public Bid opening.

1.3.5 The Bidder shall refer to the Purchaser all queries for resolution of any conflicts found in information contained in this document in accordance with the procedures set forth in Section 2.6 "Request for IFB Clarifications".

1.3.6 Prospective Bidders shall note that the Purchaser reserves the right to exclude the successful Bidder and its prospective Sub-Contractors from the award of this Contract if the successful Bidder or its prospective Sub-Contractors have been selected for the work performed or to be performed under the BI-SC AIS Programme Management and Integration Capability (PMIC) Contract. This applies also to the Contractor's/Sub-Contractor's parent companies or subsidiaries unless the parent company or its subsidiaries will provide proof that they operate as a separate legal entity in a completely distinguishable and different business domain from that of the PMIC. Such evidence shall be presented in accordance with the prescriptions of Section 3.4.4.1 and shall be subject to the administrative evaluation detailed in Section 4.4.1.5.

1.4 Security

1.4.1 Contractor will be required to handle and store classified material to the level of "NATO SECRET" and the Contractor shall have the appropriate facility and personnel clearances. Should a Contractor be unable to perform the contract due to the fact that the facility clearance has not been provided by their respective national security agency, this lack of clearance cannot be the basis for a claim of adjustment or an extension of schedule, nor the lack of clearance be considered a mitigating circumstance in the case of an assessment of Liquidated Damages or a determination of Termination For Default by the Purchaser.

1.4.2 Contractor personnel working at NATO sites are required to possess a security clearance of "NATO SECRET". Contractor personnel without such a clearance, confirmed by the appropriate national security authority and transmitted to the cognisant NATO security officer at least fourteen (14) days prior to the site visit, will be denied access to the site. Denial of such access by the Purchaser may not be used by the Contractor as the basis for a claim of adjustment or an extension of schedule nor can the denial of access be considered a mitigating circumstance in the case of an assessment of Liquidated Damages or a determination of Termination for Default by the Purchaser. Contractor personnel who need System Administrator privileges when working on NATO SECRET systems shall be required to hold NATO CTS clearances (see SOW Section 12).

1.4.3 Bidders are advised that contract signature will not be delayed in order to allow the processing of security clearances for personnel or facilities and, should the

otherwise successful Bidder not be in a position to accept the offered Contract within a reasonable period of time, due to the fact that its personnel or facilities do not possess the appropriate security clearance(s), the Purchaser may determine the Bidder's Offer to be non-compliant and offer the Contract to the next ranking Bidder. In such a case, the Bidder who would not sign the Contract shall be liable for forfeiture of the Bid Guarantee.

1.5 Bidders Conference

1.5.1 Prospective Bidders are invited to a Bidders Conference that will be held between four to six weeks after IFB release in Brussels. The Purchaser will notify all Bidders of the final date and time. Registration forms and relevant information will be provided at the time of notification.

1.5.2 The purpose of the Bidders Conference will be to present the Project, and present the key members of the Purchaser project management team, as well as to allow the Prospective Bidders to clarify aspects of the Invitation for Bid for which they may have questions at that time.

1.5.3 The Bidder's Conference is planned to include a briefing on the bidding process; the bidding sheets; the prospective contract; and the technical and project management aspects of the project.

1.5.4 The participation to the Conference is limited to a maximum of two (2) attendees per Bidder. No exception to this number of attendees will be made. A detailed agenda for the Bidder's Conference will be sent to the participating companies in due course.

1.5.5 The potential Bidders may submit questions in writing not later than 7 days prior to the date of the Conference to the POC, at the address mentioned under Section 2.5.1 "Purchaser Point of Contact. The Purchaser will endeavour to respond to the previously submitted questions at the Bidders Conference. If any additional questions are asked by the potential Bidders at the Bidders Conference, the Purchaser might attempt to answer them at that time, but any answer that might appear to amend terms, conditions and/or specifications of the Contract shall be considered to be formally included in the Invitation for Bid only when a written amendment to the IFB issued in writing by the Purchaser.

1.5.6 Answers to all questions will be issued in writing to all Bidders as soon as practicable after the Conference, whether or not the Bidders attended the Conference. The formal written answers will be the official response of the Agency, even if the written answer differs from the verbal response provided at the Conference.

1.5.7 Notwithstanding the written answers provided by the NCI Agency after the Bidders' Conference, the terms, conditions and language of the IFB remains unaltered unless a formal IFB amendment is issued by the NCI Agency and is identified as such.

1.6 Documentation

1.6.1 All documentation, including the IFB itself, all applicable documents and any reference documents provided by the Purchaser are solely to be used for the purpose of preparing a response to this IFB. They are to be safeguarded at the appropriate level according to their classification and reference documents are provided “as is“, without any warranty as to quality or accuracy.

2 GENERAL BIDDING INFORMATION

2.1 Definitions

2.1.1 In addition to the definitions and acronyms set in the Contract Special Provisions (Part II) of the prospective Contract, and the definitions and acronyms set in the Clause entitled “Definitions of Terms and Acronyms” of the Contract General Provisions (Part III) of the prospective Contract, the following terms and acronyms, as used in this Invitation for Bid shall have the meanings specified below:

2.1.1.1 "Bidder": a firm, consortium, or joint venture which submits an offer in response to this solicitation. Bidders are at liberty to constitute themselves into any form of Contractual arrangements or legal entity they desire, bearing in mind that in consortium-type arrangements a single judicial personality shall be established to represent that legal entity. A legal entity, such as an individual, Partnership or Corporation, herein referred to as the “Principal Contractor”, shall represent all members of the consortium with the NCI Agency and/or NATO. The “Principal Contractor” shall be vested with full power and authority to act on behalf of all members of the consortium, within the prescribed powers stated in an irrevocable Power of Attorney issued to the “Principal Contractor” by all members associated with the consortium. Evidence of authority to act on behalf of the consortium by the “Principal Contractor” shall be enclosed and sent with the Bid. Failure to furnish proof of authority shall be a reason for the Bid being declared non-compliant.

2.1.1.2 "Compliance": strict conformity to the requirements and standards specified in this IFB and its attachments.

2.1.1.3 "Contractor": the awardee of this solicitation of offers, which shall be responsible for the fulfilment of the requirements established in the prospective contract.

2.1.1.4 “Firm of a Participating Country”: a firm legally constituted or chartered under the laws of, and geographically located in, or falling under the jurisdiction of a Participating Country.

2.1.1.5 “Participating Country”: any of the NATO nations contributing to the project, namely, (in alphabetical order): BELGIUM, BULGARIA, CANADA, CZECH REPUBLIC, DENMARK, ESTONIA, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, THE NETHERLANDS, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, TURKEY, THE UNITED KINGDOM and THE UNITED STATES.

2.1.1.6 “Quotation” or “Bid”: a binding offer to perform the work specified in the attached prospective Contract (Book II).

2.1.1.7 "IFB": Invitation for Bid.

2.1.1.8 The Purchaser is defined as the current NCI Agency or its legal successor.

2.2 Eligibility and Origin of Equipment and Services

2.2.1 As stated in Section 1.3.1 above only firms from a Participating Country are eligible to engage in this competitive Bidding process.

2.2.2 In addition, all contractors, sub-contractors and manufacturers, at any tier, must be from Participating Countries.

2.2.3 None of the work, including project design, labour and services shall be performed other than by firms from and within Participating Countries.

2.2.4 No materials or items of equipment down to and including identifiable Sub-assemblies shall be manufactured or assembled by a firm other than from and within a Participating Country.

2.2.5 Unless otherwise authorised by the terms of the prospective Contract, the Intellectual Property Rights to all design documentation and related system operating software shall reside in NATO member countries, and no license fees or royalty charges shall be paid by the Contractor to firms, individuals or governments other than within the NATO member community.

2.3 Bid Delivery and Bid Closing

2.3.1 All Bids shall be in the possession of the Purchaser at the address given below in Section 2.3.2 on/or before 12.00 hours (Brussels Time) on **19 OCTOBER 2016**, at which time and date Bidding shall be closed.

2.3.2 Bids shall be delivered to the following address:

2.3.2.1 By Post:

NCI Agency
ACQ/Contracting (ATTN: Mr. Peter Kowalski)
Boulevard Leopold III
1110 Brussels
Belgium

2.3.2.2 Hand Carried Service or courier:

NCI Agency
ACQ/Contracting (ATTN: Mr. Peter Kowalski)
Bâtiment Z
Avenue du Bourget 140
B-1110 Brussels
Belgium

2.3.3 Bids submitted by electronic means are not permitted and will not be considered. Bidders are advised that security or other personnel remaining on the premises outside of normal business hours may decline to sign or issue receipts for delivered items.

2.3.4 Late Bids

2.3.4.1 Bids which are delivered to the Purchaser after the specified time and date set forth above for Bid Closing are "Late Bids" and shall not be considered for award. Such Bids will be returned unopened to the Bidder at the Bidder's expense unless the Purchaser can determine that the Bid in question meets the criteria for consideration as specified below.

2.3.4.2 *Consideration of Late Bid* – The Purchaser considers that it is the responsibility of the Bidder to ensure that the Bid submission arrives by the specified Bid Closing time. Considering the number and quality of express delivery services, courier services and special services provided by the national postal systems, a late Bid shall only be considered for award under the following circumstances:

2.3.4.2.1 A contract has not already been awarded pursuant to the Invitation for Bid, and,

2.3.4.2.2 The Bid was sent to the address specified in the IFB by ordinary, registered or certified mail not later than ten (10) calendar days before the Bid closing date and the delay was due solely to the national or international postal system for which the Bidder bears no responsibility (the official postmark for ordinary and Registered Mail or the date of the receipt for Certified Mail will be used to determine the date of mailing), or,

2.3.4.2.3 The Bid was hand carried, or delivered by a private courier service and the Bidder can produce a receipt which demonstrates that the delivery was made to the correct address and received by a member of the NCI Agency and the failure to be received by the Contracting Authority was due to mishandling within the Purchaser’s organisation. Adverse weather, technical issues, traffic conditions, or circumstances of a similar nature will not be considered as grounds for acceptance of late bids.

2.3.4.3 A Late Bid which was hand-carried, or delivered by a private courier, for which a proper receipt cannot be produced, cannot be considered for award under any circumstances nor can late Bids which bear no post marks or for which documentary evidence of mailing date cannot be produced.

2.4 Requests for Extension of Bid Closing Date

2.4.1 Bidders are informed that requests for extension to the closing date for the IFB shall be submitted by the Bidder only through its respective country’s NATO Delegation or Embassy to the Purchaser Point of Contact indicated in Section

2.5.1 below. Any request for extension shall be submitted by the respective NATO Delegation or Embassy **no later than fourteen (14) calendar days** prior to the established Bid closing date. Bidders are advised to submit their request in sufficient time as to allow their respective NATO Delegation or Embassy to deliver the formal request to the Purchaser within the above time limit.

2.5 Purchaser's Point of Contact

2.5.1 The Purchaser point of contact for all information concerning this Invitation for Bid is:

Mr. Peter Kowalski, Senior Contracting Officer
Acquisition
Fax: +32.2.707.87.70
E-mail: peter.kowalski@ncia.nato.int

2.5.2 All correspondence related to the IFB will be forwarded to:

NCI Agency
Boulevard Leopold III
1110 Brussels, Belgium
Acquisition Support Group
Attn: Mr Peter Kowalski (contact details stated above)

2.6 Request for IFB Clarifications

2.6.1 Bidders, during the solicitation period, are encouraged to query and seek clarification of any matters of a contractual, administrative and technical nature pertaining to this IFB.

2.6.2 All questions and requests for clarification shall be forwarded to the Purchaser via email using the Clarification Request Form provided at Annex D of this Book I. Such questions shall be forwarded to the point of contact specified in Section 2.5.1 above and shall arrive **not later than twenty eight (28) calendar days** prior to the stated "Bid Closing Date". The Purchaser is under no obligation to answer requests for clarification submitted after this time. Requests for clarification must address the totality of the concerns of the Bidder, as the Bidder will not be permitted to revisit areas of the IFB for additional clarification except as noted in Section 2.6.3, below.

2.6.3 Additional requests for clarification are limited only to the information provided as answers by the Purchaser to Bidder requests for clarification. Such additional requests shall arrive not later than fourteen (14) calendar days before the established Bid Closing Date.

2.6.4 It is the responsibility of the Bidders to ensure that all Clarification Requests submitted bear no mark, logo or any other form or sign that may lead to reveal the Bidders' identity in the language constituting the clarification itself. This prescription is not applicable to the means used for the transmission of the clarification (i.e. email or form by which the clarification is forwarded).

2.6.5 The Purchaser declines all responsibilities associated to any and all circumstances regardless of the nature or subject matter arising from the Bidders' failure or inability to abide to the prescription in Section 2.6.4.

2.6.6 The Purchaser may provide for the removal of any form of identification in the body of the clarification request in those instances in which such practice is feasible as well as providing for a re-wording of the clarification request in those cases in which the original language submitted is deemed ambiguous, unclear, subject to different interpretation or revelatory of the Bidder's identity.

2.6.7 Bidders are advised that subsequent questions and/or requests for clarification included in a Bid shall neither be answered nor considered for evaluation.

2.6.8 Except as provided above, all questions will be answered by the Purchaser and the questions and answers (but not the identity of the questioner) will be issued in writing to all prospective Bidders. The Bidders shall immediately inform the Purchaser in the event that questions posed are not reflected in the answers published.

2.6.9 Where the extent of the changes implied by the response to a clarification request is of such a magnitude that the Purchaser deems necessary to issue revised documentation, the Purchaser will do so by the mean of the issuance of a formal IFB amendment pursuant to AC/4-DS-2261 and in accordance with Section 2.8 below.

2.6.10 The Purchaser reserves the right to reject frivolous clarification requests clearly devised or submitted for the purpose of artificially obtaining an extension of the bidding time (i.e. clarifications re-submitted using different wording where such wording does not change the essence of the clarification being requested).

2.6.11 The published responses issued by the Purchaser shall be regarded as the authoritative interpretation of the Invitation for Bid. Any amendment to the language of the IFB included in the answers will be issued as an IFB Amendment and shall be incorporated by the Bidder in his offer.

2.7 Requests for Waivers and Deviations

2.7.1 Bidders are informed that requests for alteration to, waivers or deviations from the terms and conditions of this IFB and attached Prospective Contract (Book II) will not be considered after the request for clarification process. Requests for alterations to the other requirements, terms or conditions of the Invitation for Bid or the Prospective Contract may only be considered as part of the clarification process set forth in Section 2.6 above. Requests for alterations to

the specifications, terms and conditions of the Contract which are included in a Bid as submitted may be regarded by the Purchaser as a qualification or condition of the Bid and may be grounds for a determination of non-compliance.

2.8 Amendment of the Invitation for Bid

2.8.1 The Purchaser may revise, amend or correct the terms, conditions and/or specifications and provisions of the IFB at any time prior to the date set for the Bid Closing. Any and all modifications will be transmitted to all Bidders by an official amendment designated as such and signed by the Contracting Authority. Such amendment will be accompanied by an acknowledgement of receipt which the Bidder shall complete and enclose as part of its Bid. This process may be part of the clarification procedures set forth in Section 2.6 above or may be an independent action on the part of the Purchaser.

2.8.2 The Purchaser will consider the potential impact of amendments on the ability of prospective Bidders to prepare a proper Bid within the allotted time. The Purchaser may extend the "Bid Closing Date" at its discretion and such extension will be set forth in the amendment document.

2.8.3 All revision or amendments issued by the Purchaser shall also be acknowledged by the Bidder in its Bid by completing the “Acknowledgement of Receipt of IFB Amendments” at Annex B-2. Failure to acknowledge receipt of all amendments may be grounds to determine the Bid to be non-compliant.

2.9 Modification and Withdrawal of Bids

2.9.1 Bids, once submitted, may be modified by Bidders, but only to the extent that the modifications are in writing, conform to the requirements of the IFB, and are received by the Purchaser prior to the exact time and date established for Bid Closing. Such modifications shall be considered as an integral part of the submitted Bid.

2.9.2 Modifications to Bids which arrive after the Bid Closing Date will be considered as "Late Modifications" and will be processed in accordance with the procedure set forth above concerning "Late Bids", except that unlike a "Late Bid", the Purchaser will retain the modification until a selection is made. A modification to a Bid which is determined to be late will not be considered in the evaluation and selection process. If the Bidder submitting the modification is determined to be the successful Bidder on the basis of the unmodified Bid, the modification may then be opened. If the modification makes the terms of the Bid more favourable to the Purchaser, the modified Bid may be used as the basis of contract award. The Purchaser, however, reserves the right to award a contract to the apparent successful Bidder on the basis of the Bid submitted and disregard the late modification.

2.9.3 A Bidder may withdraw its Bid at any time prior to Bid Opening without penalty. In order to do so, an authorised agent or employee of the Bidder must provide

an original statement of the firm's decision to withdraw the Bid and remove the Bid from the Purchaser's premises.

2.9.4 Except as provided in Section 2.10.4.2 below, a Bidder may withdraw its Bid after Bid Opening only by forfeiture of the Bid Guarantee.

2.10 Bid Validity

2.10.1 Bidders shall be bound by the term of their Bids for a period of twelve (12) months starting from the Bid Closing Date specified in Section 2.3.1 above.

2.10.2 In order to comply with this requirement, the Bidder shall complete the Certificate of Bid Validity set forth in Annex B-4. Bids offering less than the period of time referred to above for acceptance by the Purchaser may be determined to be non-compliant.

2.10.3 The Purchaser will endeavour to complete the evaluation and make an award within the period referred to above. However, should that period of time prove insufficient to render an award, the Purchaser reserves the right to request an extension of the period of validity of all Bids which remain under consideration for award.

2.10.4 Upon notification by the Purchaser of such a request for a time extension, the Bidders shall have the right to:

2.10.4.1 accept this extension of time in which case Bidders shall be bound by the terms of their offer for the extended period of time and the Bid Guarantee and Certificate of Bid Validity extended accordingly; or

2.10.4.2 refuse this extension of time and withdraw the Bid, in which case the Purchaser will return to the Bidder its Bid Guarantee in the full amount without penalty.

2.10.5 Bidders shall not have the right to modify their Bids due to a Purchaser request for extension of the Bid validity unless expressly stated in such request.

2.11 Bid Guarantee

2.11.1 The Bidder shall furnish with its Bid a guarantee in an amount equal to **one Hundred Fifty Thousand Euro (€150,000).** The Bid Guarantee shall be substantially similar to Annex C as an irrevocable, unqualified and unconditional Standby Letter of Credit (SLC) issued by a Belgian banking institution fully governed by Belgian legislation or issued by a non-Belgian financial institution and confirmed by a Belgian banking institution fully governed by Belgian legislation. In the latter case signed original letters from both the issuing institution and the confirming institution must be provided. The confirming Belgian bank shall clearly state that it will guarantee the funds, the drawing against can be made by the NCI Agency at its premises in Belgium. Bid Guarantees shall be made payable to the Treasurer, NCI Agency.

2.11.2 Alternatively, a Bidder may elect to post the required Guarantee by certified cheque. If the latter method is selected, Bidders are informed that the Purchaser will cash the cheque on the Bid Closing Date.

2.11.3 If the Bid Closing Date is extended after a Bidder's financial institution has issued a Bid Guarantee, it is the obligation of the Bidder to have such Bid Guarantee (and confirmation, as applicable) extended to reflect the revised Bid Validity date occasioned by such extension.

2.11.4 Failure to furnish the required Bid Guarantee in the proper amount, and in the proper form and for the appropriate duration by the Bid Closing Date may be cause for the Bid to be determined non-compliant.

2.11.5 In the event that a Bid Guarantee is submitted directly by a banking institution, the Bidder shall furnish a copy of said document in the Bid Administration Package.

2.11.6 The Purchaser will make withdrawals against the amount stipulated in the Bid Guarantee under the following conditions:

2.11.6.1 The Bidder has submitted a bid and, after Bid Closing Date (including extensions thereto) and prior to the selection the compliant bid determined to represent the best value, withdraws its Bid, or states that he does not consider its bid valid or agree to be bound by its bid;

2.11.6.2 The Bidder has submitted a compliant bid determined by the Agency to represent the best value, but the Bidder declines to sign the contract offered by the Agency, such contract being consistent with the terms of the Invitation for Bid;

2.11.6.3 The Purchaser has offered the Bidder the contract for execution but the Bidder has been unable to demonstrate compliance with the security requirements of the contract within a reasonable time; or

2.11.6.4 The Purchaser has entered into the contract with the Bidder but the Bidder has been unable or unwilling to provide the Performance Guarantee required under the terms of the contract within the time frame required.

2.11.7 Bid Guarantees will be returned to Bidders as follows:

2.11.7.1 to non-compliant Bidders forty-five (45) days after notification by the Purchaser of a non-compliant Bid (except where such determination is challenged by the Bidder; in which case the Bid Guarantee will be returned forty-five (45) days after a final determination of non-compliance);

2.11.7.2 to all other unsuccessful Bidders within thirty (30) days following the award of the contract to the successful Bidder;

2.11.7.3 to the successful Bidder upon submission of the Performance Guarantee required by the Contract or, if there is no requirement for such a Performance Guarantee, upon contract execution by both parties;

2.11.7.4 pursuant to Section 2.10.4.2 above.

2.11.8 “Standby Letter of Credit" or “SLC” as used herein, means a written commitment by a Belgian financial institution either on its own behalf or as a confirmation of the Standby Letter of Credit issued by a non-Belgian bank to pay all or part of a stated amount of money, until the expiration date of the letter, upon presentation by the Purchaser of a written demand therefore. Neither the financial institution nor the Contractor can revoke or condition the Standby Letter of Credit. The term “Belgian financial institution” includes non-Belgian financial institutions licensed to operate in Belgium.

2.12 Cancellation of Invitation for Bid

2.12.1 The Purchaser may cancel, suspend or withdraw for re-issue at a later date this IFB at any time prior to contract award. No legal liability on the part of the Purchaser for payment of any sort shall arise and in no event will any Bidder have cause for action against the Purchaser for the recovery of costs incurred in connection with preparation and submission of a Bid in response to this IFB.

2.13 Electronic Transmission of Information and Data

2.13.1 The Purchaser will endeavour to communicate answers to requests for clarification and amendments to this IFB to the prospective Bidders as soon as practicable.

2.13.2 Bidders are cautioned that the Purchaser, when permissible under security classifications, will rely exclusively on electronic mail or portal communication to manage all correspondence related to this IFB, including IFB amendments and clarifications.

2.14 Supplemental Agreements

2.14.1 Bidders are required, in accordance with the certificate at Annex B-7 of these Instructions to Bidders, to disclose any prospective Supplemental Agreements that are required by national governments to be executed by NATO/NCI Agency or successor organisations as a condition of contract performance.

2.14.2 Supplemental Agreements are typically associated with, but not necessarily limited to, national export control regulations, technology transfer restrictions and end user agreements or undertakings.

2.14.3 Bidders are cautioned that failure to provide full disclosure of the anticipated requirements and the terms thereof, to the best of the Bidder’s knowledge and experience, may result in the Purchaser withholding award of the contract or cancelling an executed contract if it is discovered that the terms of such

Supplemental Agreements contradict salient conditions of the Prospective Contract to the extent that either key objectives cannot be accomplished or basic contract principles and Purchaser rights have been abridged.

2.15 Notice of Limitations on Use of Intellectual Property Delivered to the Purchaser

2.15.1 Bidders are instructed to review Clauses 8 and 9 of the Contract Special Provisions and Clause 30 of the Contract General Provisions set forth Parts II and III of Book II herein. These Clauses sets forth the definitions, terms and conditions regarding the rights of the Parties concerning Intellectual Property developed and/or delivered under this contract or used as a basis of development under this contract.

2.15.2 Bidders are required to disclose, in accordance with Annex B-10 and Annex B-11, the Intellectual Property proposed to be used by the Bidder that will be delivered with either Background Intellectual Property Rights or Third Party Intellectual Property Rights. Bidders are required to identify such Intellectual Property and the basis on which the claim of Background or Third Party Intellectual Property is made.

2.15.3 Bidders are further required to identify any restrictions on Purchaser use of the Intellectual Property that is not in accordance with the definitions and rights set forth in the provisions of the Book II prospective Contract concerning use or dissemination of such Intellectual Property.

2.15.4 Bidders are reminded that restrictions on use or dissemination of Intellectual Property conflicting with the Book II terms and conditions or with the objectives and purposes of the Purchaser as stated in the Prospective Contract shall result in a determination of non-compliant bid.

2.16 Mandatory Quality Assurance and Quality Control Standards

2.16.1 Bidders are requested to note that, in accordance with the Certificate at Annex B-8 hereto, Bidders shall provide documentary evidence that the Bidder possesses a current certification that is compliant with the requirements of Allied Quality Assurance Publication (AQAP) 2110, ISO 9001:2008, or an equivalent QA/QC regime.

2.16.2 Bidders shall further demonstrate that such regime is applied within the Bidder's internal organisation, as well as extended to its relationships with Subcontractors.

2.16.3 If the Bidder is offering a QA/QC regime that is claimed to be equivalent to AQAP 2110 or ISO 9001:2008, the burden of proof of such equivalency shall

be on the Bidder and such evidence of equivalency shall be submitted with the Certificate at Annex B-8 in the Bid Administration Package.

2.16.4 Failure to execute this Certificate, or failure to provide documentary evidence of compliance with this requirement may result in a determination of non-compliance for the submitted Bid.

3 BID PREPARATION INSTRUCTIONS

3.1 General

3.1.1 Bidders shall prepare and submit their Bid in accordance with the requirements and format set forth in this IFB. Compliance with all bid submission requirements is mandatory. Failure to submit a bid in conformance with the stated requirements may result in a determination of non-compliance by the Purchaser and the elimination of the bid from further consideration.

3.1.2 Bidders **shall not simply restate the IFB requirements**. A Bid shall demonstrate that the Bidder understands the terms, conditions and requirements of the IFB and shall demonstrate the Bidder's ability to provide all the services and deliverables listed in the Schedules of the prospective Contract. Bidders shall take good note of Para 4.1.4 below in this regard.

3.1.3 Bidders are informed that the quality, thoroughness and clarity of the bid will affect the overall scoring of the bid. Although the Purchaser may request clarification of the bid, it is not required to do so and may make its determination on the content of the bid as written. Therefore, Bidders shall assume that inconsistencies, omissions, errors, lack of detail and other qualitative deficiencies in the submitted bid will have a negative impact on the final Best Value score.

3.1.4 Partial Bids and/or bids containing conditional statements will be declared non-compliant.

3.1.5 Bidders are advised that the Purchaser reserves the right to incorporate the successful Bidder's Offer in whole or in part by reference in the resulting contract.

3.1.6 If no specific format has been established for electronic versions, Bidders shall deliver documentation in an electronic format which is best suited for review and maintenance by the Purchaser (e.g., Project Master Schedule in MS Project format, Project Highlight Reports in MS Word).

3.1.7 All documentation submitted as part of the Bid shall be classified no higher than "NATO RESTRICTED".

3.2 Bid Package Content

3.2.1 The complete Bid shall consist of three distinct and separated parts described in the following subparagraphs. Detailed requirements for the structure and content of each of these packages are contained in these Bidding Instructions.

3.2.2 The Bid Administration Package, containing one (1) hard copy and one (1) soft copy (on CD ROM or DVD) of the documents specified in Section 3.4 below.

3.2.3 The Price Quotation Envelope, containing (1) paper original and two (2 CD ROMs or DVDs) soft copy in MS Excel format of the Price Quotation specified in Section 3.5. The soft copy shall be in MS Excel format which can be manipulated i.e. not an image and be the full and complete price proposal including the CLIN (Contract Line Item Number) Price breakdown sheets.

3.2.4 The Technical Proposal Package consisting of three (3) volumes as specified below. Each Volume shall be in a separate binder or file for ease of segregation and handling and shall each be submitted as three (3) soft copies on CD ROMs or DVDs.

3.2.4.1 Volume 1 – Management and Risk

3.2.4.2 Volume 2 – Engineering

3.2.4.3 Volume 3 – Supportability

3.2.4.4 Bidding instructions describing the expected contents of each of the three (3) volumes constituting the Technical Proposal Package are in Section 3.6 of this document. Advice to Bidders on how the Purchaser plans to conduct the technical evaluation of each of the three (3) volumes is contained in Section 4.5 of this document.

3.3 Package Marking

3.3.1 The separate parts of the bid shall be placed in outer containers for delivery. All outer containers into which bidding documents are placed shall be opaque or wrapped in opaque paper, sealed and identified with the following markings:

3.3.1.1 SEALED BID IFB-CO-13810-CS

3.3.1.2 BOX X of Y (1 of 3, 2 of 3, etc.)

3.3.1.3 NOTIFY Mr. Peter Kowalski (Ext. 8221) UPON RECEIPT

3.3.2 Each of the bid parts placed in the outer container(s) shall be separately wrapped (multiple copies of the same document may be wrapped together), and marked as follows:

3.3.2.1 Name and address of the Bidder, and

3.3.2.2 The words “SEALED BID” followed by the reference “IFB-CO-13810-CS”; and the appropriate package marking (i.e., Administration Documentation, Price Proposal etc.).

3.4 Administrative Documentation Package

3.4.1 The Package must include the original of the Bid Guarantee required by Section 2.11 of the Bidding Instructions. If the Bid Guarantee is sent to the Purchaser

directly from the Bidder's bank, a letter, in lieu of the actual Guarantee, shall be included specifying the details of the transmittal. Bidders are reminded that the Bid Guarantee shall reflect any extensions to the Bid Validity Date due to extensions in the Bid Closing Date.

3.4.2 The Package shall include the Certificates set forth in Annex B to these Bidding Instructions, signed in the original by an authorised representative of the Bidder. The Certificates are as follows:

3.4.2.1 Annex B-1 (Certificate of Legal Name of Bidder);

3.4.2.2 Annex B-2 (Acknowledgement of Receipt of IFB Amendments);

3.4.2.3 Annex B-3 (Certificate of Independent Determination);

3.4.2.4 Annex B-4 (Certificate of Bid Validity);

3.4.2.5 Annex B-5 (Certificate of Exclusion of Taxes, Duties and Charges);

3.4.2.6 Annex B-6 (Comprehension and Acceptance of Contract Special and General Provisions);

3.4.2.7 Annex B-7 (Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements) with the prospective text of such Agreements, as applicable;

3.4.2.8 Annex B-8 (Certificate of Compliance AQAP 2110 or ISO 9001:2008 or Equivalent), with a copy of the relevant quality certification attached to it.

3.4.2.9 Annex B-9 (List of Prospective Major Subcontractors);

3.4.2.10 Annex B-10 (Bidder Background IPR);

3.4.2.11 Annex B-11 (List of Subcontractor IPR);

3.4.2.12 Annex B-12 (Certificate of Origin of Equipment, Services, and Intellectual Property);

3.4.2.13 Annex B-13 (List of Proposed Key Personnel);

3.4.2.14 Annex B-14 (Certificate of Price Ceiling);

3.4.2.15 Annex B-15 (Disclosure of Conflict of Interest);

3.4.2.16 Annex B-16 (National CIS Security Authority Approval for Cryptographic Hardware and Software)

3.4.2.17 In accordance with Section 3.2.2, the administrative package shall include a hard copy and a CD-ROM/or DVD containing an electronic version of the documentation stated in Sections 3.4.2.1 through 3.4.2.16 above.

3.4.3 Documentation Disclosure of Conflict of Interest

3.4.3.1 A conflict of Interest means that because of other activities or relationships with other persons or entities, a Bidder is unable or potentially unable to render impartial assistance or advice to the Purchaser or the Bidder's objectivity in performing the prospective Contract work is, or might be otherwise impaired, or the Bidder has an unfair competitive advantage.

3.4.3.2 In compliance with Section 1.4.6, Bidders shall identify all business relationships with the PMIC Contractor or Bidder including but not limited to those resulting from ownership, share of assets, strategic business agreements regardless of their nature or financial magnitude, of which the Bidder is knowledgeable at the time of bid submission. If any of such relationships could constitute a real or apparent conflict of interest, or could otherwise, in any manner or form, influence or appear to influence the capacity of the Bidder to render unbiased service, Bidders shall submit a plan for the mitigation of the conflict detailing the measures the Bidder has or proposes to put in place for the purpose of preventing unfair advantage in relation to the performance associated with the prospective Contract.

3.4.3.3 If no conflict of interest exists, Bidders shall include a declaration to that extent signed by the individual entitled to commit the company to such statement.

3.4.4 No indication disclosing or contributing to disclose the Bid Price shall be made part of the Bid Administration Package. Failure to abide to this prescription may result in the bid being declared non-compliant.

3.5 Price Quotation

3.5.1 Package Contents

3.5.1.1 This envelope must contain the following documentation and media in the quantities provided in Section 3.2.3:

3.5.1.1.1 Annex A-1 "Bidding Sheets" and, as an annex, the complete set of sheets contained in the electronic file number "2" ("2_*IFB-CO-13810-CS Book I Annex A Bidding Sheets.xlsx*") issued as part of this IFB; and

3.5.1.1.2 CD or DVDs (two (2) copies) each containing an electronic version, ***in MS Excel***, of the documentation stated in Section 3.5.1.1.1 above.

3.5.2 General Rules

3.5.2.1 Bidders are advised that the total bid price for CLINs 1-7, 10-18 shall not exceed a total of **EUR 25,968,664**. A bid that exceeds this total shall be determined to be non-compliant and eliminated from further consideration. However, these CLINs have two separate "not-to exceed" prices to be noted and indicated in Annex A-1. The two "not-to exceed" prices are **EUR 16,740,620** for Investment and **EUR 9,228,044** for O&M. A bid submitted in

excess of the Investment "not-to exceed" price shall not be declared non-compliant if all the following conditions are met: 1) the total (Investment and O&M over a 5 year period) bid price is below the average total bid price; 2) the raw Supportability Score is above the average raw Supportability Score; 3) the bid is compliant with the Price Realism clause for the Investment bid prices that are subject to price evaluation; and 4) the bid is compliant with the Price Realism clause for the O&M bid prices that are subject to price evaluation. If a bid submitted in excess of the Investment "not-to exceed" price and does not meet the former conditions, the bid shall be determined to be non-compliant and eliminated from further consideration. A bid submitted in excess of the O&M "not-to exceed" price shall be determined to be non-compliant and eliminated from further consideration.

3.5.2.2 Bidders shall prepare their Price Quotation by completing the Bidding Sheets referred in Section 3.5.1.1.1 above, in accordance with the instructions specified in Book I Annex A-2.

3.5.2.3 The structure of the Bidding Sheets shall not be changed, other than as indicated elsewhere, nor should any quantity or item description in the Bidding Sheets. The currency(ies) of each Contract Line Item and sub-item shall be shown. The prices provided shall be intended as the comprehensive total price offered for the fulfilment of all requirements as expressed in the IFB documentation including but not limited to those expressed in the SOW.

3.5.2.4 When completing the Bidding Sheets the Bidder shall insert information in all yellow cells of the Bidding Sheets and complete the Pricing Summary as instructed. A price for each specified element needs to be supplied on each CLIN. Prices should not be grouped. The prices and quantities entered on the document shall reflect the total items required to meet the contractual requirements. The total price shall be indicated in the appropriate columns and in the currency quoted. If the price of a line item is expressed in different currencies, these shall be identified, and there shall be as many totals on that line item as there are currencies. In preparing the Price Quotation, Bidders shall ensure that the prices of the Sub-items total the price of the major item of which they constitute a part.

3.5.2.5 Bidders shall **furnish Firm Fixed Prices for all required items** in accordance with the format set forth in the Instructions for preparation of the Bidding Sheets.

3.5.2.6 Bidders shall furnish Firm Fixed Prices for all CLINs as defined in the SOW. Purchaser evaluation of the submitted bids will be on the basis of the complete submission including administrative, price and technical components for all CLINs. The Contract will be awarded for all CLINs, with CLINs 1 thru 4 being the basic contract and the work defined for CLINs 5 thru 18 being included as fourteen (14) Firm Fixed Price options to the Contract. These options may be exercised by the Purchaser, at the sole discretion of the Purchaser as described in the Book II General and Special Provisions. The Purchaser's

decision to exercise any Options will take into consideration the Contractor's successful performance on the basic contract, as well as the availability of the required funding.

3.5.2.7 Offered prices shall not be "conditional" in nature. Any comments supplied in the Bidding Sheets or in any part of the bid package which are conditional in nature, relative to the offered prices may result in a determination that the bid is non-compliant.

3.5.2.8 Bidders are responsible for the accuracy of their Price Quotations. Price Quotations that have apparent computational errors may have such errors resolved in the Purchaser's favour or, in the case of gross omissions, inconsistencies or errors, may be determined to be non-compliant. In the case of inconsistencies between the electronic version of the Bidding Sheets and the paper "hard copy" of the Bidding Sheets, the "hard copy" will be considered by the Purchaser to have precedence over the electronic version.

3.5.2.9 Bidders shall quote in their own national currency or in EURO. Bidders may also submit bids in multiple currencies including other NATO member states' currencies under the following conditions:

3.5.2.9.1 the currency is of a "participating country" in the project, **and**

3.5.2.9.2 the Bidder can demonstrate, either through sub-contract arrangements or in its proposed work methodology, that it will have equivalent expenses in that currency. All major subcontracts and their approximate anticipated value should be listed on a separate sheet and included with the Price Quotation.

3.5.2.10 The Purchaser, by virtue of his status under the terms of Article IX and X of the Ottawa Agreement, is exempt from all direct and indirect taxes (incl. VAT) and all customs duties on merchandise imported or exported.

3.5.2.11 Bidders shall therefore **exclude** from their price Bid all taxes, duties and customs charges from which the Purchaser is exempted by international agreement and are required to certify that they have done so through execution of the Certificate at Annex B-5.

3.5.2.12 Unless otherwise specified in the instructions for the preparation of Bidding Sheets in Annex A-1, all prices quoted in the proposal shall be on the basis that all deliverable items shall be delivered "Delivery Duty Paid (DDP)" in accordance with the International Chamber of Commerce INCOTERMS ® 2010.

3.5.2.13 The Bidder's attention is directed to the fact that Price Quotation shall contain no document and/or information other than the priced copies of the Bidding Sheets. Any other document will not be considered for evaluation.

3.5.2.14 All prices bid shall be clearly traceable in the detailed bidding sheets.

3.5.2.15 Any adjustment or discount to prices should be clearly traceable to the lowest level of breakdown in the bidding sheets and should not be aggregated or summed. Any lack of clarity or traceability may render the bid non-compliant.

3.5.2.16 The Bidder understands that there is no obligation under this contract for the Purchaser to exercise any of the optional line items and that the Purchaser bears no liability should it decide not to exercise the options (totally or partially). Further, the Purchaser reserves the right to order another Contractor (or the same), to perform the tasks described in the optional line items of the current contract through a new contract with other conditions.

3.5.2.17 Specific to CLIN 19, referring to Para 3.5.2.16 above, an illustrative notional scenario is presented below to illustrate how the Purchaser could exercise various Contract Options by additional sites or equipment being required:

3.5.2.17.1 **Notional Scenario** – An additional installation is required after contract award.

3.5.2.17.2 **Purchaser Exercise of Contract Options** – In this situation, the Purchaser could, under the Contract terms, exercise via a contract amendment the following CLIN 19 items:

CLIN	Description	Requirement to Fulfil
19.1	Project Management	Site Specific Project Management, Project Management for a specific quantity of Certificate Authorities, Registration Authorities, Online Certificate Status Protocol, and Timestamp.
19.2	System Engineering	Systems Engineering for a specific quantity of Certificate Authorities, Registration Authorities, Online Certificate Status Protocol, and Timestamp.
19.3	System Implementation	Implementation support and delivery of equipment for a specific quantity of Certificate Authorities, Registration Authorities, Online Certificate Status Protocol, and Timestamp.
19.4	ILS	Site-Specific ILS deliverables
19.5	Operation and Maintenance (User services only)	Initial and Follow-on Operational Support

3.5.2.17.3 In each of the sub-CLINs that could be exercised in the above notional scenario, the hours and unit prices indicated in the Option CLIN 19 for the specific activities corresponding to sub-CLIN item would be

used to calculate the firm fixed price of the additional installation to be exercised.

3.6 Technical Proposal Package

3.6.1 It is of the utmost importance that Bidders respond to all of the technical requirements of the Purchaser Statement of Work (including all Annexes) and all the bidding instructions, not only with an affirmation of compliance but also with an explanation of how each requirement will be met. To facilitate bidding and the subsequent evaluation of the Bidder's response to the various sections of the Statement of Work (including all Annexes), bids shall be organised and submitted in three (3) volumes as follows:

3.6.1.1 Volume 1 – Management and Risk – covering requirements from Sections 1, 2, 3, 8, 12, 13, 16, and annex E of the SOW, and an Executive Summary of the entire Technical Proposal;

3.6.1.2 Volume 2 – Engineering – covering requirements from Sections 4, 5, 9, 10, 11, Annex A, Annex C of the SOW; and

3.6.1.3 Volume 3 – Supportability – covering requirements from Sections 6, 7, 14, 15, and Annex B of the SOW.

3.6.2 The mapping of SOW sections to volumes has been done to facilitate a consistent organisation of the Technical Proposal and its subsequent evaluation.

3.6.2.1 The mapping shall be adhered to by Bidders even if individual requirements within sections of the SOW may seem to more logically belong in a different volume. Requirements that are answered in Volumes other than as indicated in Section 3.6.1may not be evaluated, thus affecting the Best Value score or in extreme cases resulting in a determination of non-compliance.

3.6.2.2 The proposed Technical Solution shall not be "conditional" in nature. Any comments supplied in the Technical Proposal Package which are conditional in nature, relative to the proposed Technical Solution, may result in a determination that the bid is non-compliant.

3.6.3 Bidding instructions related to each of the three (3) volumes are provided in Sections 3.6.4 through 3.6.6.

3.6.4 Volume 1 – Management and Risk

3.6.4.1 This volume will address the following elements:

3.6.4.1.1 Executive Summary

3.6.4.1.2 Table of Contents for the whole Technical Proposal

3.6.4.1.3 Overall understanding of Purchaser's requirements by the Bidder

3.6.4.1.4 Bidder Qualifications and Key Personnel

3.6.4.1.5 Project management

3.6.4.1.6 Risk management

3.6.4.1.7 Schedule management

3.6.4.1.8 Others

3.6.4.1.9 Bid-Requirements Cross-Reference Matrix (BRCM)

3.6.4.2 Executive Summary

3.6.4.2.1 Bidders shall provide an overview of the salient features of their technical proposal in the form of an Executive Summary.

3.6.4.2.2 The Executive Summary shall provide a general description of the major points contained in each of the required sections of the technical proposal (i.e. 3 volumes) and shall demonstrate the depth of the Bidder's understanding of: the project, the implementation environment, the problems and risks of project implementation foreseen by the Bidder, as well as the Bidder's ability to communicate high level concepts in an appropriate and succinct manner. The Bidder shall highlight the strengths which it and its team bring to the project in terms of minimising the problems and reducing the risks, while meeting the overall schedule, and the key points of the technical approach. This summary shall not exceed 10 pages.

3.6.4.2.3 Bidders shall explicitly state in the Executive Summary that, should their firm be selected and awarded the contract resulting from this solicitation, the delivered product(s) and services shall comply with the requirements of the Statement of Work (including all annexes).

3.6.4.3 Table of Contents

3.6.4.3.1 Bidders shall compile a detailed Table of Contents which lists not only the section headings but also the major sub-sections, and topic headings of the Bid. Heading, section and subsection titles should be appropriately descriptive in order to permit the Purchaser's bid evaluation team to locate relevant material expeditiously.

3.6.4.4 Overall Understanding of Purchaser's Requirements

3.6.4.4.1 The Bid must demonstrate the Bidder's understanding of the Purchaser's requirements as described in the Statement of Work (SOW). The strategic vision behind the E-NPKI project, the objectives, constraints

and scope must all be addressed and related to the technical solution described in the Bid.

3.6.4.5 Bidder Qualifications and Key Personnel

3.6.4.5.1 Volume 1 shall describe the company structure and activities of the prime contractor. The country in which the prime contractor is registered shall be identified and the size and location(s) of the company headquarters and subsidiary branches described. Within that structure the location and organizational unit of the office which will manage this contract shall be identified. This section shall also describe the major activities of the company and how they are distributed across the organisation.

3.6.4.5.2 Volume 1 shall describe the corporate capabilities of the Bidder, including corporate experience, corporate structure and individual skills and experience in relation to this project. In particular, the Bidder shall provide evidence of relevant and recent experience in the design, integration, testing, and implementation of at least 2 projects similar to the E-NPKI Project.

3.6.4.5.3 Volume 1 shall describe the Bidder's major proposed sub-contractors for the Project. Major proposed sub-contractors, for purposes of this section, refer to the criteria set forth in Clause 10 of the Prospective Contract General Provisions entitled "Sub-Contracts". The Bidder shall identify the firm and the nation of origin and describe the contribution which the sub-contractor is expected to make to the execution of the project. The Bidder shall also provide rationale for the selection of the sub-contractor and describe the added value the sub-contractor will bring to the execution of the project.

3.6.4.5.4 Volume 1 shall provide a description of individual skills and experience in relation to the project of all project team members and Subject Matter Experts (SMEs) foreseen to support the project team. The description shall include how each individual expertise and experience will add value to the team.

3.6.4.5.5 Volume 1 shall provide the resumes / Curricula Vitae (CV) and supporting certification documentation (e.g. Prince 2 certificates) of each proposed Key Personnel that meet or exceed the requirements in SOW Section 12.

3.6.4.6 Project Management

3.6.4.6.1 In order to demonstrate how the Bidder plans to approach the management of the project (according to SOW Section 3), the Bidder shall submit initial versions of the **Project Management Plan (PMP)** and of the **Work Breakdown Structure (WBS).**

3.6.4.6.2 The submitted documents shall include sufficient information to demonstrate the Bidder's understanding of the key challenges involved in the E-NPKI project, and demonstrate that the Bidder is proposing an approach that can deal with these challenges.

3.6.4.6.3 Project Management Plan (PMP)

3.6.4.6.3.1 The initial PMP shall following the structure called for in SOW Section 13.15.

3.6.4.6.3.2 The initial PMP shall provide detailed information on the management approach to deliver the E-NPKI from Contract award till the end of the 5 year O&M period.

3.6.4.6.3.3 The initial PMP shall demonstrate how the Project Controls required under SOW Section 3 will be implemented during the project. In particular the Bidder shall demonstrate that the Project Management methodology proposed for the project is suitable to the successful execution of the project.

3.6.4.6.3.4 The initial PMP shall also present an overall organisational description for its team that makes clear how the team will function, including, as a minimum:

3.6.4.6.3.4.1 Evidence that the team is balanced to ensure that the right team composition has been selected from a technical, experience, and managerial point of view,

3.6.4.6.3.4.2 Evidence that there are no missing skills or other gaps in the team that would increase risk or otherwise adversely affect the execution of the project,

3.6.4.6.3.4.3 A description of how the work is organised across the team,

3.6.4.6.3.4.4 A description of the internal team management measures, including company executive relationships that ensure that team members perform,

3.6.4.6.3.4.5 Evidence that appropriate contractual and managerial checks are in place to ensure that the team functions in a manner appropriate to deliver the E-NPKI project,

3.6.4.6.3.4.6 Evidence that the Bidder will ensure continuity of the team,

3.6.4.6.3.4.7 Any supporting tool that will be used by the team,

3.6.4.6.3.4.8 Any other material that will make clear that the Bidder understands how to manage the selected team, that the team composition is optimal, and will remain functional throughout the execution period, to respond to the demands of the E-NPKI project.

3.6.4.6.3.5 The initial PMP shall demonstrate that the Bidder has understood the engineering process imposed in SOW Section 4 and describe how he will support the cycle of design reviews and approvals.

3.6.4.6.3.6 The initial PMP shall also include a section which demonstrates its commitment to the achievement of project milestones as described in SOW Section 16 and the "SSS - Project milestones delivery requirements", while respecting the order of precedence of documents. This section shall address the entire E-NPKI contract duration (including support phases) as well as the complete list of implementation sites (including optional sites).

3.6.4.6.4 Work Breakdown Structure (WBS)

3.6.4.6.4.1 The initial WBS shall provide detailed information reflecting all necessary activities (phases and their major tasks/CLINs as well as the dependencies between the tasks/CLINs) for the effective planning, management and delivery of the E-NPKI capability and provisioning of E-NPKI services as required.

3.6.4.6.4.2 The initial WBS shall be consistent with the requirements of the SOW in its description of all engineering efforts for specifying, designing, developing, testing, accrediting, installing, integrating and supporting the delivery of the E-NPKI services.

3.6.4.7 Risk Management

3.6.4.7.1 The Bidder shall submit an **initial Risk Log** describing a minimum of ten (10) and a maximum of fifteen (15) most important risks to the successful completion of the project from its perspective.

3.6.4.7.2 The Risk Log shall be in accordance with SOW Section 13.2.

3.6.4.7.3 In addition to other risks, the following risks shall be addressed in the Bid:

3.6.4.7.3.1 Security accreditation

3.6.4.7.3.2 Schedule drift

3.6.4.7.3.3 Insufficient Contractor resources (manpower) for both project implementation and 5 years O&M

3.6.4.7.4 As part of the initial PMP, the Bidder shall describe how risks will be managed throughout the execution of the contract in response to the requirements of SOW Section 3.

3.6.4.8 Schedule Management

3.6.4.8.1 The Bidder shall submit an **initial Project Master Schedule (PMS)**.

3.6.4.8.2 The PMS shall be according to SOW Section 3.4.2.

3.6.4.8.3 The PMS shall include additional subordinate milestones that the Bidder plans to achieve which make clear the extent of parallel activities and the detailed phasing and dependencies of different activities.

3.6.4.8.4 The PMS shall detail the proposed implementation sequence of all the sites in SOW Annex C (see also SOW Section 16.2).

3.6.4.8.5 The PMS shall meet the project deadlines (EDC + x months) as described in SOW Section 16 and the “SSS - Project milestones delivery requirements”, while respecting the order of precedence of documents. Bidders are encouraged to propose a more aggressive schedule while maintaining an acceptable level of risks.

3.6.4.8.6 Volume 1 shall include 2 versions of the initial PMS

3.6.4.8.6.1 one version in Microsoft Project format

3.6.4.8.6.2 one version in pdf format (potentially as an annex to the initial PMP).

3.6.4.9 Others

3.6.4.9.1 Introduction

3.6.4.9.1.1 Section 1 of the SOW contains an introduction to the E-NPKI project as well as some high level requirements. For bidding purposes, in this volume, a simple affirmation that all requirements will be met is sufficient, unless otherwise stated in this document.

3.6.4.9.2 Applicable documents

3.6.4.9.2.1 Section 2 of the SOW contains the list of applicable documents. For bidding purposes, in this volume, a simple affirmation that all documents from Section 2 shall be adhered to is sufficient, unless otherwise stated in this document.

3.6.4.9.3 Implementation at Optional sites

3.6.4.9.3.1 Section 8 of the SOW contains the approach to implementing E-NPKI at optional sites. The Bid shall explain the Bidder’s approach to implementing optional sites.

3.6.4.9.4 Documentation outline

3.6.4.9.4.1 Section 13 of the SOW contains outlines of some E-NPKI documents to be delivered. For bidding purposes, in this volume, a simple affirmation that all requirements will be met is sufficient. Other sections of these Bidding

Instructions will indicate where portions of the bid need to be submitted in accordance with the formats and content described in SOW Section 13.

3.6.4.9.5 Purchaser Furnished Equipment (PFE)

3.6.4.9.5.1 The SOW Annex E provides the list of anticipated PFEs. Volume 1 of the Bid shall contain an **update of the table 11 contained in SOW Annex E**. To that respect, the Bidder shall fill in estimated quantities (for BASIC and OPTION sites) as required depending on their proposed technical solution. The update of the table 11 shall distinguish between BASIC sites and OPTION sites, and shall provide a breakdown per site.

3.6.4.9.5.2 The Bid shall demonstrate a clear understanding of PFE and shall describe how the Bidder proposes to make use of / integrate with PFE during the execution of the contract.

3.6.4.10 Bid-Requirements Cross-Reference Matrix (BRCM)

3.6.4.10.1 Volume 1 shall also contain a **Bid-Requirements Cross reference Matrix (BRCM) in the format indicated at Annex E.**

3.6.5 Volume 2 – Engineering

3.6.5.1 This volume covers the engineering activity in the E-NPKI project from analysis and design through to delivery, testing, implementation, transition and acceptance. A substantial response is expected to the system engineering requirements (SOW Section 4), site survey and system implementation requirements (SOW Sections 5 and 10), testing process requirements (SOW Section 9), security accreditation process requirements (SOW Section 11), System Requirements Specification (SRS) (SOW Annex A), and implementation scope (SOW Annex C).

3.6.5.2 System Engineering

3.6.5.2.1 SDS

3.6.5.2.1.1 The Bidder shall provide an **initial System Design Specification (SDS)** which describes its proposed technical solution and demonstrates its understanding of the requirements SOW Annex A.

3.6.5.2.1.2 The initial SDS shall follow the outline of SOW Section 13.7.

3.6.5.2.1.3 The initial SDS shall include an initial Product Breakdown Structure (PBS) focusing on specialist Products only.

3.6.5.2.1.4 The initial SDS shall demonstrate a comprehensive understanding of all of the requirements of SOW Annex A and describe how every requirement is addressed in the Bidder's proposed solution.

3.6.5.2.1.5 In particular, the initial SDS shall describe how the following requirements are planned to be addressed:

3.6.5.2.1.5.1 Disaster Recovery, Services Continuity and High Availability

3.6.5.2.1.5.2 User Experience

3.6.5.2.1.5.3 Flexibility

3.6.5.2.1.5.4 Scalability

3.6.5.2.1.5.5 Standardisation and Interoperability

3.6.5.2.1.5.6 Capacity to integrate with the applications listed in SOW Annex A

3.6.5.2.1.5.7 Capacity for the required 10% annual growth in users

3.6.5.2.1.5.8 Capacity for the required 30% annual growth in disk storage

3.6.5.2.1.5.9 Capacity for the required 30% annual growth in database table size

3.6.5.2.1.6 The initial SDS shall demonstrate a clear understanding of the System Architecture within which the E-NPKI Design will be implemented including WAN/LAN Topology, Interfaces, Context, Facilities, Domains and Boundary Protection requirements.

3.6.5.2.1.7 The initial SDS shall address Interface Dependencies and Constraints. In particular all separate interfaces described in SOW Annex A must be described in the Bidder's design.

3.6.5.2.1.8 The initial SDS shall take a realistic and comprehensive approach to the need to interface with external systems.

3.6.5.2.1.9 The initial SDS shall provide a centralized system management with support for centralized Service Operations Centres (SOCs). The primary SOC is co-located with a datacentre (DC). The alternate SOC is separate from the DCs.

3.6.5.2.1.10 The contractor shall assume that secondary authentication requirements (e.g. for HSMs in a DC) will be met through assignment of resources locally (at the relevant DC).

3.6.5.2.1.11 The initial SDS shall offer a credible and manageable solution for Continuity of Service and Disaster Recovery, including a description of the replication mechanisms between Data Centres and how and when are they exercised.

3.6.5.2.1.12 The initial SDS shall contain rationale which convinces that performance requirements defined in the SOW Annex A will be met.

3.6.5.2.1.13 The initial SDS shall show clear traceability between the Contractor's design and the requirements in SOW Annex A.

3.6.5.2.1.14 The initial SDS shall include (as annexes) all publicly available **product datasheets** for all products proposed to be part of the solution.

3.6.5.2.1.15 The initial SDS shall show a clear breakdown of all cryptographic components and provide a mapping to the specific NCSA certificate of approval for that applies to each cryptographic component.

3.6.5.2.1.16 The initial SDS shall include (as annexes) a copy of the Annex B-16 certificate as well as all National CIS Security Authority (NCSA) certificates available to the Bidder at the time of bid closing.

3.6.5.2.2 Overall System Engineering

3.6.5.2.2.1 For bidding purposes only, in volume 2, the Bidder shall commit to meet all requirements described in SOW Section 4.

3.6.5.3 Site survey and System Implementation

3.6.5.3.1 The Bidder shall provide an **initial System Implementation Plan (SIP)**, including initial Migration Plan, which describes its proposed approach to meeting of the requirements of SOW Section 5.

3.6.5.3.2 The initial SIP shall follow the outline from SOW Section 13.14.

3.6.5.3.3 The initial SIP shall cover the entire implementation scope (SOW Annex C), in terms of sites and quantities of end-entities.

3.6.5.3.4 The initial SIP shall demonstrate a clear understanding of the services to be implemented and describe the Bidder's approach to migration of users, devices, and applications.

3.6.5.3.5 The initial Migration Plan included in the initial SIP shall fully describe the Bidder's methodology and approach to the migration, including the stages he proposes be followed, the testing to be done, the roll back capabilities proposed and the way in which risks will be managed during the migration process.

3.6.5.3.6 For bidding purposes only, the Bidder shall assume that all elements of its design must be provided in full at the implementation stage and that no hardware, software or business processes exist on site in a reusable form.

3.6.5.3.7 The initial SIP shall describe the Bidder's approach to site surveys, identify the issues to be checked on site and relate the site survey to the overall implementation effort in terms of timing and purpose, in accordance with SOW sections 5, 10 and 16.

3.6.5.3.8 The initial SIP shall identify all information to be collected during site surveys, including locations and facilities which need to be inspected.

3.6.5.3.9 The initial SIP shall describe the size of team and level of effort involved for site surveys.

3.6.5.3.10 The initial SIP shall describe its proposed arrangements to ensure timely and complete delivery and installation of all relevant supplies, including all miscellaneous equipment (for example shelves, mounting brackets, power filters, signal filters, cables, installation kits) to enable the connection of E-NPKI elements to the existing infrastructure at a site.

3.6.5.3.11 The initial SIP shall describe its proposal for the implementation of the E-NPKI Reference System and Testbed.

3.6.5.3.12 In all descriptions provided, the Bidder shall be clear regarding how its approach minimises disruption to all services.

3.6.5.4 Testing process

3.6.5.4.1 The Bidder shall provide an **initial Project Test Plan (PTP)** covering all test activities described in SOW Section 9.

3.6.5.4.2 The initial PTP shall address all requirements in SOW Section 9.3.6 (except 9.3.6.2).

3.6.5.4.3 In particular, the initial PTP shall:

3.6.5.4.3.1 Cover all test phases described in SOW Section 9.2

3.6.5.4.3.2 Propose entry and exit criteria for each test phase

3.6.5.4.3.3 Address how each requirement shall be tested, the acceptance criteria, the types of testing to be undertaken and the locations at which testing will occur

3.6.5.4.3.4 Describe how the E-NPKI Reference System will be used to support testing activities

3.6.5.4.3.5 Describe how testing will be conducted, the test documentation to be provided and how test results will be validated and recorded.

3.6.5.4.3.6 Describe how failures and off specifications will be dealt with during testing.

3.6.5.4.3.7 Demonstrate a comprehensive understanding of the acceptance process / requirements at each test phase, and the linkage to a project milestone.

3.6.5.4.3.8 Be designed to minimise disruption to Users and services when new hardware and software are brought into service or when users and devices are migrated from iNPKI to E-NPKI.

3.6.5.4.3.9 In volume 2, the Bidder shall describe the test scenarios which will be developed to support service based testing and provide evidence that processes within services and activities within processes will be tested.

3.6.5.5 Security Accreditation

3.6.5.5.1 Certification Practices Statements

3.6.5.5.1.1 The Bidder shall provide 3 **initial Certification Practices Statement (CPS)** documents following the structure defined in the SOW Section 11.3.15 and SOW Annex A Chapter 3. Paragraph structure and numbering shall be maintained such that SOW Annex A Section 3.1 becomes paragraph 1 of the initial CPSes.

3.6.5.5.1.2 The Bidder shall provide detailed explanation of how the SRS requirements are implemented within the system.

3.6.5.5.2 The Bidder shall include details on how to validate the system's compliance against the SRS during the operational testing.

3.6.5.5.3 Security Risk Assessment

3.6.5.5.3.1 The Bidder shall provide an **initial Security Risk Assessment (SRA),** which describes its proposed technical solution and demonstrates its understanding of the requirements in SOW Section 11 and SOW Annex A.

3.6.5.5.3.2 The SRA shall cover 3 domains: the Protected Business Network (PBN, which operates up to NATO RESTRICTED) the Operational Network (ON, which operates up to NATO SECRET) and an Offline SSL interception Root CA, which operates up to NATO RESTRICTED.

3.6.5.5.4 Overall Security Accreditation process

3.6.5.5.4.1 In Volume 2, the Bid shall provide a description on the Bidder's approach to meeting the security accreditation process requirements of SOW Section 11, demonstrating a clear and complete understanding of the process.

3.6.6 Volume 3 – Supportability

3.6.6.1 This volume of the Technical Proposal covers the Bidder's approach to meeting requirements as described in SOW Section 6 (ILS), SOW Section 7 (Operation and Maintenance), SOW Section 14 (Quality Assurance and Control), SOW Section 15 (Configuration Management), and SOW Annex B (Service Approach).

3.6.6.2 Integrated Logistics Support

3.6.6.2.1 The Bidder shall provide an **initial Integrated Logistics Support Plan (ILSP)** which describes how the Bidder shall fulfil all ILS requirements in accordance with SOW Section 6.2.

3.6.6.2.2 In particular, the initial ILSP shall describe:

3.6.6.2.2.1 The Bidder's ILS organisation and responsibilities in relation to other disciplines in the project

3.6.6.2.2.2 The ILS procedures regarding spares provisioning, delivery and acceptance, transportation, documentation, warranty and training

3.6.6.2.2.3 The Bidder's approach regarding operation and maintenance activities described in SOW Section 7.

3.6.6.2.3 The Bidder shall demonstrate that all ILS activities and milestones are integrated into the project master schedule.

3.6.6.3 Training

3.6.6.3.1 The Bidder shall provide an **initial Training Plan** describing how he shall conduct the Training Requirements Analysis, and provide the necessary training courses in accordance with the SOW Section 6.

3.6.6.3.2 For bidding purposes, the Bidder may consider to include the initial Training Plan in the initial ILSP.

3.6.6.4 Quality Assurance

3.6.6.4.1 The Bidder shall provide an **initial Quality Assurance Plan** (QAP) which conforms to the requirements detailed in Section 14 of the SOW.

3.6.6.5 Configuration Management

3.6.6.5.1 The Bidder shall include in his Bid an **initial Configuration Management Plan (CMP)** which shall describe how Configuration Management will be performed in accordance with the requirements of the SOW Section 15.

3.6.6.6 Service Approach, and Operation & Maintenance

3.6.6.6.1 The Bidder shall provide a **draft SLA with NCI Agency** according to SOW Annex B and confirm in his Bid that he shall enter into a SLA agreement to provide the specified services.

3.6.6.6.2 The Bidder shall provide an **Initial Service Catalogue** according to SOW Annex B. The initial Service Catalogue shall include all services as described in Annex B, and shall propose at least two Service Level

Targets (SLTs) per Service and 2 Key Performance Indicators (KPIs) for each SLT.

3.6.6.6.3 The bid shall describe the **Bidder's approach to deliver services in line with ITIL V3** (see annex B Section 2.5). In particular, the bid shall elaborate on how the Bidder will meet the Operational and Maintenance requirements in SOW Section 7. All activities described in SOW Section 7 (i.e. governance, system operations, maintenance and helpdesk, non-production environment) will be described in the bid. The Bidder shall indicate the proposed number of Contractor FTE (Full Time Equivalent) to cover the activities described in SOW Section 7, from PSA to the end of the supporting period (i.e. FSA + 5 years).

3.6.6.6.4 For bidding purposes, the Bidder shall confirm in his bid that he will comply with all requirements from SOW Section 7 and Annex B as part of project execution and system lifecycle.

4 BID EVALUATION AND CONTRACT AWARD

4.1 General

4.1.1 The evaluation of Bids will be made by the Purchaser solely on the basis of the requirements specified in this IFB.

4.1.2 All bids will be evaluated solely using the formulae, evaluation criteria and factors contained herein. Technical Proposals will be evaluated strictly against the technical criteria and not against other Technical Proposals submitted.

4.1.3 The evaluation of bids and the determination as to the Best Value Score will be based only on that information furnished by the Bidder and contained in its Bid. The Purchaser shall not be responsible for locating or securing any information that is not identified in the Bid.

4.1.4 The Bidder shall furnish with its Bid all information requested by the Purchaser in Book 1, Section 3 Bid Preparation Instructions. Significant omissions and/or cursory submissions will result in a reduced Best Value Score and may result in a determination of non-compliance without recourse to further clarification. The information provided by the Bidder in its proposal shall be to a level of detail necessary for the Purchaser to fully comprehend exactly what the Bidder proposes to furnish as well as its approach and methodologies.

4.1.5 During the evaluation, the Purchaser may request clarification of the Bid from the Bidder and the Bidder shall provide sufficient detailed information in connection with such requests as to permit the Purchaser to make a final assessment of the bid based upon the facts. The purpose of such clarifications will be to resolve ambiguities in the bid and to permit the Bidder to state its intentions regarding certain statements contained therein. The purpose of the

clarification stage is not to elicit additional information from the Bidder that was not contained in the original submission or to allow the Bidder to supplement cursory answers or omitted aspects of the Bid. The Bidder is not permitted any cardinal alteration of the Bid regarding technical matters and shall not make any change to its price quotation at any time.

4.1.6 The Purchaser reserves the right, during the evaluation and selection process, to verify any statements made concerning experience, facilities, or existing designs or materials by making a physical inspection of the Bidder's facilities and capital assets. This includes the right to validate, by physical inspection, the facilities and assets of proposed subcontractors.

4.1.7 The evaluation will be conducted in accordance with NATO Infrastructure Bidding Procedures as set forth in the document, and the Best Value evaluation procedures set forth in AC/4-D(2008)0002, “Procedures and Practices for Conducting NSIP International Competitive Bidding Using Best Value Methodology”. The bid evaluation methodology to be followed, including the top-level evaluation criteria and their weighting factors, were agreed by the NATO Infrastructure Committee.

4.2 Best Value Award Approach and Bid Evaluation Factors

4.2.1 The Contract resulting from this IFB will be awarded to the Bidder whose conforming offer provides the Best Value to NATO, as evaluated by the Purchaser in compliance with the requirements of this IFB and according to the evaluation method specified in this Section 4. The top level criteria are 50% Price and 50% Technical.

4.2.2 Upon approval of the price evaluation report, the Contracts Award Board will open the technical weighting scheme and apply the technical weight to the raw Technical Score (TS) to produce the weighted technical score.

4.2.3 The weighted Technical Score will be determined according to the following formula:

$$TS = a\%*TS1 + b\%*TS2 + c\%*TS3 + d\%*TS4$$

where: TS1, TS2, TS3, TS4 ≤ 100 are the Technical Scores of each of the authorised second-level or published third-level technical sub-criteria; and a% b% c%, d%…are the related weighting factors for each of the second-level or third-level technical sub-criteria adding to 100.

4.2.4 The Purchaser’s priorities in the evaluation of the Technical Proposal are described in the form of sub criteria in Section 4.5 below. The sub criteria are listed in descending order that reflects the relative importance that the Purchaser places on each sub criterion.

4.2.5 A weighting scheme for sub-criteria values has been developed by Purchaser staff not associated with the Technical Evaluation. This weighting scheme has

been sealed and is not known to any of the Purchaser staff beyond the originator and the Chairman of the Contracts Award Board, who are not evaluators within the framework of this IFB or in any manner or form are made privy of evaluation information throughout the course of the evaluation process. The weighting scheme remains sealed until Step 4 of the evaluation process, described in Section 4.7.

4.2.6 The BV final Score (FS) will be the sum of weighted TS plus Price Score (PS), according to the following formula:

$$FS = PS*z\% + TS*(1-z\%) \leq 100$$

where: z% = 50%, is the authorised weighting factor for the Price Criterion.

4.2.7 The bid having the highest BV final score will be selected as the successful bid unless there is a statistical tie.

4.3 Evaluation Procedure

4.3.1 The evaluation will be done in a four step process, as described below:

4.3.1.1 Step 1: Administrative Compliance

4.3.1.1.1 Bids received will be reviewed for compliance with the mandatory Administrative requirements specified in Section 4.4. Bids not meeting all of the mandatory requirements may be determined to be non-compliant and not further considered in the evaluation or for award.

4.3.1.2 Step 2: Technical Evaluation

4.3.1.2.1 In Step 2 bids will have their Technical Proposals Packages evaluated against predetermined top-level criteria and identified sub-criteria (see paragraph below), and scored accordingly. This evaluation will result in “raw” or not weighted technical scores against the criteria.

4.3.1.2.2 Bidders are advised that any Bid whose Technical Proposal receives a score of less than 20% of the not weighted raw score possible in any of the sub-criteria listed in Section 4.5 of this document may be determined by the Purchaser to be non-compliant and not further considered for award.

4.3.1.3 Step 3: Price Evaluation

4.3.1.3.1 The Price Quotations of all bids remaining after Step 2 will be opened, evaluated and scored in accordance with Section 4.6.

4.3.1.4 Step 4: Determination of Apparently Successful Bidder

4.3.1.4.1 Upon completion of the Price Evaluation, the Apparent Successful Bid will be determined in accordance with Section 4.7 hereafter.

4.4 Evaluation Step 1 - Administrative Compliance

4.4.1 Bids will be reviewed for compliance with the formal requirements for Bid submission as stated in this IFB and the content of the Administrative Documentation Package. The evaluation of the Administrative Documentation Package will be made on its completeness, conformity and compliance to the requested information. This evaluation will not be scored in accordance with Best Value procedures but is made to determine if a bid complies with the requirements of the Bidding Instructions and Prospective Contract. Specifically, the following requirements shall be verified:

4.4.1.1 The Bid was received by the Bid Closing Date and Time;

4.4.1.2 The Bid is packaged and marked properly;

4.4.1.3 The Bid Administration Package contains the documentation listed in Section 3.4 above and complies with the formal requirements established in Section 3.1 above;

4.4.1.4 The Bidder has not taken exception to the Terms and Conditions of the Prospective Contract or has not qualified or otherwise conditioned its offer on a modification or alteration of the Terms and Conditions or the language of the Statement of Work (including all its Annexes); and

4.4.1.5 Evaluation of Conflict of Interest Documentation

4.4.1.5.1 The Purchaser will evaluate the Bidder submission as detailed in Section 3.4.3.2 and resort to the disqualification of the bid in those cases in which it is deemed that the Bidder's relationships with the PMIC existing or Prospective Contractor could constitute a real or apparent conflict of interest, could in any manner or form influence or appear to influence the capacity of the Bidder to render unbiased service or otherwise result in an advantage during the course of the performance under the prospective Contract and any proposed conflict of interest mitigation plan proposed by the Bidder does not satisfactorily resolve the conflict of interest in place.

4.4.1.5.2 Conversely, should the Purchaser deem that the Bidder's Conflict of Interest Mitigation Plan adequately addresses the concerns relevant to any conflict of interest, it will make such plan part of any awarded Contract and subject to the stipulation of Clause 30 of the prospective Contract Special Provisions. Equally in those cases where the Bidder declares that no apparent or real conflict of interest exists such condition shall be reflected in any resulting Contract and made subject to the prescription of Clause 30 of the prospective Contract Special Provisions.

4.4.1.5.3 In the event that, during the evaluation of the Bids, the Purchaser would determine or suspect that the Bidder has not disclosed a real or apparent conflict of interest of which it was knowledgeable at the time of Bid submission, in breach of Sections 4.4.1.5.1 and 4.4.1.5.2, Purchaser reserves the right to declare the Bid non-compliant.

4.4.2 Subject to the stipulation of Section 4.4.1.1 thru 4.4.1.5 Bids failing to conform to the above requirements may be declared non-compliant and may not undergo through further evaluation. Bids that are determined to be administratively compliant will proceed to Step 2, Technical Evaluation.

4.4.3 Notwithstanding Section 4.4.2, if it is later discovered in the evaluation of the Technical Proposal or the Price Quotation that the Bidder has taken exception to the Terms and Conditions of the Prospective Contract, or has qualified and/or otherwise conditioned his offer on a modification or alteration of the Terms and Conditions or the language of the Statement of Work (including all its Annexes), the Bidder may be determined to have submitted a non-compliant bid at the point in time of discovery.

4.5 Evaluation Step 2 - Technical Evaluation

4.5.1 The Technical Proposal will be evaluated against the criteria set forth in Section 4.2 above. In this section those criteria will be expanded to identify sub criteria considered important by the Purchaser during bid evaluation. Sub criteria appear in descending order of importance within the criterion of which they form a part. For some sub-criteria, there may be additional supporting factors at the next lower level. These lower level factors are not published here but are predetermined and included in the Technical Evaluation Weighting Scheme sealed before Bid Opening. Within each of the three volumes of the Technical Proposal the criteria and their sub criteria are identified as follows:

4.5.2 Volume 1 - Management and Risk

4.5.2.1 Criteria – Management (25% of the Technical Proposal)

4.5.2.1.1 Sub criteria in descending order of importance:

4.5.2.1.1.1 Overall understanding of the objectives / scope / requirements of the E-NPKI project

4.5.2.1.1.2 Bidder Qualifications and Key Personnel

4.5.2.1.1.3 Commitment to Project Milestones and a schedule which shows how they will be achieved

4.5.2.1.1.4 Quality and completeness of the initial Project Management Plan and WBS

4.5.2.1.1.5 Quality of the Project Management Communications proposed in the bid. In particular the approach to status reporting, communications tools and web space.

4.5.2.1.1.6 Compliance with requirements in Section 3.6.4.9. In particular completeness and quality of the PFE list, and commitment to integrate with PFE.

4.5.2.1.1.7 Quality of the Executive Summary

4.5.2.2 Criteria – Risk (20% of the Technical Proposal)

4.5.2.2.1 Sub criteria in descending order of importance:

4.5.2.2.1.1 Overall level of risk according to the initial Risk Log

4.5.2.2.1.2 Quality of the initial Risk Log and relevance of the risks identified

4.5.2.2.1.3 Adequacy and pertinence of the mitigation measures proposed for the risks identified in the initial Risk Log

4.5.2.2.1.4 Adequacy of the Bidder's proposal to manage risk throughout the project

4.5.3 Volume 2 - Engineering

4.5.3.1 Criteria – Engineering (25% of the Technical Proposal)

4.5.3.1.1 Sub criteria in descending order of importance:

4.5.3.1.1.1 Quality and completeness of the initial Certification Practices Statements

4.5.3.1.1.2 Quality and completeness of the initial System Design Specification (SDS) document, and commitment to meet all System Engineering requirements

4.5.3.1.1.3 Quality and completeness of the initial Security Risk Assessments (SRA)

4.5.3.1.1.4 Quality and completeness of the Bidder's approach to meeting the security accreditation process requirements

4.5.3.1.1.5 Quality and completeness of the initial System Implementation Plan (SIP), including site survey process and initial Migration plan.

4.5.3.1.1.6 Quality and completeness of the testing process and initial Project Test Plan (PTP)

4.5.4 Volume 3 – Supportability

4.5.4.1 Criteria – Supportability (30% of the Technical Proposal)

4.5.4.1.1 Sub criteria in descending order of importance:

4.5.4.1.1.1 Sound Service Approach and Operation and Maintenance approach in line with SOW, and commitment to comply with requirements of SOW Section 7 and SOW Annex B.

4.5.4.1.1.2 Completeness and quality of the initial ILSP ensuring that proposed ILS arrangements are optimized and acceptable, and in line with SOW

4.5.4.1.1.3 Realistic and credible initial Training Plan, and in line with SOW

4.5.4.1.1.4 Completeness and Quality of the initial CMP, and in line with SOW

4.5.4.1.1.5 Initial Quality Assurance Plan testifies that QA processes are mature and comprehensive, and in line with SOW

4.6 Evaluation Step 3 - Price Evaluation

4.6.1 The Bidder's Price Quotation will be first assessed for compliance against the following criteria:

4.6.1.1 The Price Quotation meets the requirements set forth in the Bid Preparation Section and the Instructions for Preparation of the Bidding Sheets in Annex A-2.

4.6.1.2 Detailed pricing information has been provided and is adequate, accurate, traceable, and complete; and

4.6.1.3 The Price Quotation meets requirements for price realism and balance as described below in Section 4.6.4. and do not exceed the defined ceilings as per Para 3.5.2.1.

4.6.2 A bid which fails to meet the compliance standards defined in this section may be declared non-compliant and may not be evaluated further by the Purchaser.

4.6.3 Basis of Price Comparison

4.6.3.1 The Purchaser will convert all prices quoted into EURO for purposes of comparison and computation of price scores and compliance with stated price ceilings. The exchange rate to be utilised by the Purchaser will be the average of the official buying and selling rates of the European Central Bank at close of business on the last working day preceding the Bid Closing Date.

4.6.3.2 The Evaluated Bid Price to be inserted into the formula specified at Section 4.6.7 will be derived from the Grand Total of the Schedule of Supplies and Services calculated as follows:

- The Sum of the Firm - Fixed Prices offered for CLINS 1-7 and 10-18, as detailed below:

CLIN Number	CLIN Name

1.0	PROJECT MANAGEMENT
2.0	SYSTEMS ENGINEERING
3.0	SYSTEM IMPLEMENTATION
4.0	INTEGRATED LOGISTICS SUPPORT (ILS)
5.0	OPERATIONS AND MAINTENANCE (OPTION)
6.0	IMPLEMENTATION AT NATO-HQ (OPTION)
7.0	IMPLEMENTATION AT NAEW&C (OPTION)
10.0	IMPLEMENTATION AT NCIA (OPTION)
11.0	IMPLEMENTATION AT NSPA (OPTION)
12.0	IMPLEMENTATION AT STO (OPTION)
13.0	IMPLEMENTATION AT NAGSMA (OPTION)
14.0	IMPLEMENTATION AT NAHEMA (OPTION)
15.0	IMPLEMENTATION AT NETMA (OPTION)
16.0	IMPLEMENTATION AT NAPMA (OPTION)
17.0	IMPLEMENTATION AT NDC (OPTION)
18.0	IMPLEMENTATION AT NSO (OPTION)

4.6.4 Price Balance and Realism

4.6.4.1 In the event that the successful Bidder has submitted a price quotation that is less than two thirds of the average of the remaining compliant bids, the Purchaser must ensure that the successful Bidder has not artificially reduced the offered price to assure contract award. As such, the Purchaser will request the firm to provide clarification of the bid and will inform the national delegation of the firm. In this regard, the Bidder shall provide an explanation to both Purchaser and their national delegation on the basis of one of the following reasons:

4.6.4.1.1 An error was made in the preparation of the price quotation. The Bidder must document the nature of the error and show background documentation regarding the preparation of the price quotation that convincingly demonstrates that an error was made by the Bidder. In such a case the Bidder may request to remain in the competition and accept the contract at the bid price, or to withdraw from the competition;

4.6.4.1.2 The Bidder has a competitive advantage due to prior experience or internal business/technological processes that demonstrably reduce cost to the Bidder resulting in an offered price that is realistic. The Bidders explanation must support the technical proposal offered and convincingly and objectively describe the competitive advantage of and savings achieved by the advantage over the standard marked costs, practices and technology;

4.6.4.1.3 The Bidder understands that the submitted price quotations are unrealistically low in comparison with the level of effort required. In this case, the Bidder is required to estimate the potential loss and show that the financial resources of the Bidder are adequate to withstand such a reduction in revenue.

4.6.4.1.4 If a Bidder fails to submit a comprehensive and convincing explanation for one of the based above, the Purchaser shall declare the bid non-compliant and the Bidder will so be notified in accordance with the procedures set forth in paragraph 13(iii)(b) of AC/4-D/2261(1996 Edition). Non-compliance for reasons of bid realism is a basis for lodging a complaint under the dispute procedure.

4.6.4.1.5 If the Purchaser accepts the Bidders explanation of a mistake and allows the Bidder to accept the contract at the Bid price or the explanation regarding competitive advantage in convincing, the Bidder shall agree that the supporting pricing data submitted with this bid will be the basis to determine fair and reasonable pricing for all subsequent negotiations for modifications or additions to the contract and that no revisions of proposed prices will be made.

4.6.5 In the case of incrementally funded projects, the cost and pricing methodology used by the winning Bidder on the base contract will be used as the basis for all follow-on contracts or amendments to the base contract where these are proposed for IC agreement without competition.

4.6.6 Determination of the Price Score. Once the technical report has been approved by the Contract Awards Board and all issues of compliance completed, the price quotations will be opened and evaluated. The Price Score shall be determined according to the following formula:

4.6.7 PS = 100*(1-(Bid Price / (2 x Average Bid Price))

4.6.8 where: Bid Price and Average Bid Price will be the investment cost or the Present Value of the system life-cycle cost as per the authorisation.

4.7 Evaluation Step 4 – Calculation of Best Value Scores

4.7.1 Upon conclusion and approval of the Price Evaluation results, the pre-determined third level weighting scheme for the Technical Evaluation will be unsealed and the scores for the Engineering, Management, Supportability, and Risk factors will be calculated for each compliant bid. Then all partial scores will be fed into the formula stated in Section 4.2.3 in order to obtain the Best Value Score of each bid.

4.7.2 The highest scored bid will be recommended as the Apparent Successful Bid.

4.7.3 A statistical tie is deemed to exist when the final scores of the highest scoring bids are within one point of each other. The Purchaser will then resolve the

statistical tie by awarding the contract to the Bid with the highest weighed technical score.

Annex A Bidding Sheets

Provided as Excel Workbook file (“2_IFB-CO-13810-CS Book I Annex A Bidding Sheets.xlsx”)

Annex A-1. Bidding Sheets

On behalf of the firm stated below I hereby offer the Purchaser the services and deliverables (collectively referred as "ITEMS") set forth in the attached schedules[1], at the specified prices, and subject to the terms and conditions stated in IFB-CO-13810-CS.

Date : .....

Signature : .....

Name & Title : .....

Company : .....

Bid Reference : .....

[1] Bidders must fill out, print, and attach to this cover page a hardcopy of the worksheets contained in the file "2_IFB-CO-13810-CS - Book I Annex A Bidding Sheets.xlsx" that was provided to them as part of the IFB package.

Annex A-2. Instructions for the Preparation of Bidding Sheets

1. INTRODUCTION

Bid pricing requirements as addressed in this Annex are mandatory. Failure to abide to the prescriptions of bid submission referred in this section may lead to the bid being declared non-compliant and not being taken into consideration for award.

No alteration of the bidding sheets including but not limited to quantity indications, descriptions or titles are allowed with the sole exception of those explicitly indicated as allowed in this document. Additional price columns may be added if multiple currencies are bid, including extra provisions for all totals.

2. GENERAL REQUIREMENTS

Bidders shall follow the specific instructions provided in each worksheet.

Bidders shall insert information in all yellow cells.

The prices and quantities entered on the document shall reflect the total items required to meet the contractual requirements. The total price shall be indicated in the appropriate columns.

In preparing the Bidding Sheets, Bidders shall ensure that the prices of the Sub-items total the price of the major item of which they constitute a part.

All metrics (e.g., cost associated with labour) will be assumed to be standard or normalised to 7.6 hour/day, for a five day working week at NATO sites and Contractor facilities located within Europe and 8 hours/day at NATO sites and Contractor facilities located in the United States.

Should the bid be in other than Euro currency, the award of the contract will be made in the currency or currencies of the bid.

Bidders are advised that formulae are designed to ease evaluation of the Bidders proposal have been inserted in the electronic copies of the Bidding Sheets. Notwithstanding this the Bidder remains responsible for ensuring that their figures are correctly calculated and should not rely on the accuracy of the formulae electronic copies of the Bidding Sheets.

If the Bidder identifies an error in the spreadsheet, it should notify the Purchaser who will make a correction and notify all the Bidders of the update.

Any discounted or reduced prices offered by the Bidder must be traceable to a CLIN or CLINs at the lowest level. Prices and detail of the traceability of application of the discount shall be clearly identified in the supporting detail sheets and applied at the unit price level.

3. STRUCTURE OF BIDDING SHEETS.

The Bidding Sheets provided in MS Office Excel format are organised according to the following structure:

- Instructions
- Section 1:
  - CLIN Summary Sheet
  - Detailed CLIN Summary Sheet
  - Site Summary Sheet
  - Delivery per Site Sheet
  - CLIN X Sheets

- Section 2:
  - Detailed Bidding Sheets

4. COMPLETING SECTION 1 (CLIN Summary Sheet, Detailed CLIN Summary Sheet, Site Summary Sheet and CLIN X Sheets)

Section 1, CLIN X Sheets correspond to the Schedule of Supplies and Services of the Prospective Contract. Each Work Package (WP) included in the contract is represented by a detailed schedule showing the Contract Line Items (CLINs) included within the scope of the Work Package (Detailed bidding sheet tabs) and a detailed cost breakdown attached to each WP schedule.

4.1 Filling the CLIN Summary Sheet, Detailed CLIN Summary Sheet, Site Summary Sheet and CLIN X Sheets

Bidders shall fill in the corresponding sheets in Section 1 (except the “Delivery per Site” Sheet) based on the information provided in the detailed bidding sheets (CLIN Price Breakdown sheets). The detailed bidding sheets are broken down in to the categories listed in Section 5. Bidders are expected to aggregate the prices in the detailed bidding sheets that make up the line items in the Section 1 summary sheets. The line items in the Section 1 summary sheets shall be all INCLUSIVE of the price being bid in order to fulfil the requirement for the line item in the CLIN X Summary Sheets. Bidders shall make sure that the total price indicated in the Detailed Bidding Sheets matches the price stated in the Section 1 summary sheets for the same corresponding CLIN or sub-CLIN.

In the CLIN Summary and Detailed CLIN Summary Sheets Bidders shall enter the prices of each CLIN in the corresponding column for each line item. The Investment

and O&M prices are separated by each CLIN X Sheet and relevant Detailed Bidding Sheets.

In the Site Summary Sheet, Bidders shall enter the corresponding prices for each CLIN across each location indicated. The prices shall be broken down into the following categories which are further described below in Section 5:

- Materials
- Labour
- Travel

These prices are to be aggregated in the total lines per CLIN and Overall Totals across all the locations and CLINs.

Bidders shall enter the corresponding values in yellow and ensure that the prices indicated match the prices stated in the detailed bidding sheets for each sheet in Section 1.

5. COMPLETING SECTIONS (Detailed Bidding Sheets)

Bidders are instructed to prepare their cost proposals in sufficient detail to permit thorough and complete evaluation. If multiple currencies are included in the price offer, the following sheets shall be duplicated and not modified for each currency bid: 1) CLIN Summary Sheet, 2) Detailed CLIN Summary Sheet, 3) Site Summary Sheet and 4) Detailed CLIN Pricing Breakdown Sheets. In addition, for each additional currency, the Bidders shall add two columns ("Unit Price", and "Total Firm Fixed Price) in the CLIN X Pricing Sheets and change the currency in the header of the columns as necessary. Each Detailed CLIN Pricing Breakdown Sheet shall correspond to the CLIN X Pricing Sheet currency columns as appropriate.

5.1. MATERIAL

A. Purchased Parts: Provide a consolidated priced summary of individual material quantities included in the various tasks, orders, or contract line items being proposed and the basis for pricing.

(1) Raw Material: Consists of material in a form or state that requires further processing. Provide priced quantities of items required for the proposal. Show total cost.

(2) Standard Commercial Items: Consists of items that the Bidder normally fabricates, in whole or in part, and that are generally stocked in inventory. Provide an appropriate explanation of the basis for pricing on attached schedule.

(3) The Bidder shall provide a level of detail down the unique sellable item level (e.g. smartcards, OCSP, RAs, etc.)

(4) The Bidder shall group the materials offered per defined E-NPKI service (Business Services and Support Services – see SOW Annex B Section 2.2.4)

(5) The Bidder shall provide unit prices that shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance. Factors for overhead shall be applied in the MATERIAL LABOUR OVERHEAD section of the detailed bidding sheet to the total cost of material.

5.2 DIRECT LABOUR

Show the hourly rate by year and the total hours for the categories and disciplines of direct labour proposed.

Unit prices shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance. Factors for overhead shall be applied in the DIRECT LABOUR OVERHEAD section of the detailed bidding sheet to the total cost of direct labour.

5.3 SUBCONTRACT LABOUR

Show the hourly rate by year and the total hours for the categories and disciplines of subcontract labour proposed Unit prices shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance. Factors for overhead shall be applied in the SUBCONTRACT LABOUR OVERHEAD section of the detailed bidding sheet to the total cost of subcontract labour.

5.4 TRAVEL

Show the number of trips being made, the number of people travelling, the number of days per trip, the cost of traveling (e.g. flight costs), and the daily per diem rate.

Insert comments/descriptions/references/explanation of calculation method under the 'Notes' column including the location & reference to SOW.

5.5 OTHER DIRECT COSTS

A. Special Tooling/Equipment. Identify and support specific equipment and unit prices. Use a separate schedule if necessary.

B. Individual Consultant Services. Identify and support the proposed contemplated consulting. State the amount of services estimated to be required and the consultant’s quoted daily or hourly rate.

C. Other Costs. List all other direct charge costs not otherwise included in the categories described above (e.g., services of specialized trades, computer services, preservation, packaging and packing, leasing of equipment, ex-pat costs etc.) and provide bases for pricing.

6. GRAND TOTAL

This is the Bidders final Firm Fixed Price total for the identified CLIN or sub-CLIN and should match the price entered in the corresponding summary sheets in Section 1 of the bidding sheets.

7. SPECIAL INSTRUCTIONS

7.1 “Not-to Exceed” Ceilings are addressed by separate sheets within the bidding sheets. Each CLIN has been broken down by sub-CLIN indicated on the CLIN X Sheet and shall be broken down in the corresponding detailed bidding sheets accordingly.

7.2 System Implementation

The Bidders shall provide a price for each sub-CLIN “Site-Specific System Implementation deliverables – Technical Services” and CLINs “Site-Specific System Implementation deliverables – User Services” for each Option CLIN based on the item highlighting colour of the “Delivery per Site” Tab. The Bidders shall provide a price for each Site Specific Deliverable highlighted in GREEN in the Technical Services sub-CLIN and shall provide a price for each Site Specific Deliverable highlighted in YELLOW in the User Services sub-CLIN.

7.3 Option CLIN 19

The Bidders shall provide a price for the sub-CLINs of CLIN 19 such that if an additional installation, activity, or hardware/software is required to be procured, CLIN 19 can be exercised by the sub-CLINs as needed by the Purchaser. The unit price for each sub-CLIN is to be indicated by the Bidder in the Calendar Year selected at the top of the detailed bidding sheets. The corresponding labour rates, materials, etc., per year are to be entered into the detailed bidding sheets and used as a basis for exercising these Option sub-CLINs in a later year. The sub-CLIN prices per annum, on the detailed bidding sheets, shall be consistent with the unit prices in all other CLINs.

7.4 Warranty Activities (SOW Reference 6.9 and 7.5)

The Bidders shall include the prices for the Warranty Activities within the prices each unit of hardware and software being procured.

Annex B Prescribed Administrative Forms and Certificates

Annex B-1. Certificate of Legal Name of Bidder

This Bid is prepared and submitted on behalf of the legal corporate entity specified below:

FULL NAME OF CORPORATION: _____

DIVISION (IF APPLICABLE): _____

SUB DIVISION (IF APPLICABLE): _____

OFFICIAL MAILING ADDRESS

_____

_____

_____

E-MAIL ADDRESS: _____

TELEFAX No: _____

POINT OF CONTACT REGARDING THIS BID:

NAME: _____
POSITION: _____
TELEPHONE: _____

ALTERNATIVE POINT OF CONTACT:

NAME: _____
POSITION: _____
TELEPHONE: _____

_____ _____
Date Signature of Authorised Representative

_____
Printed Name

_____
Title

_____
Company

Annex B-2. Acknowledgement of Receipt of IFB Amendments

I confirm that the following amendments to Invitation for Bid IFB-CO-13810-CS have been received and the Bid, as submitted, reflects the content of such amendments.

Amendment no.	Date of Issued	Date of receipt	Initials

_____ Date

_____ Signature of Authorised Representative

_____ Printed Name

_____ Title

_____ Company

Annex B-3. Certificate of Independent Determination

It is hereby stated that:

a. We have read and understand all documentation issued as part of IFB-CO-13810-CS. Our Bid submitted in response to the referred solicitation is fully compliant with the provisions of the IFB and the prospective contract.

b. Our Bid has been arrived at independently, without consultation, communication or agreement, for the purpose of restricting competition, with any other Bidder or with any competitor;

b. The contents of our Bid have not been knowingly disclosed by the Bidder and will not knowingly be disclosed by the Bidder prior to award, directly or indirectly to any other Bidder or to any competitor; and

c. No attempt has been made, or will be made by the Bidder to induce any other person or firm to submit, or not to submit, a Bid for the purpose of restricting competition.

Date : .....

Signature : .....

Name & Title : .....

Company : .....

Bid Reference : .....

Annex B-4. Certificate of Bid Validity

I, the undersigned, as an authorised representative of the firm submitting this Bid, do hereby certify that the pricing and all other aspects of our Bid will remain valid for a period of twelve months from the Bid Closing Date of this Invitation for Bid.

.....	.....
Date	Signature of Authorised Representative
	.....
	Title
	.....
	Company

Annex B-5. Certificate of Exclusion of Taxes, Duties and Charges

I hereby certify that the prices offered in the price quotation of this Bid exclude all taxes, duties and customs charges from which the Purchaser has been exempted by international agreement.

…….
Date

…….
Signature of Authorised Representative

…….
Title

…….
Company

Annex B-6. Comprehension and Acceptance of Contract Special and General Provisions

The Bidder hereby certifies that he has reviewed the Special Contract Provisions and the NCI Agency General Provisions set forth in the Prospective Contract, Book II of this Invitation for Bid. The Bidder hereby provides its confirmation that he fully comprehends the rights, obligations and responsibilities of the Contractor as set forth in the Articles and Clauses of the Prospective Contract. The Bidder additionally certifies that the offer submitted by the Bidder is without prejudice, qualification or exception to any of the Terms and Conditions and he will accept and abide by the stated Special and General Provisions if awarded the contract as a result of this Invitation for Bid.

…….
Date

…….
Signature of Authorised Representative

…….
Title

…….
Company

Annex B-7. Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements

I, the undersigned, as an authorised representative of _____, certify the following statement:

All supplemental agreements, defined as agreements, documents and/or permissions outside the body of the Contract but are expected to be required by my Government, and the governments of my subcontractors, to be executed by the NCI Agency, or its legal successors, as a condition of my firm's performance of the Contract, have been identified, as part of the Bid.

These supplemental agreements are listed as follows:

Examples of the terms and conditions of these agreements have been provided in our Offer. The anticipated restrictions to be imposed on NATO, if any, have been identified in our offer along with any potential conflicts with the terms, conditions and specifications of the Prospective Contract. These anticipated restrictions and potential conflicts are based on our knowledge of and prior experience with such agreements and their implementing regulations. We do not certify that the language or the terms of these agreements will be exactly as we have anticipated.

The processing time for these agreements has been calculated into our delivery and performance plans and contingency plans made in the case that there is delay in processing on the part of the issuing government(s).

We recognise that additional supplemental agreements, documents and permissions presented as a condition of Contract performance or MOU signature after our firm would be selected as the successful Bidder may be cause for the NCI Agency, or its legal successors, to determine the submitted bid to be non-compliant with the requirements of the IFB;

We accept that should the resultant supplemental agreements issued in final form by the government(s) result in an impossibility to perform the Contract in accordance with its schedule, terms or specifications, the contract may be terminated by the Purchaser at no cost to either Party.

…….
Date

…….
Signature of Authorised Representative

…….
Title

…….
Company

Annex B-8. Certificate of Compliance AQAP 2110 or ISO 9001:2008 or Equivalent

I hereby certify that _____(name of Company) possesses and applies Quality Assurance Procedures/Plans that are equivalent to the AQAP 2110 or ISO 9001:2008 as evidenced through the attached documentation[2].

_____ _____

Date Signature of Authorised Representative

_____

Printed Name

_____

Title

_____

Company

[2] Bidders must attach copies of any relevant quality certification.

Annex B-9. List of Prospective Major Subcontractors

Name and Address of Subcontractor	DUNS Number [3]	Primary Location of Work	Items/Services to be Provided	Estimated Value of Subcontract

Date

Signature of Authorised Representative

Printed Name

Title

Company

[3] Data Universal Numbering System (DUNS). Bidders are requested to provide this data in order to help NCIA to correctly identify major (one that exceeds 15% of total contract value) Subcontractors. If a Subcontractor's DUNS is not known this field may be left blank.

Annex B-10. Bidder Background IPR

I, the undersigned, as an authorised representative of Bidder _____, warrant, represent, and undertake that:

a. The Contractor Background IPR specified in the table below will be used for the purpose of carrying out work pursuant to the prospective Contract.

ITEM	DESCRIPTION

b. The stated Bidder has and will continue to have, for the duration of the prospective Contract, all necessary rights in and to the Background IPR specified above.

c. The Background IPR stated above complies with the terms specified in the Book II prospective contract General and Special Provisions.

_____ _____

Date Signature of Authorised Representative

_____

Printed Name

_____

Title

_____

Company

Annex B-11. List of Subcontractor IPR

I, the undersigned, as an authorised representative of Bidder _____, warrant, represent, and undertake that:

a. The Subcontractor IPR specified in the table below will be used for the purpose of carrying out work pursuant to the prospective Contract.

ITEM	DESCRIPTION

b. The stated Bidder has and will continue to have, for the duration of the prospective Contract, all necessary rights in and to the IPR specified above necessary to perform the Contractor's obligations under the Contract.

c. The Subcontractor IPR stated above complies with terms specified in the Book II prospective contract General and Special Provisions.

_____ _____

Date Signature of Authorised Representative

_____

Printed Name

_____

Title

_____

Company

Annex B-12. Certificate of Origin of Equipment, Services, and Intellectual Property

The Bidder hereby certifies that, if awarded the Contract pursuant to this solicitation, he will perform the Contract subject to the following conditions:

(a) none of the work, including project design, labour and services shall be performed other than by firms from and within participating NATO member countries;

(b) no material or items of equipment down to and including identifiable sub-assemblies shall be manufactured or assembled by a firm other than from and within a participating NATO member country. (A sub-assembly is defined as a portion of an assembly consisting of two or more parts that can be provisioned and replaced as an entity); and

(c) the intellectual property rights for all software and documentation incorporated by the prospective Contractor and/or its Sub-contractors into the work shall vest with persons or legal entities from and within NATO participating nations and no royalties or licence fees for such software and documentation shall be paid by the Contractor to any source that does not reside within a NATO participating nation

_____ _____

Date Signature of Authorised Representative

_____

Printed Name

_____

Title

_____

Company

Annex B-13. List of Proposed Key Personnel

Position	SOW Reference	Labour Category	Name	Designation Period
Project Manager	3.3.2.4.1			EDC thru Contract completion
Technical Lead	3.3.2.4.2			EDC thru Contract completion
Test Director	3.3.2.4.3			EDC thru Contract completion
Service Delivery Manager	3.3.2.4.4			EDC thru Contract completion

Date

Signature of Authorised Representative

Printed Name

Title

Company

Annex B-14. Certificate of Price Ceiling

I hereby certify that the total price offered in the price quotation of this Bid for CLINs 1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 17 and 18 of the Bidding Sheets does not exceed **EUR 25,968,664** (twenty-five million nine hundred sixty-eight thousand six hundred sixty-four Euro) as described in Section 3.5.2.1 of Book I.

I hereby certify that the total price offered in the price quotation of this Bid for the O&M portion of CLINs 1, 2, 3, 4, 5, 6, 7, 10, 11, 12, 13, 14, 15, 16, 17 and 18 of the Bidding Sheets does not exceed **EUR 9,228,044** (nine million two hundred twenty-eight thousand forty-four Euro) as described in Section 3.5.2.1 of Book I.

Note: Price information of your Bid shall not be disclosed in the Bid Administration Package, or the Technical Proposal Package.

_____ _____

Date Signature of Authorised Representative

_____

Printed Name

_____

Title

_____

Company

Annex B-15. Disclosure of Conflict of Interest

I, the undersigned, as an authorised representative of _____, (*company name*) certify that[4]:

(check one of the following statements:)

☐ a real or apparent conflict of interest as defined in Section 3.4.4 of the Bidding Instructions does not exist.

☐ a real or apparent conflict of interest as defined in Section 3.4.4 of the Bidding Instructions may exist and a plan for the mitigation of the conflict is provided in attachment to this Certificate.

(check one of the following statements:)

☐ business relationships as defined under Section 3.4.4 of the Bidding Instructions do not exist.

☐ business relationships as defined under Section 3.4.4 of the Bidding Instructions exist and have been identified in attachment to this Certificate.

_____ _____

Date Signature of Authorised Representative

_____

Printed Name

_____

Title

_____

Company

[4] Bidders are to check the appropriate box(es).

Annex B-16. National CIS Security Authority Approval for Cryptographic Hardware and Software

I hereby certify that _____ (name of Company) has secured approval letters and/or certificates for all cryptographic Hardware and Software included within this bid and have coordinated with the National CIS Security Authorities of a participating NATO Nation to ensure that these approval letters and/or certificates will be delivered to the Purchaser prior to conclusion of the bid evaluation. I certify that all cryptographic components necessary to implement this project have been identified in the table below.

ITEM	Nation of Manufacture	NATO Nation CIS Security Authority (NCSA)	NCSA Approval Date	Full NCSA POC Details including email address
[e.g. Certificate Authority]				
[e.g. Registration Authority]				
[e.g. Card Management System]				
[e.g. Online Certificate Status Protocol Server]				
[e.g. Timestamp]				
[e.g. Hardware Security Module]				
[e.g. Smartcard]				

Date

Signature of Authorised Representative

Printed Name

Title

Company

Annex C Bid Guarantee - Standby Letter of Credit

Standby Letter of Credit Number:

Issue Date: _____

Beneficiary: NCI Agency, Financial Management Office
Boulevard Leopold III, B-1110, Brussels
Belgium

Expiry Date: _____

1. We, (issuing bank) hereby establish in your favour our irrevocable standby letter of credit number {number} by order and for the account of (NAME AND ADDRESS OF BIDDER) in the original amount of € 150,000 (One Hundred Fifty Thousand Euro). We are advised this Guarantee fulfils a requirement under Invitation for Bid IFB-CO-13810-CS dated _____.

2. Funds under this standby letter of credit are available to you upon first demand and without question or delay against presentation of a certificate from the NCI Agency Contracting Officer that:

a) (NAME OF BIDDER) has submitted a Bid and, after Bid Closing Date (including extensions thereto) and prior to the selection of the lowest priced, technically compliant Bid, has withdrawn its Bid, or stated that he does not consider its Bid valid or agree to be bound by its Bid, or

b) (NAME OF BIDDER) has submitted a Bid determined by the Agency to be the lowest priced, technically compliant Bid, but (NAME OF BIDDER) has declined to execute the contract offered by the Agency, such contract being consistent with the terms of the Invitation for Bid, or

c) The NCI Agency has offered (NAME OF BIDDER) the contract for execution but (NAME OF BIDDER) has been unable to demonstrate compliance with the security requirements of the contract within a reasonable time, or

d) The NCI Agency has entered into the contract with (NAME OF BIDDER) but (NAME OF BIDDER) has been unable or unwilling to provide the Performance Guarantee required under the terms of the contract within the time frame required.

3. This Letter of Credit is effective the date hereof and shall expire at our office located at (Bank Address) on _____. All demands for payment must be made prior to the expiry date.

4. It is a condition of this letter of credit that the expiry date will be automatically extended without amendment for a period of sixty (60) calendar days from the current

or any successive expiry date unless at least thirty (30) calendar days prior to the then current expiry date the NCI Agency Contracting Officer notifies us that the Letter of Credit is not required to be extended or is required to be extended for a shorter duration.

5. We may terminate this letter of credit at any time upon sixty (60) calendar days notice furnished to both (NAME OF BIDDER) and the NCI Agency by registered mail.

6. In the event we (the issuing bank) notify you that we elect not to extend the expiry date in accordance with paragraph 4 above, or, at any time, to terminate the letter of credit, funds under this credit will be available to you without question or delay against presentation of a certificate signed by the NCI Agency Contracting Officer which states

"The NCI Agency has been notified by {issuing bank} of its election not to automatically extend the expiry date of letter of credit number {number} dated {date} pursuant to the automatic renewal clause (or to terminate the letter of credit). As of the date of this certificate, no suitable replacement letter of credit, or equivalent financial guarantee has been received by the NCI Agency from, or on behalf of (NAME OF BIDDER), and the NCI Agency, as beneficiary, hereby draws on the standby letter of credit number _____ in the amount of € (Amount up to the maximum available under the LOC), such funds to be transferred to the account of the Beneficiary number _____ (to be identified when certificate is presented)."

Such certificate shall be accompanied by the original of this letter of credit and a copy of the letter from the issuing bank that it elects not to automatically extend the standby letter of credit, or terminating the letter of credit.

7. The Beneficiary may not present the certificate described in paragraph 6 above until 20 (twenty) calendar days prior to a) the date of expiration of the letter of credit should {issuing bank} elect not to automatically extend the expiration date of the letter of credit, b) the date of termination of the letter of credit if {issuing bank} notifies the Beneficiary that the letter of credit is to be terminated in accordance with paragraph 6 above.

8. Multiple drawings are allowed.

9. Drafts drawn hereunder must be marked, "Drawn under {issuing bank} Letter of Credit No. {number}" and indicate the date hereof.

10. This letter of credit sets forth in full the terms of our undertaking, and this undertaking shall not in any way be modified, amended, or amplified by reference to any document, instrument, or agreement referred to herein (except the International Standby Practices (ISP 98) hereinafter defined) or in which this letter of credit is referred to or to which this letter of credit relates, and any such reference shall not be deemed to incorporate herein by reference any document, instrument, or agreement.

11. We hereby engage with you that drafts drawn under and in compliance with the terms of this letter of credit will be duly honoured upon presentation of documents to us on or before the expiration date of this letter of credit.

12. This Letter of Credit is subject to The International Standby Practices-ISP98 (1998 Publication) International Chamber of Commerce Publication No.590.

Annex D Clarification Request Form

INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE

INVITATION FOR BID
IFB-CO-13810-CS

Provide Enterprise NATO-PKI (E-NPKI)

Annex D CLARIFICATION REQUEST FORM

INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE

ADMINISTRATION or CONTRACTING				
Serial NR	**IFB REF**	**QUESTION**	**ANSWER**	**Status**
A.1.				
A.2.				
A.3.				
A.4.				

INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE

PRICE Serial NR	IFB REF	QUESTION	ANSWER	Status
P.1				
P.2				
P.3				
P.4				
P.5				
P.6				

INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE

TECHNICAL Serial NR	IFB REF	QUESTION	ANSWER	Status
T.1				
T.2				
T.3				

Annex E Bid-Requirements Cross Reference Matrix (BRCM) [*AMD 1 NOTE: This revised Annex E replaces the IFB version in its entirety*]

Bidders shall provide the BRCM in Excel format according to the template “Book I Annex E BRCM”.

The BRCM shall be completed as per the following instructions:

- “**Reference Document**”, the document from which the requirement is defined.

- “**Reference ID**”, the reference of the section/requirement under consideration. The “Reference ID” column shall cover:
  - “Bidding Instruction” references covering sections 3.6.4, 3.6.5, and 3.6.6 of this document. “Bidding Instruction” references shall be provided in the format [BI - #] where “#” represents the actual paragraph number.
  - “SOW Requirement” references covering all ‘shall’ statement of the SOW (including SOW annexes A, B and C). SOW Requirement References shall be provided in the following format:
    - For the SOW: [SOW - #] where “#” represents the actual requirement (i.e. paragraph) number
    - For SOW Annex A (SRS): [SRS - #] where “#” represents the actual requirement number
    - For SOW Annex B: [SOW Annex B - #] where “#” represents the actual requirement (i.e. paragraph) number
    - For SOW Annex C: [SOW Annex C - #] where “#” represents the actual requirement (i.e. paragraph) number

- “**Description**”: the actual text of the section/requirement under consideration.
-
- “**Bid Reference**” indicating where in their Bid the associated Bid Instruction Reference and/or SOW Requirement Reference is/are addressed. Bid Reference shall be provided in the form “Volume # - Doc # - Section #”

- “**Remarks**”, as applicable. The column “Remarks” might be used by the Bidders to provide a brief description of how the Bidder meets the requirement, to facilitate the reading, but any such descriptions will not form part of the formal evaluation.

- "**Compliance statement**": the way and extent the Bid covers and complies with the section/requirement under consideration, using the following classifications:
  - "Provided/Detailed": The bidder states providing a document or details at the mentioned reference. Such a classification is expected for all BIs and the majority of the SOW and SRS requirements.
  - "Partial": The bidder states fulfilling the requirement but only describes part of it. Such a classification is expected for a small number of SOW and SRS requirements.
  - "Deviation proposed": The bidder states tacking and describing an alternative approach to fulfil the section/requirement under consideration. Such a classification is expected for a very limited amount of SOW and/or SRS requirements.
  - "Not detailed": The bidder states fulfilling the requirement, but does not detail/justify how. It is expected that some requirements from the SOW or SRS cannot be justified/detailed at the bidding stage.

One copy of the duly completed BRCM shall be included in the Technical Proposal Package (Volume 1).

Bidders shall note that, to facilitate the bidding process, the BRCM template already contains the vast majority of BIs and associated descriptions in the columns "Reference ID" and "Description" respectively. However, it is the Bidders' sole responsibility to ensure that all BIs (together with SOW references) are properly addressed and complete in the BRCM.

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
1.0	**PROJECT MANAGEMENT**							
1.1	**Plans**	**See below**	**1**	**See below**	**See below**	**See below**		
1.1.1	Project Management Plan (PMP)	Electronic	1	EDC + 4 Weeks and as changes occur	Project Website	3.2		
1.1.2	Configuration Management Plan (CMP)	Electronic	1	EDC + 8 Weeks and as changes occur	Project Website	15.1		
1.1.3	Quality Assurance Plan (QAP)	Electronic	1	EDC + 8 Weeks and as changes occur	Project Website			
1.2	**Project Management Office**	**See below**	**1**	**EDC + 4 Weeks**	**N/A**	**3.3**		
1.3	**Project Planning Documents**	**Electronic**	**1**	**See below**	**See below**	**NA**		
1.3.1	Product Breakdown Structure (PBS)	Electronic	1	EDC + 8 Weeks and as changes occur	Project Website	3.4.1		
1.3.2	Product Flow Diagram (PFD)	Electronic	1	EDC + 8 Weeks and as changes occur	Project Website	3.4.1		
1.3.3	Project Master Schedule (PMS)	Electronic	As required	Monthly	Project Website	3.4.2		
1.4	**Risk Log**	**Electronic**	**As required**	**EDC + 4 weeks and as changes occur**	**Project Website**	**3.5, 11.2**		
1.5	**Issue Log**	**Electronic**	**As required**	**EDC + 4 weeks and as changes occur**	**Project Website**	**3.6, 11.3**		
1.6	**Project Status Reports (PSR)**	**Electronic**	**As required**	**Monthly. Each PSR to be delivered 3rd working day of the month.**	**Project Website**	**3.9.1**		
1.7	**Meeting Minutes**	**Electronic**	**As required**	**3 days after corresponding meeting**	**Project Website**	**3.9.2**		
1.8	**Information Sheet**	**Electronic**	**1**	**Design review**	**Project Website**	**3.9.6**		
1.0	**Total CLIN 1.0**							
2.0	**SYSTEMS ENGINEERING**							
2.1	**Orientation Workshop**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.1.1	Orientation Workshop Documentation	Electronic	1	1 week before the workshop	Project Website	4.2		
2.1.2	Orientation Workshop	Meeting	1	EDC + 4 weeks	NCIA	4.2		
2.1.3	Orientation Workshop Minutes	Electronic	1	1 week after the workshop	Project Website	3.9.2		
2.2	**System Requirements Analysis and Review**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.2.1	System Requirements Review (SRR)	Meeting	1	EDC + 8 Weeks	NCIA	4.3		
2.2.2	System Requirements Specification Change Requests	Electronic	1	EDC + 8 Weeks	Project Website	4.3, 13.5, 13.6		
2.2.3	SRR Minutes	Electronic	1	1 week after the review meeting	Project Website	3.9.2		
2.3	**Operational Acceptance Tests (OAT)**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.3.1	OEM Manuals to support OAT	Electronic	1	4 Weeks before OAT starts	Project Website	4.4, 9.2, 6.3, 13.16		
2.3.2	Initial Custom Manuals to support OAT	Electronic	1	4 Weeks before OAT starts	Project Website	4.4, 9.2, 6.3, 13.16		
2.3.3	System Tests Documentation Package to support OAT	Electronic	1	4 Weeks before OAT starts	Project Website	9.2 , 9.3		
2.3.4	Certification Practice Statement (CPS) to support OAT	Electronic	1	4 Weeks before OAT starts	Project Website	9.2, 11.3		
2.3.5	TRR meeting and associated report	Meeting / Electronic	1	before OAT start date	NCIA, Project Website	9.1		
2.3.6	Support OAT campaign	Meetings	1	EDC + 14 Weeks	Contractor premises	4.4, 9.2		
2.3.7	Updated System Tests Documentation Package as a result of OAT, in particular Test Report	Electronic	1	1 Week after OAT end date	Project Website	4.4, 9.2		
2.3.8	STR meeting and associated report	Meeting / Electronic	1	after OAT campaign	NCIA, Project Website	9.1		
2.4	**System Design**	**See Below**	**See Below**	**See Below**	**See Below**	**4.5.2 and See Below**		
2.4.1	**Preliminary Design**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.4.1.1	System Design Documentation Package (SDS, ICDs, Security Accreditation Documentation Package, RTM) to support the PDR	Electronic	1	4 Weeks before PDR	Project Website	4.5.2, 11.3		
2.4.1.2	Preliminary Design Review (PDR)	Meeting	1	EDC + 20w	NCIA	4.5.3		
2.4.1.3	PDR report	Electronic	1	1 Week after PDR	Project Website	4.5.4		
2.4.1.4	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation Documentation Package, RTM) as a result of PDR	Electronic	1	2 Weeks after PDR	Project Website	4.5.5, 11.3		
2.4.2	**Critical Design**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.4.2.1	System Design Documentation Package (SDS, ICDs, Security Accreditation Documentation Package, RTM) to support the CDR	Electronic	1 + updates as needed	4 Weeks before CDR	Project Website	4.5.2, 11.3		
2.4.2.2	Recommended Spare Parts List (RSPL)	Electronic	1 + updates as needed	4 Weeks before CDR	Project Website	6.6		
2.4.2.3	Critical Design Review (CDR)	Meeting	1	EDC + 28 Weeks	NCIA	4.5.3		
2.4.2.4	CDR report	Electronic	1	1 Week after CDR	Project Website	4.5.4		
2.4.2.5	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation Documentation Package, RTM) as a result of CDR	Electronic	1 + updates as needed	2 Weeks after CDR	Project Website	4.5.5, 11.3		

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
2.5	**Security Accreditation**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.5.1	**Security Working Group (SWG)**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.5.1.1	Documentation to support SWG meetings	Electronic	As required	2 Weeks before SWG meeting	Project Website	11.2		
2.5.1.2	SWG meetings	Meeting	As required	As required (every 2 months before PSA, every 4 months after PSA)	NCIA	11.2		
2.5.1.3	SWG meetings minutes	Electronic	As required	3 Days after SWG meeting	Project Website	11.2,3.9.2		
2.5.2	**Security Accreditation Documentation**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.5.2.1	Security Risk Assessment (SRA)	Electronic	3 (ON, PBN, and SSL interception) or combined into 1 SRA + updates as needed	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	11.3		
2.5.2.2	System Specific Security Requirements Statement (SSRS)	Electronic	3 (ON, PBN, and SSL interception) + updates as needed	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	11.3		
2.5.2.3	Certificate Practise Statement	Electronic	3 (ON, PBN, and SSL interception) + updates as needed	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	11.3		
2.5.2.4	(generic) Security Operating Procedures (SecOPs)	Electronic	3 (ON, PBN, and SSL interception) + updates as needed	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	11.3		
2.5.2.5	(generic) Security Test and Verification Plan (STVP)	Electronic	3 (ON, PBN, and SSL interception) + updates as needed	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	11.3		
2.5.2.6	System Interconnection Security Requirements Statement (SISRS)	Electronic	As required	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	11.3		
2.5.2.7	(generic) Site Security Compliance Statement (SSCS)	Paper, Electronic	2 per site (1 for ON, 1 for PBN) + as needed for SSL Interception	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	11.3		
2.5.2.8	Limited Security Accreditation (LSA) statements and/or Interim Security Accreditation (ISA) statements	Electronic	As required	As required	Project Website	11.1		
2.5.3	**Software Approval**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.5.3.1	Software Approval Documentation Package	Electronic	1 + updates As required	4 Weeks before test session	Project Website	4.7, 11.4		
2.5.3.2	Support Software Security and Technical Tests	As required	1 + As required	As required	NCIA	4.7, 11.4		
2.5.3.3	Support IV&V testing	As required	1 + As required	As required	NCIA	4.7, 11.4		
2.5.3.4	Updated Product Baseline	As required	1 + As required	As required	Project Website & NCIA	4.7, 11.4		
2.6	**Base Line Acceptance Tests (BLAT)**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.6.1	System Tests Documentation Package to support BLAT	Electronic	1	3 Weeks before BLAT start date	Project Website	9.2.4, 9.3		
2.6.2	OEM Manuals to support BLAT	Electronic	1	3 Weeks before BLAT start date	Project Website	6.3, 9.2, 13.16		
2.6.3	Custom Manuals to support BLAT	Electronic	1	3 Weeks before BLAT start date	Project Website	6.3, 9.2, 13.16		
2.6.4	TRR meeting and associated report	meeting / Electronic	1	before BLAT start date	NCIA, Project Website	9.1		
2.6.5	BLAT test campaign	As required	1	start: EDC + 33 Weeks	Project Website	4.8 and See Below		
2.6.6	Updated System Tests Documentation Package as a result of BLAT, in particular Test Report	Electronic	1	1 Week after BLAT end date	Project Website	9.3		
2.6.7	Updated Product Baseline	As required	1	As required	Project Website & NCIA	4.7, 11.4		
2.6.8	FCA report	Electronic	1	1 Week after BLAT test campaign end date	Project Website	9.2.4, 15.6		
2.6.9	STR meeting and associated report	Meeting / Electronic	1	after BLAT campaign	NCIA, Project Website	9.1		
2.7	**Reference System Implementation**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.7.1	SIP (initial version, covering Reference System implementation)	Electronic	1	4 Weeks before HW/SW shipment	Project Website	5.3		
2.7.2	Inventory / Material Data Sheet	Electronic	1	10 Days before shipment	Project Website	6.5.3		
2.7.3	Custom form 302 (if required)	Electronic	1	10 Days before shipment	Project Website	6.5.6		
2.7.4	Notice of shipment	Electronic	1	10 Days before shipment	Project Website	6.5.7		
2.7.5	Recommended Spare Parts List (RSPL)	Electronic	1	10 Days before shipment	Project Website	6.6		
2.7.6	Recommended Tools and Test equipment List (RTTL)	Electronic	1	10 Days before shipment	Project Website	6.7		
2.7.7	Cryptographic equipment and documentation	Electronic	As required	10 days before delivery	Project Website	6.5.2		
2.7.8	Personnel Security Clearances (PSC)	Electronic	As required	10 days before delivery	Project Website	5.4.2		
2.7.9	Materials (technical services and user services, including spare parts as required) and associated delivery, installation, configuration and integration of the E-NPKI Reference System within the IV&V SL Environment. Consumables will be delivered at a central location to be determined.	HW/SW / Labour	1	4 Weeks before BLAT start date	NCIA	9.2.4, Annex C, 6.9		
2.7.10	Special to Type Tools and Test Equipment: provision and installation (if required)	HW / SW / Labour	Testbed	4 Weeks before BLAT start date	NCIA	6.7, Annex C, 6.9		
2.7.11	As-built drawings	Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	6.3		
2.7.12	PCA report	Electronic	1	1 Week after BLAT test campain end date	Project Website	5.5.5, 9.2.4, 15.6		
2.7.13	Localised version of Security Operating Procedures (SecOPs)	Electronic	2 (ON and PBN) + updates as needed	2 Weeks before BLAT start date	Project Website	11.3		
2.7.14	Localised version of Security Test and Verification Plan (STVP)	Electronic	2 (ON and PBN) + updates as needed	2 Weeks before BLAT start date	Project Website	11.3		
2.7.15	Localised version of Site Security Compliance Statement (SSCS)	Paper, Electronic	2 per site (1 for ON, 1 for PBN)	2 Weeks before BLAT start date	Project Website	11.3		
2.7.16	Training Materials	Paper, Electronic	See "Delivery per site"	As required to align with the SIP	Sites	6.4		
2.7.17	On-site training	Paper, Electronic	See "Delivery per site"	As required to align with the SIP	Sites	6.4		
2.7.18	Site installation and Activation checklist	Electronic	1	1 Week after PCA	Project Website	5.5.7		

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
2.8	**Service Approach**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
2.8.1	Service lifecycle model (for business services and support services)	Electronic	1	3 Weeks before BLAT start date	Project Website	4.10, Annex B 2.5		
2.8.2	Service Catalogue for support services SS 1.0 and SS 2.0	Electronic	1	3 Weeks before BLAT start date	Project Website	4.10, Annex B		
2.8.3	SLA / SLTs / KPIs for support services SS 1.0 and SS 2.0	Electronic	1	3 Weeks before BLAT start date	Project Website	4.10, Annex B		
2.8.4	Service Performance Monitoring and Reporting Plan for support services SS 1.0 and SS 2.0	Electronic	1	3 Weeks before BLAT start date	Project Website	4.10, Annex B		
2.8.5	Service Maintenance Plan for Support services SS 1.0 and SS 2.0	Electronic	1	3 Weeks before BLAT start date	Project Website	4.10, Annex B		
2.8.6	Service IT-Continuity Plan for Support services SS 1.0 and SS 2.0	Electronic	1	3 Weeks before BLAT start date	Project Website	4.10, Annex B		
2.8.7	ITSM Tools in support of SS 1.0 and SS 2.0	HW/SW	1	3 Weeks before BLAT start date	Project Website	4.10, Annex B, 6.9		
2.8.8	Support Services SS 1.0 and SS 2.0 activated and accepted	As required	1	EDC + 10M	NCIA	Annex B		
2.9	**Site Surveys for PSA sites**	**See Below**	**See Below**	**See Below**	**See Below**	**NA**		
2.9.1	Site Survey WorkBook (SSWB) Template	Electronic	1	In time for Reference System implementation	Project Website	10		
2.9.2	Site Survey Report (SSR)	Electronic	See "Delivery per site"	4 Weeks before CDR (all done)	Project Website, site	10		
2.9.3	Letter to the Site POC	Electronic	See "Delivery per site"	4 Weeks before CDR (all done)	Project Website, site	10		
2.0	**Total CLIN 2.0**							
3.0	**SYSTEM IMPLEMENTATION**							
3.1	**Implementation Plan (PSA and FSA sites)**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
3.1.1	SIP (final version)	Electronic	1	PSD+1 Month, and As required	Project Website	5.3		
3.1.2	SIP (annexes) - 1 per site	Electronic	See "Delivery per site"	8 Weeks before implementation at the site	Project Website	5.3		
3.2	**Site Surveys for FSA sites**	**See Below**	**See Below**	**See Below**	**See Below**	**NA**		
3.2.1	Site Survey WorkBook (SSWB) Template	Electronic	1	2 Months before system implementation at FSA sites start	Project Website	10		
3.2.2	Site Survey Report (SSR)	Electronic	See "Delivery per site"	2 Months before site implementation	Project Website, site	10		
3.2.3	Letter to the Site POC	Electronic	See "Delivery per site"	2 Months before site implementation	Project Website, site	10		
3.3	**Implementation (PSA and FSA sites)**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
3.3.1	**Preparation for installation**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
3.3.1.1	Evidence of TEMPEST Certification (if required)	Electronic	See "Delivery per site"	10 Days before shipment	Project Website	5.4		
3.3.1.2	Site Verification Survey report (if required)	Electronic	See "Delivery per site"	1 Month before site installation	Project Website	5.4		
3.3.1.3	Inventory / Material Data Sheet (MDS)	Electronic	See "Delivery per site"	10 Days before shipment	Project Website	6.5.3		
3.3.1.4	Custom form 302 (if required)	Electronic	See "Delivery per site"	10 Days before shipment	Project Website	6.5.6		
3.3.1.5	Notice of shipment	Electronic	See "Delivery per site"	10 Days before shipment	Project Website	6.5.7		
3.3.1.6	Personnel Security Clearances (PSC)	Electronic	See "Delivery per site"	10 Days before shipment	Project Website	5.4.2		
3.3.2	**Site installation and activation**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
3.3.2.1	Materials (Technical services, i.e. CAs, RAs, OCSP), including miscellaneous equipment and spare parts as required, including Testbed.	HW/SW	See "Delivery per site"	Site installation (according to SIP)	Sites	5.5.2, Annex C, 6.9		
3.3.2.2	Materials (User services): Smartcards, Card readers, Certificates for all Users and Devices (front-end, facility, back-end, testbeds). Exact quantities to be defined during project execution (in particular during site surveys). Consumables will be delivered at a central location to be determined.	HW/SW	See "Delivery per site"	Site installation (according to SIP)	Sites	5.5.2, Annex C, 6.9		
3.3.2.3	Special to Type Tools and Test Equipment for Testbeds: provision and installation (if required)	HW / SW / Labour	Testbed	As required to align with the SIP	See Annex C	6.7, Annex C, 6.9		
3.3.2.4	Equipment delivery, installation, configuration and integration, and activation (Technical Services)	Labour	See "Delivery per site"	Site installation (according to SIP)	Sites	5.5.2, Annex C		
3.3.2.5	Equipment delivery, installation, configuration, integration, migration, activation (User Services)	Labour	See "Delivery per site"	Site installation (according to SIP)	Sites	5.5.2, Annex C		
3.3.2.6	System Tests Documentation Package to support Site activation	Electronic	See "Delivery per site"	4 Weeks before site installation	Project Website	5.5.3, 9.3		
3.3.2.7	OEM Manuals	Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	6.3, 13.16		
3.3.2.8	Custom Manuals	Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	6.3, 13.16		
3.3.2.9	TRR meeting and associated report	Meeting / Electronic	See "Delivery per site"	before Site activation tests start date	Sites, Project Website	9.1		
3.3.2.10	Site activation tests	labour	See "Delivery per site"	Site installation (according to SIP)	Sites	5.5.3		
3.3.2.11	Updated System Tests Documentation Package as a result of Site Installation and Activation in particular Test Report	Electronic	See "Delivery per site"	1 Week after site activation	Project Website	5.5.3, 9.3		
3.3.2.12	Localised version of Security Operating Procedures (SecOPs)	Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	5.5.4 , 11.3		
3.3.2.13	Localised version of Security Test and Verification Plan (STVP)	Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	5.5.4 , 11.3		
3.3.2.14	Localised version of Site Security Compliance Statement (SSCS)	Paper, Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	5.5.4 , 11.3		
3.3.2.15	Recommended Spare Parts List (RSPL)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	6.6		
3.3.2.16	Recommended Tools and Test equipment List (RTTL)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	6.7		
3.3.2.17	Cryptographic equipment and documentation	Hardware, Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	6.5.2		
3.3.2.18	As-built drawings	Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	6.3		
3.3.2.19	PCA report	Electronic	See "Delivery per site"	Site installation (according to SIP)	Project Website	5.5.5, 15.6		
3.3.2.20	Migration From I-NPKI to E-NPKI	labour	See "Delivery per site"	Site installation (according to SIP)	Project Website	5.5.6		
3.3.2.21	STR meeting and associated report	Meeting / Electronic	See "Delivery per site"	after site installation	NCIA, Project Website	9.1		
3.3.2.22	Site installation and Activation checklist	Electronic	See "Delivery per site"	1 Week after site activation	Project Website	5.5.7		
3.3.2.23	Training Materials	Paper, Electronic	See "Delivery per site"	4 weeks before training session	Sites	6.4		
3.3.2.24	On-site training	Paper, Electronic	See "Delivery per site"	As required to align with the SIP	Sites	6.4		
3.4	**Security Accreditation**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
3.4.1	**Security Working Group (SWG)**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
3.4.1.1	Documentation to support SWG meetings	Electronic	As required	2 Weeks before SWG meeting	Project Website	11.2		
3.4.1.2	SWG meetings	Meeting	As required	As required (every 2 months before PSA, every 4 months after PSA)	NCIA	11.2		
3.4.1.3	SWG meetings minutes	Electronic	As required	3 Days after SWG meeting	Project Website	11.2,3.9.2		

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
3.4.2	**Security Accreditation Documentation**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
3.4.2.1	Updated Security Risk Assessment (SRA) - if required	Electronic	As required	As required	Project Website	11.3		
3.4.2.2	Updated System Specific Security Requirements Statement (SSRS) - if required	Electronic	As required	As required	Project Website	11.3		
3.4.2.3	Updated Certificate Practise Statement - if required	Electronic	As required	As required	Project Website	11.3		
3.4.2.4	Updated (generic) Security Operating Procedures (SecOPs) - if required	Electronic	As required	As required	Project Website	11.3		
3.4.2.5	Updated (generic) Security Test and Verification Plan (STVP) - if required	Electronic	As required	As required	Project Website	11.3		
3.4.2.6	Updated System Interconnection Security Requirements Statement (SISRS) if required	Electronic	As required	As required	Project Website	11.3		
3.4.2.7	Updated (generic) Site Security Compliance Statement (SSCS) - if required	Paper, Electronic	As required	As required	Project Website	11.3		
3.4.2.8	Limited Security Accreditation (LSA) statements and/or Interim Security Accreditation (ISA) statements - if required	Electronic	As required	As required	Project Website	11.1		
3.4.3	**Software Approval**	**See Below**	**See Below**	**See Below**	**See Below**	**See Below**		
3.4.3.1	Updated Software Approval Documentation Package - if required	Electronic	As required	As required	Project Website	4.7, 11.4		
3.4.3.2	Support Software Security and Technical Tests - if required	As required	As required	As required	NCIA	4.7, 11.4		
3.4.3.3	Support IV&V testing - if required	As required	As required	As required	NCIA	4.7, 11.4		
3.4.3.4	Updated Product Baseline - if required	As required	As required	As required	Project Website & NCIA	4.7, 11.4		
3.5	**Service Approach**	**See Below**	**See Below**	**Completed at PSA**	**See Below**	**See Below**		
3.5.1	Service Catalogue for Business services and Support Service 3.0	Electronic	1	PSD+4M	Project Website	5.6, Annex B		
3.5.2	SLA / SLTs / KPIs for Business services and Support Service 3.0	Electronic	1	PSD+4M	Project Website	5.6, Annex B		
3.5.3	Service Performance Monitoring and Reporting Plan for Business services and Support Service 3.0	Electronic	1	PSD+4M	Project Website	5.6, Annex B		
3.5.4	Service Maintenance Plan for Business services and Support Service 3.0	Electronic	1	PSD+4M	Project Website	5.6, Annex B		
3.5.5	Service IT-Continuity Plan for Business services and Support Service 3.0	Electronic	1	PSD+4M	Project Website	5.6, Annex B		
3.5.6	Additional ITSM Tools - if required (in particular to support SS 3.0)	HW/SW	See "Delivery per site"	As required to align with the SIP	NCIA	5.6, Annex B, 6.9		
3.5.7	Business Services and Support Service 3.0 activated and accepted	As required	1	Acceptance completed at PSA	NCIA	Annex B		
3.5.8	Service Operation and Continuous Service improvement for Support Services SS1.0 and SS2.0	As required	1	From BLAT to PSA	NCIA	Annex B		
3.0	**Total CLIN 3.0**							
4.0	**INTEGRATED LOGISTICS SUPPORT (ILS)**							
4.1	**Integrated Logistics Support Plan (ILSP)**	**Electronic**	**1**	**4 weeks before CDR**	**Project Website**	**6.2**		
4.2	**Training**	**See below**	**See below**	**See below**	**See below**	**See below**		
4.2.1	Training Needs Analysis (TNA) report (as part of site surveys)	Electronic	See "Delivery per site"	with site survey reports	Project Website	6.4		
4.2.2	Training Program/Plan	Electronic	1	with ILSP	Project Website	6.4		
4.2.3	Training Materials	Electronic	See "Delivery per site"	4 weeks before first training session	See below	6.4		
4.2.3.1	Instructor's Guide	Electronic	See "Delivery per site"	1st version: 4 Weeks before first training session Other version: as required to align with SIP	Project Website	6.4		
4.2.3.2	Student Manual	Electronic	See "Delivery per site"	1st version: 4 Weeks before first training session Other version: as required to align with SIP	Project Website , sites	6.4		
4.2.3.3	CBT	Electronic	See "Delivery per site"	1st version: 4 Weeks before first training session Other version: as required to align with SIP	Project Website, NCIA	6.3		
4.3	**Configuration, Issues and Changes Management Package**	**See below**	**See below**	**See below**	**See below**	**See below**		
4.3.1	Configuration Item Management Database (CMDB)	Electronic	1	as required to align with the CMP	NCIA	15, Annex B		
4.3.2	Software Licenses Repository	Electronic	1	first version for PSA and updated version on FSA	Project Website	15, Annex B		
4.3.3	Change Management Documentation Package (Change requests …)	Electronic	1	as required	Project Website	15, Annex B		
4.3.4	Issues, Incidents and Problems Management Documentation Package	Electronic	1	as required	Project Website	15, Annex B		
4.3.5	CSA Reports	Electronic	as required	as required	Project Website	15.5		
4.0	**Total CLIN 4.0**							
	TOTAL FIRM-FIXED PRICE - CLINS 1 thru 4							

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
5.0	**OPERATIONS AND MAINTENANCE (OPTION)**							
5.1	**Initial Operational Support (i.e. from PSA to FSA)**	**See below**	**See below**	**from PSA to FSA**	**See below**	**See below**		
5.1.1	Governance activities	Labour	As required	As required	Annex C	7.2		
5.1.2	System operations activities	Labour	As required	As required	Annex C	7.3		
5.1.3	Maintenance and Help-Desk activities	Labour	As required	As required	Annex C	7.4		
5.1.4	Non-production environment activities	Labour	As required	As required	Annex C	7.5		
5.1.5	RESERVED							
5.1.6	Updates to Service Catalogue for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.1.7	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.1.8	Updates to Service Performance Monitoring and Reporting Plan for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.1.9	Updates to Service Maintenance Plan for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.1.10	Update to Service IT-Continuity Plan for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.1.11	Service Operation and Continuous Service improvement for Business Services and Support Services	As required	As required	As required	Annex C	Annex B		
5.1.12	Updates to ITSM Tools - if required	HW/SW	As required	As required	Annex C	Annex B		
5.1.13	Service Performance Reports (SLA, KPIs, SLTs)	Paper, Electronic	Monthly	As required	Project Website	Annex B		
5.1.14	Service Support Reports (Service specific)	Paper, Electronic	Monthly	As required	Project Website	Annex B		
5.1.15	Service Performance Review	Meeting	Monthly	As required	NCIA	Annex B		
5.1.16	Service Performance Review Minutes	Electronic	As required	Meeting + 3 days	Project Website	Annex B		
5.2	**Follow-on Support (Year 1)**	**See below**	**See below**	**From FSA to FSA + 1 year**	**See below**	**See below**		
5.2.1	Governance activities	Labour	As required	As required	Annex C	7.2		
5.2.2	System operations activities	Labour	As required	As required	Annex C	7.3		
5.2.3	Maintenance and Help-Desk activities	Labour	As required	As required	Annex C	7.4		
5.2.4	Non-production environment activities	Labour	As required	As required	Annex C	7.5		
5.2.5	RESERVED							
5.2.6	Updates to Service Catalogue for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.2.7	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.2.8	Updates to Service Performance Monitoring and Reporting Plan for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.2.9	Updates to Service Maintenance Plan for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.2.10	Update to Service IT-Continuity Plan for Business services and Support Services, if required	Electronic	As required	As required	Project Website	4.10, 5.6, Annex B		
5.2.11	Service Operation and Continuous Service improvement for Business Services and Support Services	As required	As required	As required	Annex C	Annex B		
5.2.12	Updates to ITSM Tools - if required	HW/SW	As required	As required	Annex C	Annex B		
5.2.13	Service Performance Reports (SLA, KPIs, SLTs)	Paper, Electronic	Monthly	As required	Project Website	Annex B		
5.2.14	Service Support Reports (Service specific)	Paper, Electronic	Monthly	As required	Project Website	Annex B		
5.2.15	Service Performance Review	Meeting	Monthly	As required	NCIA	Annex B		
5.2.16	Service Performance Review Minutes	Electronic	As required	Meeting + 3 days	Project Website	Annex B		
5.3	**Follow-on Support (Year 2)**	**See below**	**See below**	**From FSA + 1 Year to FSA + 2 Years**	**See below**	**See below**		
5.3.1	Follow-on Support Year 2. See CLIN 5.2 for details	HW / SW / Labour	As required	See below	As required	4.10, 5.6, 6.9, 7.2, 7.3, 7.4, 7.5, Annex B		
5.4	**Follow-on Support (Year 3)**	**See below**	**See below**	**From FSA + 2 Years to FSA + 3 Years**	**See below**	**See below**		
5.4.1	Follow-on Support Year 3. See CLIN 5.2 for details	HW / SW / Labour	As required	See below	As required	4.10, 5.6, 6.9, 7.2, 7.3, 7.4, 7.5, Annex B		
5.5	**Follow-on Support (Year 4)**	**See below**	**See below**	**From FSA + 3 Years to FSA + 4 Years**	**See below**	**See below**		
5.5.1	Follow-on Support Year 4. See CLIN 5.2 for details	HW / SW / Labour	As required	See below	As required	4.10, 5.6, 6.9, 7.2, 7.3, 7.4, 7.5, Annex B		
5.6	**Follow-on Support (Year 5)**	**See below**	**See below**	**From FSA + 4 Years to FSA + 5 Years**	**See below**	**See below**		
5.6.1	Follow-on Support Year 5. See CLIN 5.2 for details	HW / SW / Labour	As required	See below	As required	4.10, 5.6, 6.9, 7.2, 7.3, 7.4, 7.5, Annex B		
5.0	**Total CLIN 5.0**							

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
6.0	**IMPLEMENTATION AT NATO-HQ (OPTION)**							
6.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
6.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
6.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
6.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
6.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
6.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
6.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
6.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
6.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
6.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
6.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
6.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
6.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
6.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
6.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
6.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
6.0	**Total CLIN 6.0**							
7.0	**IMPLEMENTATION AT NAEW&C (OPTION)**							
7.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
7.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
7.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
7.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
7.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
7.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
7.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
7.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
7.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
7.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
7.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
7.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
7.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
7.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
7.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
7.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
7.0	**Total CLIN 7.0**							
8.0	**IMPLEMENTATION AT JEWCS (OPTION)**							
8.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
8.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
8.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
8.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
8.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
8.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
8.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
8.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
8.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
8.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
8.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
8.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
8.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
8.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
8.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
8.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
8.0	**Total CLIN 8.0**							
9.0	**IMPLEMENTATION AT NIFC (OPTION)**							
9.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
9.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
9.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
9.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
9.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
9.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
9.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
9.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
9.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
9.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
9.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
9.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
9.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
9.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
9.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
9.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
9.0	**Total CLIN 9.0**							

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
10.0	**IMPLEMENTATION AT NCIA (OPTION)**							
10.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
10.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
10.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
10.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
10.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
10.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
10.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
10.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
10.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
10.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
10.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
10.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
10.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
10.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
10.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
10.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
10.0	**Total CLIN 10.0**							
11.0	**IMPLEMENTATION AT NSPA (OPTION)**							
11.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
11.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
11.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
11.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
11.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
11.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
11.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
11.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
11.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
11.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
11.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
11.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
11.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
11.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
11.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
11.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
11.0	**Total CLIN 11.0**							
12.0	**IMPLEMENTATION AT STO (OPTION)**							
12.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
12.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
12.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
12.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
12.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
12.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
12.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
12.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
12.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
12.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
12.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
12.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
12.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
12.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
12.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
12.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
12.0	**Total CLIN 12.0**							
13.0	**IMPLEMENTATION AT NAGSMA (OPTION)**							
13.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
13.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
13.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
13.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
13.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
13.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
13.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
13.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
13.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
13.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
13.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
13.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
13.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
13.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
13.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
13.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
13.0	**Total CLIN 13.0**							
14.0	**IMPLEMENTATION AT NAHEMA (OPTION)**							
14.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
14.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
14.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
14.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
14.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
14.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
14.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
14.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
14.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
14.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
14.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
14.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
14.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
14.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
14.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
14.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
14.0	**Total CLIN 14.0**							
15.0	**IMPLEMENTATION AT NETMA (OPTION)**							
15.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
15.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
15.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
15.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
15.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
15.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
15.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
15.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
15.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
15.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
15.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
15.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
15.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
15.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
15.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
15.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
15.0	**Total CLIN 15.0**							
16.0	**IMPLEMENTATION AT NAPMA (OPTION)**							
16.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
16.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
16.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
16.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
16.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
16.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
16.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
16.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
16.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
16.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
16.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
16.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
16.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
16.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
16.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
16.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
16.0	**Total CLIN 16.0**							

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
17.0	**IMPLEMENTATION AT NDC (OPTION)**							
17.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
17.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
17.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
17.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
17.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
17.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
17.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
17.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
17.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
17.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
17.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
17.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
17.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
17.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
17.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
17.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
17.0	**Total**							
18.0	**IMPLEMENTATION AT NSO (OPTION)**							
18.1	**Project Management**	**See below**	**See below**	**See below**	**See below**	**See below**		
18.1.1	Site-Specific Project Management deliverables (As required)	Electronic	As required	As required to align with the SIP	Project Website	8		
18.2	**System Engineering**	**See below**	**See below**	**See below**	**See below**	**See below**		
18.2.1	Site-Specific System Engineering deliverables (if required)	Electronic	As required	As required to align with the SIP	Project Website	8		
18.3	**System Implementation**	**See below**	**See below**	**See below**	**See below**	**See below**		
18.3.1	Site-Specific System Implementation deliverables - Technical Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
18.3.2	Site-Specific System Implementation deliverables - User Services	HW / SW / Labour / Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8, 6.9		
18.4	**ILS**	**See below**	**See below**	**See below**	**See below**	**See below**		
18.4.1	Site-Specific ILS deliverables (if required)	Electronic	See "Delivery per site"	As required to align with the SIP	Project Website	8		
18.5	**Operation and Maintenance (User services only)**	**See below**	**See below**	**See below**	**See below**	**See below**		
18.5.1	Initial Operational Support - User Services only. See CLIN 5.1 for details	HW/SW/Labour	As required	From Site activation to FSA	As required	7, Annex B		
18.5.2	Follow-on Support Year 1 - User Services only. See CLIN 5.2 for details	HW/SW/Labour	As required	From FSA to FSA + 1 Year	As required	7, Annex B		
18.5.3	Follow-on Support Year 2 - User Services only. See CLIN 5.3 for details	HW/SW/Labour	As required	From FSA + 1 Year to FSA + 2 Years	As required	7, Annex B		
18.5.4	Follow-on Support Year 3 - User Services only. See CLIN 5.4 for details	HW/SW/Labour	As required	From FSA + 2 Years to FSA + 3 Years	As required	7, Annex B		
18.5.5	Follow-on Support Year 4 - User Services only. See CLIN 5.5 for details	HW/SW/Labour	As required	From FSA + 3 Years to FSA + 4 Years	As required	7, Annex B		
18.5.6	Follow-on Support Year 5 - User Services only. See CLIN 5.6 for details	HW/SW/Labour	As required	From FSA + 4 Years to FSA + 5 Years	As required	7, Annex B		
18.0	**Total CLIN 17.0**							
19.0	**IMPLEMENTATION AT ADDITIONAL SITES (OPTION)**							
19.1	**Project Management**	**TBD**	**TBD**	**TBD**	**TBD**	**8**	TBD	TBD
19.1.1	Site-Specific Project Management deliverables (As required)	TBD	TBD	TBD	TBD	8	TBD	TBD
19.1.1.1	Certificate Authorities (CA)	TBD	1	TBD	TBD	8		
19.1.1.2	Registration Authorities (RA)	TBD	1	TBD	TBD	8		
19.1.1.3	Online Certificate Status Protocol (OCSP)	TBD	1	TBD	TBD	8		
19.1.1.4	Timestamp	TBD	1	TBD	TBD	8		
19.2	**System Engineering**	**TBD**	**TBD**	**TBD**	**TBD**	**8**	TBD	TBD
19.2.1	Site-Specific System Engineering deliverables (if required)	TBD	TBD	TBD	TBD	8	TBD	TBD
19.2.1.1	Certification Practice Statement (CPS)	TBD	1	TBD	TBD	8		
19.2.1.2	Security Risk Assessment (SRA)	TBD	1	TBD	TBD	8		
19.2.1.3	System Security Requirement Statement (SSRS)	TBD	1	TBD	TBD	8		
19.2.1.4	CA	TBD	1	TBD	TBD	8		
19.2.1.5	RA	TBD	1	TBD	TBD	8		
19.2.1.6	OCSP	TBD	1	TBD	TBD	8		
19.2.1.7	Timestamp	TBD	1	TBD	TBD	8		
19.3	**System Implementation**	**TBD**	**TBD**	**TBD**	**TBD**	**8**	TBD	TBD
19.3.1	Site-Specific System Implementation deliverables - Technical Services	TBD	TBD	TBD	TBD	8	TBD	TBD
19.3.3.1	Certificate Authorities (CA)	TBD	1	TBD	TBD	8		
19.3.3.2	Registration Authorities (RA)	TBD	1	TBD	TBD	8		
19.3.3.3	Online Certificate Status Protocol (OCSP)	TBD	1	TBD	TBD	8		
19.3.3.4	Timestamp	TBD	1	TBD	TBD	8		
19.3.2	Hardware	TBD	TBD	TBD	TBD	8, 6.9	TBD	TBD
19.3.2.1	Certificate Authorities	TBD	1	TBD	TBD	8, 6.9		
19.3.2.2	Registration Authorities	TBD	1	TBD	TBD	8, 6.9		
19.3.2.3	Online Certificate Status Protocol	TBD	1	TBD	TBD	8, 6.9		
19.3.2.4	Tokens (Smart Cards)	TBD	TBD	TBD	TBD	8, 6.9	TBD	TBD
19.3.2.4.1	Tokens (Smart Cards) Quantity 1,000-2,000	TBD	1,000-2,000	TBD	TBD	8, 6.9		
19.3.2.4.2	Tokens (Smart Cards) Quantity 2,001-5,000	TBD	2,001-5,000	TBD	TBD	8, 6.9		
19.3.2.4.3	Tokens (Smart Cards) Quantity (Bidder to specify)	TBD		TBD	TBD	8, 6.9		
19.3.2.4.4	Tokens (Smart Cards) Quantity (Bidder to specify)	TBD		TBD	TBD	8, 6.9		
19.3.2.4.5	Tokens (Smart Cards) Quantity (Bidder to specify)	TBD		TBD	TBD	8, 6.9		
19.3.2.5	Token Readers (Card Readers)	TBD	TBD	TBD	TBD	8, 6.9	TBD	TBD
19.3.2.5.1	Token Readers (Card Readers) Quantity 1-100	TBD	1-100	TBD	TBD	8, 6.9		
19.3.2.5.2	Token Readers (Card Readers) Quantity 101-500	TBD	101-500	TBD	TBD	8, 6.9		
19.3.2.5.3	Token Readers (Card Readers) Quantity 501-1,000	TBD	501-1,000	TBD	TBD	8, 6.9		
19.3.2.6	Timestamp	TBD	1	TBD	TBD	8, 6.9		
19.3.3	Software	TBD	TBD	TBD	TBD	8, 6.9	TBD	TBD

CLIN	DESCRIPTION	DELIVERY FORM	QTY	DELIVERY DATE	DESTINATION (Incoterm 2010 DDP at location specified below, unless otherwise stated herein contract)	SOW REFERENCE	Unit Price	Firm-Fixed Price
19.3.3.1	Certificate Authorities	TBD	1	TBD	TBD	8, 6.9		
19.3.3.2	Registration Authorities	TBD	1	TBD	TBD	8, 6.9		
19.3.3.3	Online Certificate Status Protocol	TBD	1	TBD	TBD	8, 6.9		
19.3.3.4	Tokens Middleware	TBD	1	TBD	TBD	8, 6.9		
19.3.3.5	Certificates (User Identites + Devices + Applications)	TBD	TBD	TBD	TBD	8, 6.9	TBD	TBD
19.3.3.5.1	Certificates (User Identites + Devices + Applications) Quantity 0-1,000	TBD	1-1,000	TBD	TBD	8, 6.9		
19.3.3.5.2	Certificates (User Identites + Devices + Applications) Quantity 1,001-2,000	TBD	1,001-2,000	TBD	TBD	8, 6.9		
19.3.3.5.3	Certificates (User Identites + Devices + Applications) Quantity 2,001-5,000	TBD	2,001-5,000	TBD	TBD	8, 6.9		
19.3.3.6	Timestamp	TBD	1	TBD	TBD	8, 6.9		
19.3.4	Site-Specific System Implementation deliverables - User Services	TBD	TBD	TBD	TBD	8, 6.9	TBD	TBD
19.4	**ILS**	**TBD**	**TBD**	**TBD**	**TBD**	**8**	TBD	TBD
19.4.1	Site-Specific ILS deliverables (if required)	TBD	TBD	TBD	TBD	8	TBD	TBD
19.5	**Operation and Maintenance (User services only)**	**TBD**	**TBD**	**TBD**	**TBD**	**8**	TBD	TBD
19.5.1	Initial Operational Support. See CLIN 5.1 for details	TBD	TBD	TBD	TBD	7, Annex B	TBD	TBD
19.5.2	Follow-on Support Year 1. See CLIN 5.2 for details	TBD	TBD	TBD	TBD	7, Annex B	TBD	TBD
19.5.3	Follow-on Support Year 2. See CLIN 5.3 for details	TBD	TBD	TBD	TBD	7, Annex B	TBD	TBD
19.5.4	Follow-on Support Year 3. See CLIN 5.4 for details	TBD	TBD	TBD	TBD	7, Annex B	TBD	TBD
19.5.5	Follow-on Support Year 4. See CLIN 5.5 for details	TBD	TBD	TBD	TBD	7, Annex B	TBD	TBD
19.5.6	Follow-on Support Year 5. See CLIN 5.6 for details	TBD	TBD	TBD	TBD	7, Annex B	TBD	TBD

SITE SPECIFIC DELIVERABLES (ALL CLIN 5)

| SITEs DATA | | | | | TYPE | | TECHNICAL SERVICES | | | PSA Milestone | FSA Milestone | Eligibility to NSIP | | SITE-SPECIFIC DELIVERABLES | | | | |

Project Milestone Delivery Requirements				
Milestone	**Description**	**Due Date for Purchaser Written Acceptance**	**Associated CLINs**	**SOW Reference**
1	System Requirements Review (SRR)	EDC + 8 Weeks	CLINs 2.1, 2.2, 2.3	16.3
2	Operational Acceptance Tests (OAT)	EDC + 16 Weeks	CLINs 2.1, 2.2, 2.3	16.4
3	System Design Review (SDR)	EDC + 28 Weeks	CLINs 1, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9	16.5
4	Baseline Acceptance Test (BLAT)	EDC + 40 Weeks	CLINs 1, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9	16.6
5	Preliminary System Acceptance (PSA)	EDC + 64 Weeks	CLINs 1, 3, 4	16.7
6	Final System Acceptance (FSA)	EDC + 132 Weeks	CLINs 1, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 3, 4, 5.1	16.9

NATO Communications and Information Agency
Agence OTAN d'information et de communication

Provide Enterprise NATO Public-Key Infrastructure (E-NPKI)

AMD 4 TO IFB-CO-13810-CS

BOOK II - PART IV SOW Annex A

SYSTEM REQUIREMENT STATEMENT (SRS)

Table of Contents

1 Introduction 6
1.1 Purpose 6
1.2 Scope 6
1.3 Background 6
1.4 Definitions 7
1.4.1 Actor Definitions 7
1.4.2 Artefact Definitions 8
1.4.3 Other Definitions 9
1.4.4 Security Definitions 9
1.5 Overview 10
1.6 SRS Conventions 11
1.7 Standards and Specifications 11
1.8 Verification Methods 11
1.8.1 Inspection 12
1.8.2 Analysis 12
1.8.3 Testing 12
2 General System Description 12
2.1 Product Perspective 12
2.2 General Constraints 16
2.2.1 Relationships with other programs 16
2.2.2 Existing Capabilities 16
2.2.3 Operating Environment 17
3 Functional Requirements 18
3.1 Introduction to Certificate Policy 18
3.1.1 Overview of Certificate Policy 18
3.1.2 Certificate Policy Identification 18
3.1.3 PKI Participants 18
3.1.4 Certificate Usage 22
3.2 Publication and Repository Responsibilities 22
3.2.1 Repositories 22
3.2.2 Publication of certification information 23
3.2.3 Time or frequency of publication 23
3.2.4 Access controls on repositories 24
3.3 Identification and Authentication 24
3.3.1 Naming 24
3.3.2 Initial identity validation 26
3.3.3 Identification and authentication for re-key requests 32
3.3.4 Identification and authentication for revocation request 33
3.4 Certificate Life-Cycle Operational Requirements 33
3.4.1 Certificate Application 33
3.4.2 Certificate application processing 36
3.4.3 Certificate issuance 37
3.4.4 Certificate acceptance 39
3.4.5 Key pair and certificate usage 39
3.4.6 Certificate renewal 41
3.4.7 Certificate re-key 42
3.4.8 Certificate modification 43

3.4.9 Certificate revocation and suspension 45
3.4.10 Certificate status services 49
3.4.11 End of subscription 51
3.4.12 Key escrow and recovery 52
3.5 Facility, Management, and Operational Controls 53
3.5.1 Physical controls 53
3.5.2 Procedural controls 56
3.5.3 Personnel controls 60
3.5.4 Audit logging procedures 61
3.5.5 Records archival 68
3.5.6 Key changeover 73
3.5.7 Compromise and disaster recovery 74
3.5.8 CA or RA termination 76
3.6 Technical Security Controls 77
3.6.1 Key pair generation and installation 77
3.6.2 Private Key Protection and Cryptographic Module Engineering Controls 84
3.6.3 Other aspects of key pair management 88
3.6.4 Activation data 89
3.6.5 Computer security controls 91
3.6.6 Life cycle technical controls 94
3.6.7 Network security controls 95
3.6.8 Time-stamping 96
3.7 Certificate, CRL, and OCSP Profiles 97
3.7.1 Certificate profile 97
3.7.2 CRL profile 105
3.7.3 OCSP profile 106
3.8 Compliance Audit and Other Assessments 108
3.9 Other Business and Legal Matters 108
3.9.1 Fees 108
3.9.2 Financial responsibility 108
3.9.3 Confidentiality of business information 109
3.9.4 Privacy of personal information 109
3.9.5 Intellectual property rights 110
3.9.6 Representations and warranties 110
3.9.7 Disclaimers of warranties 110
3.9.8 Limitations of liability 110
3.9.9 Indemnities 110
3.9.10 Term and termination 110
3.9.11 Individual notices and communications with participants 110
3.9.12 Amendments 110
3.10 Performance criteria 110
3.10.1 Certification Authorities 110
3.10.2 Registration Authorities 111
3.10.3 End Entities 111
3.10.4 OCSP Service 111
3.10.5 Timestamping Service 111
4 Non-functional Requirements 112
4.1 Quality Requirements 112

4.1.1 Reliability 112
4.1.2 Data Integrity 117
4.1.3 Usability 117
4.1.4 Efficiency (Performance) 124
4.1.5 Maintainability and Supportability 126
4.1.6 Portability 128
4.1.7 Usage scope and limitations 130
4.2 Design Constraints 131
4.2.1 Database Management 131
4.2.2 Architectural Constraints 132
4.3 Documentation Requirements 133
4.3.1 On-line Help 133
4.3.2 Target Architecture 136
4.4 Security Requirements 137
4.4.1 Compliance with Bi-SC AIS Security Requirements 137
4.4.2 Confidentiality 142
4.4.3 Data Protection Policy 143
4.4.4 Preservation of Digital Information of Permanent Value 144
4.4.5 Data Definition 145
4.4.6 Metadata 146
4.4.7 Packaging 146
4.4.8 Authentication 146
4.4.9 Authorisation 148
4.5 Computer Resource Requirements 148
4.5.1 Hardware and Software Components 148
4.5.2 Configuration Management Tools 150
4.6 Interoperability 150
4.6.1 General 150
4.6.2 Interface Mechanisms 151
4.6.3 Interfaces 156
4.7 Applicable Standards 158
4.7.1 Technical Standards 159
4.7.2 Quality Standards 160
4.7.3 Programming Standards 161
4.8 Deployable Systems 161
4.9 Information Exchange Requirements (IERs) 161
4.9.1 Information Products 161
4.9.2 Interfaces 161
4.10 Integration with existing systems and applications 163

1 Introduction

1.1 Purpose

This System Requirement Specification (SRS) describes the external behaviour of the system to be delivered under the *Enterprise NATO Public Key Infrastructure (E-NPKI)* project. It also describes non-functional requirements, design constraints and other factors necessary to provide a comprehensive description of the requirements for the system.

1.2 Scope

This SRS supports the NATO Capability Package (CP) CP 0A0155 *Electronic Information Security Services (INFOSEC),* project number 0IS03072 *"Provide NATO Public Key Infrastructure."*

The Enterprise NATO Public Key Infrastructure (E-NPKI) project is to provide the Alliance with a set of security services enabling confidentiality, integrity, authentication, and non-repudiation.

The principal aim of this project is to serve as a highly scalable network and user domain authentication, identification and security supporting framework as well as providing a confidentiality service to support community of interest separation. The E-NPKI will provide the key and information management functions to other CIS security services by means of lifecycle certificate management.

This Infrastructure will be made up of certificate authorities, registration authorities, revocation services, end entity support (tokens, clients, etc.), security and audit tools, software and software integration support, and the processes, resources and services required to operate an effective public key based security infrastructure.

1.3 Background

The E-NPKI will be a capability that allows trusted third parties such as authorized Certification Authorities (CAs) to vouch for subscribers' identities by binding public keys to subscribers' identity attributes in the form of electronic certificates. It will publish the authentic public key values (certificates) in support of public key cryptographic processes, which allow subscribers to authenticate themselves – to each other, to processes and to systems – and to encrypt and decrypt messages based on knowledge derived from each other's public and private keys.

1.4 Definitions

1.4.1 Actor Definitions

1.4.1.1 Certification Authority (CA)

An entity authorised to create, sign, issue and manage public key certificates.

1.4.1.2 End-Entity (EE)

An item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, service, application, or a group of such items that has recognizably distinct existence and requires a digital certificate.

1.4.1.3 Registration Authority (RA)

An entity that enters into an agreement with a CA to implement the registration, identification and authentication processes by collecting and verifying subscribers' identity and information that is to be entered into public key certificates.

1.4.1.4 Repository

A central place in which an aggregation of data is kept and maintained in an organized way.

1.4.1.5 Subscriber

A subscriber is the entity whose name appears as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with the E-NPKI CertP. Subscribers also include persons who hold Trusted Roles within the E-NPKI.

1.4.1.6 Sponsor

The person assigned to manage an Information Technology products such as workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components or cryptographically aware applications. These components shall be under the cognisance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

1.4.1.7 Relying Party

Relying parties include E-NPKI End-Entities and external PKI End-Entities. Additionally, any PKI aware devices, software, and users who are able to validate E-NPKI certificate chains up to a trusted certificate authority are also considered to be a relying party.

1.4.1.8 Hardware Security Module (HSM)

A Hardware Security Module (HSM) is a dedicated cryptographic processor which is designed for the protection and management of the cryptographic keys throughout their life cycle. The HSM is a physical device which provides tamper evidence such as logging and alerting and tamper resistance such as deleting keys upon tamper detection.

1.4.1.9 User

A user in the context of this document is a generic term which refers to a person having access to a device or system. It is also a generic term used by operating systems to denote a person with access rights on that system. In the context of E-NPKI, the equivalent terminology for an E-NPKI enrolled user is a subscriber.

1.4.1.10 Relying Party

A relying party is the entity who trusts the validity of the binding of the subscriber's name to a public key. This reliance may result from using another subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate.

1.4.1.11 E-NPKI Administrator

E-NPKI Administrator – role authorized to install, configure, and maintain the Certificate Issuing and Management Component (CIMC); establish and maintain ***user*** accounts; configure profiles and audit parameters; and generate Component keys.

1.4.1.12 E-NPKI Officer

E-NPKI Officer – role authorized to request or approve certificates or certificate revocations.

1.4.1.13 E-NPKI Operator

E-NPKI Operator – role authorized to perform system backup and recovery.

1.4.1.14 E-NPKI Auditor

E-NPKI Auditor – role authorized to view and maintain audit logs.

1.4.2 Artefact Definitions

1.4.2.1 Certificate Policy (CertP)

Definition from RFC 3647: A Certificate Policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. A CertP may be used by a relying party to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application.

1.4.2.2 Certificate Practice Statement (CPS)

Definition from RFC 3647: A more detailed description of the practices followed by a CA in issuing and otherwise managing certificates may be contained in a Certification Practice Statement (CPS) published by or referenced by the CA. According to the American Bar Association Information Security Committee's Digital Signature Guidelines (hereinafter "DSG")(1) and the Information Security Committee's PKI Assessment Guidelines (hereinafter "PAG")(2), "a CPS is a statement of the practices which a certification authority employs in issuing certificates." [ABA1, ABA2] In general, CPSs also describe practices relating to all certificate lifecycle services (e.g., issuance, management, revocation, and renewal or re-keying), and CPSs provide details concerning other business, legal, and technical matters.

1.4.2.3 Certificate Revocation List (CRL)

An artefact signed by a CA that contains a list of all certificates that have been revoked, the reason for the revocation, and the date on which they were revoked.

1.4.2.4 Credentials

The set of all E-NPKI certificates and private keys held by an End-Entity.

1.4.3 Other Definitions

1.4.3.1 Anonymity

Anonymity is the ability to issue credentials to End-Entities that cannot be later traced back to the specific entity within any system.

1.4.3.2 Pseudonymity

Pseudonymity is the ability to issue credentials to entities that preserve the privacy of the entity. The entity cannot be directly identified from their credentials outside the E-NPKI system, but can be later traced back to the specific entity within the E-NPKI system. This may, for example, be through the use of a GUID that is recorded against a specific entity.

1.4.4 Security Definitions

1.4.4.1 Identification

Identification is the process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. [NIST 800-47].

The process that enables, generally by the use of unique machine-readable names, recognition of users or resources as identical to those previously described to the data processing system or network [AAP-31].

1.4.4.2 Authentication

Authentication - to ensure the reliable identification and authentication of persons, devices and services accessing CIS handling NATO classified information.[AC/35-D/2004-REV3] Authentication is the act of verifying the claimed identity of an entity. [AAP-31]

Authorization is the granting of rights [ISO 7498-2]. Note - Authorisation includes the granting of access based on access rights [AAP-31].

1.4.4.3 Accountability

Accountability is the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action [Source: NIST SP-800-12].

The property that ensures that the actions of an entity may be traced uniquely to that entity [AAP-31].

1.4.4.4 Data Integrity

The data quality that exists as long as accidental or malicious destruction, alteration, or loss of data does not occur [AAP-31].

1.4.4.5 Service Integrity

The ability of a service, once obtained, to be provided without excessive impairments. *Note:* For a telecommunication service this is characterized by the transmission performance of the system used [AAP-31].

1.4.4.6 System Integrity

The degree to which wholeness or soundness of a system is maintained [AAP-31].

1.4.4.7 Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ISO7498-2].

1.4.4.8 Non-repudiation

The measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipients.

1.5 Overview

This SRS comprises 4 sections:

- Section 1 provides an introduction and the use of this document.
- Section 2 provides an overall description of the ***E-NPKI*** Services, roles involved and project constraints.

- Sections 3 and 4 contain the Functional and Non-Functional Requirements comprising the required functionality and their associated requirement attributes.

1.6 SRS Conventions

To clarify between descriptive text and requirements statements within the SRS, requirements are preceded by a “Requirement ID:” and are included as Blue text.

Requirement ID: SRS-31

- The system requirements, defined in this document, are individually identified by a unique number which shall be used at all times as the specific reference for each.

No meaning is associated with the order of serial numbering. There could be gaps in numbering and requirement identifiers in a group do not have to be sequential.

Requirement ID: SRS-33

- The use of shall, should and will is defined as follows:
- **Shall**: This requirement is mandatory and must be implemented.
- **Will:** This term is not implemented within the SRS requirements
- **Should:** This term is not implemented within the SRS requirements
- **Shall not**: means that the definition is an absolute prohibition of the specification.

1.7 Standards and Specifications

Requirement ID: SRS-36

1.8 Changes to standards and specifications are anticipated prior to the deployment of the E-NPKI capability. In cases in which changes are identified prior to the end of the System Design Review (SDR) Phase, no additional cost shall accrue to the change in standard/specification. Changes in standards/specifications as part of a normal technological GEN/maintenance path (e.g., Windows 7 to Windows 10, Server 2012 to Server 2015, .NET Framework 3.5 to.NET Framework 4.0, or Certificate Policy changes which only require configuration changes to the contractor’s E-NPKI solution) shall not lead to additional cost. Verification Methods

The requirements in this SRS will be verified through qualification, herein defined as an endorsement with a guarantee and supporting documentation that the item being qualified satisfies the specified requirement(s). The different verification methods applicable to the requirements herein are described in the following paragraphs.

Note: In some cases, more than one verification method might be required in order to verify fulfilment of a requirement.

1.8.1 Inspection

Inspection is the visual examination of an item (hardware and software) and associated descriptive documentation. Verification is based on the human senses (sight, touch) or other means that use simple measurement and handling methods. No stimulus is necessary. Passive resources such as meter rule, gauge may be used.

For Non-Developmental Items (NDI), Modified NDI and Developmental Items, hardware inspection is used to determine if physical constraints are met, and hardware and/or software, inspection is used to determine if physical quantity lists are met.

1.8.2 Analysis

Analysis is the review and processing of design products (documentation, drawings, presentations, etc.) or accumulated data obtained from other qualification methods, such as manufacturer's tests of a product to be mass-produced, to verify that the system/component design meets required design criteria.

1.8.3 Testing

Testing is the operation of the system, or a part of the system, under controlled and specified conditions, generally using instrumentation, other special test equipment or specific test patterns to collect data for later analysis. This verification method usually requires recorded results to verify that the requirements have been satisfied.

2 General System Description

2.1 Product Perspective

A notional overview of the E-NPKI architecture is shown in Figure 1 - High Level Architecture of E-NPKI.

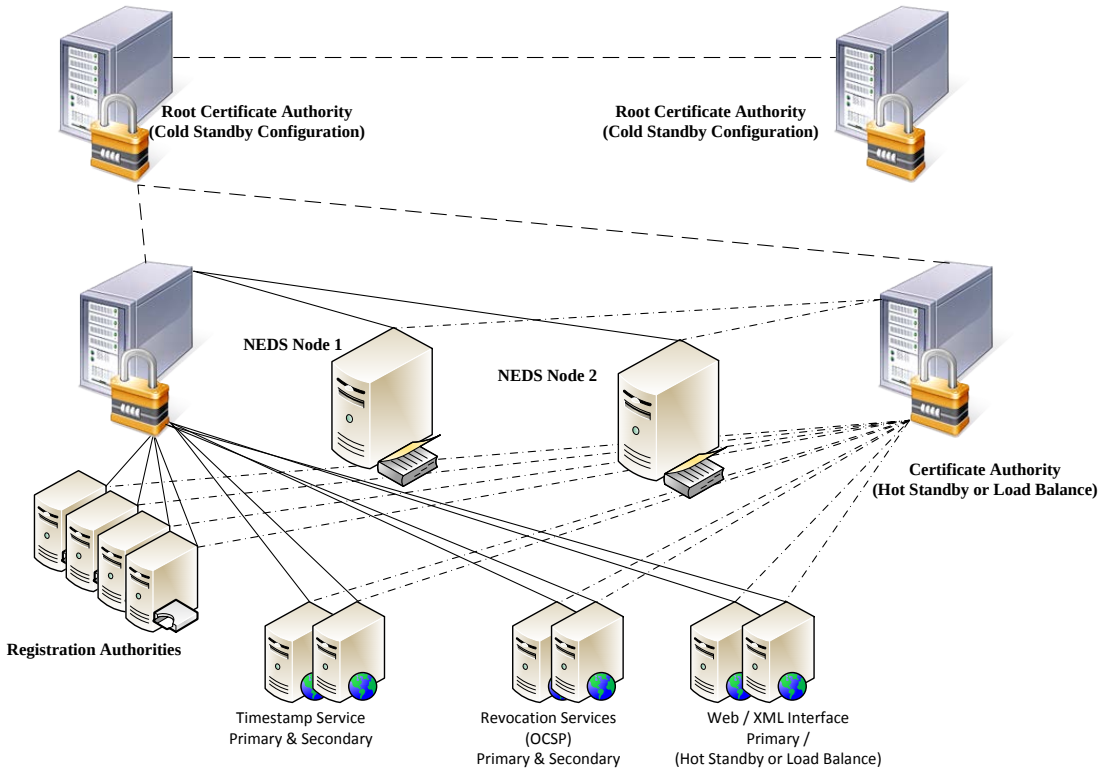

Figure 1 - High Level Architecture of E-NPKI

The Enterprise NATO Public Key Infrastructure will provide for a key certificate management infrastructure supporting the NATO Alliance across all levels of command.

For NATO to venture into the conduct of net centric operations, where there is no pre-established trust between information originator and information consumer (e.g. NATO staff officer communicating to a non-governmental organisation (NGO)) there is a need to establish implicit trust within the information to be conveyed. E-NPKI by means of its standardised and uniform approach to the management of electronic certificates will establish these implicit trust arrangements. For these trust arrangements to become ubiquitous, an all-encompassing Enterprise NATO Public Key Infrastructure needs to be acquired, implemented and operated to allow for every participant to register with the infrastructure, obtain his NATO electronic certificate and start protecting and authenticating his information with his personal electronic E-NPKI certificates.

This project details the operational requirements for all aspects of the E-NPKI including the E-NPKI interoperability needs with NATO external parties.

Requirement ID: SRS-2560

•The E-NPKI capability shall be based on 2 levels of CAs deployed within a four-tier architecture. Tier 1 is the E-NPKI Root CA, which is deployed and operated by DACAN with a backup Root CA deployed and operated by EUDAC.

The subscribers of the E-NPKI will reside in the NATO UNCLASSIFIED/NATO RESTRICTED and NATO SECRET/MISSION SECRET security domains throughout the NATO Enterprise (including the new NATO HQ). E-NPKI subscribers are referred to as End Entities (EE). An EE may be a person, a hardware device or a software application. All are pervasive across the entire networks in scope. EEs may be implemented in hardware or software cryptographic modules depending on the relevant Policy Identifier and threat environment.

NPKI services are intended to support all Military functions of the Essential Operational Capabilities (EOCs).

Tier 2 will comprise the subordinate CAs operated by NCI Agency. This is depicted in **Figure 2 - E-NPKI Hierarchy (**NSV-1), the high level system view of the E-NPKI hierarchy. Initially there will be 14 Certificate Authorities (See REF: SOW Annex C **Table 7 - List of Sites)**, however this number is expected to grow as the system matures and expands.

At Tier 3 are the Registration Authorities which provide the interfaces between End Entities and the CAs for the management of the key and certificate lifecycle.

At Tier 4 are the E-NPKI subscribers, end devices, certificates and associated card readers.

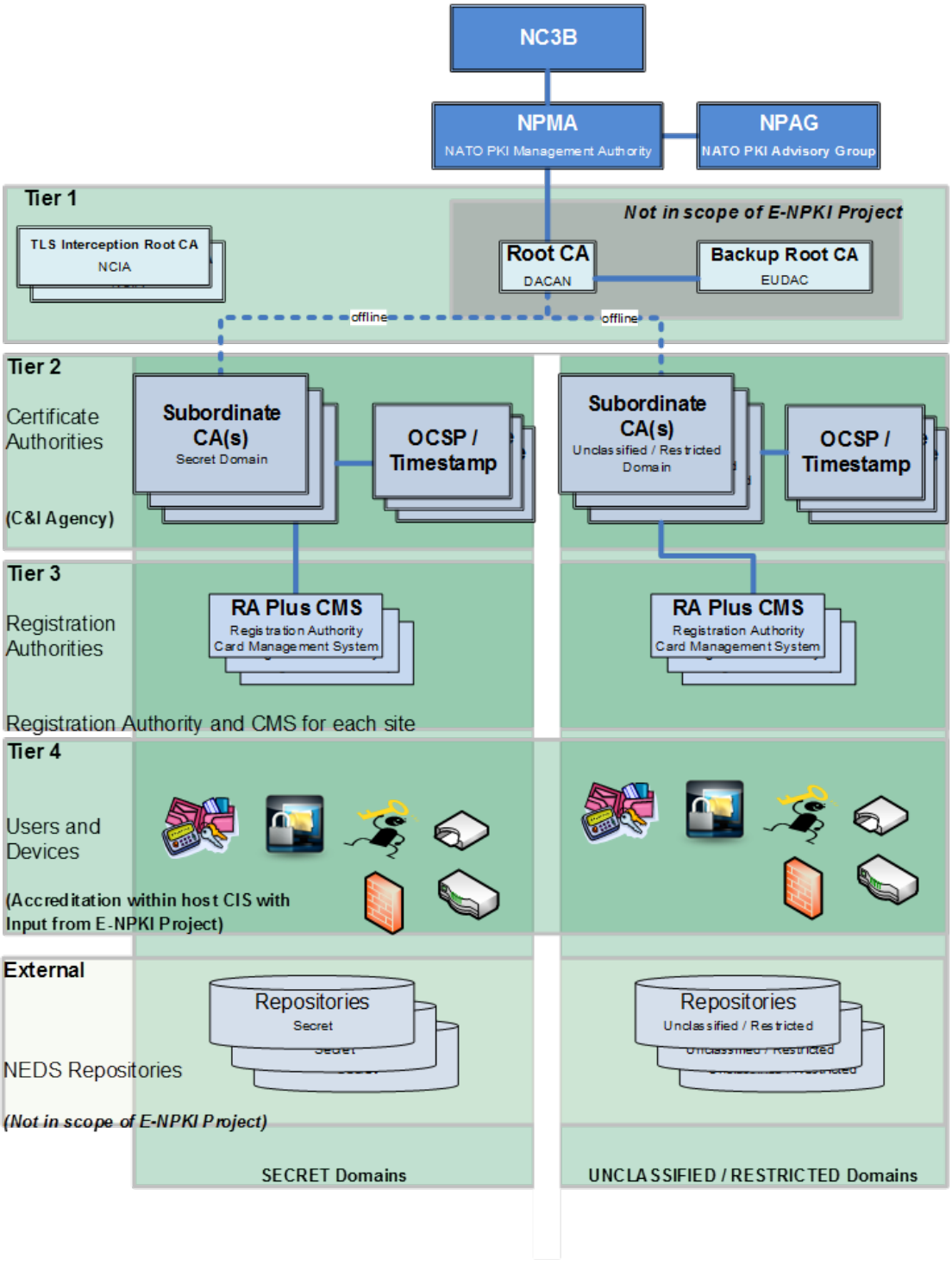

Figure 2 - E-NPKI Hierarchy (NSV-1)

Requirement ID: SRS-482

•E-NPKI services shall support the Unclassified and Restricted classification domains based on a common core of PKI service components.

Requirement ID: SRS-484

•E-NPKI services shall support Secret level domains based on an infrastructure separate from the Unclassified and Restricted domains.

2.2 General Constraints

2.2.1 Relationships with other programs

The ***E-NPKI*** is part of the Bi-SC AIS as defined in the Bi-SC AIS Reference Architecture (See REF: SOW 2.1.5.1.

The Bi-SC AIS is NATO's Command and Control Information System used throughout the NATO Command Structure, in NATO Command Deployments and in NATO Exercises. The Bi-SC AIS is in turn one element of NATO's overall CIS Capability, which includes a number of strategic sub-systems such as the NATO Core Communications Network, Planning, Intelligence, Theatre Missile Defence, and Deployable CIS and so on.

The capability to be acquired under the *INFOSEC* Services Capability Package is to be a fully integrated element of the Bi-SC AIS.

In this context, ***E-NPKI*** will co-exist with Intelligence Functional Services (Intel-FS), Logistics Functional Services (LOG FS), Maritime Functional Services (MCCIS), Land Functional Services (LC2IS), Air Functional Services (AirC2IS), Planning Functional Services (TOPFAS) and other functional services (such as Common Operational Picture, JCOP or NCOP; or Joint C2 Functional Services, JC2IS) as they become available.

E-NPKI will be integrated with Bi-SC AIS core services (directory, registry, e-mail, etc) as much as possible. The proper interfaces will be established with other services/systems using NATO Network Enabled Capability (NNEC) guidance, Service Oriented Architecture (SOA) implementation and STANAG based information exchange baselines.

2.2.2 Existing Capabilities

The interim NPKI system (iNPKI) currently exists on both the protected business network (PBN) and the Operational Network (ON). As of mid-2015 the iNPKI serves a client base with a combined total of 10,000 users and devices. iNPKI is predicted to be serving in excess of 20,000 users and devices at the time E-NPKI reaches PSA.

The iNPKI implements a subset of the architecture specified in the E-NPKI project, and implements the RSA/SHA256 algorithm suite instead of elliptic curves.

The architecture of the Tier2 iNPKI components is shown in the following diagram.

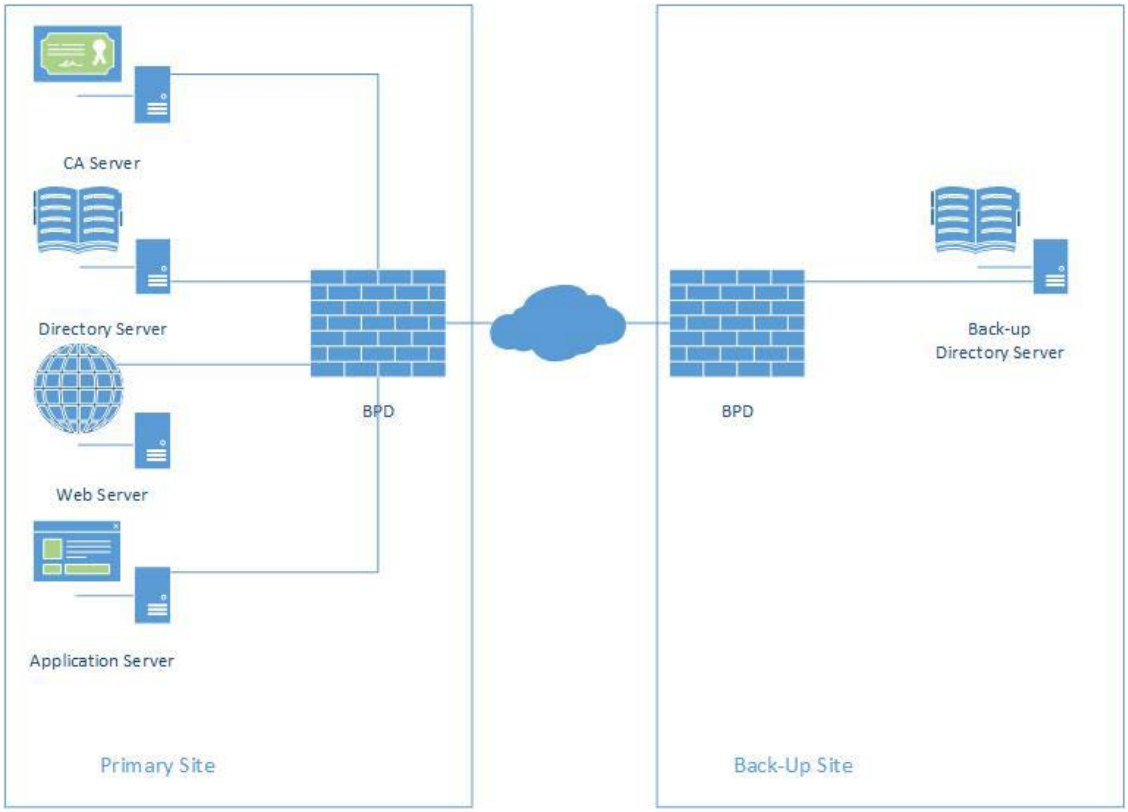

Figure 3 - iNPKI Tier 2 High Level Architecture

2.2.3 Operating Environment

The E-NPKI operates in two online domains and a third offline domain. These domains include the Operational Network (ON), the Protected Business Network (PBN), and an offline Root CA for signing SSL Interception proxy certificates operating on the PBN.

Requirement ID: SRS-2811

•The 3 separate Certification Practice Statement (CPS) documents shall appropriately reflect the requirements of the E-NPKI Certificate Policy (CertP), the results of the Security Risk Assessment (SRA) and the System Security Requirements Statement.

3 Functional Requirements

3.1 Introduction to Certificate Policy

3.1.1 Overview of Certificate Policy

Chapter 3 of this SRS is maintained in the structure of the planned Certification Practices statement which will later be delivered by the contractor as a formal deliverable. Much of the content of this section is derived from the NATO Public Key Infrastructure Certificate Policy.

3.1.2 Certificate Policy Identification

In the past NATO has implemented hardware and software token based policies. E-NPKI will require unique policy identifiers to cover PIV-(C) subscribers, X.509 subscribers, PIV devices, O/S devices, and other configurations with unique requirements.

Requirement ID: SRS-2125

•The E-NPKI shall support the implementation of multiple policies without the requirement to create additional CAs.

3.1.3 PKI Participants

The following sections introduce the E-NPKI and community roles involved in issuing and maintaining key management certificates.

3.1.3.1 Certification Authorities

A Certification Authority (CA) is an entity authorised by the NATO PKI Management Authority (NPMA) to create, sign, issue and manage public key certificates. A E-NPKI CA is comprised of the hardware, software, personnel and procedures that are required to implement the certificate lifecycle management described in this SRS. A E-NPKI CA is responsible for all aspects of the issuance and management of a certificate. This includes control over the registration process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key.

Requirement ID: SRS-2129

•All aspects of the E-NPKI CA services, operations and infrastructure related to certificates issued under this project shall be performed in accordance with the requirements, representations, and warranties of the E-NPKI CertP and the E-NPKI CA CPS. Any E-NPKI CA requirement expressed in this SRS applies to all E-NPKI CA types unless expressly stated otherwise.

Within NATO there are 2 tiers of certification authorities defined, Tier 1 and Tier 2 CAs.

The Tier 1 offline Root CAs have two profiles. The first profile is the Enterprise offline Root CAs provided and operated by DACAN. The second profile is the

offline SSL interception Root CAs to be provided under this project and operated under NATO responsibility co-located with the subordinate CAs.

Requirement ID: SRS-2131

•As the E-NPKI is hierarchical in nature, Tier 2 E-NPKI CAs which issue certificates to subscribers shall be subordinate to the DACAN E-NPKI Root CA

3.1.3.2 Registration Authorities

Requirement ID: SRS-2127

•A registration authority (RA) is an entity that enters into an agreement with a E-NPKI CA to implement the registration and identification and authentication processes by collecting and verifying subscribers' identity and information that is to be entered into public key certificates. The RA shall perform its functions in accordance with a CA CPS approved by the E-NPKI CA and the NPMA.

The division of subscriber registration responsibilities between an E-NPKI CA and RA is flexible within this document to accommodate for potential differences between PKI products.

Requirement ID: SRS-2133

•The division of responsibilities shall be described in the CPS documentation.

3.1.3.3 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with the E-NPKI CertP. The targeted E-NPKI subscribers include but are not limited to the following categories of entities that wish to communicate securely:

· NATO military and civilian personnel, and Government contractor personnel;

· Personnel from Governments and Ministries of Foreign Affairs (MFAs) and Defence (MODs) of NATO nations;

· Personnel from Non-NATO governments, MFAs, MODs and International Organisations personnel, and their Government contractor personnel; and

· Information Technology products such as workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components or cryptographically aware applications. These components shall be under the cognisance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key. The person assigned to manage one of these devices is referred to as the Sponsor of the device. The E-NPKI Sponsor works with the E-NPKI CAs and RAs to register devices and shall meet the obligations of subscribers as defined throughout this document. Within this document these IT products are referred to as "devices."

· In this document when the term subscriber is used in conjunction with a responsibility to perform some action regarding the proper use of or protection of PK credentials to access or protect NATO information assets, the reader can also assume that that responsibility also is attributed to relying parties who are involved in legitimate information exchange with other NATO subscribers.

NPKI CAs and RAs are technically subscribers to the E-NPKI; however, the term subscriber as used in this document refers only to those who request certificates for uses other than certificate management. The certificates used by E-NPKI CA and RA personnel for purposes other than certificate management qualify as subscriber certificates in this document.

3.1.3.4 Relying Parties

A relying party is the entity who trusts the validity of the binding of the subscriber's name to a public key. This reliance may result from using another subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A relying party shall determine the suitability of the certificate for the intended purpose prior to use. The relying party may use information in the certificate (such as Certificate Policy identifiers) to determine this suitability. A relying party may be a subscriber of the E-NPKI, or a subscriber of a separate PKI that has a formally approved trust relationship with the E-NPKI (e.g. is cross-certified or otherwise interoperable with the E-NPKI.) Relying parties include subscribers, subordinate E-NPKI CA's and RA's which require a reliance on certificates issued by the E-NPKI. Relying parties are not necessarily subscribers to the E-NPKI, nor an interoperable PKI as defined by the E-NPKI Interoperability Directive (See REF: SOW 2.3.8).

3.1.3.5 Other Participants

E-NPKI CAs operating under the E-NPKI Certificate Policy require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. As these related authorities may differ in implementation between NATO military and civil bodies, they are not identified in this document.

Requirement ID: SRS-2141

- These authorities and the services they provide to the E-NPKI CA shall be documented in each of the E-NPKI CA CPS based on the results of the Site Surveys.

The NATO PKI Management Authority (NPMA) is a body established by the NC3B to oversee the creation, update and approval of Certificate Policies, including evaluation of changes requested by NATO civil and military bodies, and plans for implementing any accepted changes.

The NPMA shall review the results of E-NPKI CA compliance audits to determine if the E-NPKI CAs are adequately meeting the stipulations of

approved CPS documents, and make recommendations to the E-NPKI CAs regarding corrective actions, or other measures that might be appropriate, such as revocation of E-NPKI CA certificates.

Requirement ID: SRS-2143

- The E-NPKI system shall implement all requirements and recommendations from the NPMA.

- The NPMA shall establish the suitability of external policies for compatibility with at least one NATO Certificate Policy in support of cross-certification in cases where the technical mechanism of "policy mapping" is being considered. The NPMA shall establish the suitability of external PKIs for other forms of interoperability as documented. (See REF: SOW 2.3.8). The NPMA shall provide guidance to NATO Program and Project Managers and NATO SAAs regarding the appropriateness of certificates associated with the E-NPKI Certificate Policies for specific implementations.

The NATO PKI Advisory Group (NPAG) provides subject matter experts to advise the NPMA on legal issues, technical issues, and current NATO standard operating procedures upon request of the NPMA.

The nationally manned Military Committee Distribution and Accounting Agency (DACAN) arranges for the production, accounting, and distribution of all keying material used by NATO. DACAN serves as the trusted agent responsible for the management of keying material necessary to ensure the confidentiality, integrity, availability, and authenticity of NATO information, communications, and automated information systems. DACAN will provide these services as the E-NPKI Root CA and perform as the ultimate trust point in the NATO domain to enforce the E-NPKI Certificate Policies.

The nationally manned Military Committee European Distribution and Accounting Agency (EUDAC) serves as the trusted agent, in co-operation with DACAN, for the distribution of keying material. EUDAC will serve as the E-NPKI Root CA backup site and will assume the responsibilities of DACAN as the ultimate trust point in the NATO domain to enforce the E-NPKI Certificate Policies if necessary.

The NCI Agency Cyber Security Service Line (CSSL) and its subordinate elements manage, operate and control on behalf of all subscribers, the E-NPKI core infrastructure (Certification Authorities, Timestamping Services, OCSP Services.) The NCI Agency CSSL monitor the registration Authorities, which are operated by local staff at each site of the NATO Command Structure (NCS), Agencies, and Headquarters.

The Security Accreditation Authority (SAA) is the body responsible for approving the implementation of CIS within an organisation. Within NATO there are currently three SAAs; SHAPE/INTEL for Allied Command Operations (ACO), the NATO Office of Security for NATO HQ and NATO civil Agencies,

and the Allied Command Transformation (ACT) CIS division. Together, these three accreditation authorities form the NATO CIS Security Accreditation Board (NSAB). The NSAB is responsible for the accreditation of the E-NPKI. The NOS is responsible for the inspection of the E-NPKI.

3.1.4 Certificate Usage

Requirement ID: SRS-486

•The E-NPKI shall provide for electronic certificates that allow for the signature of electronic documents with an equivalent level of legal authenticity as current documents attributed with handwritten signatures.

Requirement ID: SRS-487

•The E-NPKI shall support five primary security services: access control, confidentiality, integrity, authentication and non-repudiation. The E-NPKI supports these security services by providing Identification and Authentication (I&A), integrity, and technical non-repudiation through digital signatures, and confidentiality through key establishment in support of symmetric encryption algorithms.

Policy Object Identifiers (OIDs) are used within the E-NPKI CertP and in issued certificates to indicate a unique set of requirements. Each grouping applies to a combination of both signing and confidentiality certificates.

Requirement ID: SRS-488

•The E-NPKI shall be capable of supporting multiple policies for certificates, with the ability to identify each one with unique policy Object Identifiers OIDs.

3.2 Publication and Repository Responsibilities

3.2.1 Repositories

X.500 directories are procured by a separate NATO Enterprise Directory System (NEDS) contract in support of E-NPKI and other requirements.

3.2.1.1 External X.500 Directory obligations

The NEDS project will provide a redundant X.500 directory service consisting of at least two nodes within each E-NPKI CA security domain.

Requirement ID: SRS-2600

•The E-NPKI shall support the directory services provided by NEDS.

The NEDS system will provide a system availability of 99.5%, with a maximum of 15 minutes to restore service for both read and write access.

If an E-NPKI CA supports an additional security domain not supported by NEDS, an OLA is required between E-NPKI and the X.500 directory supporting that domain.

Requirement ID: SRS-2602

•E-NPKI system shall have tools to monitor and report on E-NPKI and directory compliance with the OLA(s).

Provision of Certificates and CRLs to and from a NATO Nation or external entities (e.g. PfP, International Organisations, etc.) in a timely fashion is the responsibility of the repository.

Requirement ID: SRS-2611

•The E-NPKI shall support X.500 strong bind (Certificate based) write access to all directories.

All external directories will support anonymous access for reading CRLs.

3.2.2 Publication of certification information

Requirement ID: SRS-2613

•E-NPKI CAs shall publish certificates to NEDS where NEDS is available.

Requirement ID: SRS-2604

•E-NPKI CAs shall publish certificates to the appropriate directory, using LDAP or LDAPS, where NEDS is not in scope (for example AOM).

Requirement ID: SRS-2605

•Where an E-NPKI CA supports multiple security Domains split across multiple directories, the E-NPKI CA shall be capable of determining the correct directory to write to, based on the DN structure of the End-Entity certificate.

Requirement ID: SRS-2607

•In the event of a write error to the directory (e.g. NEDS component outage) the E-NPKI shall automatically connect to the next available (backup) directory to publish the information.

Requirement ID: SRS-2795

•E-NPKI shall support LDAP forwarding information provided from the NEDS directory components.

3.2.3 Time or frequency of publication

Requirement ID: SRS-2606

•E-NPKI shall automatically publish CRLs and ARLs to the directory based on a configurable schedule immediately after the CRLs and ARLs are signed.

Requirement ID: SRS-2609

•In the event of certificate revocation, the E-NPKI shall automatically publish a CRL without waiting for the next publication interval.

Requirement ID: SRS-2614

•E-NPKI CAs shall publish certificates to NEDS immediately after they are signed.

3.2.4 Access controls on repositories

Requirement ID: SRS-2610

•E-NPKI CAs and RAs shall use X.500 strong bind (certificate based) authentication to read from or write to the directory.

3.3 Identification and Authentication

3.3.1 Naming

3.3.1.1 Types of names

Requirement ID: SRS-492

•The E-NPKI shall support the assignment of a unique X.501 Distinguished Name (DN) in accordance with RFC3280 and RFC5280 to each subscriber.

This information will normally be already present in the directory.

Requirement ID: SRS-2616

•The E-NPKI RA shall use the DN from the directory to populate the certificate subject name field in accordance with RFC3280 and RFC5280.

This information will be provided by the directory.

Requirement ID: SRS-493

•E-NPKI shall support the subjectAltName certificate extension in accordance with RFC3280 and RFC5280.

Requirement ID: SRS-494

•E-NPKI shall support the inclusion of distinguished names (DN) in the form of a X.501 UTF8 Printable String which shall not be empty.

3.3.1.2 Need for names to be meaningful

Requirement ID: SRS-495

•The E-NPKI Naming shall be flexible to align with the NATO organisational naming and functional role structures which are implemented within the Directory Services component. As an example, for ACO, this is documented in the ACO PE and CE naming structure.

Requirement ID: SRS-496

•The E-NPKI shall support the use of the "organization" attribute with a value "o=NATO" as the root of the naming structure provided by the external directory services.

Requirement ID: SRS-2031

•The E-NPKI shall not be dependent on the use of the "country" attribute within the directory hierarchy.

Requirement ID: SRS-2034

•The E-NPKI shall be able to interoperate with external directories and PKI implementations which have directory tree roots defined in accordance with ACP133.

Requirement ID: SRS-2032

•The E-NPKI shall function in accordance with this SRS with an external X.500 directory which supports the inclusion of all directory attributes defined in ACP133.

Requirement ID: SRS-2585

•The E-NPKI shall support the directory tree structure and naming convention defined by the NATO Enterprise Directory System.

Requirement ID: SRS-2586

•The E-NPKI shall support the established root of the directory tree structure defined as "o=nato"

Requirement ID: SRS-2033

•The E-NPKI shall not be reliant on the existence within a distinguished name of any attributes other than "organization" and "common name." (e.g. cn=npkirootca, o=nato) (i.e. all other DN attributes could be omitted in a directory entry.)

Requirement ID: SRS-2587

•The E-NPKI shall support all distinguished name attributes that are supported by ACP-133.

3.3.1.3 Anonymity or pseudonymity of subscribers

Requirement ID: SRS-497

•The E-NPKI system shall not permit the creation of anonymous identities.

Requirement ID: SRS-499

•CA's providing pseudonymity services shall provide automated mechanisms to explicitly map these identities to the persons holding them.

Requirement ID: SRS-2071

•The E-NPKI system shall be configurable to prevent the creation of pseudonymous end-entities.

Requirement ID: SRS-500

•The E-NPKI system shall be configurable to prevent the creation of pseudonymous end-entities which include the non-repudiation key usage extension value.

3.3.1.4 Rules for interpreting various name forms

As the establishment of names is the responsibility of the directory service or another separate authoritative data source, there is no requirement on the E-NPKI.

3.3.1.5 Uniqueness of names

Requirement ID: SRS-501

•Distinguished names shall be unique for all End-Entities of the E-NPKI. For each subscriber, the middle name, or additional numbers are appended to the commonName if required to ensure uniqueness of the Distinguished Name (DN).

3.3.1.6 Recognition, authentication, and role of trademarks

As the establishment of names is the responsibility of the directory service or another separate authoritative data source, there is no requirement on the E-NPKI.

3.3.2 Initial identity validation

3.3.2.1 Method to prove possession of private key

Requirement ID: SRS-2035

•The E-NPKI system shall enforce the same requirements for sponsors and subscribers providing proof of possession of private keys under their control.

Requirement ID: SRS-502

•Prior to the issuance of certificates, the Issuing E-NPKI RA and subscriber shall mutually authenticate each other's identity.

Requirement ID: SRS-505

•Proof of possession of the private key shall be implemented in all certificate issuance scenarios.

Requirement ID: SRS-503

•Acceptable mechanisms for this authentication shall include pre-shared secret and PKIX Certificate Management Protocol (CMP) defined in RFC4210.

Requirement ID: SRS-504

•Proof of possession of the private key shall be achieved by the subscriber using its private key to sign a value and providing that value to the issuing E-NPKI CA. The issuing E-NPKI CA shall be capable of validating the signature using the party's public key.

Requirement ID: SRS-2620

•The E-NPKI shall implement PKIX Certificate Management Protocol (CMP) defined in RFC4210.

Requirement ID: SRS-507

•Non-Repudiation identity certificates shall be established within a process that binds the identity attributes of the E-NPKI subscriber uniquely with the certificate.

Requirement ID: SRS-2155

•The E-NPKI shall enforce subscriber digital signature key pair generation within the hardware token.

Requirement ID: SRS-2157

•The E-NPKI workflow shall enforce the generation of key pairs in the presence of the subscriber or sponsor as appropriate.

Requirement ID: SRS-2156

•The E-NPKI shall prove possession of the private key based on an approved method described within the E-NPKI Certificate Policy.

3.3.2.2 Authentication of organisation identity

Requirement ID: SRS-2016

•The E-NPKI CA and RA shall be capable of validating the organizational affiliation of all trusted role personnel.

Requirement ID: SRS-2017

•In addition to making access control decisions based on the membership in a trusted role, the E-NPKI CA and RA shall be capable of enforcing Access control decisions on CA and RA Trusted roles based on the organizational affiliation of the subscriber or trusted role.

Requirement ID: SRS-2018

•The granularity of control shall be flexible to allow for access control to be managed securely and efficiently.

Requirement ID: SRS-2036

•The granularity of control shall allow for access control to be restricted to a single organization or OU (or other directory attribute) in the directory.

Requirement ID: SRS-2037

•The granularity of control shall allow for access control to be restricted to a grouping of multiple OU (or other directory attribute) selections in the directory.

3.3.2.3 Authentication of individual identity

Requirement ID: SRS-2837

•All smartcard issuance shall be implemented through the Card Management System components of the Registration Authority.

Requirement ID: SRS-2838

•Physical Access Control shall be implemented on the PBN only. ON smartcards shall not be enabled for PACS.

Requirement ID: SRS-2013

•The E-NPKI shall be capable of leveraging identity information from Identity Management components existing within NATO.

Requirement ID: SRS-2812

•The E-NPKI RA components shall be capable of personalizing the tokens with the information from the registration process.

Requirement ID: SRS-2813

•Where the existing CMS components for PACS include printing capabilities, this requirement shall be met by integrating with the existing CMS as identified below.

Requirement ID: SRS-2814

•Where no CMS components are in place, the E-NPKI shall provide the full CMS including camera and printing capabilities.

Requirement ID: SRS-2831

•The scope of CMS is defined in sections 2 through 4 of FIPS201-2 (See Ref 2.2.4.) The CMS shall support all biometric capture requirements of FIPS 201-2 chapter 2, but the vendor is only required to provide hardware to support image capture and printing. See details in CR#15 through CR#18 for information by site.

Requirement ID: SRS-2833

•Visual personalization of the card shall include but is not limited to Name, Picture, Organization, Logos, Clearance, and expiry.

Requirement ID: SRS-2834

•Visual design and security features (including micro printing, security laminates and ultraviolet ink shall be agreed with the system accreditor.

Requirement ID: SRS-2014

•The E-NPKI shall be capable of integrating with Card Management Systems supporting the FIPS-201 standard for integration with existing Physical Access Control systems within NATO on the PBN.

Requirement ID: SRS-2161

•The E-NPKI shall integrate with the CITI manageID CMS.

Requirement ID: SRS-2722

•The E-NPKI shall integrate with the Entrust IdentityGuard CMS.

Requirement ID: SRS-2723

•The E-NPKI shall integrate with the XTec AuthentX Basic Enrolment Station CMS.

Requirement ID: SRS-2163

•Where the above identified CMS implementations require additional components to meet the requirements of this SRS (e.g. to implement certificate lifecycle management for FIPS 201 tokens) the E-NPKI system shall incorporate those components, integration, and documentation as part of their solution at no additional cost to NATO.

Requirement ID: SRS-2015

•The E-NPKI shall demonstrate a proven track record for integration with multiple vendors Physical Access Control (PACS) Card Management systems (CMS) including Biometrics, without requiring custom modifications to the E-NPKI Certification Authorities.

Requirement ID: SRS-508

•Face to face identification and authentication of the subscriber or sponsor shall be implemented and enforced by the E-NPKI.

Requirement ID: SRS-2019

•The E-NPKI shall keep a record of the type and details of identification based on the comparison of the identity of the individual against a configurable number of pieces of Government or NATO issued photographic identification (notarised copies or originals).

Requirement ID: SRS-509

•The E-NPKI system shall electronically record the ID and the details of a configurable number of pieces of Government or NATO issued photographic identification (notarised copies or originals).

Requirement ID: SRS-527

•The E-NPKI system shall electronically record the date on which the face to face authentication occurred

Requirement ID: SRS-510

•The E-NPKI shall enforce face to face authentication of all subscribers and sponsors periodically.

Requirement ID: SRS-515

•The E-NPKI shall enforce Identification and authentication of a sponsor following the procedures established for subscribers as if that sponsor was applying for the certificate on its own behalf.

Requirement ID: SRS-516

•The E-NPKI CA or RA shall electronically record the evidence and verification of the sponsor's individual authority to receive the keys for that device or software.

Requirement ID: SRS-2039

•Enforcement of face to face authentication shall be electronically implemented in a manner which prevents the issuance of credentials to subscribers who have not met the requirements of this paragraph including the periodic renewal of face to face authentication.

Requirement ID: SRS-511

•The time between face to face authentications shall be configurable (for example, at least once every three years.)

Requirement ID: SRS-2162

•The E-NPKI shall automatically use email or other facilitative information to notify end-entities of their requirements to report for face to face authentication at a configurable time before the face to face period (and certificates) expire.

Requirement ID: SRS-512

•Biometrics shall be supported by E-NPKI to use as amplifying identity evidencing attributes, in the event that the E-NPKI arrangements within that command require the support of these attributes.

Requirement ID: SRS-2164

•The E-NPKI shall be capable of supporting all biometric information types defined within the FIPS 201 standards without requiring changes of existing E-NPKI software or hardware components.

Requirement ID: SRS-2165

•Implementing a new biometric capture device on the contractor provided CMS shall only require the attachment and configuration of the appropriate biometric scanning device.

Requirement ID: SRS-2166

•The E-NPKI shall support the existing FIPS 201 compliant biometric scanning equipment included within the already fielded CMS solutions identified within this SRS.

Requirement ID: SRS-2038

•Support for writing Biometric data objects to smart cards by the CMS shall be in accordance with FIPS 201 in all cases where FIPS 201 Smart cards are in use.

3.3.2.4 Non-verified subscriber information

Requirement ID: SRS-517

•The E-NPKI shall electronically record the evidence and verification of all subscriber information to be included within a certificate during the enrolment process.

Requirement ID: SRS-519

•The E-NPKI shall electronically record facilitative information (such as contact telephone numbers and email addresses not included in the certificate) but does not need to formally verify this information.

3.3.2.5 Validation of authority

Requirement ID: SRS-520

•The E-NPKI shall validate and record evidence ascertaining that the subscriber has the authorisation to act on behalf of the organisation before issuing certificates that contain explicit or implicit organisation affiliations. Examples of these include organisation, group, and role certificates, and CA/RA server certificates.

3.3.2.6 Criteria for interoperation

Requirement ID: SRS-2073

•E-NPKI shall support interoperability based on the import of Trusted Root Certification Authorities into Browser, Application, and Operating System Root CA Certificate Stores.

Requirement ID: SRS-2072

•E-NPKI Shall support Cross Certification.

Requirement ID: SRS-2074

•E-NPKI shall support path discovery and path validation of cross certified certificates stored in the NATO Enterprise Directory System.

Requirement ID: SRS-2080

•E-NPKI shall support path discovery and path validation of cross certified certificates stored in the application and browser certificate stores (published via Group Policy Objects.)

Requirement ID: SRS-2075

•All E-NPKI components shall correctly interpret and comply with information published in the Certificate Policies extension.

Requirement ID: SRS-2076

•All E-NPKI components shall correctly interpret and comply with information published in the Policy Mappings extension.

Requirement ID: SRS-2077

•All E-NPKI components shall correctly interpret and comply with information published in the Path Length Constraints extension.

Requirement ID: SRS-2078

•All E-NPKI components shall correctly interpret and comply with information published in the Name Constraints extension.

Requirement ID: SRS-2079

•All E-NPKI components shall correctly interpret and comply with information published in the Inhibit Any-Policy extension.

3.3.3 Identification and authentication for re-key requests

3.3.3.1 Identification and authentication for routine re-key

Requirement ID: SRS-521

•The E-NPKI shall only accept requests for re-key made by the end-entity in whose name the keys have been issued or from the E-NPKI CA or RA.

Requirement ID: SRS-2624

•Written notification of changes to device sponsors shall be captured by the E-NPKI RA.

Requirement ID: SRS-2625

•The E-NPKI RA shall implement mechanisms to capture the change of sponsor and to automatically link the new sponsor identity to each of the devices.

Requirement ID: SRS-522

•All requests for re-key shall be authenticated by the E-NPKI CA, and the subsequent response shall be authenticated by the subscriber based on the mechanisms in paragraph 3.3.2.1 above.

Requirement ID: SRS-523

•A subscriber requesting re-key shall only be able to authenticate the request for re-key using its valid Digital Signature key pair up to the maximum period between in person authentication defined in paragraph 3.3.2.3 above.

Requirement ID: SRS-525

•When any of the subscriber keys required to complete the authentication has expired, the E-NPKI shall enforce the request for re-key to be authenticated in the same manner as the initial registration.

Requirement ID: SRS-526

•If the subscriber or Sponsor fails to appear for face to face registration before the required period has expired, all currently valid certificates issued to the subscriber or device shall be revoked.

Requirement ID: SRS-2168

•The E-NPKI shall automatically generate a list of subscribers for whom the face to face registration requirements are about to expire within a configurable threshold.

Requirement ID: SRS-2167

•The E-NPKI shall automatically generate a list of subscribers for whom the face to face registration requirements are no longer met.

Requirement ID: SRS-2785

•E-NPKI operators shall also be able to manually generate lists on demand for users where face to face registration requirements are expired or about to expire.

Requirement ID: SRS-2786

•Generated lists shall be rendered in CSV format.

3.3.3.2 Identification and authentication for re-key after revocation

Requirement ID: SRS-524

•In the event of certificate revocation, the E-NPKI shall enforce authentication in the same manner as for initial registration prior to certificate rekey.

3.3.4 Identification and authentication for revocation request

Requirement ID: SRS-528

•The E-NPKI shall authenticate a request for revocation of a certificate.

Requirement ID: SRS-2040

•The E-NPKI shall validate and record the data used to authenticate revocation requests.

3.4 Certificate Life-Cycle Operational Requirements

3.4.1 Certificate Application

3.4.1.1 Who can submit a certificate application

Requirement ID: SRS-530

•The E-NPKI shall record the details regarding the submission of certificate applications for subscribers and devices.

3.4.1.2 Enrolment process and responsibilities

Requirement ID: SRS-2152

•The CA or RA shall enforce the completion of all certificate enrolment steps prior to certificate issuance.

Requirement ID: SRS-2825

Within each security domain, E-NPKI RA functionality is divided into two separate functionalities; Token issuance (See SRS 2047) and device certificate issuance. (See SRS-2826.)

Requirement ID: SRS-2826

•Additional RA functionality is required within the Service Kiosk or NCIA CSU to manage issuance of device certificates and to manage certificate profiles for users.

Requirement ID: SRS-2827

•The RA components defined in SRS-2047,SRS-2825 and SRS-2826 shall be capable of providing redundancy between them to avoid single points of failure within a site.

Requirement ID: SRS-2828

•Registration Authority services on each domain of each site shall have an availability of 99.5%

Requirement ID: SRS-533

•The applicant (subscriber or sponsor) and the E-NPKI RA shall perform the following steps when an applicant applies for a certificate:

Requirement ID: SRS-534

- The applicant and the E-NPKI RA shall establish and record identity of subscriber (per Section 3.3.2);

Requirement ID: SRS-535

- The applicant (or the client application on behalf of the applicant) shall generate a public/private key pair for each certificate required, or in the case of devices which are unable to generate a public/private key pair the sponsor shall request the generation of the public/private key pair by the CA;

Requirement ID: SRS-536

- The E-NPKI CA or RA shall establish that the public key forms a functioning key pair with the private key held by the subscriber;

Requirement ID: SRS-537

- The E-NPKI RA shall verify any roles or authorizations including explicit durations;

Requirement ID: SRS-544

- The E-NPKI RA shall record these authorizations and durations.

Requirement ID: SRS-538

- The RA shall enforce the subscriber to sign the subscriber agreement, of the applicable terms and conditions governing their use of the certificate.

Requirement ID: SRS-2626

•The RA shall digitally archive the subscriber agreement.

Requirement ID: SRS-2836

•Policy permits the use of the newly issued credential to digitally sign the electronic subscriber agreement in order to eliminate the need to scan additional paper records.

These steps may be performed in any order that is convenient for the E-NPKI CA, RA, and subscribers which does not defeat security.

Requirement ID: SRS-2588

•The order of steps shall not result in a process which permits the bypassing or defeating of system security.

Requirement ID: SRS-542

•The E-NPKI RA shall provide and enforce workflows to ensure that all steps are completed.

Requirement ID: SRS-545

•The E-NPKI RA workflows shall be able to track authorizations (including their duration), face to face authentication timelines, and certificate expiry.

Requirement ID: SRS-531

•The E-NPKI RA shall be able to process bulk applications for individuals or devices within an organisation.

Requirement ID: SRS-541

•The E-NPKI RA shall verify and record the details of verification that bulk applications on behalf of End-Entities are only be made by persons authorised to make such applications.

Requirement ID: SRS-540

•All communications among E-NPKI CAs and RAs supporting the certificate application and issuance process shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued.

Requirement ID: SRS-2628

•Communications supporting the issuance of certificates shall be protected using certificates implementing the same policy OID, or another mechanism of at least equivalent strength as determined by the SAA).

Requirement ID: SRS-2629

•Communications supporting the issuance of certificates shall be protected by certificates and keys stored in an approved hardware token as defined in section 3.6 of the SRS.

Requirement ID: SRS-2630

•Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means of at least equivalent strength of the data to be protected as determined by the SAA by the certificates being issued.

Requirement ID: SRS-2631

•Any electronic transmission of shared secrets shall be protected by certificates and keys stored in an approved hardware token as defined in section 3.6 of the SRS.

3.4.2 Certificate application processing

3.4.2.1 Performing identification and authentication functions

Requirement ID: SRS-543

•Upon receiving a request for certificate issuance, the E-NPKI shall complete the following tasks:

Requirement ID: SRS-2041

- The E-NPKI RA shall verify the enrolment process and responsibilities have been completed in accordance with 3.4.1.2.

Requirement ID: SRS-2042

- The E-NPKI RA shall verify the accuracy and integrity of the information in the certificate request.

Requirement ID: SRS-2043

- The E-NPKI CA or RA shall complete building the certificate, if the enrolment and verification steps have been met.

Requirement ID: SRS-2153

•The E-NPKI CA shall sign the certificate, if the enrolment and verification steps have been met

Requirement ID: SRS-2044

- The E-NPKI CA or RA shall make the certificate available to the subscriber as described in sections 3.2 and 3.4.3 of the SRS.

3.4.2.2 Approval or rejection of certificate applications

Requirement ID: SRS-2045

•The E-NPKI CA or RA shall digitally record details regarding the approval or rejection of certificate applications.

Requirement ID: SRS-2627

•The details shall include the documentation submitted during the certificate application, the reason for rejection (if the request is not approved, and the signed subscriber agreement.

Requirement ID: SRS-2787

•The E-NPKI RA shall be capable of generating reports on the approved/rejected certificates.

3.4.2.3 Time to process certificate applications

Requirement ID: SRS-546

•The E-NPKI shall implement workflows and automation in order to minimize the manpower requirements necessary to operate the E-NPKI.

Requirement ID: SRS-2047

•The E-NPKI Registration Authority integration, workflows, and automation shall allow for the issuance and management of tokens by physical security (Security pass issuance) offices without the requirement for additional manpower for all sites implementing FIPS 201 compliant card management systems.

Requirement ID: SRS-2048

•The E-NPKI Registration Authority integration, workflows, and automation shall allow for the management of certificate lifecycles without the requirement for additional manpower.

Requirement ID: SRS-2788

•Workflows shall enforce multi-person control where required by the E-NPKI CertP.

Requirement ID: SRS-2789

•E-NPKI workflows shall also enforce completion of all mandatory steps and fields before moving on to following steps for issuance.

3.4.3 Certificate issuance

3.4.3.1 CA actions during certificate issuance

The E-NPKI issuance and publication of a certificate indicates a complete approval of the certificate application.

Requirement ID: SRS-2049

•The E-NPKI certificate issuance workflow shall provide a clear indication of the activities required prior to certificate issuance.

Requirement ID: SRS-2632

•The E-NPKI certificate issuance workflow shall require acknowledgement or other action from the relevant trusted role of the activities as they are completed. For example the digital archiving of the subscriber agreement and an automatic check box from the application if proof of possession of the private key is correct.

Requirement ID: SRS-2050

•The E-NPKI certificate issuance workflow shall provide a clear indication of certificate issuance at the end of the workflow process.

Requirement ID: SRS-447

•The E-NPKI shall validate identity attributes, related to entity's role within the local domain against the entity's organizational roles, before including the attributes in digital certificates.

Requirement ID: SRS-2046

•The E-NPKI certificate issuance workflow shall be managed and technically controlled exclusively by the E-NPKI Trusted Roles.

Requirement ID: SRS-467

•For all E-NPKI Trusted roles, the System shall be able to generate digital certificates associating an entity with the entity's role and profile within the domain.

3.4.3.2 Notification to subscriber by the CA of issuance of certificate

Where enrolment is completed directly at the CA or RA, notification is deemed to be completed at the end of a successful enrolment process which includes the publication of the certificate within the directory. Where remote enrolment is completed, the publication of the signed certificate within the directory is deemed to be the notification. Notification of certificate issuance to other parties within this document is deemed to be the publication of the relevant certificates within the directory.

Requirement ID: SRS-2052

•The E-NPKI CA or RA shall as a minimum provide the subscriber with a simple "success" dialog box where the subscriber is enrolling for certificates in person at the RA or via an online protocol.

Requirement ID: SRS-2053

•The E-NPKI shall send an automated message to the facilitative contact details provided during enrolment advising the subscriber when a return to the RA is required to complete the enrolment process

Requirement ID: SRS-548

•The E-NPKI shall send an automated message to the facilitative contact details provided during enrolment advising the subscriber of the issuance of the certificates and providing instructions on the retrieval of the certificates.

3.4.4 Certificate acceptance

3.4.4.1 Conduct constituting certificate acceptance

Requirement ID: SRS-549

•The E-NPKI shall ensure through its automated workflow that a subscriber (or sponsor) acknowledges receipt of a certificate and acceptance of the subscriber agreement.

Requirement ID: SRS-562

•The E-NPKI automated workflow shall automatically store the subscriber and sponsor agreements during each face to face authentication.

Requirement ID: SRS-2051

•The E-NPKI workflow shall automatically locate the latest signed subscriber or sponsor agreement during each face to face authentication.

Requirement ID: SRS-2633

•The E-NPKI workflow shall automatically update the face to face deadline status for all devices assigned to the sponsor each time the sponsor completes a face to face.

Requirement ID: SRS-2634

•The E-NPKI workflow shall automatically locate the latest signed subscriber or sponsor agreement each time a certificate request, renewal, modification or revocation is requested by that subscriber or sponsor.

3.4.4.2 Publication of the certificate by the CA

Requirement ID: SRS-2635

•The E-NPKI CA shall not publish the certificate, or otherwise make it available unless all of the required workflow activities have been completed.

3.4.4.3 Notification of certificate issuance by the CA to other entities

Requirement ID: SRS-2636

•Publication of the certificate into the directory shall be the only step required of the E-NPKI CA to notify other entities of certificate issuance.

3.4.5 Key pair and certificate usage

3.4.5.1 CA private key and certificate usage

Requirement ID: SRS-550

•E-NPKI Root CAs shall implement technical controls to ensure that its certificate signing private key is used only for the following purposes:

Requirement ID: SRS-2174

•to sign subordinate CA certificates and CRLs.

Requirement ID: SRS-2173

•to issue certificates to their own trusted roles as defined in SRS Section 3.1.3

Requirement ID: SRS-2177

•E-NPKI Root CAs shall have a certificate capable of supporting the following signature services:

Requirement ID: SRS-2176

•to sign the CA Database for the provision of internal integrity services.

Requirement ID: SRS-2175

•to sign audit data in order to preserve its integrity.

Requirement ID: SRS-2790

•E-NPKI Root CAs for SSL interception certificates shall only issue subordinate certificates to SSL interception proxies operating on the PBN.

Requirement ID: SRS-2185

•E-NPKI Root CAs shall implement technical controls to prevent the issuance of certificates to subscribers and devices other than internal trusted role certificates for managing the CA.

Requirement ID: SRS-551

•E-NPKI Tier 2 CAs shall implement technical controls to enforce that its certificate signing private key is used only for the following purposes:

Requirement ID: SRS-2178

- to sign CRLs.

Requirement ID: SRS-2184

- to sign Subordinate CA certificates

Requirement ID: SRS-2179

- to issue certificates to their own trusted roles as defined in SRS Section 3.1.3

Requirement ID: SRS-2180

- to issue certificates to subscribers and devices with end entity certificate profiles as defined in SRS Section 3.7.1

Requirement ID: SRS-2181

•E-NPKI Tier 2 CAs shall have a certificate capable of supporting the following signature services:

Requirement ID: SRS-2182

•to sign the CA Database for the provision of internal integrity services.

Requirement ID: SRS-2183

•to sign audit data in order to preserve its integrity.

Requirement ID: SRS-2054

•E-NPKI Tier 2 CAs that issue Subordinate CA certificates (Determined by the presence of the "Basic Constraints" extension populated with "Subject Type = CA") shall implement technical controls to prevent the issuance of certificates to subscribers and devices other than internal trusted role certificates for managing the CA.

Requirement ID: SRS-552

•E-NPKI Tier 2 CAs that issue certificates to subscribers and devices, other than internal trusted role certificates for managing the CA, shall implement technical controls to prevent the issuance of Subordinate CA certificates (Determined by the presence of the "Basic Constraints" extension populated with "Subject Type = CA").

Requirement ID: SRS-553

•A E-NPKI CA shall enforce that credentials keys issued to its personnel to access and operate E-NPKI CA software are used only for such purposes.

3.4.5.2 RA private key and certificate usage

Requirement ID: SRS-554

•E-NPKI RAs shall enforce that credentials issued to its personnel to access and operate RA system are used only for such purposes.

3.4.5.3 Subscriber private key and certificate usage

Requirement ID: SRS-555

•Non-repudiation credentials shall only be implemented when there is a clear body of evidence to show that the private key is only in the possession of the subscriber. This includes the requirement for evidence to show that the encrypted private key is not subject to offline password brute force attacks against software cryptographic modules.

3.4.5.4 Relying party public key and certificate usage

3.4.6 Certificate renewal

Certificate renewal is defined as the process of re-issuing a certificate to extend its expiry date without changing the key pair.

Requirement ID: SRS-556

•E-NPKI CA Certificate renewal functionality shall be configurable to allow it to be disabled if required by policy.

Requirement ID: SRS-557

•E-NPKI CA Certificate renewal functionality shall conform to the same requirements as Certificate rekey defined in 3.4.7 below.

3.4.7 Certificate re-key

Certificate rekey is defined as the process of re-issuing a certificate with a new key pair to extend its expiry date without changing the identity or other certificate extensions.

3.4.7.1 Circumstance for certificate re-key

Renewal of certificates at a configurable time prior to their expiry is required to ensure that certificates do not expire. Also relevant are the determination of continued need for the certificates, face to face authentication requirements, and operational impact.

Requirement ID: SRS-558

•E-NPKI CAs shall be capable of automated rekeying of certificates which have not been revoked prior to their expiry subject to the conditions of section 3.3.3.

Requirement ID: SRS-2055

•E-NPKI CAs, RAs, and E-NPKI End Entity Software shall work together to request or push re-keys of end entity certificates at a configurable time prior to the expiry of certificates.

Requirement ID: SRS-2637

•Where E-NPKI End Entity software is in use it shall request rekey from the CA at a configurable interval prior to the expiry of the subscriber or device certificates

Requirement ID: SRS-2056

•Where certificate re-key is dependent on a renewal of face-to-face authentication, automated notification to the subscriber or sponsor of this requirement shall be triggered by the E-NPKI RA and completed prior to the scheduled End-Entity triggering of the automated re-key.

Requirement ID: SRS-2188

•The timeframe and methods for notification shall be configurable.

3.4.7.2 Who may request certification of a new public key

Requirement ID: SRS-560

•The re-key process shall be capable of being initiated by both the holder of the certificate, (or the sponsor of the certificate in the case of devices) or the CA / RA managing those certificates.

3.4.7.3 Processing certificate re-keying requests

Requirement ID: SRS-561

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.3.3.1 and 3.4.2 of this document.

3.4.7.4 Notification of new certificate issuance to subscriber

Requirement ID: SRS-2011

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.4.3.2 of this document.

3.4.7.5 Conduct constituting acceptance of a re-keyed certificate

Requirement ID: SRS-563

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.4.4.1 of this document.

3.4.7.6 Publication of the re-keyed certificate by the CA

Requirement ID: SRS-564

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.4.4.2 of this document.

3.4.7.7 Notification of certificate issuance by the CA to other entities

Requirement ID: SRS-565

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.4.3.2 of this document.

3.4.8 Certificate modification

Certificate Modification is defined as the changing of certificate extensions (excluding the validity period or the key pair.)

Requirement ID: SRS-2059

•Certificate Modification shall include the ability to enforce re-key for the current active certificates.

Requirement ID: SRS-2060

•Where Certificate Modification includes the change of the subscriber distinguished name, the CA shall continue to maintain the subscribers archived encryption certificates and distribute them to the new distinguished name.

Requirement ID: SRS-566

•NPKI Certificate modification functionality, shall include support for mandatory re-key.

Requirement ID: SRS-2638

•If rekey is implemented during certificate modification, the restriction on validity period within this paragraph is not relevant.

Requirement ID: SRS-567

•NPKI Certificate modification functionality shall enforce the requirements defined in section 3.4.7 of this document.

3.4.8.1 Circumstance for certificate modification

A certificate modification might be required for a number of reasons, including:

•Following a change of name by a subscriber (e.g. marriage) that results in a new common name (CN).

•Following a reorganisation of affiliation resulting in a change of distinguished name (DN) other than the CN

•Following a change in policy OIDs or policy constraints

•For a CA certificate following a change in namespace constraints

3.4.8.2 Who may request certificate modification

Requirement ID: SRS-2010

•The modification process shall be capable of being initiated by both the holder of the certificate, (or the sponsor of the certificate in the case of devices) or the CA / RA managing those certificates.

3.4.8.3 Processing certificate modification requests

Requirement ID: SRS-569

•NPKI RAs shall verify that the subscriber can demonstrate continued possession of the private key.

•· Repeat the identification requirements stipulated in section 3.3.2

•· Verify that the authority of the subscriber to hold the certificate is still valid.

•· Verify that the requested modifications are permitted by the relevant CPS

Requirement ID: SRS-570

•NPKI RAs shall have a workflow to support the;

•· Repetition of the identification requirements stipulated in section 3.3.2

•· Verification that the authority of the subscriber to hold the certificates is still valid.

•· Verification that the requested modifications are permitted.

3.4.8.4 Notification of new certificate issuance to subscriber

Requirement ID: SRS-571

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.4.3.2 of this document.

3.4.8.5 Conduct constituting acceptance of modified certificate

Requirement ID: SRS-572

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.4.4.1 of this document.

3.4.8.6 Publication of the modified certificate by the CA

Requirement ID: SRS-573

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.4.4.2 of this document.

3.4.8.7 Notification of certificate issuance by the CA to other entities

Requirement ID: SRS-574

•The E-NPKI CA and RA shall enforce the requirements defined in section 3.4.3.2 of this document.

3.4.9 Certificate revocation and suspension

3.4.9.1 Circumstances for revocation

Requirement ID: SRS-2639

•E-NPKI Revocation service shall support the documentation of revocation circumstances based on the population of the reason code extension within CRLs.

Requirement ID: SRS-2640

•E-NPKI shall implement a Revocation workflow to assist with the data capture and audit requirements of certificate revocation.

3.4.9.2 Who can request revocation

Requirement ID: SRS-2641

•E-NPKI Revocation workflow shall capture and archive the identity of the revocation requestor.

3.4.9.3 Procedure for revocation request

Requirement ID: SRS-575

•Revocation requests shall be authenticated and authorised by E-NPKI CAs and RAs.

Requirement ID: SRS-2061

•The E-NPKI Trusted roles shall attempt to notify the subscriber or sponsor of the certificate to minimise operational impact.

Requirement ID: SRS-576

•The E-NPKI shall include technical mechanisms to record the authentication of a revocation request, and any resulting actions taken by the E-NPKI trusted roles including, in the case where a certificate is revoked, a full justification for the revocation.

Requirement ID: SRS-577

•Based on the input of the DN to be revoked, the E-NPKI CA or RA shall look up the Facilitative information to enable notification of the subscriber or sponsor of the revocation of their certificate.

Requirement ID: SRS-578

•Where a cross-certificate or E-NPKI CA certificate is revoked by the E-NPKI Root CA, the revocation shall be published in the Authority Revocation List (ARL) of the Issuing E-NPKI Root CA.

Requirement ID: SRS-2724

•Once revoked, certificates shall not be removed from the Certificate Revocation list even after the expiry of the certificate.

3.4.9.4 Revocation request grace period

Requirement ID: SRS-2642

•The E-NPKI CA and RA revocation workflow shall log both the start time of the workflow and the end time of the workflow in order to provide data to support the relevant SLAs.

3.4.9.5 Time within which CA must process the revocation request

Requirement ID: SRS-2643

•Once the requirement to revoke a certificate has been ascertained, the revocation shall be completed within 1 hour.

Requirement ID: SRS-452

•In the event of a certificate revocation, the CA shall immediately issue an updated Revocation list (CRL or ARL as appropriate).

Requirement ID: SRS-451

•Revocation services shall be available 24 hours a day and 7 days a week continuous.

Requirement ID: SRS-2189

•The availability of revocation services within the Datacenters (inclusive of OCSP and CRLs) shall be 99.99% with the assumption that the underlying wide area network availability is not a factor.

Requirement ID: SRS-2198

•The end to end availability of revocation services (inclusive of OCSP and CRLs) for all sites connected via dual communications paths shall be 99.5% with the assumption that the underlying network availability is not a factor within a single site.

Requirement ID: SRS-2199

•The end to end availability of revocation services (inclusive of OCSP and CRLs) for all sites connected via a single communications path shall be 98%.

3.4.9.6 Revocation checking requirement for relying parties

Requirement ID: SRS-579

•All E-NPKI components shall validate certificate chains through any available certificate status service, including OCSP and CRLs.

Caching of CRLs or OCSP responses is permitted for short periods of time, (e.g. for applications which validate the same CRL several times during application start-up.)

Requirement ID: SRS-2154

•E-NPKI Components shall not cache CRLs for the lifetime of the CRL.

Requirement ID: SRS-581

•When CRLs or OCSP responses are to be cached, the maximum cache lifetime shall be configurable.

Requirement ID: SRS-2201

•ENPKI components shall be capable of setting the maximum cache lifetime to 0 minutes where required by policy.

Requirement ID: SRS-2197

•When all revocation services are temporarily unavailable, E-NPKI components shall be able to use the valid cached revocation information.

3.4.9.7 CRL issuance frequency

Requirement ID: SRS-448

•Certification Authorities shall be capable of publishing Certificate Revocation Lists (CRLs) at intervals which are configurable to any time period.

Requirement ID: SRS-449

•Certification Authorities shall be capable of publishing CRLS immediately when a certificate is revoked.

Requirement ID: SRS-450

•NPKI CAs shall overwrite superseded CRLs in the repository upon writing of the latest CRL.

Requirement ID: SRS-440

•The E-NPKI Administrator Trusted Role shall be able to configure the frequency of CRL publishing.

Requirement ID: SRS-2081

•E-NPKI CAs shall be capable of populating the thisUpdate (Effective Date) field of the CRL and ARL.

Requirement ID: SRS-2082

•E-NPKI CAs shall be capable of populating the nextUpdate field of the CRL and ARL.

Requirement ID: SRS-2083

•E-NPKI CAs shall be capable of populating the Issuing Distribution Point extension inclusive of the "DistributionPointName", "Only Contains User Certs", "Only contains CA Certs", and "Indirect CRL" attributes.

Requirement ID: SRS-2084

•E-NPKI CAs shall be capable of signing CRLs and ARLs with a SHA-384 hash and ECDSA-384 signature.

Requirement ID: SRS-2085

•E-NPKI CAs shall support the issuance of Complete CRLs.

Requirement ID: SRS-2088

•E-NPKI CAs shall support the issuance of Partitioned CRLs.

Requirement ID: SRS-2086

•The E-NPKI CAs shall not remove expired certificates from CRLs.

3.4.9.8 Maximum latency for CRLs

Requirement ID: SRS-582

•NPKI CAs shall support the configuration and adjustment of CRL publishing to account for non-availability of directory services, or to address propagation delays where directory services are deployed into alliance operations and missions (AOM).

Requirement ID: SRS-2202

•NPKI CAs shall support the configuration and adjustment of the "nextUpdate" value within CRLs

3.4.9.9 On-line revocation/status checking availability

Requirement ID: SRS-583

•OCSP responders shall conform to the same technical and security standards as the NPKI CA(s) which it supports. This requirement is not intended to prevent the OCSP responder from providing certificate status services to E-NPKI subscribers from other PKI CAs which have interoperability agreements in place with the E-NPKI.

Requirement ID: SRS-2203

•OCSP responders shall meet the same system security and availability requirements as the certificate repository. Specifically, the OCSP responder shall have the same redundancy requirements as the certificate repository. The hardware cryptographic module for the OCSP responder shall meet the standards as defined for the CA hardware cryptographic module.

The overall requirements for revocation status availability combining CRLs and OCSP are defined in section 3.4.10.2

Requirement ID: SRS-2206

•Independently of the directories, each OCSP server shall provide an availability of 99.5%

3.4.9.10 On-line revocation checking requirements

Subscribers are permitted to choose between the use of any available revocation checking mechanism including WEB, file share, OCSP and CRLs. The requirements for validating certificate paths are the same regardless of which mechanism is chosen.

3.4.9.11 Other forms of revocation advertisements available

Requirement ID: SRS-2209

•E-NPKI CAs shall be configurable to publish CRLS to file shares and WEB servers.

Requirement ID: SRS-2210

•E-NPKI CAs shall published any configured CRL location within the CDP or AIA fields of the certificate as appropriate.

3.4.9.12 Special requirements re key compromise

Placeholder (no requirement.)

3.4.9.13 Circumstances for suspension

Requirement ID: SRS-2012

•E-NPKI Certificate suspension functionality, if implemented, shall be disabled.

3.4.10 Certificate status services

3.4.10.1 Operational characteristics

Requirement ID: SRS-456

•The implementation of certificate status services via OCSP within E-NPKI clients, shall be capable of verifying the validity of certificates in an automated and transparent fashion to the subscriber.

Requirement ID: SRS-457

•The certificate status services shall be based on the use of well-defined certificate extensions within certificates to automate the downloading of revocation information without the need for subscriber input.

Requirement ID: SRS-2024

•OCSP Servers shall be capable of supporting Dynamic responses to OCSP requests as defined in RFC6960.

Requirement ID: SRS-2025

•OCSP Servers shall be capable of supporting Static responses to OCSP requests.

Requirement ID: SRS-2027

•OCSP Servers shall be capable of retrieving the correct CRL for a certificate based on the CRL Distribution Point (CRL DP) populated within the certificate.

Requirement ID: SRS-2066

•OCSP servers shall support the receipt of OCSP requests signed with SHA-256 / ECDSA-256.

Requirement ID: SRS-2067

•OCSP servers shall support the receipt of OCSP requests signed with SHA-384 / ECDSA-384.

Requirement ID: SRS-2062

•OCSP servers shall support the generation of OCSP responses signed with SHA-256 / ECDSA-256.

Requirement ID: SRS-2063

•OCSP servers shall support the generation of OCSP responses signed with SHA-384 / ECDSA-384.

Requirement ID: SRS-2028

•In the event of the failure of the primary directory, OCSP Servers shall be able to dynamically switch to one of the available backup directories for retrieving Certificate revocation lists.

Requirement ID: SRS-2070

•E-NPKI client software shall be capable of finding OCSP services based on the population of the Authority Information Access (AIA) attribute within E-NPKI Certificates.

Requirement ID: SRS-2020

•E-NPKI client software shall support the generation and use of digitally signed OCSP requests.

Requirement ID: SRS-2021

•E-NPKI client software shall support the generation and use of random nonces within OCSP requests.

Requirement ID: SRS-2022

•The use of nonces within OCSP requests shall be configurable to support the enabling and disabling of nonces within E-NPKI client software.

Requirement ID: SRS-2029

•E-NPKI client software shall support the generation of OCSP Requests signed with SHA-256 / ECDSA-256.

Requirement ID: SRS-2065

•E-NPKI client software shall support the generation of OCSP Requests signed with SHA-384 / ECDSA-384.

Requirement ID: SRS-2064

•E-NPKI client software shall support the receipt of OCSP Responses signed with SHA-256 / ECDSA-256.

Requirement ID: SRS-2068

•E-NPKI client software shall support the receipt of OCSP Responses signed with SHA-384 / ECDSA-384.

3.4.10.2 Service availability

Requirement ID: SRS-458

•OCSP Servers shall be implemented in such a way as to provide high availability delivery of certificate status information.

Requirement ID: SRS-459

•OCSP Servers shall be implemented in a redundant configuration, including geographic and network diversity.

Requirement ID: SRS-460

•OCSP Services shall be available 24 hours a day and 7 days a week with each OCSP server achieving an availability of 99.5%, independent of the status of other OCSP servers.

3.4.11 End of subscription

NATO is a dynamic employer with a significant degree of rotation within its staff due to the nature of the organisation. The procedures for ending a subscriber's

relationship with the E-NPKI need to be as easy and simple as possible. The majority of the activities to allow a subscriber to cease membership with the PKI without jeopardising the Confidentiality, Integrity, or Availability of NATO information are already covered by existing security processes including the out briefing process, and the cryptographic indoctrination processes.

Where end of subscription is due to revocation of credentials, follow the specific paragraphs regarding revocation first prior to following these procedures.

Requirement ID: SRS-2213

•The E-NPKI system shall be able to identify the relevant out processing workflows based on the input of the Common Name from a subscriber's certificate.

Requirement ID: SRS-2214

•E-NPKI out-processing workflows shall implement the following activities for all subscribers changing roles or leaving the organization:

Requirement ID: SRS-2215

- For a sponsor, the transfer of his sponsor duties to a new individual

Requirement ID: SRS-2216

- Review and implement archiving and data recovery requirements with the subscriber.

Requirement ID: SRS-2217

- Revocation of subscriber certificates.

Requirement ID: SRS-2218

- Reset hardware tokens to factory state and return to inventory.

Requirement ID: SRS-2219

- Record the acknowledgement by the trusted role and the out-processing subscriber of the destruction of personalized tokens not suitable for retention in inventory.

Requirement ID: SRS-2220

- Where the subscriber is in possession of certificates implemented in software, or where the device permits export of private key material, remind the subscriber of the need to continue to maintain the confidentiality of the PIN due to the inherent vulnerabilities of software cryptographic modules.

Requirement ID: SRS-2221

- Recording an acknowledgement by the subscriber of his continued responsibility for the security of the cryptographic credentials previously in his possession.

3.4.12 Key escrow and recovery

3.4.12.1 Key escrow and recovery policy and practices

Requirement ID: SRS-2222

•See section 3.6.2 of this document for further information on key backup, key escrow and key archive provisions. The provision of recovered confidentiality keys to any person other than the certificate owner shall be governed by the data recovery policy of the E-NPKI CA. The data recovery policy shall be an integral part of the E-NPKI CA CPS and shall be approved by the NPMA and the relevant SAA. NATO security policy shall be the driving factor in the determination of the procedures for key recovery.

Requirement ID: SRS-2223

•The E-NPKI system security mechanisms shall control the recovery of any key material held within the E-NPKI system under multi-person control.

3.5 Facility, Management, and Operational Controls

3.5.1 Physical controls

3.5.1.1 Site location and construction

The E-NPKI CA sites satisfy the requirements for a NATO Class 1 Security Area including;

- a clearly defined and protected perimeter through which all entry and exit is controlled;
- an entry control system which admits only those individuals appropriately cleared and specifically authorised to enter the area;
- specification of the level of classification and the category of the information normally held in the area, i.e. the information to which entry gives access;
- be manually or electronically monitored for unauthorised intrusion at all times;
- ensure personnel not on the access list are properly escorted and supervised;
- ensure a site access log is maintained and inspected periodically; and
- ensure all removable media and papers containing sensitive plaintext information are stored in containers meeting the requirements of (See REF: SOW 2.1.6.3).

Requirement ID: SRS-2644

•The E-NPKI Contractor shall implement physical access control mechanisms to the E-NPKI system (to all racks holding E-NPKI equipment) to prevent access to the E-NPKI system by non-E-NPKI personnel in accordance with NATO policy (See REF: SOW 2.1.6.3).

Requirement ID: SRS-2839

•Physical Access control shall be either mechanical or electronic locks certified in accordance with NATO policy with two person access control implemented. (See REF: SOW 2.1.6.3).

All RA sites will be located in areas that satisfy the controls required for a NATO Class II Security Area including:

- a clearly defined and protected perimeter through which all entry and exit is controlled;
- an entry control system which admits unescorted access only to those individuals who are security cleared and specifically authorised to enter the area.
- For all other individuals, provision shall be made for escorts or equivalent controls; to prevent unauthorised access to NATO classified information and uncontrolled entry to areas subject to technical security inspection.

3.5.1.2 Physical access

Requirement ID: SRS-2645

•In addition to the site security requirements identified above, a separate log of visitors entering and leaving the controlled area of the CA shall be maintained.

•Where a PIN or password is recorded, it shall be stored in a security container accessible only to authorised personnel.

3.5.1.3 Power and air conditioning

A NPKI CA shall ensure that the power and air conditioning facilities are sufficient to support the operation of the NPKI CA system.

3.5.1.4 Water exposures

Requirement ID: SRS-2647

•CA equipment shall be mounted into 19” racks, at least 1.20 meter above the floor.

3.5.1.5 Fire prevention and protection

The area hosting the E-NPKI CA components ensures a high protection against flames and smoke, the secured area is equipped with a fire extinguishing system and a smoke channel.

3.5.1.6 Media storage

E-NPKI media storage is temperature and humidity controlled via an air conditioning system and access is controlled through an access list. NCI Agency CS SL Division Security Officer is responsible for the correctness of the access list.

The Optical ROM media storage is located in the crypto room which is separated from the E-NPKI CA system. Optical media are both retained onsite to facilitate fast recovery, and copied offsite.

3.5.1.7 Waste disposal

Requirement ID: SRS-2650

•All media used for the storage of information such as keys, activation data or E-NPKI CA configuration shall be disposed of in accordance with NATO policy.

•The NPKI NUNR CA hardware platform hard disks shall be disposed of in accordance with NATO policy.

•When no longer required, the HSM shall be zeroised to prevent any possibility of re-using the NPKI NUNR CA private keys, and returned to cryptographic inventory.

•After cessation of operation, the tokens of NPKI NUNR CA Officer and NPKI NUNR CA Auditor, the HSM Administrator and HSM Operator shall be zeroised and returned to the cryptographic inventory.

Requirement ID: SRS-2651

•In the event of media or HSM components under warranty, the failed units shall not require return to the vendor in order to receive warranty replacement.

Requirement ID: SRS-2652

•Failed component shall be destroyed in accordance with NATO policy.

3.5.1.8 Off-site backup

Requirement ID: SRS-2224

•The E-NPKI system shall include all hardware and software necessary to implement secure backup of all E-NPKI information in a format which supports transportation or transmission of that data to an off-site back-up facility, have the same level of Procedural Controls as the E-NPKI CA site.

Requirement ID: SRS-2225

•E-NPKI system information transmitted across or stored on NATO networks or infrastructure shall be encrypted to prevent access by anyone other than the appropriate E-NPKI Trusted Roles.

Requirement ID: SRS-2227

•E-NPKI system information stored on physical media shall be encrypted to prevent access by anyone other than the appropriate E-NPKI Trusted Roles.

Requirement ID: SRS-2226

•These E-NPKI encryption mechanisms shall also be approved by a National CIS Security Authority of a NATO Nation in compliance with (See REF: SOW 2.1.6.8).

3.5.2 Procedural controls

3.5.2.1 Trusted roles

3.5.2.1.1 NPKI CA Trusted Roles

Requirement ID: SRS-586

•NPKI CA shall ensure a separation of duties for critical E-NPKI CA functions to prevent one person from maliciously using the E-NPKI CA system without detection.

Requirement ID: SRS-2793

•Trusted roles shall be in accordance with the CIMC Protection Profile as shown in Figure 4.

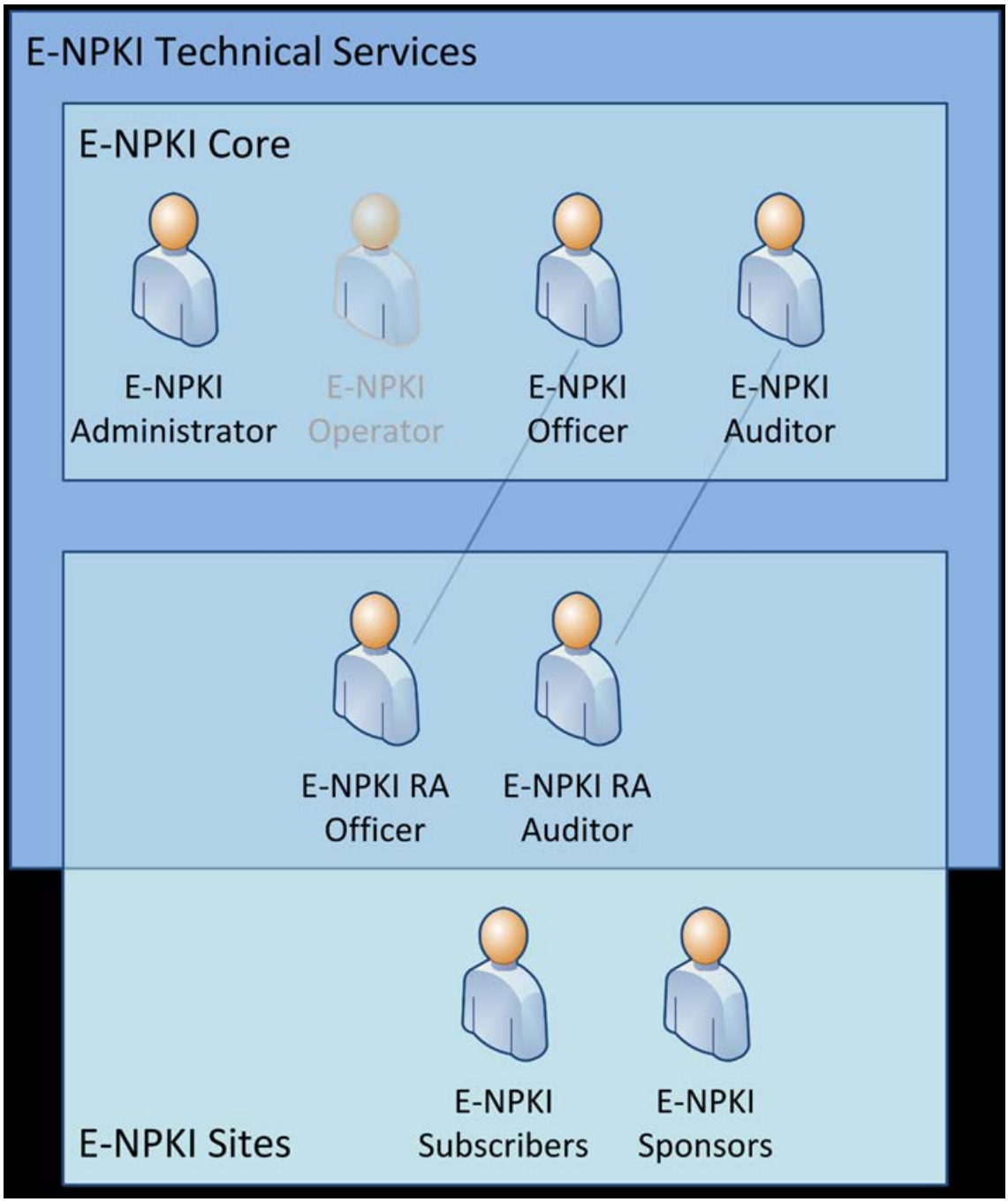

Figure 4 - E-NPKI Technical Services

Requirement ID: SRS-2230

•The E-NPKI Certification Authorities shall implement and enforce as a minimum, three separate roles; the E-NPKI Auditor, E-NPKI Administration, and E-NPKI Officer roles as defined in the CIMC Protection Profile.

Requirement ID: SRS-2235

•If not implemented as a separate role, the functions of the E-NPKI Operator role shall be combined with a compatible role to be agreed by the System Accreditation Authority and NATO PKI Management Authority. (Normally the E-NPKI Administrator.)

Requirement ID: SRS-2228

•Each subscriber's system access shall be limited to those actions for which he or she is required to perform in fulfilling his or her responsibilities.

Requirement ID: SRS-587

•A E-NPKI CA shall assign distinct E-NPKI personnel roles, distinguishing between day-to-day operation of the E-NPKI CA system, the management and audit of those operations and the management of substantial changes to requirements on the system including its policies, procedures or personnel.

Requirement ID: SRS-588

•The division of responsibilities between the roles shall be defined in the E-NPKI CA CPS.

Requirement ID: SRS-589

•The roles implemented by E-NPKI shall provide strong resistance to insider attack.

Requirement ID: SRS-2229

•The E-NPKI shall prevent bypass of its trusted roles by any administrator or administrators outside of the E-NPKI trusted roles including Domain or Enterprise Administrators.

Requirement ID: SRS-590

•The E-NPKI system shall limit access to the software that controls the E-NPKI CA operations to only those personnel responsible for the duties outlined in the CPS shall have access to the software that controls the E-NPKI CA operation.

3.5.2.1.2 NPKI RA Trusted Roles

Requirement ID: SRS-592

•A minimum of two trusted roles shall be implemented and enforced within the E-NPKI RAs; Auditor and Officer.

3.5.2.2 Number of persons required per task

Requirement ID: SRS-2310

•The minimum number of persons required for implementing a multi-person control tasks shall be configurable for each task.

Requirement ID: SRS-2236

•The following tasks shall require action by at least two persons, (2 of N person control) before they are completed:

Requirement ID: SRS-2305

- Key Recovery of any escrowed private key.

Requirement ID: SRS-644

- Configuration changes to E-NPKI CAs.

Requirement ID: SRS-2311

- Creation, management, or deletion of trusted roles.

Requirement ID: SRS-598

- E-NPKI CA key generation.

Requirement ID: SRS-2237

- E-NPKI CA rekey.

Requirement ID: SRS-2306

- E-NPKI CA key backup

Requirement ID: SRS-2307

- E-NPKI CA key recovery

Requirement ID: SRS-2308

- Archiving or deleting CA audit logs.

Requirement ID: SRS-2309

- Physical access to the Certification Authority server equipment.

3.5.2.3 Identification and authentication for each role

Requirement ID: SRS-595

•Each of these trusted role certificates and accounts (with the exception of E-NPKI CA signing certificates) shall:

•· be directly attributable to an individual;

•· not be shared;

•· be restricted to actions authorised for that role through the use of E-NPKI CA software, operating system and procedural controls.

3.5.2.4 Roles requiring separation of duties

Requirement ID: SRS-599

•NPKI CAs shall implement and enforce a separation of Roles and duties for E-NPKI Administrator, E-NPKI Operator, and E-NPKI Auditor to ensure that the same person cannot hold multiple roles.

Requirement ID: SRS-2243

•If implemented as a separate role, E-NPKI CAs shall implement separation of Roles and duties for the E-NPKI Officer role.

Requirement ID: SRS-600

•NPKI RAs shall implement separation of Roles and duties for E-NPKI Operator, and E-NPKI Auditor to ensure that the same person cannot hold multiple roles.

3.5.3 Personnel controls

All personnel performing duties with respect to the operation of the E-NPKI shall:

• Be appointed in writing;

• Be bound by contract and job description to the terms and conditions of the position they are to fill as defined by the position description;

• Have received comprehensive training with respect to the duties they are to perform;

• Be bound by NATO Security Policy not to disclose sensitive E-NPKI security-relevant information or Subscriber information;

• Not be assigned duties that may cause a conflict of interest with their E-NPKI duties.

Requirement ID: SRS-2797

•The E-NPKI system shall function fully based on the manning of roles as defined in the SRS section 3.5 and the NATO and contractor staffing levels defined within the SOW.

3.5.3.1 Qualifications, experience, and clearance requirements

Requirement ID: SRS-2659

•Onsite E-NPKI contractor personnel shall hold at least a NATO SECRET Security Clearance. Contractor personnel with administrative access or requiring access to CA or OCSP systems shall hold at least a COSMIC TOP SECRET Security Clearance in accordance with SOW Section 12.1.3 and 12.1.4.

3.5.3.2 Background check procedures

Requirement ID: SRS-2660

•All background checks are performed in accordance with NATO Security Policy.

3.5.3.3 Training requirements

Requirement ID: SRS-2661

•All E-NPKI personnel including contractors shall receive comprehensive training in:

•☐ the NPKI CA/RA security principles and mechanisms;

•☐ all NPKI software versions in use on the NPKI CA system;

- all NPKI duties they are expected to perform; and
- disaster recovery and business continuity procedures.

3.5.3.4 Retraining frequency and requirements

Requirement ID: SRS-2664

- E-NPKI personnel shall be retrained when changes occur in E-NPKI CA or RA systems.

3.5.3.5 Job rotation frequency and sequence

Requirement ID: SRS-2665

- The E-NPKI contractor shall ensure that any change in the staff shall not affect the operational effectiveness of the service or security of the system.

3.5.3.6 Sanctions for unauthorized actions

Requirement ID: SRS-2662

- In the event of actual or suspected unauthorised action by a E-NPKI contractor person performing duties with respect to the operation of an E-NPKI CA or RA, the SAA or NPKI CA shall be authorised to suspend his or her access to the E-NPKI CA system and initiate, if appropriate, disciplinary actions.

- The NPMA in conjunction with the relevant SAA shall perform an analysis to determine if the E-NPKI CA certificate should be revoked based on the unauthorised actions.

3.5.3.7 Independent contractor requirements

Requirement ID: SRS-2663

- Contractor access to the E-NPKI CA site shall be in accordance with the site physical access rules in place.

3.5.3.8 Documentation supplied to personnel

Requirement ID: SRS-2666

- The E-NPKI shall make available to its CA and RA personnel the Certificate Policies it supports, its CPS, and any specific statutes, policies or contracts relevant to their position. Additionally, information describing the operation of relevant hardware and software in use shall also be made available to the appropriate CA and RA personnel.

3.5.4 Audit logging procedures

E-NPKI is to provide and record traceability of changes (data, objects, products, key data elements) for use by authorised subscribers to:

- Gather further information about the data element in question

- Resolve conflicts

•Classify data elements according to their sources

•Discover and remove errors.

Requirement ID: SRS-1549

•E-NPKI shall use the details of the Logged-in subscriber including the relevant protocol or application information to maintain the audit traceability.

Requirement ID: SRS-1551

•All errors and faults in E-NPKI shall be recorded in an error log which shall be both centrally and locally maintained.

Requirement ID: SRS-1552

•E-NPKI error logs shall contain all required information in order to provide the support staff with interpretable and comprehensive information about the cause and nature of the error/change.

Requirement ID: SRS-1553

•E-NPKI shall allow an authorised subscriber to display the audit traceability for those objects authorised for that subscriber.

Requirement ID: SRS-1554

•E-NPKI shall allow an authorised subscriber to view client activity and error logs.

3.5.4.1 Types of events recorded

3.5.4.1.1 User Auditing

Requirement ID: SRS-1558

•E-NPKI shall record in traceable logs all selected transactions, database activities, technical events (e.g., dataset synchronisation, directory replication) and accessing of data.

Requirement ID: SRS-1559

•E-NPKI shall ensure that any information object can always be traced to its original source (i.e., Organisational Node, subscriber and/or system).

Requirement ID: SRS-1560

•E-NPKI shall provide audit capability for all types of objects.

Requirement ID: SRS-1561

•E-NPKI shall maintain a record of the date, time and subscriber that created an object.

Requirement ID: SRS-1562

•E-NPKI shall maintain a record of the date, time, details of the change and subscriber that last modified an object.

Requirement ID: SRS-1564

•If so configured, E-NPKI shall ensure operations at the business object level are recorded in traceable logs.

Requirement ID: SRS-1565

•If so configured, E-NPKI shall ensure subscriber operations at system function level are recorded in traceable logs.

Requirement ID: SRS-1566

•If so configured, E-NPKI shall support audit trailing to all subscriber and E-NPKI system actions and messages on sending, deleting and viewing to log all subscriber activities.

Requirement ID: SRS-1567

•If so configured, E-NPKI shall log all configurations changes with the trace to persons or systems.

Requirement ID: SRS-1568

•If so configured, E-NPKI shall log the use of all E-NPKI system functions and their corresponding messages including data exchanges with the trace to persons or systems.

Requirement ID: SRS-1569

•If so configured, in case of a subscriber action, E-NPKI shall log at a minimum:

•subscriber

•Timestamp

•Function name(s)

Requirement ID: SRS-1570

•If so configured, in case of changes, E-NPKI shall log at a minimum:

•subscriber

•Timestamp

•Fieldname

•New value

•Old value

Requirement ID: SRS-1571

•E-NPKI shall archive the audit log after a period of time as configured by an authorised subscriber. By default the log shall be archived after one day.

Requirement ID: SRS-1572

•If log activity reaches the limit of the log file size before one day has completed, E-NPKI shall create another log file and continue logging.

Requirement ID: SRS-1556

•E-NPKI shall allow an authorised subscriber to select the events to be logged.

3.5.4.1.2 System Monitoring

Requirement ID: SRS-1574

•E-NPKI shall generate and maintain an Audit Log for each of the following auditable events, shall associate individual subscriber identities to those events, and shall include date and time of the event, type of event, subscriber identity, and the outcome (success or failure) of the event:

•System start-up and shutdown,

•Log-on and log-off of individual subscribers,

•Changes to permissions and privileges of users and groups,

•Changes to security relevant system management function,

•Any access to audit log,

•Deletion, creation or alteration of the security audit records,

•All privileged operations,

•All updates of E-NPKI access rights,

•All attempts to delete, write or append the Audit files.

Requirement ID: SRS-1575

•E-NPKI shall raise an alarm to the appropriate trusted role and the Enterprise Management System when the Audit Log reaches 90% of its maximum permitted size.

Requirement ID: SRS-1576

•E-NPKI shall use integrity checking countermeasures to ensure that the Audit Log has been archived successfully.

Requirement ID: SRS-1577

•E-NPKI shall support the following warning system events:

•Almost out of disk space: E-NPKI server specific

•Almost out of table space: E-NPKI server specific

Requirement ID: SRS-1578

•E-NPKI shall support the following error system events:

•Crashing of software components

•Unplanned and recovering of a connection with a terminator

•Incorrect received data

•Replication failure

Requirement ID: SRS-1579

•E-NPKI shall allow an E-NPKI Auditor to display system events using standard system management tools like the Windows Management Console.

Requirement ID: SRS-1580

•E-NPKI shall allow an authorised subscriber to filter system events by date/time range, event Identifier, event type, category, description text, OS User/OS User Group, or source.

Requirement ID: SRS-1581

•E-NPKI shall allow an authorised subscriber to perform system event log clearing and backup.

Requirement ID: SRS-1582

•E-NPKI shall allow an authorised subscriber to sort the system event log on date/time, event Identifier, event type, category, description text, OS User/OS User Group, or source.

Requirement ID: SRS-1583

•E-NPKI shall be able to generate debug messages with multiple levels of verboseness.

Requirement ID: SRS-1584

•E-NPKI shall allow an authorised subscriber to dynamically set (i.e., a node configuration setting) the level of verboseness for debug messages.

Requirement ID: SRS-1585

•When a system event of type error arises, E-NPKI shall generate a message including the type of error and display them directly to the subscriber

Requirement ID: SRS-1586

•E-NPKI shall log a memory dump of the whole system when E-NPKI crashes.

Requirement ID: SRS-1588

•E-NPKI shall allow an authorised subscriber to review the performance log.

Requirement ID: SRS-601

•E-NPKI CAs and RAs shall record in audit log files all events relating to the security of the E-NPKI CA system. These include as a minimum such events as:

•system start-up and shutdown;

•CA application start-up and shutdown;

•attempts to create, remove, set passwords or change the system privileges of the E-NPKI privileged roles;

•changes to E-NPKI CA configuration and/or keys;

•changes to certificate creation policies e.g., validity period;

•login and logoff attempts;

•unauthorised attempts at network access to the E-NPKI CA system;

•unauthorised attempts to access system files;

•generation of own and subordinate subscriber keys;

•creation and revocation of certificates;

•attempts to initialise remove, enable, and disable subscribers, and update and recover their keys;

•Failed read-and-write operations on the certificate and CRL to the relevant directory.

•Access or modification to the audit file

•Archive of E-NPKI CA data

•Audit log errors

•Database management

•DN changes made by the E-NPKI CA or RA

Requirement ID: SRS-602

•The E-NPKI system shall also collect and consolidate electronically at the primary CA in Mons, security information not E-NPKI CA-system generated such as:

•· physical access logs to the CA / OCSP / Timestamp systems;

•· system configuration changes and maintenance to the E-NPKI system hardware, operating system, and all installed software on the E-NPKI;

•· personnel changes for E-NPKI personnel including RA Operators; (This item can be met through the Trusted role subscriber agreements in electronic format.);

- discrepancy and compromise reports for all E-NPKI components including tokens;
- Records of the destruction of media containing key material, activation data, or personal subscriber information.
- Security relevant logs from the Directory
- DN changes made by entities other than the E-NPKI CA or RA Officers
- Firewall and IDS Logs

3.5.4.2 Frequency of processing log

Requirement ID: SRS-2667

•E-NPKI CAs and RAs shall ensure that their audit logs are reviewed by the local E-NPKI Auditor at least once every week and all significant events are explained in an audit log summary.

Requirement ID: SRS-2668

•Such reviews shall verify as a minimum that the log has not been tampered with, and then briefly inspect all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

Requirement ID: SRS-2669

•Supporting manual and electronic logs from the NPKI CA and RA shall be compared where any action is deemed suspicious.

Requirement ID: SRS-2670

•Actions taken following these reviews shall be documented.

Requirement ID: SRS-2671

•The E-NPKI CA and RA system shall provide tools to verify the integrity of the log file.

Requirement ID: SRS-2672

•The E-NPKI CA and RA shall provide tools to assist in searching through the log files to identify alerts and irregularities.

3.5.4.3 Retention period for audit log

Requirement ID: SRS-638

•The E-NPKI CA and RA components shall be capable of digitizing and signing all paper based logs.

Requirement ID: SRS-2245

•The E-NPKI trusted role for the review of audit log data shall be defined in the E-NPKI CA or RA CPS.

Requirement ID: SRS-632

•E-NPKI CAs and RAs shall have sufficient disk storage space to retain its audit logs online for at least two months.

Requirement ID: SRS-633

•NPKI CAs and RAs shall be able to archive audit logs on a configurable time interval in accordance with section 3.5.5.

3.5.4.4 Protection of audit log

Audit log information is considered to be sensitive information as defined in section 3.9.4.

Requirement ID: SRS-637

•Audit log information shall be appropriately classified and protected in accordance with NATO Security Policy.

Requirement ID: SRS-634

•The electronic audit log system shall include mechanisms to protect the log files from unauthorised access, modification, and deletion.

3.5.4.5 Audit log backup procedures

Requirement ID: SRS-649

•The E-NPKI system shall automatically back up audit logs and audit summaries at configurable intervals.

3.5.5 Records archival

Long-term preservation is part of the lifecycle for all information of permanent value. It has to be considered during the planning and incorporated during the design, procurement, and implementation of any NATO system. It concerns the information held within NATO systems; the functionality of the systems does not have to be preserved.

The term 'Information of permanent value' includes both:

Structured data: characterized by a presence of a scheme, e.g. as an XML schema definition, an ADatP-3 message structure, or included implicitly e.g. through a database table structure.

Unstructured data: it does not contain any schema. E.g. free text descriptions.

Requirement ID: SRS-1657

•E-NPKI shall be in accordance with the Directive on the Preservation of NATO Digital Information of Permanent Value (AC/324-D(2014)0008).

3.5.5.1 Types of records archived

Requirement ID: SRS-642

•CA and RA archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the E-NPKI.

Requirement ID: SRS-643

•At a minimum, the following data shall be archived.

- CA and RA accreditation documentation;
- CPS documents for E-NPKI CA and RAs;
- any contractual agreements to which the E-NPKI CA or RA is bound;
- system equipment configuration;
- modifications or updates to any of the above data items;
- certificate requests and revocation requests including bulk requests;
- subscriber identity authentication documentation as required by Section 3.2.3;
- subscriber agreements;
- documentation of receipt and acceptance of certificates as described in Section 4.3;
- documentation of receipt of tokens as described in Section 4.3.1;
- all certificates and CRLs (or other revocation information) as issued or published;
- security audit data (in accordance with Section 5.4.1);
- other data or software sufficient to verify archive contents
- all work related communications to or from the NPMA, other E-NPKI CAs or RAs, and compliance auditors.

Requirement ID: SRS-650

•Online Electronic storage capacity for the E-NPKI archived information shall be sufficient to cover 10 years of operational data.

Requirement ID: SRS-651

•The E-NPKI archiving and verification system shall be fully self-contained.

3.5.5.1.1 Text

Requirement ID: SRS-1671

•Documents consisting primarily of textual descriptions are the most prevalent and important category of information of permanent value in the NATO context. Text documents might also include embedded diagrams, pictures, or other non-text material. These items shall not be separated from the text and kept as part of the document.

3.5.5.1.1.1 Text documents

Requirement ID: SRS-1673

•E-NPKI shall preserve the integrity of text, diagram and figures, pagination and navigation (formatting)

Requirement ID: SRS-1674

•E-NPKI shall preserve document metadata.

Requirement ID: SRS-1675

•E-NPKI shall include fonts, layout information and indices.

Requirement ID: SRS-1676

•The format for text documents, including common MS Office document formats (docx, xlsx, pptx) shall be the following:

•ISO 32000-1 :2008, Document management – Portable document format – Part 1 : PDF 1.7, conformance level : PDF/A-2a

3.5.5.1.2 Still Images

Still images are visual representations, including photographs, graphs, and diagrams. Still images can be divided into two main types, bitmap (or raster) images and vector images.

Bitmap images are typically photographs produced by scanners and cameras at a fixed resolution.

Vector images consist of scalable objects.

Both types can be combined, e.g. in course of action diagrams where a bitmap image of an area can have symbology vector overlays.

Requirement ID: SRS-1688

•E-NPKI shall preserve the resolution (clarity, colours), scalability and ability to render the image.

Requirement ID: SRS-1689

•E-NPKI shall preserve image metadata.

Requirement ID: SRS-1690

•E-NPKI shall preserve the level of compression of the image. There shall be a preference for lossless compression.

Requirement ID: SRS-1691

•E-NPKI shall prefer larger resolution images for their preservation

3.5.5.1.2.1 Bitmap/raster images

Requirement ID: SRS-1693

•The format for bitmap images shall be any of the following:

•ISO/IEC 15444-1 :2004, Information technology – JPEG 2000 image coding system, Part 1 (J2K_C_LL, Core Coding, Lossless Compression)

•ISO/IEC 10918-1 :1994, Information Technology – Digital compression and coding of continuous-tone still images

•Adobe TIFF UNC (uncompressed bitmap), part of TIFF 6.0 (1992)

•Adobe TIFF G4 (compressed bitmap, part of TIFF 6.0 (1992)

3.5.5.1.2.2Vector images

Requirement ID: SRS-1695

•The format for vector images shall be the following:

•W3C Scalable Vector Graphics (SVG) 1.1, 2011

Requirement ID: SRS-1669

•The format for data sets and any structured information not fitting other content types shall be any of the following:

•IETF RFC 4180:2005, Common Format and MIME Type for Comma-Separated Values (CSV) Files.

•Extensible Markup Language (XML), v1.1 2nd Edition, W3C Recommendation, 29 September 2006.

•XML Schema Definition Language (XSD) 1.1 Part 1: Structures and Part 2: Datatypes, W3C Recommendation, 5 April 2012.

3.5.5.2 Retention period for archive

Requirement ID: SRS-652

•NPKI collected information defined within section 3.5.5.1 shall be kept, without any loss of data, for a period of 30 years.

Requirement ID: SRS-2261

•The ability to process these archives shall be maintained for at least the applicable retention period above.

3.5.5.3 Protection of archive

Requirement ID: SRS-653

•Archive media shall be stored in a separate, safe, secure storage facility.

Requirement ID: SRS-654

•Prior to archive, records shall be labelled with the E-NPKI CA's distinguished name, the date, and the classification.

3.5.5.4 Archive backup procedures

Requirement ID: SRS-2263

•The E-NPKI system shall automatically back up the data archive at configurable intervals using the principle of Disk-to-Disk backup.

3.5.5.5 Requirements for time-stamping of records

Requirement ID: SRS-2264

•All records to be archived from the E-NPKI shall be timestamped in conformance with section 3.6.8

Private encryption keys escrowed within the E-NPKI system are not included within this requirement.

3.5.5.6 Archive collection system (internal or external)

Requirement ID: SRS-2673

The E-NPKI Archive system shall support data synchronization across 3 datacentres.

Requirement ID: SRS-2841

•The management of the archive component at each datacentre shall be done through the same management interface.

Requirement ID: SRS-2842

•The archive component shall be redundantly connected to the LAN and redundantly connected to any additional network required for storage access.

Requirement ID: SRS-2840

•The E-NPKI archive shall be dimensioned to support all the relevant data based on current estimates of numbers and sizes of information objects and provide an additional 30% of space a year for 10 years.

Requirement ID: SRS-2843

•A failure to a single archive node shall not result in an outage or degradation of performance to the archive component.

3.5.5.7 Procedures to obtain and verify archive information

Requirement ID: SRS-655

•Media storing E-NPKI archive information shall be automatically verified upon creation.

Requirement ID: SRS-656

•Periodically, a statistical sample of archived information shall be tested to verify the continued integrity and readability of the information.

Requirement ID: SRS-2266

•The E-NPKI shall provide all software and hardware required to perform the verification of archive information.

3.5.6 Key changeover

Requirement ID: SRS-657

•E-NPKI shall support CA key changeovers, initiated by the CA, provided that the previous certificate(s) have not expired or been revoked.

Requirement ID: SRS-2271

•Tier 2 CAs shall be capable of initiating Certificate rekeying to the superior offline root CA based on a PKCS#10 Certificate request as the only supported mechanism.

Requirement ID: SRS-2272

•Tier 2 CAs shall prevent the initiation of Certificate rekeying in any other manner.

Requirement ID: SRS-658

•The procedures, protocols, and data structures required to ensure that a CA key changeover does not require an immediate re-key of any subordinate CA, subscriber, or device shall be defined within the CA CPS.

Requirement ID: SRS-2273

•E-NPKI CAs shall be able to issue CRLs signed by the old CA private key until the expiry of all end entity certificates signed by the old CA private key

Requirement ID: SRS-2275

•E-NPKI CAs shall be capable of supporting the issuance of Indirect CRLs.

Requirement ID: SRS-659

•Tier 2 CAs shall be capable of verifying certificate chains via link certificates implemented by CAs in Tier 1 or Tier 2. A link certificate in the context of this project is the signing of the old CA certificate with the new CA certificate plus the signing of the new CA certificate by the old CA certificate. This is in addition to the signing of the Tier 2 certificate by the Tier 1 Root CA.

Requirement ID: SRS-2274

•E-NPKI CAs shall be capable of issuing link certificates. (Old CA private key signing new CA Certificate and New CA private key signing old CA Certificate.)

Requirement ID: SRS-2276

•All E-NPKI components shall be capable of performing path validation for certificates which include link certificates.

3.5.7 Compromise and disaster recovery

3.5.7.1 Incident and compromise handling procedures

Requirement ID: SRS-660

•The implementation of CA hardware and software across the three NATO Data centres shall fully meet the business continuity and disaster recovery requirements of this project without reliance on external capabilities not provided by the E-NPKI project.

Requirement ID: SRS-2277

•E-NPKI system and services shall meet the end to end service availability and disaster recovery requirements of this SRS.

Requirement ID: SRS-2278

•E-NPKI system design shall not assume that all services on which it relies provide 100% availability.

Requirement ID: SRS-661

•Where E-NPKI is unable to meet availability requirements based on the available NEDS service, E-NPKI shall provide additional components to ensure that the E-NPKI system meets the documented availability requirements

3.5.7.2 Computing resources, software, and/or data are corrupted

Requirement ID: SRS-663

•The E-NPKI shall include mechanisms to detect the failure of the systems and network environments including CAs, repositories and other critical infrastructure components in a timely fashion such that the business continuity requirements and system availability targets are met.

Requirement ID: SRS-2279

•All E-NPKI components housed within the Datacenters shall integrate with the existing NATO Service Management Centre components.

Requirement ID: SRS-2280

•All E-NPKI components housed within the Datacenters shall support SNMP v3

Requirement ID: SRS-670

•The E-NPKI system shall be designed to restore service prior to further degradation of service which would be caused by the expiry of CRLs.

Requirement ID: SRS-664

•The E-NPKI system shall include mechanisms to centrally notify the SMC that a failure has occurred (and any automated actions which have already taken place to correct the failure.)

Requirement ID: SRS-665

•Each E-NPKI CA shall be capable of automated failover without operator intervention.

3.5.7.3 Entity private key compromise procedures

3.5.7.3.1 Signature key compromise

Requirement ID: SRS-667

•In the event of signature key compromise, E-NPKI CAs shall include tools and procedures to support the investigation of the compromise.

Requirement ID: SRS-668

•The CA shall support the export of Distinguished Names, issued certificates, and certificate state from the database, online audit, and archive in support of compromise investigations.

Requirement ID: SRS-669

•The CA shall be able to identify any gaps in audit logs (e.g. where CA was shut down) to aid in incident management.

Requirement ID: SRS-2282

•The CA shall be able to revoke any certificate based on the certificate serial number or distinguished name.

3.5.7.3.2 Confidentiality key compromise

Requirement ID: SRS-2283

•The E-NPKI system shall include tools and procedures to support the discovery of information encrypted with a compromised confidentiality key.

Requirement ID: SRS-2284

•The E-NPKI system shall include tools and procedures to support the recovery of information encrypted with a compromised confidentiality key.

Requirement ID: SRS-2285

•The E-NPKI system shall include tools and procedures to support the re-encryption of recovered information encrypted with a new confidentiality key.

3.5.7.4 Business continuity capabilities after a disaster

Requirement ID: SRS-671

•In the event that an E-NPKI CA site implements its disaster recovery plan, (e.g. in anticipation of an impending natural disaster), the deployed architecture shall be capable of an orderly handover of CA data and control to the secondary CA site without the loss of data.

Requirement ID: SRS-672

•Orderly handover shall be completed including the shutdown of the CA infrastructure within 15 minutes.

Requirement ID: SRS-673

•In the event that a E-NPKI CA site availability is compromised without advanced warning, the E-NPKI system shall be capable of automated implementation of its disaster recovery plan (i.e. without manual intervention.).

Requirement ID: SRS-674

•In the event of an automated implementation of disaster recovery, data loss shall be limited to non-completed transactions and the last completed transaction if it has not completed its replication to the secondary site.

Requirement ID: SRS-675

•Loss of service of one site shall not cause data corruption at other sites. Partially completed transactions or replications shall be handled without corruption to the database.

Requirement ID: SRS-677

•Method of resolution of partially completed transactions shall be logged by the CA into its audit file.

Requirement ID: SRS-676

•Automated failover to an alternate node shall be completed within 15 minutes (measured from the time the failure occurs to the time the alternate site is providing full service.)

Requirement ID: SRS-678

•Loss of NEDS availability within the scope of the defined NEDS service availability shall not cause data corruption on the E-NPKI system.

3.5.8 CA or RA termination

Requirement ID: SRS-2287

•The E-NPKI CA shall include tools to support the retention and archive of the E-NPKI CA's keys database and information in line with the archive requirements in section 3.5.5 of this document.

Requirement ID: SRS-2288

•Where the CA Termination is due to a hardware or software version update, the E-NPKI CA shall include tools to bulk transfer subscribers and devices to the new CA.

Requirement ID: SRS-2289

•Software upgrades to the E-NPKI system shall not require the termination of a CA or a transfer or rekeying of subscribers.

3.6 Technical Security Controls

Requirement ID: SRS-1453

•E-NPKI shall be compliant with NATO document (See REF: SOW 2.1.6.1) for the protection of NATO classified information, supporting systems services and resources in CIS, or other storing devices, processing and transmitting systems.

Requirement ID: SRS-1454

•E-NPKI shall operate in the "System High" mode of operation. That is, all individuals with access to the system are cleared to the highest classification of the of information stored, processes or transmitted within the system, but not all individuals with access to the system have a common need to know for the information stored, processed or transmitted within the system.

3.6.1 Key pair generation and installation

3.6.1.1 Key pair generation

Requirement ID: SRS-679

•NPKI CA confidentiality and digital signature key pairs shall be generated in the CA hardware cryptographic module conforming to 3.6.2.1.

Requirement ID: SRS-680

•E-NPKI OCSP confidentiality and digital signature key pairs shall be generated in the OCSP hardware cryptographic module conforming to 3.6.2.1.

Requirement ID: SRS-681

•If implemented, E-NPKI OCSP confidentiality key pairs shall be generated in the OCSP hardware cryptographic module conforming to 3.6.2.1.

Requirement ID: SRS-682

•E-NPKI Timestamping confidentiality and digital signature key pairs shall be generated in the Timestamping hardware cryptographic module conforming to 3.6.2.1.

Requirement ID: SRS-683

•If implemented, E-NPKI Timestamping confidentiality key pairs shall be generated in the Timestamping hardware cryptographic module conforming to 3.6.2.1.

Requirement ID: SRS-684

•E-NPKI RA confidentiality and digital signature key pairs shall be generated in the RA hardware cryptographic module conforming to 3.6.2.1.

Requirement ID: SRS-685

•If implemented, E-NPKI RA confidentiality key pairs shall be generated in the RA hardware cryptographic token conforming to 3.6.2.1

Requirement ID: SRS-686

•For E-NPKI End Entities implemented with hardware tokens, digital signature key pairs shall be generated in the E-NPKI End Entities hardware cryptographic token conforming to 3.6.2.1.

Requirement ID: SRS-687

•For E-NPKI End Entities implemented with hardware tokens, confidentiality key pairs shall be generated in the E-NPKI End Entities hardware cryptographic token conforming to 3.6.2.1, or in the CA hardware cryptographic module.

Requirement ID: SRS-688

•For E-NPKI End Entities implemented in software, digital signature key pairs shall be generated in the End Entities cryptographic software conforming to 3.6.2.1.

Requirement ID: SRS-689

•For E-NPKI End Entities implemented in software, confidentiality key pairs shall be generated in the End Entities cryptographic software conforming to 3.6.2.1 or by the CA or RA using techniques of equivalent strength as the end entity software cryptographic module.

Requirement ID: SRS-690

•Non-repudiation key pairs shall only be generated in end entity hardware cryptographic modules conforming to 3.6.2.1.

3.6.1.2 Private key delivery to subscriber

Requirement ID: SRS-691

•If the private confidentiality key is not generated by the prospective certificate holder it shall be either delivered to the subscriber in an on-line transaction in accordance with RFC4210 Certificate Management Protocol, or via an equally secure manner approved by the NPMA.

Requirement ID: SRS-692

•The E-NPKI RA system shall maintain accountability for the location and state of all cryptographic tokens that it has issued.

Requirement ID: SRS-693

•The E-NPKI RA shall maintain a complete list of tokens, the identity of the person to whom they were issued, and their status (e.g. if they have been reported lost.)

Requirement ID: SRS-697

•For audit purposes, RAs shall have a mechanism to verify that E-NPKI hardware tokens remain within the intended person's possession, and validate its state over the lifecycle of the token.

Requirement ID: SRS-694

•Under no circumstances shall anyone other than the subscriber have access to private signing keys.

Requirement ID: SRS-695

•The E-NPKI shall not permit the issuance of Signing certificates that corresponds to a private key that is shared by multiple subscribers.

Requirement ID: SRS-696

•For cases where there are several persons acting in one capacity, (e.g. a release authority for NATO Messaging Service) the E-NPKI shall support the insertion of an attribute or extension within the subscriber's certificate to denote this authority instead of shared signing keys.

3.6.1.3 Public key delivery to certificate issuer

Requirement ID: SRS-704

•Public keys shall be delivered to the E-NPKI in a way that binds the applicant's verified identification to the public key being certified.

Requirement ID: SRS-705

•This binding shall be accomplished using means that are as secure as the security offered by the keys being certified.

Requirement ID: SRS-706

•The binding shall be accomplished using a combination of cryptographic, physical, procedural, and other appropriate methods.

Requirement ID: SRS-707

•The public key shall be delivered to the E-NPKI CA either via an online transaction in accordance with the RFC4210 Certificate Management Protocol, or via an equally secure manner approved by the NPMA.

Requirement ID: SRS-708

•Trusted role certificates shall implement a cryptographic binding with the E-NPKI CA in accordance with the RFC4210 Certificate Management Protocol or via an equally secure cryptographic protocol approved by the NPMA.

Requirement ID: SRS-709

•E-NPKI Tier 2 CAs shall implement the PKCS#10 data structure for delivery of the CA Public key to the E-NPKI Root CA via NPMA approved CIS Security channels.

Requirement ID: SRS-710

•In those cases where public/private key pairs are generated by the E-NPKI CA on behalf of the subscriber, the E-NPKI CA shall implement secure mechanisms

to ensure that the software cryptographic module or hardware token in which the public/private key pair is held is securely sent to the proper subscriber.

Requirement ID: SRS-2674

•The E-NPKI CA shall implement secure mechanisms to ensure that the token is not activated prior to receipt by the proper subscriber.

3.6.1.4 CA public key delivery to relying parties

Requirement ID: SRS-700

•E-NPKI enabled applications shall protect the integrity of the E-NPKI Root CA certificate at all times.

Requirement ID: SRS-698

•The E-NPKI and the relying parties shall work together to ensure the authenticated and integral delivery of the E-NPKI Root CA certificate. Acceptable mechanisms for Root CA certificate delivery include but are not limited to:

•· CAs or RAs loading the E-NPKI Root CA certificate and subordinate CA certificate onto tokens delivered to relying parties via secure mechanisms;

•· secure distribution of the E-NPKI Root CA certificate and subordinate CA Certificate through secure out-of-band mechanisms;

•· comparison of certificate hashes or fingerprints against the E-NPKI Root CA certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and

•· loading certificates from web sites secured with a currently valid NATO certificate of equal assurance level than the certificate being downloaded.

•· pushing the E-NPKI Root CA Certificate via Group Policy Object

Requirement ID: SRS-699

•NATO Enterprise systems shall store the E-NPKI Root CA certificate such that unauthorised alteration or replacement is readily detectable and preventable (i.e. does not succeed in replacing the existing Root CA certificate).

Requirement ID: SRS-701

•Hardware tokens and cryptographic modules shall store the Root CA certificate within the hardware token.

Requirement ID: SRS-702

•Software cryptographic modules shall store the Root CA certificate in either the software cryptographic module, or in another protected certificate store.

Requirement ID: SRS-703

•All cryptographic modules shall verify that the public key and certificate delivered matches the private key stored within the cryptographic module.

3.6.1.5 Key sizes

Requirement ID: SRS-711

•All E-NPKI components shall support the generation and verification of ECDH 384 bit keys and certificates as the required asymmetric key length appropriate for the protection of AES 256 bit symmetric keys by end entities.

Requirement ID: SRS-712

•All E-NPKI components shall also support the generation of ECDH 256 bit keys.

Requirement ID: SRS-713

•All E-NPKI components shall support the generation and verification of ECDSA 384 bit keys and certificates.

Requirement ID: SRS-714

•All E-NPKI components shall also support the generation of ECDSA 256 bit keys to support legacy end entity applications.

Requirement ID: SRS-715

•All E-NPKI components shall support the generation and verification of SHA 384 bit hashes.

Requirement ID: SRS-2291

•All E-NPKI components shall support the generation and verification of SHA 256 bit hashes.

Requirement ID: SRS-716

•All E-NPKI components shall be able to support the verification of SHA-1 hashes.

Requirement ID: SRS-717

•If encrypting information, all E-NPKI components shall support the generation and use of AES 256 bit keys.

Requirement ID: SRS-718

•All E-NPKI components shall be configurable to allow the specification of minimum acceptable key lengths independently for each symmetric and asymmetric algorithms used.

Requirement ID: SRS-720

•All E-NPKI components shall be configurable to allow the specification of allowable symmetric and asymmetric algorithms to be used by each E-NPKI Component.

Requirement ID: SRS-2290

•All E-NPKI end entity components shall be capable of validating RSA signatures with key lengths up to 4096 bits in combination with any of the hash algorithms stated above.

Requirement ID: SRS-719

•Additional algorithms and key lengths implemented within COTS products but not specified here shall not be removed from the E-NPKI products, but shall be configurable within the product to determine their availability for use.

3.6.1.6 Public key parameters generation and quality checking

Requirement ID: SRS-461

•All E-NPKI components shall always generate and check Public key parameters in accordance with the standard that defines the crypto algorithm in which the parameters are to be used. For example, public key parameters for use with algorithms defined in the Digital Signature Standard (See REF: SOW 2.2.3) shall be generated and tested in accordance with (See REF: SOW 2.2.3).

Requirement ID: SRS-462

•Whenever a cryptographic algorithm is described in (See REF: SOW 2.2.3), the parameter generation and checking requirements and recommendations of (See REF: SOW2.2.3) shall be required of all entities generating key pairs whose public components are to be certified by the E-NPKI.

Requirement ID: SRS-822

•All cryptographic components provided by the E-NPKI project shall be capable of generating their own key pairs securely within the cryptographic module.

Requirement ID: SRS-824

•E-NPKI CAs shall be able to generate keys (when required by legacy end entities) and sign certificates for end entities based on all asymmetric algorithms in paragraph 3.6.1.5 with configurable certificate lifetimes for all other entities of the E-NPKI system.

3.6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols like the Transport Layer Security (TLS) that provide authenticated connections using encryption certificates.

Requirement ID: SRS-2798

•The E-NPKI shall be configurable to issue dual usage certificates only for specific certificate profiles required to support approved applications such as TLS.

Requirement ID: SRS-722

•The use of a key pair to both sign a block of data and also to encrypt the same information is referred to as a dual usage key pair. E-NPKI End Entities shall not permit dual usage key pairs. E-NPKI policy prohibits the use of a single key pair for both confidentiality services and for signature services in support of data integrity or non-repudiation.

Requirement ID: SRS-2799

•The E-NPKI application integration shall leverage certificate profiles to prevent the issuance of dual usage certificate profiles for any application other than integrated authentication and session key establishment.

3.6.1.7.1 Confidentiality

Requirement ID: SRS-724

•Asymmetric keys are normally used for exchange and establishment of keys used for session and data confidentiality. The certificate keyUsage field shall be used in accordance with RFC3280 and RFC5280.

Requirement ID: SRS-729

•One of the following keyUsage values shall be present in all confidentiality certificates: keyEncipherment, keyAgreement, or dataEncipherment.

3.6.1.7.2 Digital Signature

Asymmetric keys are normally used for authentication, non-repudiation and message integrity.

Requirement ID: SRS-2800

•For Digital Signature certificates and profiles, the certificate keyUsage field shall be used in accordance with RFC3280 and RFC5280.

Requirement ID: SRS-726

•One or both of the following keyUsage values shall be present in all signing certificates except CA Certificates: digitalSignature, or nonRepudiation.

Requirement ID: SRS-727

•The following value shall be present in E-NPKI CA certificate signing certificates: keyCertSign.

Requirement ID: SRS-728

•One or both of the following additional values shall be present in E-NPKI CA certificate signing certificates:CRLSign or Offline cRLSign.

Requirement ID: SRS-725

•E-NPKI CA signing keys are the only keys permitted to be used for signing certificates and CRLs.

Requirement ID: SRS-2292

•E-NPKI CA Signing certificates shall be the only certificate type to include the keyCertSign keyUsage value.

3.6.2 Private Key Protection and Cryptographic Module Engineering Controls

3.6.2.1 Cryptographic module standards and controls

Requirement ID: SRS-774

•Tokens implementing CA certificates, OCSP Certificates, code signing, Timestamping, and CA or RA Trusted Roles shall be handled as COMSEC Controlled Items (CCI) in accordance with (See REF: SOW 2.1.3.4).

When unlocked with their passwords, E-NPKI tokens are to be handled as assets classified at the highest level of classification of the CIS into which they are inserted.

Requirement ID: SRS-776

•When used in conformance with the E-NPKI Certificate Policy and the relevant CPS, E-NPKI end subscriber tokens (other than those identified in SRS 774) shall be suitable for handling as NATO Unclassified (but still high value) assets when removed from their reader and not in use.

Requirement ID: SRS-2321

•For certificates that assert the *nonRepudiation* bit, no one shall have access to the private signing key but the subscriber named in the certificate.

Requirement ID: SRS-2304

•All cryptographic modules shall be operated such that the private asymmetric cryptographic keys shall never be output in plaintext. No private key shall appear unencrypted outside a cryptographic module.

3.6.2.2 Private key (n out of m) multi-person control

Requirement ID: SRS-597

•Where multi-person control is required, it shall be implemented in such a way that it is not possible for one trusted role person to bypass security without collusion of a second trusted role person.

Requirement ID: SRS-646

•Subscribers, Administrators or other privileged roles external to the boundary of the E-NPKI system shall not be able to create, manipulate, or access trusted roles within the E-NPKI system.

Requirement ID: SRS-733

•At least two staff (2 of M persons) performing duties associated with the identical E-NPKI trusted roles, shall be enforced by the E-NPKI system to participate in any function requiring multi-person control.

Requirement ID: SRS-2593

•Workflows shall not be used in circumstances that would violate two person control requirements, such as CA key generation or trusted Root Certificate import into the subordinate CA.

Requirement ID: SRS-2239

•Where permitted by security, multi-person control shall be implemented via workflows instead of requiring the trusted roles to be simultaneously at the terminal.

Requirement ID: SRS-2312

•Where workflows are not permitted by security, the E-NPKI system shall require the configured number of trusted role persons to be authenticated during the transaction.

Requirement ID: SRS-2238

•The E-NPKI shall implement workflows for all end entity activities requiring multi-person person control to allow for partially completed activities to be queued for further approval by another authorized subscriber.

3.6.2.3 Private key escrow

Requirement ID: SRS-731

•Private confidentiality keys shall be escrowed by the E-NPKI CA in support of data recovery of information encrypted by E-NPKI enabled applications.

3.6.2.4 Private key backup

Requirement ID: SRS-737

•Hardware cryptographic modules containing E-NPKI CA private signature keys shall be capable of backup in encrypted format by an E-NPKI CA subject to the security audit requirements of Section 4.5.1 and for storage only within a COMSEC vault.

Requirement ID: SRS-739

•The security of the backup shall be to the same level as the original key.

Requirement ID: SRS-740

•Subscriber digital signature private keys shall not be backed up or escrowed.

Requirement ID: SRS-741

•Subscriber confidentiality key management private keys shall be backed-up by the E-NPKI CA through mechanisms defined within the E-NPKI CA CPS.

3.6.2.5 Private key archival

Requirement ID: SRS-743

•Escrowed key material shall be retained for a period of 30 years after the expiry of the key material.

3.6.2.6 Private key transfer into or from a cryptographic module

Requirement ID: SRS-744

•Subscriber digital Signature private keys shall be prevented from export from a subscriber's cryptographic module.

Requirement ID: SRS-745

•Where CA digital Signature private keys need to be transferred to another hardware security module for the purpose of hot standby or disaster recovery, this transfer shall be under multi-person control.

Requirement ID: SRS-2589

•CA digital Signature private keys shall not be exported in clear text form.

Requirement ID: SRS-2590

•Transfer between CAs shall be accomplished via direct communications between HSMs.

3.6.2.7 Private key storage on cryptographic module

Requirement ID: SRS-746

•All E-NPKI cryptographic modules shall be certified and approved by a NATO CIS Security Authority as providing an adequate level of protection for the storage of the private key.

Requirement ID: SRS-773

•Smart Cards, or other removable cryptographic tokens shall only be deployed to operate within a single E-NPKI security level; either Unclassified / Restricted or Secret.

3.6.2.8 Method of activating private key

Requirement ID: SRS-747

•The subscriber shall be authenticated to the cryptographic module before the activation of the private key.

Requirement ID: SRS-2591

•The minimum authentication mechanism shall be in the form of a password.

Requirement ID: SRS-2592

•Stronger authentication mechanisms might be required by the SAA (e.g. biometrics) commensurate with the operating environment.

The insertion and activation of a token within an inappropriate CIS Security Domain is to be treated as a cryptographic violation as defined in (See REF: SOW 2.1.3.4).

Requirement ID: SRS-2801

•The E-NPKI shall, through the selection of appropriate middleware and orthogonal smart cards for different domains, prevent the activation of a token within an inappropriate CIS Security Domain.

Requirement ID: SRS-771

•Smart Card specific middleware shall not be installed on CIS operating at different security levels, unless the purpose of installing the middleware is to explicitly prevent the use of the inappropriate smart card within that domain.

Requirement ID: SRS-2313

•The E-NPKI shall provide workflows to support the investigation and resolution of security violations detected within the E-NPKI system.

Requirement ID: SRS-2314

•The E-NPKI shall provide workflows to support the investigation and resolution of manually entered security violations detected externally to the E-NPKI system.

Requirement ID: SRS-772

•In the event of a CIS Security violation, the certificates involved shall be immediately revoked.

3.6.2.9 Method of deactivating private key

Requirement ID: SRS-777

•When the software or hardware cryptographic module is deactivated, all cryptographic keys (symmetric or asymmetric) shall be cleared from general purpose memory before the memory is de-allocated.

Requirement ID: SRS-778

•Any disk space where keys were stored (symmetric or asymmetric) shall be over-written before the space is released to the operating system.

Requirement ID: SRS-779

•The cryptographic module shall automatically deactivate its private keys after a system configurable period of inactivity.

Requirement ID: SRS-2294

•Deactivation timeouts shall be configurable per site to allow configuration as required by the local SAA.

Deactivation timeouts are not applicable to IT infrastructure components which are by their nature always on. (e.g. web servers or PKI infrastructure components.)

Requirement ID: SRS-790

•When deactivated, hardware tokens shall protect private keys from unauthorised access (even in encrypted format.)

3.6.2.10 Method of destroying private key

Requirement ID: SRS-796

•All E-NPKI Cryptographic components shall be capable of destroying their own private keys when they are no longer needed.

Requirement ID: SRS-797

•This requirement shall not negate any applicable escrow requirements.

Requirement ID: SRS-798

•Tokens and Hardware Security Modules shall be designed and approved in a way that does not require the physical destruction of hardware to zeroize non-personalised cryptographic modules for re-use within the same security domain.

3.6.2.11 Cryptographic Module Rating

Requirement ID: SRS-732

•All E-NPKI products and components implementing cryptography or requiring E-NPKI Trusted Role Certificates shall be approved by a NATO Nation CIS Security Authority. This includes but is not limited to Card Management Systems, Certificate Authorities, Registration Authorities, Online Certificate Status Protocol servers, Timestamp Servers, Hardware Security Modules, Smartcards, Trusted Platform Modules (TPM), and PKI client software.

3.6.3 Other aspects of key pair management

3.6.3.1 Public key archival

Requirement ID: SRS-799

•The Issuing E-NPKI CA shall archive digital signature certificates based on the requirements of 3.5.5.

Requirement ID: SRS-800

•The Issuing E-NPKI CA shall maintain end entity confidentiality key management certificates within the E-NPKI Escrow along with the relevant private key.

3.6.3.2 Certificate operational periods and key pair usage periods

Requirement ID: SRS-801

•E-NPKI CAs shall be able to sign certificates based on all asymmetric algorithms in paragraph 3.6.1.5 with configurable certificate lifetimes.

Requirement ID: SRS-802

•E-NPKI CAs shall be able to establish independent configurable default certificate lifetimes based on a certificate profiles, token types, or key lengths.

Requirement ID: SRS-2322

•E-NPKI CAs shall be able to enforce independent configurable maximum certificate lifetimes based on a certificate profiles, token types, or key lengths for the certificates that it issues.

3.6.4 Activation data

3.6.4.1 Activation data generation and installation

Requirement ID: SRS-825

•Any activation data shall be unique and unpredictable.

Requirement ID: SRS-826

•The activation data, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected as determined by the security risk assessment.

3.6.4.1.1 Subscriber Cryptographic Module Activation Data

Requirement ID: SRS-827

•Where passwords are used, a subscriber shall have the capability to change its password at any time.

Requirement ID: SRS-828

•Cryptographic module activation codes shall be configurable to match the requirement identified as an output of the security risk assessment to include the following attributes:

Requirement ID: SRS-2295

•Minimum password length

Requirement ID: SRS-2296

•Maximum password age

Requirement ID: SRS-2297

•Password complexity

Requirement ID: SRS-2298

•Maximum number of incorrect authentication attempts

3.6.4.1.2 Activation Data for Initial Keying Of Cryptographic Module

Requirement ID: SRS-830

•One time activation data required for initial keying/certifying of the cryptographic module shall be managed by the E-NPKI CA or RA and distributed securely out of band to the subscriber.

Requirement ID: SRS-829

•One time initialisation data shall be configurable to match the requirement identified as an output of the security risk assessment to include the following attributes:

Requirement ID: SRS-2300

•Minimum length

Requirement ID: SRS-2301

•Maximum age

Requirement ID: SRS-2302

•Complexity

Requirement ID: SRS-2303

•Maximum number of incorrect authentication attempts

3.6.4.2 Activation data protection

Requirement ID: SRS-831

•Data used for subscriber initialisation and activation shall be protected from unauthorised use by a combination of cryptographic procedural, and physical access control mechanisms.

Requirement ID: SRS-832

•The level of protection shall be adequate to deter a motivated attacker with substantial resources to a level approved by NATO within the security risk assessment.

Requirement ID: SRS-833

•If a reusable password scheme is used, the mechanism shall include a facility to lock the account after a configurable number of login attempts.

3.6.4.3 Other aspects of activation data

Requirement ID: SRS-2299

•If activation data is transmitted, it shall be via an appropriately protected channel, which is distinct in time and place from the associated cryptographic module.

Requirement ID: SRS-2323

•Any electronic secure channel for delivery of activation data or shared secret (e.g., password) shall be of strength commensurate with the private key being protected and ensure that only the PKI Sponsor can decrypt it.

3.6.5 Computer security controls

3.6.5.1 Specific computer security technical requirements

The following INFOSEC functionalities are provided by the BI-SC AIS:

Confidentiality. On the Operational Network (ON), military-grade NATO IP cryptographic equipment (NICE) will provide confidentiality to subscriber data.

On the Protected Business Network (PBN), approved IP cryptographic equipment will provide confidentiality to subscriber data. Most of this equipment is PKI enabled.

Information exchange between these security domains will be achieved through appropriate boundary protection services (BPS).

PKI enabled software application layer mechanisms are used for Community-of-Interest (COI) separation.

Integrity. Digital signatures and authentication services are used by various protocols (e.g., SNMP, IPSEC) to provide integrity and strong authentication to subscriber data and network configurations.

Requirement ID: SRS-1458

•The security settings of E-NPKI shall be compliant with the Bi-SC AIS Community Security Requirement Statement (CSRS) for the following areas:

•Bi-SC AIS Security Settings

•File Systems

Requirement ID: SRS-1459

•E-NPKI shall be capable of operation across security domains including national, NATO, coalition and mission.

Requirement ID: SRS-1460

•E-NPKI performance shall not be degraded by the presence of multiple security domains.

Requirement ID: SRS-1461

•E-NPKI shall be compliant with the security infrastructure as provided by the Bi-SC AIS.

Requirement ID: SRS-1462

•E-NPKI shall adhere to NATO INFOSEC Security Policy as described in the SOW Section 11.

Requirement ID: SRS-834

•Each E-NPKI CA server and RA workstation/appliance shall include, as a minimum, the following functionality as applicable:

- access control to E-NPKI CA/RA services and E-NPKI roles;
- enforced separation of duties for E-NPKI roles;
- identification and authentication of E-NPKI roles and associated identities;
- object re-use or separation for E-NPKI CA/RA random access memory and files;
- use of cryptography for session communication and database security;
- archival of E-NPKI CA/RA and subscriber history and audit data;
- audit of security related events;
- self-test of security related E-NPKI CA/RA services;
- trusted path for identification of E-NPKI roles and associated identities;
- recovery mechanisms for keys and the E-NPKI CA/RA system;
- Boundary protection device protecting the E-NPKI element from the general purpose network.

Requirement ID: SRS-2315

•All E-NPKI servers and workstations shall be configured in accordance with all relevant NCIRC Configuration Guides.

Requirement ID: SRS-2316

•All E-NPKI servers and workstations shall operate with the minimal number of accounts required for administration and operation.

Requirement ID: SRS-835

•Software which provides additional security functionality to the E-NPKI such as Antivirus software shall be implemented as long as the additional software does not interfere with the evaluated configuration of the E-NPKI product.

Requirement ID: SRS-836

•Any software which interferes with the evaluated configuration or does not increase security functionality to the E-NPKI shall not be installed on E-NPKI CA or RA systems.

Requirement ID: SRS-2675

•All software shall be approved by the NCIA CCP process and listed on the relevant Approved fielded products List (AFPL) prior to installation on NATO CIS.

3.6.5.2 Computer security rating

The Security settings in effect on the NS Operational Network (ON) environment are categorised using the categories below.

•Account Policies. Password policies, account lockout policies and Kerberos policies.

•Local Policies. Audit policy, user rights assignment, security options.

•Event Log Settings. Settings for event log parameters itself (e.g., max size of audit file).

•Restricted Groups. Membership of security-sensitive User groups.

•System Services. Start-up and permission for system services.

•Registry. Permissions for Windows registry keys.

•File System Permission. Permissions for folders and files.

•Removal Of Certain Folders and Files. Removal of some default files and registry keys.

•Installation of Devices. Settings for installation of specific hardware devices (e.g., floppy drives, microphones, etc.).

•Configuration of Specific Windows Software Modules. Settings for use of security related Windows software modules like DHCP, RAS, etc.

•BIOS Settings. Security related configuration data for BIOS.

Details of standards applicable to the security settings are given in NCIRC Security Settings for the deployed server and workstation operating systems.

Requirement ID: SRS-1465

•E-NPKI shall be capable of operating within the ON and MS WAN environment (including servers, network, services and workstations) in the presence of the currently approved NATO Security Settings. Any deviations from the approved security settings shall be identified by the Contractor prior to testing and shall be subject to approval of the Purchaser.

Requirement ID: SRS-837

•The E-NPKI CA and RA systems shall be certified compliant to the CIMC Protection Profile Security Level 3 or equivalent.

Requirement ID: SRS-838

•CA and RA certification and approval shall be performed by a NATO Nation CIS Authority for the security relevant elements of the E-NPKI CA and RA.

Requirement ID: SRS-839

•Such an evaluation shall include system-level analysis.

Requirement ID: SRS-840

•The selection and use of other Common Criteria Protection Profiles, which have been certified by a NATO National Security Authority (NSA) shall be utilised where appropriate.

Requirement ID: SRS-841

•The scope of the E-NPKI CA and RA evaluation requirement shall include any component such as a Card Management System (CMS) which relies upon the provision of E-NPKI CA or RA Trusted Role Certificates in order to function.

Requirement ID: SRS-842

•Compliance certification shall require a formal evaluation and certification by a NATO Nation CIS Security AUTHORITY or NSA as appropriate.

The CIMC requirement of the E-NPKI Certificate Policy does not imply that all certificate life cycle management functions must reside within the CIMC boundary. Notably, it allows for some life cycle management functions to be initiated by certificate subscribers or certificate sponsors using their own end systems.

Requirement ID: SRS-845

•Certificate subscribers or certificate sponsors are permitted to complete most life cycle management functions provided that they have been authorised by a E-NPKI CA or RA to do so. All life cycle management functions that are performed by certificate subscribers or certificate sponsors shall be done by PKIX Certificate Management Protocol (CMP) defined in RFC4210 or by other mechanisms of equal security to be approved by the NPMA.

3.6.6 Life cycle technical controls

3.6.6.1 System development controls

Requirement ID: SRS-846

•Equipment (hardware and software) procured to operate the E-NPKI infrastructure shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection.

Requirement ID: SRS-847

•Equipment developed for the E-NPKI infrastructure shall be developed in a controlled environment.

Requirement ID: SRS-848

•The design and development process shall be supported by third party verification of process compliance and ongoing Risk Assessments to influence security safeguard design and minimise residual risk.

Requirement ID: SRS-849

•E-NPKI CAs and OCSP servers shall have dedicated hardware platforms.

3.6.6.2 Security management controls

Requirement ID: SRS-850

•The E-NPKI CA equipment shall be dedicated to administering a key management infrastructure.

Requirement ID: SRS-851

•The configuration of the E-NPKI CA system, as well as any modifications and upgrades, shall be documented as part of the system configuration management.

Requirement ID: SRS-852

•The E-NPKI CA system shall not have installed applications or software components, which are not part of the E-NPKI CA configuration.

Requirement ID: SRS-853

•A formal configuration management methodology shall be used for installation and ongoing maintenance of E-NPKI CA systems.

Requirement ID: SRS-854

•There shall be a mechanism for detecting unauthorised modifications to the E-NPKI CA system software or configuration.

3.6.6.3 Life cycle security controls

Requirement ID: SRS-855

•Equipment updates shall be purchased or developed in the same manner as original equipment.

Requirement ID: SRS-856

•Equipment updates shall be installed by trusted and trained personnel in a defined manner.

3.6.7 Network security controls

Requirement ID: SRS-857

•All E-NPKI CA servers**, OCSP servers, and TimeStamp servers** shall be protected from attack through any open or general purpose network with which they connected.

Requirement ID: SRS-858

•Such protection shall be provided as a minimum through the installation of a boundary protection device configured to allow only the protocols and commands required for the operation of the E-NPKI CA.

Requirement ID: SRS-2320

•In Addition, mechanisms such as host-based firewall shall also be implemented to block incoming and outgoing services not required to perform the CA, RA, OCSP, or time-stamping functions.

Requirement ID: SRS-2318

•For CA and RA components, either remote management and login shall be disabled, or remote maintenance shall be conducted via an end-to-end (administrator machine to component) virtual private network using cryptography commensurate with the strength of the E-NPKI keys being issued.

Requirement ID: SRS-2319

•Network protocols not required for CA or RA operation or remote administration shall be disabled.

Requirement ID: SRS-2829

•Pin Entry Device (PED) functionality shall be locally implemented and is not permissible to perform remotely.

3.6.7.1 Cross Domain Support

Requirement ID: SRS-1467

•E-NPKI services shall operate in multiple security domains including the PBN (NATO UNCLASSIFIED/NATO RESTRICTED), and the ON (NATO SECRET/MISSION SECRET) where rules, regulations and category of personnel are different. In order to enable information and synchronisation to be available across these domains, multiple procedures and devices are and will be available in support of these exchanges.

Cross-domain support service is necessary when E-NPKI is used in a distributed environment for creating and feeding the Information Products from various sources spread across different Security Domains

The NATO IEG supports different scenarios in order to meet operational needs for Cross-domain information exchange as described in AC/322-D0030-Rev5.

Requirement ID: SRS-1471

•E-NPKI shall support cross-security domain information exchange including the formal security approval through the NATO accreditation process for each cross-domain connection and information exchange.

3.6.8 Time-stamping

Requirement ID: SRS-2835

•The E-NPKI secure time-stamping service shall be installed at all locations including CA and OCSP services including both production and non-production environments.

Requirement ID: SRS-859

•The E-NPKI secure time-stamping service shall meet the same system availability requirements as the CA.

Requirement ID: SRS-860

•Specifically, the time-stamping service shall have the same redundancy requirements as a CA.

Requirement ID: SRS-861

•The hardware cryptographic module for the Time-stamping service shall meet the standards as defined for the CA hardware cryptographic module.

3.7 Certificate, CRL, and OCSP Profiles

3.7.1 Certificate profile

3.7.1.1 Version number(s)

Requirement ID: SRS-2324

•The E-NPKI CA shall issue X.509 Version 3 certificates, in accordance with the RFC3280 and RFC5280 Certificate and CRL Profile.

Requirement ID: SRS-2794

•E-NPKI shall take into consideration any change to X.509 versions along with contract execution.

Requirement ID: SRS-2325

•The E-NPKI hardware and software shall support every base (non-extension) X.509 fields:

Requirement ID: SRS-2326

•Signature

Requirement ID: SRS-2327

•Issuer

Requirement ID: SRS-2328

•Validity

Requirement ID: SRS-2329

•Subject

Requirement ID: SRS-2332

•Subject Public Key Information: Algorithm ID, key

Requirement ID: SRS-2330

•Version

Requirement ID: SRS-2331

•Serial Number

3.7.1.2 Certificate extensions

Requirement ID: SRS-2333

•All subscriber E-NPKI hardware and software shall correctly process the extensions identified in the PKIX certificate and CRL profile (RFC3280 and RFC5280.)

Requirement ID: SRS-2334

•The certificate Policies field shall be set as critical in all Tier 2 and Tier 3 E-NPKI certificates.

Requirement ID: SRS-2335

•In the case of Cross certification, the Signing Root CA shall not change the Subject Key Identifier (SKI) in the issued cross-certificate from the SKI contained in the original self-signed Root CA certificate.

Requirement ID: SRS-2337

•The E-NPKI Root CAs shall support the population of the following extensions within their certificates:

Extension	**Value** (**Example**)
Authority Key Identifier	KeyID=99 a4 2d 2b f9 56 1f 15 73 15 89 93 b9 ec db f1 4d 14 cb ab
Subject Key Identifier	KeyID=99 a4 2d 2b f9 56 1f 15 73 15 89 93 b9 ec db f1 4d 14 cb ab
Basic Constraints (CRITICAL)	Subject Type=CA Path Length Constraint=2
Key Usage (CRITICAL)	Certificate Signing, Off-line CRL Signing, CRL Signing (06) **(No other attributes permitted)**

Requirement ID: SRS-2336

•The E-NPKI subordinate CAs shall support the population of the following extensions within their certificates:

Extension	**Value** (Example)
Authority Key Identifier	KeyID=b3 c5 0b 74 ff fa 77 8c 38 c1 90 06 8a 48 1b db c0 f2 05 3e

Subject Key Identifier	KeyID=99 a4 2d 2b f9 56 1f 15 73 15 89 93 b9 ec db f1 4d 14 cb ab
Basic Constraints (CRITICAL)	Subject Type=CA Path Length Constraint=1
Key Usage (CRITICAL)	Certificate Signing, Off-line CRL Signing, CRL Signing (06) **(No other attributes permitted)**
Certificate Policies (Critical)	[1]Certificate Policy: Policy Identifier=1.3.26.1.9.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ia.nato.int/NPKI/CertP.pdf [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=NATO Notice Number=1 Notice Text=Limited Liability. See CertP-Responsabilite limitee. Voir Cert. [2]Certificate Policy: Policy Identifier=1.3.26.1.9.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ia.nato.int/NPKI/CertP.pdf [2,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference:

	Organization=NATO Notice Number=1 Notice Text=Limited Liability. See CertP-Responsabilite limitee. Voir Cert.
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL31 OU=InternetCA Rev2 O=NATO [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://NITCDSAREV2.NCSA.NATO.INT/cn=WinCombined2,ou=InternetCA%20Rev2,o=NATO?certificateRevocationList?base
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://OCSP.nato.int [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://NCIANUNRDSAREV3.ncia.nato.int/cn=NCIANUNRCAV3,o=NATO?cACertificate;binary [3]Authority Info Access

	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://NCIANUNRBUDSAREV3.ncia.nato.int/cn=NCIANUNRCAV3,o=NATO?cACertificate;binary

Requirement ID: SRS-2482

•OCSP Server Certificates shall contain the following extensions:

Extension	**Value** (Example)
Authority Key Identifier	KeyID=b3 c5 0b 74 ff fa 77 8c 38 c1 90 06 8a 48 1b db c0 f2 05 3e
Subject Key Identifier	KeyID=99 a4 2d 2b f9 56 1f 15 73 15 89 93 b9 ec db f1 4d 14 cb ab
Basic Constraints (CRITICAL)	Subject Type=CA Path Length Constraint=1
Key Usage (CRITICAL)	Certificate Signing, Off-line CRL Signing, CRL Signing (06) **(No other attributes permitted)**
Extended Key Usage	1.3.6.1.5.5.7.3.9 (OCSP Signing)
Certificate Policies (Critical)	[1]Certificate Policy: Policy Identifier=1.3.26.1.9.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ia.nato.int/NPKI/CertP.pdf [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=NATO Notice Number=1

	Notice Text=Limited Liability. See CertP-Responsabilite limitee. Voir Cert. [2]Certificate Policy: Policy Identifier=1.3.26.1.9.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ia.nato.int/NPKI/CertP.pdf [2,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Reference: Organization=NATO Notice Number=1 Notice Text=Limited Liability. See CertP-Responsabilite limitee. Voir Cert.
CRL Distribution Point	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL31 OU=InternetCA Rev2 O=NATO [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://NITCDSAREV2.NCSA.NATO.INT/cn=WinCombined2,ou=InternetCA%20Rev2,o=NATO?certificateRevocationList?base

Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://OCSP.nato.int [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://NCIANUNRDSAREV3.ncia.nato.int/cn=NCIANUNRCAV3,o=NATO?cACertificate;binary [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://NCIANUNRBUDSAREV3.ncia.nato.int/cn=NCIANUNRCAV3,o=NATO?cACertificate;binary

Requirement ID: SRS-2388

•The E-NPKI subscriber certificates (Subscribers and Devices) shall correctly process the extensions identified in the PKIX certificate and CRL profile (RFC3280 and RFC 5280.)

3.7.1.3 Algorithm object identifiers

Requirement ID: SRS-2391

•CAs shall use at least SHA-256 hash algorithm when generating digital signatures.

Requirement ID: SRS-2392

•All E-NPKI components shall be capable of verifying signatures based on SHA-1.

Requirement ID: SRS-2390

•Certificates shall use OIDs from the following table for signatures.

Name	**OID**

ecdsa-with-SHA384	1.2.840.10045.4.3.3
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA1	1.2.840.10045.4.3.1
id-RSASSA-PSS	1.2.840.113549.1.1.10
sha512WithRSAEncryption	1.2.840.113549.1.1.13
sha384WithRSAEncryption	1.2.840.113549.1.1.12
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha1WithRSAEncryption	1.2.840.113549.1.1.5

Requirement ID: SRS-2421

•Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. All E-NPKI components shall be capable of verifying PSS padded RSA signatures with the hash algorithms and OIDs specified in the table below.

Name	**OID**
id-sha1	1.3.14.3.2.26
id-sha256	2.16.840.1.101.3.4.2.1
id-sha384	2.16.840.1.101.3.4.2.2
id-sha512	2.16.840.1.101.3.4.2.3

Requirement ID: SRS-2433

•Certificates shall use OIDS from the following table for identifying the algorithm for which the subject key was generated.

Name	**OID**
id-ecPublicKey	1.2.840.10045.2.1
id-ecDH	1.3.1321.1.12
rsaEncryption	1.2.840.113549.1.1.1

Requirement ID: SRS-2432

•Where certificates contain an elliptic curve public key, the parameters shall be specified as one of the curves named in the following table.

Name	**OID**
ansip256r1	1.2.840.10045.3.1.7
ansip384r1	1.3.132.0.34

3.7.1.4 Name forms

Requirement ID: SRS-2463

•Every DN shall be in the form of an X.501 UTF8String.

3.7.1.5 Name constraints

Requirement ID: SRS-2464

•The E-NPKI system shall correctly process the Name Constraints extension within cross-certificates issued by Root CAs.

3.7.1.6 Certificate Policy object identifier

Requirement ID: SRS-2465

•E-NPKI subordinate CAs shall ensure that one or more of the relevant Policy OIDs are contained within the certificates it issues appropriate to the level of assurance with which it was issued.

3.7.1.7 Usage of Policy Constraints extension

Root CA's support the ability to insert the Policy Constraints extension within cross-certificates they issue.

Requirement ID: SRS-2802

•The E-NPKI system shall support the ability to correctly process all Policy Constraints extensions within cross-certificates.

3.7.1.8 Policy qualifiers syntax and semantics

Requirement ID: SRS-2468

•The implementation of the policy qualifiers extension by E-NPKI CAs within certificates shall be configurable.

3.7.1.9 Processing semantics for the critical Certificate Policies extension

Requirement ID: SRS-2467

•Critical extensions shall be interpreted as defined in RFC3280 and RFC5280.

3.7.2 CRL profile

3.7.2.1 Version number(s)

Requirement ID: SRS-2469

•E-NPKI CAs shall issue X.509 version two (2) CRLs in accordance with the RFC3280 and RFC5280 Certificate and CRL Profile.

3.7.2.2 CRL and CRL entry extensions

Requirement ID: SRS-453

•All subscriber E-NPKI software shall correctly process all CRL extensions identified in the RFC3280 and RFC5280 Certificate and CRL profile.

Requirement ID: SRS-454

•NPKI CAs shall correctly implement all CRL extensions identified in the RFC3280 and RFC5280 Certificate and CRL profile.

Requirement ID: SRS-2470

- Version

Requirement ID: SRS-2471

- Issuer

Requirement ID: SRS-2472

- Effective date

Requirement ID: SRS-2473

- Next update

Requirement ID: SRS-2474

- Signature algorithm

Requirement ID: SRS-2475

- Signature hash algorithm

Requirement ID: SRS-2476

- CRL Number

Requirement ID: SRS-2477

- Authority Key Identifier

Requirement ID: SRS-2478

•NPKI CAs shall correctly implement all CRL entry extensions identified in the RFC3280 and RFC5280 Certificate and CRL profile.

Requirement ID: SRS-2479

- Serial Number

Requirement ID: SRS-2480

- Revocation date

Requirement ID: SRS-455

- CRL Reason Code

3.7.3 OCSP profile

3.7.3.1 Version number(s)

Requirement ID: SRS-2293

•E-NPKI CAs shall implement OCSP version 1 in accordance with the RFC6960 OCSP Profile.

3.7.3.2 OCSP extensions

Requirement ID: SRS-2511

•E-NPKI OCSP Responders shall be capable of handling OCSP requests with the following base attributes:

Requirement ID: SRS-2512

- Protocol version

Requirement ID: SRS-2513

- Service request

Requirement ID: SRS-2514

- Target certificate identifier

Requirement ID: SRS-2515

- E-NPKI OCSP Responders shall be capable of handling OCSP requests with the following optional extensions:

Requirement ID: SRS-2516

- Nonce

Requirement ID: SRS-2519

•E-NPKI OCSP Responders shall be capable of generating OCSP responses with the following base attributes:

Requirement ID: SRS-2520

- Protocol version

Requirement ID: SRS-2521

- Identifier of the responder

Requirement ID: SRS-2522

- Timestamp when the response was generated (producedAt)

Requirement ID: SRS-2527

- Responses for each of the certificates in a request.

Requirement ID: SRS-2528

- Signature algorithm OID

Requirement ID: SRS-2529

- Signature

Requirement ID: SRS-2523

•E-NPKI OCSP Responders shall be capable of generating OCSP responses with the following extensions:

Requirement ID: SRS-2524

- thisUpdate

Requirement ID: SRS-2525

- nextUpdate

Requirement ID: SRS-2526

- revocationTime

Requirement ID: SRS-2530

•E-NPKI OCSP Responders shall be capable of generating OCSP responses with the following attributes for each certificate response answered:

Requirement ID: SRS-2531

- Target certificate Identifier

Requirement ID: SRS-2532

- Certificate Status Value (Good, Revoked, Unknown)

Requirement ID: SRS-2533

- Extended revoked definition response extension

Requirement ID: SRS-2026

•OCSP Servers shall be capable of populating the thisUpdate field of the OCSP response with the thisUpdate value from the authoritative CRL or ARL.

Requirement ID: SRS-2030

•OCSP Servers shall be capable of populating the nextUpdate field of the OCSP response with the nextUpdate value from the authoritative CRL or ARL.

Requirement ID: SRS-2481

•The use of nonces within OCSP requests shall be configurable to support the enabling and disabling of nonces within E-NPKI client software.

3.8 Compliance Audit and Other Assessments

Document structure placeholder. No requirements

3.9 Other Business and Legal Matters

3.9.1 Fees

3.9.1.1 Certificate issuance or renewal fees

Requirement ID: SRS-2535

•The E-NPKI system shall include workflows and tools to permit CAs and RAs to attribute the cost for licences, smartcards, and other components against a relevant cost centre in an automated rule based manner.

Requirement ID: SRS-2536

•The E-NPKI system shall be able to configure the components for cost recovery independently for each cost centre.

3.9.2 Financial responsibility

Document structure placeholder. No requirements

3.9.3 Confidentiality of business information

Document structure placeholder. No requirements

3.9.4 Privacy of personal information

3.9.4.1 Privacy plan

E-NPKI must be used in compliance with the E-NPKI Data Protection Policy specified below. The policy affords protection according to the following outline conditions which must be supported by appropriate technical and/or procedural measures as required.

Requirement ID: SRS-2676

•Certificates and CRLs published in public directories shall not contain sensitive personal information or classified NATO information. Sensitive personal information shall not be disclosed without the prior consent of the subscriber, unless required by the SAA based on NATO rules and regulations. Release of classified NATO information is subject to the requirements of NATO Security Policy.

•Inspection information shall be appropriately classified and shall not be disclosed to anyone for any purpose other than inspection and system security purposes.

3.9.4.2 Information treated as private

Requirement ID: SRS-2539

•The E-NPKI system shall protect all E-NPKI subscriber and Sponsor personally identifying information that is collected but not included in certificates from unauthorized disclosure.

Requirement ID: SRS-2540

•The E-NPKI system shall handle all such information as sensitive, and access shall be restricted to those with an official need-to-know in order to perform their official duties.

Requirement ID: SRS-2541

•Private keys shall be held in strictest confidence. Private keys generated or escrowed by the by E-NPKI CAs shall never appear in an unencrypted form outside the CAs equipment or approved cryptographic module.

3.9.4.3 Information not deemed private

Requirement ID: SRS-2542

•A certificate should only contain information that is relevant and necessary to effect transactions with the certificate. Information included in certificates, CRLs, and certificate status requests and responses shall not be deemed private, and is not subject to the protections outlined in the other subsections of Section 3.9.4.

3.9.4.4 Responsibility to protect private information

Requirement ID: SRS-2543

•The E-NPKI System shall include technical mechanisms to ensure that any keys held by a CA shall be released only to an organizational authority, in accordance with the CPS, organizational policy, and the E-NPKI Certificate Policy.

3.9.5 Intellectual property rights

Document structure placeholder. No requirements

3.9.6 Representations and warranties

Document structure placeholder. No requirements

3.9.7 Disclaimers of warranties

Document structure placeholder. No requirements

3.9.8 Limitations of liability

Document structure placeholder. No requirements

3.9.9 Indemnities

Document structure placeholder. No requirements

3.9.10 Term and termination

Document structure placeholder. No requirements

3.9.11 Individual notices and communications with participants

Document structure placeholder. No requirements

3.9.12 Amendments

Document structure placeholder. No requirements

3.10 Performance criteria

3.10.1 Certification Authorities

Requirement ID: SRS-2095

•E-NPKI Certification Authorities shall be scaled to handle 250,000 subscribers and devices without requiring modifications.

Requirement ID: SRS-2100

•E-NPKI HSMs shall be capable of handling 2000 ECDSA 384 signatures per second.

Requirement ID: SRS-2101

•E-NPKI CAs shall be capable of managing 100 simultaneous Registration Authority connections.

3.10.2 Registration Authorities

Requirement ID: SRS-2096

•E-NPKI RAs shall be capable of generating an ECDSA signature within 0.25 seconds.

Requirement ID: SRS-2103

•E-NPKI RAs shall be capable of processing 100 new enrolment requests per day.

3.10.3 End Entities

Requirement ID: SRS-2097

•E-NPKI end entities shall be able to generate ECDSA 384 keys within 30 Seconds.

Requirement ID: SRS-2102

•E-NPKI clients shall be capable of generating an ECDSA signature within 0.25 seconds

3.10.4 OCSP Service

Requirement ID: SRS-2098

•E-NPKI OCSP service shall be capable of precomputing hashes for 250,000 subscribers and devices (average 3 certificates per subscriber or device) within 15 minutes.

Requirement ID: SRS-2832

•If required to support Nonces based on the results of the Security Risk Assessment, the OCSP Service shall be capable of sustaining 750,000 responses within a 15 minute window.

3.10.5 Timestamping Service

Requirement ID: SRS-2099

•E-NPKI Timestamp service shall be capable of handling 2000 ECDSA 384 signatures per second.

4 Non-functional Requirements

4.1 Quality Requirements

4.1.1 Reliability

4.1.1.1 General

Reliability is defined as the capability of the software product to maintain a specified level of performance when used under specified conditions.

A failure is defined as an error or cessation in the operation of the software requiring, as a minimum, a restart of the application.

For services, a failure is characterized by the inability of the Service to perform its operation.

For browser-based applications, an error requiring the subscriber to restart the application in the browser shall be considered a failure.

Requirement ID: SRS-624

•The E-NPKI hardware and software at each installed operational location shall exhibit a mean-time-between-failure (MTBF) characteristic of less than 1 failure every 24 hours and that shall not be affected by the total number of nodes which are active during that period. The MTBF measurement shall not include failures resulting from factors determined to be external to E-NPKI (e.g., loss of domain controller).

Requirement ID: SRS-625

•E-NPKI shall gracefully degrade in the condition where the following Core Services are not available:

•Directory Services

•Enterprise Management Services

•E-mail Services

•Networking and Security Services

•A graceful degradation means all E-NPKI functions unrelated to the unavailable services shall continue to work. The capability shall not raise exceptions, or even crash, but shall elegantly notify the subscribers and if possible shall continue to provide some functions using local cache.

4.1.1.2 Availability

Availability is defined as the capability of the software product to be in a state to perform a required function at a given point in time, under stated conditions of use.

Requirement ID: SRS-758

•E-NPKI non-availability time shall be measured by adding the Downtime period (time elapsed from Time of Occurrence to Time of Recovery) for each system, service or application failure.

Requirement ID: SRS-759

•Measurements of availability shall not include failures resulting from factors determined to be external to E-NPKI (e.g., loss of domain controller, loss of network connectivity).

Requirement ID: SRS-629

•E-NPKI End-entities shall not experience interruption of communication with E-NPKI Services as a result of limited bandwidth.

•Limited bandwidth is defined as bandwidth of less than 16 kbps.

Requirement ID: SRS-630

•E-NPKI End-entities shall not experience interruption of communication with E-NPKI Services as a result of high latency.

•High latency is defined as latency exceeding 1100 ms packet round trip time.

Requirement ID: SRS-631

•E-NPKI shall be available in operational HQs, static and deployed, 24 hours a day, 7 days a week, with an availability rate of 99.5 %.

Requirement ID: SRS-755

•In case of a E-NPKI Server failure, E-NPKI shall be capable of automated switching to an E-NPKI Backup Server within 10 minutes.

Requirement ID: SRS-756

•E-NPKI operation shall not be interrupted during incorporation of in-service equipment updates or maintenance software updates.

4.1.1.3 Accuracy

Accuracy is defined as the degree of conformity of a measured or calculated value to its actual or specified value.

Requirement ID: SRS-761

•E-NPKI shall provide accuracy of timing for product time stamps (e.g., time of update) to 10 ms of the system time.

4.1.1.4 Survivability

In engineering, survivability is the quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance.

E-NPKI is expected to ensure the survival of data and associated functional services in defined conditions.

4.1.1.4.1 General

Requirement ID: SRS-766

•The design and implementation of E-NPKI shall not contain single points of failure.

Requirement ID: SRS-767

•E-NPKI shall provide a Mean Time To Repair (MTTR) of 1 day or less for CA, RA, OCSP, and Timestamp systems.

Requirement ID: SRS-2553

•MTTR values from each subsystem shall not reduce the required system or subsystem availability.

4.1.1.4.2 Network/Hardware Survivability

Requirement ID: SRS-784

•E-NPKI shall support fail-over in its architecture. E-NPKI Client software shall be able to survive failure of application server without crashing or affecting the stability of the system.

Requirement ID: SRS-786

•If WAN connectivity is unavailable, E-NPKI shall continue to perform all functions that do not require WAN connectivity, such as maintenance of local information, administration of local systems and local data dissemination.

Requirement ID: SRS-788

•E-NPKI shall not cause data corruption or loss of data integrity due to connection failure or other hardware/software failures.

4.1.1.4.3 Service Survivability

Requirement ID: SRS-791

•E-NPKI shall continue to provide Functional Services, including Applications and Interfaces, and ensure the preservation and availability of existing data, objects and products, at the LAN level following the loss of any components and/or services of the Bi-SC AIS on WAN level.

4.1.1.4.4 Data Survivability

Data survivability shall be supported in two distinct ways:

Backups: taking periodic full or incremental 'snapshots' of the data store to mitigate the risk of system/storage failure

Archiving: removing and storing data that is no longer required for use from the system, thus reducing the size of the data store (and improving performance)

This sections discusses the requirements for backups.

Requirement ID: SRS-792

•E-NPKI shall provide the ability to perform full and incremental backups of E-NPKI data and software without impacting system availability.

Requirement ID: SRS-793

•E-NPKI shall permit backup and archiving of both the complete E-NPKI Repository and selected Information Elements.

Requirement ID: SRS-794

•E-NPKI shall allow an authorised subscriber to archive data that is not currently required in order to reduce the number of records to be maintained.

Requirement ID: SRS-795

•E-NPKI shall be able to make full and incremental backups of all or selected data (Information Elements) at the local node, automatically at a configurable frequency.

Requirement ID: SRS-2803

•E-NPKI shall be able to make full and incremental backups of all or selected data (Information Elements) at the local node, triggered manually by the appropriate Trusted Role.

Requirement ID: SRS-804

•Archived E-NPKI data shall be searchable/readable and E-NPKI shall provide for restoring it to a specified repository as required.

Requirement ID: SRS-805

•Recovery of archives in E-NPKI shall allow data to be overwritten or appended as required by the Administrator.

Requirement ID: SRS-1214

•E-NPKI shall support to transfer the backup and archive data to a transportable media.

4.1.1.5 Error Handling (Fault Tolerance)

The Error Handling capability is defined as the ability of the software product to maintain a specified level of performance in cases of software faults or of infringement of its specified interface.

This section contains the requirements concerning errors, warnings and notifications that subscribers will encounter or be confronted with.

E-NPKI is expected to handle errors in a way that helps subscribers rather than disturb or otherwise hinder their work.

Requirement ID: SRS-806

•E-NPKI shall automatically report errors and suggest corrective actions with respect to the creation, change, exchange and storage of data elements, objects and products.

Requirement ID: SRS-807

•E-NPKI messages (e.g., error, warning, notification, and informational messages) shall contain initiating module information, context sensitive help OR directives on where to find answers and solutions.

Requirement ID: SRS-809

•E-NPKI shall report errors in context (e.g., given within the same page where they are encountered).

Requirement ID: SRS-810

•In E-NPKI, invalid entries shall be highlighted or marked so they can be quickly identified and corrected.

Requirement ID: SRS-814

•E-NPKI shall have single-click closable pop-up screens or windows when used to report about errors.

Requirement ID: SRS-811

•E-NPKI shall limit the number of error reports that are displayed to the subscriber (i.e., do not show multiple error reports for the same error).

Requirement ID: SRS-812

•E-NPKI shall notify the subscriber for potential loss/deletion of information objects during modification of any information object (e.g., by cascading deletion). When prompted by a warning notification about the data that might be lost/deleted, the subscriber shall be able to choose the action that shall be taken by the system (e.g., cancel, continue).

Requirement ID: SRS-813

•E-NPKI shall avoid the loss of subscriber-entered data due to receipt of an error or other message. Subscriber input shall not be lost, discarded or corrupted unless a subscriber actually chooses to delete or reset his input. These requirements do not apply to data that has a security reason for being removed.

Requirement ID: SRS-817

•In E-NPKI the content of the error message shall allow for re-creation of the conditions when the problem occurred (e.g., the appropriate screen and information content that caused the problem).

Requirement ID: SRS-816

•E-NPKI shall provide a gradual degradation of E-NPKI services (i.e., normal to degraded then to off-line) in the presence of fault conditions.

4.1.2 Data Integrity

Requirement ID: SRS-930

•Data integrity shall be applied to information exchanged between and stored by each E-NPKI Services.

Requirement ID: SRS-932

•E-NPKI shall provide an ability to perform cascade deletion of the lower level entities that are dependent on higher level entities.

Requirement ID: SRS-933

•E-NPKI shall implement a two-phase deletion process (i.e., a logical/soft delete with a separate controlled permanent deletion/purging) for entities, unless there is an approved security reason for doing so.

Requirement ID: SRS-934

•E-NPKI shall allow an authorised trusted role to reverse a deletion of a 'soft deleted' entity as long as it does not violate other referential integrity constraints, unless there is an approved security reason for doing so.

Requirement ID: SRS-935

•The Purge (i.e., permanent deletion) functionality in E-NPKI shall be limited to authorised trusted roles.

Requirement ID: SRS-936

•E-NPKI shall contain residual information protection mechanisms to ensure that purged information is no longer accessible.

Requirement ID: SRS-937

•E-NPKI shall ensure that newly created objects do not contain deleted or undefined information (i.e. information that has been logically deleted).

4.1.3 Usability

Usability is defined as the capability of the software product to be understood, learned, used and attractive to the subscriber, when used under specified conditions.

4.1.3.1 Appropriateness recognisability

E-NPKI requires a subscriber-friendly interface for operators who vary considerably in their experience in the intelligence domain, technical skills, and frequency and time spent using the system. In order to help the subscriber feel at ease with the system, some general principles are to be followed. They ensure that the system interface is as close as possible to common applications that the operators are used to manipulate on their personal computers. These principles are mainly the ones standardised in the ISO 9241, particularly in parts 10 to 17. The following requirements represent the main aspects of the norm to

be respected by E-NPKI. They deal with dialogue principles along with data presentation and availability of accurate guidance information.

Requirement ID: SRS-950

•E-NPKI shall comply with the following dialogue principles:

•Suitability for the task: the dialogue shall be suitable for the subscriber's task and skill level.

•Self-descriptiveness: the dialogue shall make it clear what the subscriber shall do next.

•Controllability: the subscriber shall be able to control the pace and sequence of the interaction.

•Conformity with subscriber expectations: the dialogue shall be consistent and correspond to the subscriber characteristics, such as task knowledge, education and experience, and to commonly accepted conventions.

•Suitability for individualization: the dialogue shall be able to be customized to suit the subscriber.

•Suitability for learning: the dialogue shall support and guide the subscriber in learning how to use of the system.

Requirement ID: SRS-951

•E-NPKI shall comply with the following criteria of information presentation:

•Clarity: information shall be conveyed quickly and accurately

•Discriminability: information shall be able to be distinguished accurately

•Conciseness: the system shall provide only the information necessary to complete the task

•Consistency: the same information shall be presented in the same way throughout the application

•Detectability: the subscriber's attention shall be directed to the information required

•Legibility: information shall be easy to read

•Comprehensibility: the meaning of the information shall be clearly understandable

•Unambiguity: the information shall not be open to varying interpretation. Units of measure shall be displayed where appropriate.

Requirement ID: SRS-952

•E-NPKI subscriber guidance information shall be readily distinguishable from other displayed information. This information shall be provided to the subscriber through prompts, feedback, status information and error management:

•Prompts indicate that the system is available for input.

•Feedback provides information in response to the subscriber's input.

•Status is subscriber guidance information that indicates the current state of components in the system hardware and/or software.

•Errors management in human computer interaction include management of:

•System malfunctions due to a software or hardware failure (e.g., a problem with the disk drive),

•subscriber inputs not recognized by the system,

•Data entry or logical errors on the part of the subscriber,

•Unexpected consequences resulting from subscriber inputs.

Requirement ID: SRS-953

•E-NPKI shall use menu dialogues when use of the system is infrequent and the subscriber does not know what options are available. The following aspects shall be considered in order to give the subscriber the useful information in due time and low effort:

•Menu structure, such as logical categories, grouping options and ordering items

•Menu navigation, including titles and access time

•Option selection and execution, including selection methods, use of the keyboard

•Menu presentation, including placement and use of icons

4.1.3.2 Operability

4.1.3.2.1 Ease of Navigation

Requirement ID: SRS-956

•E-NPKI shall include a status bar, which shall provide meaningful information and quick access to certain functions.

Requirement ID: SRS-957

•E-NPKI shall provide on-screen 'drill-down' features to view lower-level details (where and whenever lower level details are available).

Requirement ID: SRS-958

•When the subscriber is working in E-NPKI at a 'drill-down' lower level, changes to the current view shall produce a result at the same level (i.e., the subscriber shall not have to 'drill-down' again to re-establish the current view following a change).

Requirement ID: SRS-960

•E-NPKI shall support editing of information in a logical order. In E-NPKI the subscriber interface forms shall be navigable using the tab key in a logical order. This means that the tab order shall represent the same logical order shown on screen.

Requirement ID: SRS-961

•In E-NPKI, navigation shall be possible with both keyboard and mouse and both shall be self-explanatory.

Requirement ID: SRS-962

•In E-NPKI, functionality hierarchy and branching logic shall be clear and uniform. It shall be obvious where to find the information and/or function the subscriber is looking for.

Requirement ID: SRS-963

•E-NPKI shall provide subscriber interface layouts which are uniform and standardised.

Requirement ID: SRS-964

•In E-NPKI, the submit button for a form shall become disabled on click and re-enabled after any change to the entry content. This prevents clicking twice or more times resulting in duplicate entries.

Requirement ID: SRS-965

•In E-NPKI the ENTER key shall not trigger form submission, especially in cases where forms are too long to display on one screen (e.g., if the submit button falls below the initially visible area).

Requirement ID: SRS-966

•In E-NPKI, scrolling bars (i.e., horizontal and vertical) shall be available when information does not fit onto one screen.

4.1.3.2.2 User interface Requirements

4.1.3.2.2.1 Role-based Presentation

Requirement ID: SRS-971

•E-NPKI shall work on the principle of 'visibility' which means the application shows subscribers whatever they need for the current task without distracting or overwhelming them with unrelated tasks or options.

Requirement ID: SRS-972

•In E-NPKI, subscriber-accessed information shall be filtered according to the subscriber's role and organization, so that subscribers can only see what they are allowed to view and/or change (including both data and functionality).

Requirement ID: SRS-973

•E-NPKI shall only show functionality (e.g., menu items, buttons, selections) that is appropriate to the situation based on subscriber role and permissions and object status. E-NPKI shall hide or clearly disable (e.g., grey out) functionality not appropriate at the time, including items on second-level and lower-level menus and dialogue boxes.

Requirement ID: SRS-974

•E-NPKI subscriber interfaces shall be minimised according to what the subscriber can do. The subscriber interface shall only show entities and attributes (e.g., forms and fields) and functions (e.g., menus and buttons) that are actually available within the security authorisation of the subscriber. Disabled functions due to permissions shall not be shown at all.

4.1.3.2.2.2 Input Requirements

Requirement ID: SRS-976

•In E-NPKI it shall be unambiguous and clear what information in what format is required for each field.

4.1.3.2.2.3 Real-Estate Management

Requirement ID: SRS-985

•E-NPKI shall keep data input page size limited to one screen in order to reduce the need for scrolling to see the submit button.

Requirement ID: SRS-986

•E-NPKI shall be used onto different screen sizes and pages shall not be designed to a fixed screen size. E-NPKI pages shall expand to the right size of the subscriber screen to the extent where the UI is not distorted.

Requirement ID: SRS-987

•E-NPKI shall allow grouping of items with expand/minimise buttons (Microsoft Explorer style) in tree views, or using a "group by column" feature in tabular views.

Requirement ID: SRS-988

•E-NPKI shall provide wizards if input of certain information requires filling out more than one form, or require a form larger than one screen. This means long forms or lists shall be split up over different subpages (or tabs) within the wizard.

4.1.3.2.2.4 Defaults

Requirement ID: SRS-992

•E-NPKI shall provide data defaults where applicable.

4.1.3.2.2.5 Menus, Mouse Actions and Shortcuts

Requirement ID: SRS-994

•Interactions with E-NPKI with a mouse or keyboard shall produce similar results in and throughout all applications.

4.1.3.2.2.6 Data Entry

Requirement ID: SRS-1005

•E-NPKI shall not lose, discard, or corrupt subscriber input without subscriber consent, unless there is an approved security reason for doing so.

4.1.3.2.2.7 User Feedback

Requirement ID: SRS-1007

•E-NPKI shall inform a subscriber that processing has started, after the subscriber has initiated an action.

Requirement ID: SRS-1009

•E-NPKI shall provide prompts (i.e. allow cancellation or confirmation) when input or changes could be lost due to navigation or logging out.

Requirement ID: SRS-1010

•E-NPKI shall provide subscriber feedback on required fields which have not been correctly entered.

4.1.3.2.2.8 Appearance

Similar parts of the application should have similar subscriber interfaces and layouts throughout the application.

Requirement ID: SRS-1013

•The design of the subscriber interface shall be based on a single theme with variations. E-NPKI shall have a common look and feel carried across the entire application's subscriber interface within which a small number of similar but easily distinguished layouts are used.

Requirement ID: SRS-1014

•Visual elements and interaction schemes of the E-NPKI subscriber Interface shall be reused on similar functions and features. Uniformity is created this way, which helps subscribers to understand where they are and what they can do.

Requirement ID: SRS-1015

•A consistent font shall be used across E-NPKI applications.

Requirement ID: SRS-1016

•The E-NPKI subscriber interface shall be structured so that options, features and functions of the application are organised in a way that reflects their relationships.

4.1.3.2.2.9 Standard Functionality

Requirement ID: SRS-1021

•E-NPKI shall support copying and pasting from other applications via the Clipboard.

Requirement ID: SRS-1022

•E-NPKI shall allow an operation to apply to multiple-selected objects where possible.

Requirement ID: SRS-1030

•E-NPKI shall provide undo/redo functionality for changes to objects to the largest extent possible (not limited to formatting), at least until the last save action.

Requirement ID: SRS-1033

•E-NPKI shall clearly display the Organisational Node and mode of operation (e.g., Operational, Exercise, Training) in which the subscriber is currently working.

4.1.3.3 Language Requirements

Requirement ID: SRS-1036

•E-NPKI shall use UK English as the default language. This shall apply to all system and supporting components, including views, dialogs, help screens, tooltips, CBT, error/notification/warning messages and documentation.

4.1.3.4 Time Zone

Requirement ID: SRS-1062

•E-NPKI shall use and store data internally as Zulu time (i.e. GMT) as standard time.

Requirement ID: SRS-1063

•E-NPKI shall present data with its time-zone in Zulu time by default.

Requirement ID: SRS-1064

•If so selected by the subscriber, E-NPKI shall present data in the local time of any other possible time zone.

Requirement ID: SRS-1065

•E-NPKI shall clearly identify time values as Zulu (e.g., 0815Z) or Local in subscriber displays and logs.

Requirement ID: SRS-1066

•E-NPKI shall represent all date/time data according to ISO 8601.

4.1.3.5 Accessibility

Accessibility is a set of features that make an application usable for people with certain disabilities.

For E-NPKI, colour blindness (i.e., any deficiencies in colour perception) is the main concern.

Requirement ID: SRS-1046

•The E-NPKI subscriber interface shall be suitable for colour blind subscribers:

•Selected elements of the GUI shall not be only identified by a difference of colour.

•Sufficient contrast shall be used throughout the application.

•Highlighting information shall not rely on colours only.

Requirement ID: SRS-1047

•The E-NPKI accessibility features shall apply to the application subscriber interface, including the help pages, CBT pages, and error/warning/notification messages.

Requirement ID: SRS-1048

•E-NPKI shall scale the subscriber interface to fit the screen when low resolutions are used for poor vision accessibility.

Requirement ID: SRS-1049

•Information on screens in E-NPKI shall contain text. Reliance on pictures or icons alone is not desired.

Requirement ID: SRS-1050

•The E-NPKI subscriber interface shall support a minimum resolution of 1280x1024.

4.1.4 Efficiency (Performance)

Efficiency (Performance) is defined as the capability of the software product to provide appropriate performance, relative to the amount of resources used, under stated conditions.

Requirement ID: SRS-1070

•E-NPKI Server functionalities shall be available within a maximum of ten minutes after the Operating System of each E-NPKI server is started.

Requirement ID: SRS-1071

•E-NPKI subscriber functionality shall be available within one minute after accessing or starting the E-NPKI subscriber application.

Requirement ID: SRS-1073

•E-NPKI shall never block new incoming service requests when performing time-consuming services.

Requirement ID: SRS-1074

•E-NPKI shall support near real-time exchange of information between E-NPKI operational instances connected through a Local Area Network (LAN).

4.1.4.1 Performance and Bandwidth Efficiency

Requirement ID: SRS-1077

•E-NPKI shall be designed and implemented to minimise use of network bandwidth and computational resources.

4.1.4.2 Performance Depending on Network Status

A degraded network mode of operation is when the NS/mission-specific WAN or NS/mission-specific LAN is providing a reduced level of service that might impact one or more of the E-NPKI services (or Application and Interface Products). For example, reduction in service due to bandwidth limitations or a communication degradation affecting some part of the LAN and/or WAN.

Requirement ID: SRS-1082

•When in a degraded network, E-NPKI shall be capable of providing the same range and level of service to individual subscribers with some reduction in performance.

Requirement ID: SRS-1084

•E-NPKI shall automatically detect degraded performance (whether from network bottlenecks, server load, or other external reasons) and ask the subscriber to allow limitation of the subscriber interface accordingly.

4.1.4.3 Performance by Site Category

Requirement ID: SRS-1086

•E-NPKI shall support at least 500 concurrent active sessions on a single CA Server. These active sessions include for example concurrent RA connections and end entity certificate lifecycle management connections.

4.1.4.4 Performance by Key Use Cases

Requirement ID: SRS-1090

•E-NPKI performance shall be compliant with the performance requirements described below. Those performance characteristics shall take into consideration only the network load arising from E-NPKI; the communication delays on the underlying network due to other Bi-SC systems shall not be included in the measurement. The performance characteristics shall be measured using:

•client access across the relevant network (i.e., not running the browser/client on the server),

•a repository that mirrors an operational repository in numbers and types of entities (i.e., size and composition) and variation of data (i.e., content),

•the reference system or hardware that is of equal or lower specification,

•the standard browser for the Bi-SC AIS (i.e., Internet Explorer),

•workstations of equal or lower specification than standard Bi-SC AIS workstation,

•local-area network connectivity of 100Mb/sec or less,

•for cases involving WAN connection, wide-area network connectivity of less than or equal to 1000Kb/sec and latency of 500ms or greater.

4.1.4.4.1 Search for Information

Requirement ID: SRS-1095

•E-NPKI CAs shall perform a database query search returning 5000 results within five seconds.

Requirement ID: SRS-2734

•E-NPKI CA, RA, and End Entity software shall perform a directory search returning 500 results within five seconds.

4.1.4.4.2 Display Information

Requirement ID: SRS-1097

•E-NPKI shall display user profile information including certificates within one second.

4.1.4.4.3 Information Exchange Performance

Requirement ID: SRS-1105

•E-NPKI shall support near real time exchange of information between Organizational Nodes which are not geographically co-located.

4.1.4.4.4 Web Service Performance

Requirement ID: SRS-1109

•E-NPKI shall support near real-time exchange of information with authorised external systems via identified web services.

4.1.5 Maintainability and Supportability

Maintainability and supportability refer to the ability of the system to be effectively maintained and supported in the field. Attributes include the ability to implement improvements or adaptation of the system to reflect changes in environment and in requirements and functional specifications.

Software maintainability is defined as the capability of the software product to be modified. Modifications might include corrections, improvements or

adaptation of the software to changes in environment, and in requirements and functional specifications.

4.1.5.1 Installation

Requirement ID: SRS-1114

•E-NPKI components shall be capable of being installed by a Windows Installer or similar service/product installation package in any Bi-SC AIS approved platform.

Requirement ID: SRS-1115

•E-NPKI shall be capable of being installed and correctly run on multi-processor and multi-core systems.

Requirement ID: SRS-1128

•E-NPKI shall provide an installation supported by a complete, clearly-worded Installation Manual.

Requirement ID: SRS-1129

•E-NPKI shall ensure the ability to re-run, allow addition or removal of components that have been or are still to be installed.

4.1.5.2 Uninstallation

Requirement ID: SRS-1138

•E-NPKI shall provide a capability to completely uninstall E-NPKI application(s)/component(s).

Requirement ID: SRS-1140

•E-NPKI shall ensure that an application can only be uninstalled by an authorised administrator.

4.1.5.3 Co-existence

Co-existence is defined as the ability of the software to co-exist with other independent software in a common environment sharing common resources.

Requirement ID: SRS-1146

•Installing, running and uninstalling the capability shall not adversely impact other applications or the system it is installed on, running on or uninstalled from.

4.1.5.4 Configuration

Requirement ID: SRS-1150

•E-NPKI shall ensure that the application stores subscriber configuration data in subscriber Profile to prevent log-in delays, etc.

4.1.5.5 Remote automated deployment and reporting

Requirement ID: SRS-1152

•E-NPKI shall support remote deployment of all E-NPKI client components and updates using Microsoft System Center Configuration Manager.

Requirement ID: SRS-1153

•E-NPKI shall support remote restore of all E-NPKI client components and updates using Microsoft System Center Configuration Manager.

Requirement ID: SRS-1154

•E-NPKI shall support remote configuration of all E-NPKI client components and updates using Microsoft System Center Configuration Manager.

Requirement ID: SRS-1155

•E-NPKI shall support configuration reporting of E-NPKI components using Microsoft System Centre Configuration Manager.

Requirement ID: SRS-1156

•E-NPKI shall support collection and reporting of asset inventory metrics for all E-NPKI components using Microsoft System Centre Configuration Manager, including:

•Memory

•Operating System

•Peripherals

•Services

•Login tracking

•Software existence and usage

•Licensing

Requirement ID: SRS-1157

•E-NPKI shall provide for remote un-installation of the E-NPKI client components using Microsoft System Centre Configuration Manager.

4.1.6 Portability

Portability is defined as the capability of the software product to be transferred from one environment to another.

4.1.6.1 Environment

Requirement ID: SRS-1161

•E-NPKI server components shall run successfully on 64-bit environments.

Requirement ID: SRS-2106

•E-NPKI client components shall run successfully on both 32-bit and 64-bit environments.

Requirement ID: SRS-1163

•E-NPKI shall define a minimum required resource profile for the physical environments of each type of E-NPKI deployment described in the SRS.

Requirement ID: SRS-2596

•The resource profile shall contain at least the physical infrastructure resources (processing, memory, storage, monitoring, management and security) so that the physical environment is compliant to this document.

Requirement ID: SRS-1164

•E-NPKI shall define a minimum required resource profile for the virtualized environments of each type of E-NPKI deployment described in the SRS. This requirement is only applicable to components which do not implement Hardware Security Modules.

Requirement ID: SRS-2597

•The resource profile shall contain at least the virtual infrastructure resources (processing, memory, storage, monitoring, management and security) and dedicated reservations so that the virtual environment is compliant to this document.

Requirement ID: SRS-1165

•Any E-NPKI components which implement a web capability shall be able to be run in the following browser versions:

•9.0 (and greater) of Internet Explorer, Safari, Chrome, Firefox.

Requirement ID: SRS-1166

•E-NPKI shall support the use of IPv6 without impaired functionality and performance within a network environment.

Requirement ID: SRS-2109

•E-NPKI server components implementing HSMs shall be deployed on a physical environment.

Requirement ID: SRS-1168

•E-NPKI shall not rely on the NetBIOS interface to communicate with other applications, clients or management services. Disabling NetBIOS shall not affect the applications operation or interoperability in any way.

4.1.6.2 Scalability

Scalability is defined as a desirable property of a system, a network or process, which indicates its ability to either handle growing amounts of work in a graceful manner, or be readily enlarged.

Requirement ID: SRS-1171

•E-NPKI shall be scalable and technically upgradeable to maintain performance against threat growth.

Requirement ID: SRS-1172

•E-NPKI shall use an architecture that allows vertical scalability.

Requirement ID: SRS-1173

•E-NPKI shall use an architecture that allows horizontal scalability.

Requirement ID: SRS-1174

•E-NPKI shall be dimensioned and configured to scale in performance to support a 10% increase in subscribers and devices per year at each site and a 30% growth in data a year for 10 years without degradation of performance.

Requirement ID: SRS-1175

•The E-NPKI database shall be dimensioned to support all the relevant data based on current estimates of numbers and sizes of information objects and provide an additional 30% of space a year for 10 years.

4.1.6.3 Customisability

Requirement ID: SRS-1178

•E-NPKI shall allow subscribers to quickly revisit recent functions and features and to save 'favourites' of features and functions that are often used.

Requirement ID: SRS-1179

•E-NPKI shall allow the subscriber to set up personal preferences for layout and content.

Requirement ID: SRS-1187

•E-NPKI shall persist subscriber customization settings.

4.1.7 Usage scope and limitations

NATO intends to be able to manage, install and use E-NPKI using their own resources on sites and locations decided by NATO without restriction on the Product.

Requirement ID: SRS-1190

•E-NPKI shall be installable and executable by NATO resources only.

Requirement ID: SRS-1191

•E-NPKI shall bear no limitation on the usage scope in term of time, duration and location of usage.

Requirement ID: SRS-1192

•E-NPKI usage shall be permitted for any type of event or activities. Including but not limited to training, demonstration, exercise, static, deployed, mobile, civil or military locations, aircrafts or ships.

Requirement ID: SRS-1193

•The movement of the user base (users or device quantities) from one network domain to another domain shall not lead to additional licences costs if the total quantity of software and/or licences does not increase.

Requirement ID: SRS-2844

•E-NPKI services shall be available to relying parties of Federated infrastructures.

Requirement ID: SRS-2845

•Access to OCSP, timestamp and other E-NPKI services by those Federated identities, shall not result in additional costs for NATO.

4.2 Design Constraints

4.2.1 Database Management

Requirement ID: SRS-1200

•E-NPKI components shall handle information (receive, search, extract) and ensure that it is persistent. For that purpose, one or more Databases will be present and the following requirements shall apply.

4.2.1.1 General

Requirement ID: SRS-1202

•E-NPKI shall provide database administration, monitor and management capability.

Requirement ID: SRS-1203

•E-NPKI shall provide auditing and logging mechanism for all database activities.

Requirement ID: SRS-1205

•E-NPKI shall provide a database query capability to support complex queries.

Requirement ID: SRS-1216

•E-NPKI shall support LDAP, LDAPS, and ODBC database interfaces for the connection to external PACS systems.

4.2.1.2 Data Replication

The basic function of the data replication service is to make the same planning data or operational data available on both the source and destination databases

on different servers separated by a wide area network. Replication can also simply have redundancy purposes.

Requirement ID: SRS-1230

•E-NPKI shall provide the necessary mechanisms to ensure complete, accurate, timely, confidential and consistent data coherence between the different distributed Organizational Nodes of the system.

Requirement ID: SRS-1231

•E-NPKI data replication shall replicate automatically information held in a database whenever it is created/changed/deleted, and that is recognised by the replication mechanism. It shall replicate to all co-operating systems/nodes that have been configured to exchange this information.

Requirement ID: SRS-1232

•E-NPKI shall allow an authorised subscriber to choose a full replication of selected data types from source to destination database.

Requirement ID: SRS-1233

•E-NPKI shall replicate new data that is inserted in the source database.

Requirement ID: SRS-1234

•E-NPKI shall allow an authorised subscriber to selectively identify the data to be replicated.

Requirement ID: SRS-1235

•E-NPKI shall allow E-NPKI System Administrators to configure to whom (i.e., what systems/nodes) information flows.

Requirement ID: SRS-1236

•E-NPKI shall allow an authorised subscriber to specify intervals of replication.

4.2.2 Architectural Constraints

4.2.2.1 General

Requirement ID: SRS-1239

•E-NPKI shall be compliant with the standards given in the section "Applicable Standards". Any proposed deviation shall be approved by the Purchaser.

Requirement ID: SRS-1244

•E-NPKI shall, where applicable, make use of REST architecture to make resources available over a URL in promotion of interoperability.

4.2.2.2 COTS selection and integration

Requirement ID: SRS-1250

•E-NPKI shall be based on COTS in its architecture in place of dedicated solutions when the functionalities of a COTS matches the requirements for a Service with no or minimal adaptation.

Requirement ID: SRS-1251

•When no or minimal adaptation is necessary for the COTS integration, E-NPKI shall use COTS with no additional layer to masquerade nor shield the COTS and the complete functionalities of the COTS shall be available to E-NPKI Services.

Requirement ID: SRS-1252

•E-NPKI adaptations shall be delivered as additional modular Services that complement the COTS native functionalities.

4.3 Documentation Requirements

4.3.1 On-line Help

4.3.1.1 General

Requirement ID: SRS-1341

•E-NPKI is used by organizations in various time zones throughout NATO territories and other areas of NATO operations. During crisis, use of E-NPKI will be high and over extended working hours. Full on-line help capability shall be required to supplement the E-NPKI help-desks.

Requirement ID: SRS-1342

•E-NPKI shall support on-line help describing all functionality of the E-NPKI capability.

Requirement ID: SRS-1343

•The E-NPKI on-line help shall translate every use case and usage scenario into a browsing sequence. Every browsing sequence shall be structured according to the subscriber workflow.

Requirement ID: SRS-1344

•E-NPKI on-line help shall describe each E-NPKI function, the interrelationships between and the logical sequence of functions.

Requirement ID: SRS-1345

•E-NPKI on-line help shall explain all menu items, dialog windows, data entry and query fields implemented in the E-NPKI Product Baseline.

Requirement ID: SRS-1346

•The E-NPKI on-line help shall include a glossary providing definitions of all terms and acronyms implemented in the E-NPKI Product Baseline.

Requirement ID: SRS-1347

•All definitions in the E-NPKI glossary shall be available in roll-over, pop-up windows linked to every appearance in on-line help of the corresponding term or acronym.

Requirement ID: SRS-1348

•In E-NPKI, each dialogue, menu item, toolbar item, function, field or button (each item on the screen) shall have an on-line help option. This shall be clearly visible, but not intrusive.

Requirement ID: SRS-1349

•The E-NPKI on-line help function shall provide meaningful advice and hints to subscribers appropriate to the actions they are trying to take.

Requirement ID: SRS-1350

•The E-NPKI on-line help shall be concise, compact and clear to the subscriber.

Requirement ID: SRS-1351

•The on-line help shall include snapshots of E-NPKI screens, windows, and dialogue boxes. The snapshots shall be provided in a suitable lightweight format (e.g., GIF, PNG) approved by the Purchaser.

Requirement ID: SRS-1352

•Pictures in the E-NPKI on-line help showing more than five GUI elements/controls shall have a clickable image map describing each element.

Requirement ID: SRS-1353

•If the E-NPKI on-line help topic requires a large picture that does not fit on a normal page, a reduced copy shall be additionally included on the Help page that expands to its full size on subscriber request.

Requirement ID: SRS-1354

•The E-NPKI on-line help shall be context-sensitive (i.e., based on a specific point in the state of the software and providing help for the situation that is associated with that state on action being performed).

Requirement ID: SRS-1355

•All context-sensitive GUI elements in the on-line help shall be linked to the relevant subscriber Manual topics.

Requirement ID: SRS-1356

•In E-NPKI, all source code elements shall be configured to link the GUI elements to their context-sensitive topics.

Requirement ID: SRS-1357

•E-NPKI shall contain help functions that provide access to interactive training sessions to guide subscribers through procedures and functions.

Requirement ID: SRS-1358

•The E-NPKI on-line help shall be given by a small pop-up screen or infotip screen. This screen shall appear quickly and be very easy to hide, for instance clicking anywhere within it.

Requirement ID: SRS-1359

•E-NPKI on-line help shall open a dedicated web page when the subscriber request access to the full content of the on-line help. The on-line help shall not be preventing the subscriber to perform on the E-NPKI GUI.

Requirement ID: SRS-1360

•E-NPKI shall allow the subscriber to hide the on-line help screen just by clicking anywhere else, or there shall be another single action hiding mechanism.

4.3.1.2 Help Search

Requirement ID: SRS-1362

•The E-NPKI on-line help shall be organised in the following two sections:

•Contents, providing access to all help pages and organized in a logical manner by topic or procedure

•Index, providing subscribers with both the ability to search for keywords in all Help pages and retrieve a list of those pages in which those keywords appear and the ability to select and trigger such a query from a list of all keywords.

Requirement ID: SRS-1363

•E-NPKI shall be able to display search query results for finding help items in the online help in a list. E-NPKI shall display the help item when the subscriber selects a query result in this list.

4.3.1.3 Help Format

Requirement ID: SRS-1365

•The E-NPKI on-line help shall be prepared as a compiled/scripted HTML help file (.chm) which shall include all project-related source elements and graphics.

4.3.1.4 Frequently Asked Questions (FAQ)

Requirement ID: SRS-1367

•E-NPKI shall provide a list of Frequently Asked Questions. FAQs shall be available to support the NCIA Help Desk and other support organisations.

Requirement ID: SRS-1368

•E-NPKI shall allow the subscriber to display the E-NPKI FAQ.

Requirement ID: SRS-1369

•E-NPKI shall allow the subscriber to search the E-NPKI FAQ

Requirement ID: SRS-1370

•E-NPKI shall allow the E-NPKI subscriber or E-NPKI Administrator to ask questions to the NCIA Help Desk in electronic form by using the E-NPKI FAQ.

Requirement ID: SRS-1371

•E-NPKI shall support answering the E-NPKI subscriber or E-NPKI Administrator questions by sending back existing or newly-added FAQ entries.

4.3.2 Target Architecture

Requirement ID: SRS-1373

•E-NPKI shall be equipped with an E-NPKI Target Architecture (TA) Document.

Requirement ID: SRS-1374

•The E-NPKI Target Architecture Document shall describe:

•General description of the E-NPKI modules, services and components and their relations

•The static structure of the E-NPKI modules, services and components

•The dynamic behaviour of the E-NPKI modules, services and components

•How data is persisted by the E-NPKI modules, services and components

Requirement ID: SRS-1375

•The E-NPKI Target Architecture Document shall be compliant with the NATO Architecture Framework (v3) views.

Requirement ID: SRS-1376

•The E-NPKI Target Architecture Document shall be delivered in a structured data format such as XML files or structured database suitable for use in a commercial architecture tool and reused in the NAR. Images and drawings (MS Visio, PowerPoint) can be supporting the TA, but shall not be accepted as the TA.

Requirement ID: SRS-1377

•The E-NPKI Target Architecture Document shall be delivered in a structured format compatible for incorporation in the NATO Architecture Repository (NAR):

•[TOOL_SUITE_NAME] tool suite; used for documenting and publishing the process models

•Microsoft Excel; Used for publishing a selection of the architecture views (matrixes);

•Microsoft Visio; Used for publishing a selection of the architecture views (as drawings);

•Microsoft PowerPoint; Used publishing a selection of the architecture views (as drawings);

•Microsoft Word; Used for publishing a selection of the architecture views (descriptions).

4.4 Security Requirements

4.4.1 Compliance with Bi-SC AIS Security Requirements

4.4.1.1 Web Security Features

4.4.1.1.1 Validation of Input

Improper validation of input from web requests may expose vulnerabilities that an attacker can use to attack backend end components (e.g., databases) through the web application.

Requirement ID: SRS-1484

•E-NPKI shall ensure that all input values are validated before they are used, including:

•Data types (e.g., string, integer, real)

•Allowed character sets

•Minimum and maximum length

•Whether null is allowed

•Whether the actual parameter is required or not

•Whether duplicates are allowed

•Numeric range

•Specific patterns (e.g., regular expression)

Requirement ID: SRS-1485

•E-NPKI shall automatically validate entries into E-NPKI Services to ensure they conform to the required formats and limits.

Requirement ID: SRS-1486

•E-NPKI shall automatically verify entries into E-NPKI Services to ensure the subscriber is authorised to effect such changes.

4.4.1.1.2 Enforcement of Access Control

Improper access control features can be exploited to access other subscribers' accounts, view sensitive files or use unauthorized functions.

Requirement ID: SRS-1489

•E-NPKI shall ensure that privilege restrictions of authenticated E-NPKI Trusted Roles are properly enforced.

Requirement ID: SRS-1490

•E-NPKI shall not rely on the secrecy of identification information (i.e., IDs) for protection.

Requirement ID: SRS-1491

•E-NPKI shall prevent 'forced browsing' past access control checks. For purposes of this document, forced browsing is an attack the aim of which is to enumerate and access resources that are not referenced by the application, but still can be accessible.

Requirement ID: SRS-1492

•E-NPKI shall prevent 'path traversal' attacks. For purposes of this document, a path traversal attack is one that aims to unauthorised navigate through the file system and access files and directories that are stored outside web root folder, particularly by manipulating variables that reference files with 'dot-dot-slash (../)' sequences. Path traversal attacks includes providing relative path information as part of a request (e.g., ../../etc/passwd).

Best practices suggest that most directories should not be readable, and very few files, if any should be marked executable.

Requirement ID: SRS-1493

•E-NPKI shall securely configure and enforce file permissions. Unless specifically authorised by the Purchaser, only files that are specifically intended to be presented shall be marked as readable.

Requirement ID: SRS-1494

•E-NPKI shall prevent compromise of information via client-side caching, including best practice use of mechanisms such as HTTP headers and meta tags.

4.4.1.1.3 Authentication and Session Management

Improper protection of account credential or session may compromise passwords, keys, session cookies or other tokens, allowing an attacker to bypass authentication restrictions or assume other subscribers' identities

Requirement ID: SRS-1498

•E-NPKI shall enforce 'strong passwords'. The minimum length of E-NPKI subscriber passwords shall be configurable.

Requirement ID: SRS-2115

•The use of alpha, numeric and special symbols within E-NPKI subscriber passwords shall be configurable.

Requirement ID: SRS-1499

•E-NPKI shall require subscriber's passwords to be changed within a period configurable for the security domain.

Requirement ID: SRS-1501

•E-NPKI shall deny the re-use of a configurable number of previous passwords.

Requirement ID: SRS-1502

•E-NPKI shall lock subscriber smartcards for which a configurable number of failed login attempts have been made to await administrator action. By default, E-NPKI shall lock subscriber accounts after ten failed login attempts.

Requirement ID: SRS-2735

•E-NPKI shall lock subscriber software cryptographic modules for which a configurable number of failed login attempts have been made to await administrator action. By default, E-NPKI shall lock subscriber accounts after five failed login attempts.

Requirement ID: SRS-1504

•Failed logins into E-NPKI shall be logged.

Requirement ID: SRS-1505

•E-NPKI shall enforce password change control. To change a password, the subscriber shall be required to provide both their current password and the new password. The new password shall require entering twice to make sure the subscriber doesn't make any mistakes when entering the new password.

Requirement ID: SRS-1506

•E-NPKI shall protect authentication details (i.e. passwords) in storage. All authentication details shall be stored in either hashed or encrypted form to protect them from exposure, regardless of where they are stored.

Requirement ID: SRS-1507

•In situations where a plaintext password is required, E-NPKI shall use encryption to store the password. Passwords shall not be hard-coded in any source code. Decryption keys shall be strongly protected to prevent unauthorised access.

Requirement ID: SRS-1508

•E-NPKI shall protect subscriber credentials in transit. E-NPKI shall employ encryption of the entire login transaction using TLS or similar technologies. This requirements shall only be applicable for the option when no domain authentication is used.

Requirement ID: SRS-1509

•E-NPKI shall protect session IDs. E-NPKI shall protect the subscriber's entire session via TLS to ensure that the session ID (e.g., session cookie) cannot be read off the network. Session IDs shall never be included in any URL or sent in the referrer header to prevent caching by the browser. Session IDs shall be long, complicated random numbers which cannot be easily guessed. Session IDs chosen by a subscriber shall not be accepted.

Requirement ID: SRS-1510

•E-NPKI shall allow the system administrator to set a "timeout" period which shall automatically log-out any sessions which have been inactive for that period of time. The system administrator shall be able to disable this feature.

4.4.1.1.4 Cross-Site Scripting (XSS)

Without proper protection, a web application can be used as a mechanism to transport an attack to an end subscriber's browser, causing a subscriber's web browser to execute a malicious script. A successful attack can disclose an end subscriber's session token, attack the local machine or spoof content to fool the subscriber.

Requirement ID: SRS-1514

•E-NPKI shall perform validation of all headers, cookies, query strings, form fields and hidden fields.

Requirement ID: SRS-1515

•E-NPKI shall ensure that the HTTP TRACE method is turned off on all web servers to prevent compromise of cookie data.

Requirement ID: SRS-1516

•E-NPKI shall encode subscriber-supplied output to prevent XSS.

4.4.1.1.5 Injection Flaws (SQL)

Web applications pass certain parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application. Injecting valid SQL queries through the Username and password fields could allow the application to send the query through to the database, allowing the attacker to query the database or authenticate using someone else's credentials

Requirement ID: SRS-1519

•E-NPKI shall constrain the input by validating it for type, length, format and range.

Requirement ID: SRS-1520

•E-NPKI shall use type-safe SQL parameters. Input shall be treated as a literal value, and E-NPKI shall not treat it as executable code.

Requirement ID: SRS-1521

•E-NPKI shall use filter routines that sanitise the code, adding escape characters that have special meaning to SQL.

Requirement ID: SRS-1522

•E-NPKI shall create custom error pages to prevent server error messages from being disclosed.

4.4.1.1.6 Buffer Overflow

Web application components that do not properly validate input can be 'crashed', and in some cases used to take control of a process. These components can include CGI, libraries, drivers and web application server services or components. An attacker may take full control of the system being targeted or kill a process.

Requirement ID: SRS-1525

•E-NPKI shall be configured with the latest patches to the web and application server products.

Requirement ID: SRS-1526

•E-NPKI shall ensure that application code which accepts input from subscribers via the HTTP request provides appropriate size checking on all inputs.

4.4.1.1.7 Improper Error Handling

Improper handling of error conditions which occur during normal operation can expose vulnerabilities. If an attacker can cause errors to occur that the web application cannot handle, they may gain detailed system information, deny service, cause security mechanisms to fail or, in some cases, crash the server.

Requirement ID: SRS-1529

•E-NPKI shall use custom error pages to prevent server error messages from being disclosed.

4.4.1.1.8 Application Denial of Service

Due to Application coding errors, it may be possible for an attacker to consume web application resources to a point where other legitimate subscribers can no longer access or use the application. Attackers may also be able to lock subscribers out of their accounts or cause the entire application to fail.

Requirement ID: SRS-1535

•E-NPKI shall protect against application denial of service.

Requirement ID: SRS-1537

•E-NPKI shall limit the number of requests a subscriber can have active at any one time.

4.4.1.1.9 Unsecured Configuration Management

A strong server configuration standard is critical to secure a web application. These servers have many configuration options that affect security and are not generally secure by default. For example, if a web application is not secured, an attacker may be able via directory traversals to get to directories where passwords are stored.

Requirement ID: SRS-1541

•E-NPKI security mechanisms shall be properly configured according to best practices:

•Disabling unused services on the E-NPKI servers

•Disabling default accounts, and accounts no longer used

•Correctly configuring permissions and accounts

•Correctly configuring logging and alerts

Requirement ID: SRS-1542

•E-NPKI components shall be configured with the latest security patches and updated with the latest security guidelines from NATO.

4.4.1.2 File System

Requirement ID: SRS-1544

•E-NPKI shall support access to the underlying file system using Windows standards, including Long File Names and legal naming characters.

Requirement ID: SRS-1545

•E-NPKI shall allow saving to and opening from (Secure) Bi-SC AIS-supported devices, including:

•Local drives,

•NTFS drives,

•FAT32 drives,

•Remote (network) machines mapped by drive letters and UNC paths,

•Compressed/uncompressed drives.

4.4.2 Confidentiality

Confidentiality is defined as ensuring that data is not disclosed to unauthorised parties, usually through the use of encryption

Requirement ID: SRS-1626

•In line with C-M(2002)49-COR5, the Security Classification in E-NPKI shall include:

•Policy Identifier/ Information Ownership: e.g., NATO, NATO/EAPC (Euro-Atlantic Partnership Council), RS (Resolute Support);

•Classification Marking: e.g., Unclassified, Restricted, Confidential, Secret;

•Category/Caveats: e.g., Releasable to AUS/FIN, Releasable to ISAF, Releasable to Coalition.

Requirement ID: SRS-1627

•In E-NPKI system components, the Security Classification of sensitive information shall be established as a domain value as part of the security accreditation process.

Requirement ID: SRS-1630

•E-NPKI shall insert a Security Classification construct into headers/footers and metadata of generated, created or exported reports, MS Office files and PDF files. The subscriber shall be prompted during the process.

•By default E-NPKI shall propose the highest classification level of the selected objects.

•If no classification is specified for the selected objects, then the repository classification level shall be proposed.

•The subscriber shall be able to override the proposed classification level by choosing another.

Requirement ID: SRS-1631

•If a file is being generated or exported in a format that does not use headers/footers, E-NPKI shall include a Security Classification into an appropriate part of the file so that it is clearly visible to the subscriber.

4.4.3 Data Protection Policy

4.4.3.1 General

4.4.3.2 Protection of System and Information

Requirement ID: SRS-1636

•E-NPKI shall ensure that the system, the information and functionalities are only available to authorised subscribers using authorised functionality.

Requirement ID: SRS-1637

•E-NPKI shall ensure that access to system and information available subscribers only via authorised E-NPKI applications, unless specifically authorised.

Requirement ID: SRS-1638

•E-NPKI shall ensure that mechanisms to provide access to system and information via authorised E-NPKI applications shall not, as a side effect, also provide access via non-authorised applications.

Requirement ID: SRS-1642

•E-NPKI shall contain residual information protection mechanisms to ensure that deleted information is no longer accessible.

Requirement ID: SRS-1643

•E-NPKI shall ensure that newly created objects do not contain information that shall not be accessible.

4.4.3.3 Protection of Personal Information

Requirement ID: SRS-1651

•E-NPKI shall provide protection and management of Personal Information.

4.4.4 Preservation of Digital Information of Permanent Value

4.4.4.1 Content

Content for long-term preservation can be distinguished by seven major types:

•Data sets

•Text

•Still Images

•Moving Images

•Sound

•Geospatial

•Web archive

Requirement ID: SRS-1660

•E-NPKI shall be able to present digital information of permanent value in a sustainable format suitable for long-term preservation.

4.4.4.1.1 Data sets

Data sets are collections of individual value or larger coherent structures such as messages. The data set might be an export from a database or the results of an information exchange between systems.

There is typically a structure associated with the data set, either implicitly contained within the data set (e.g. a table structure of an Excel document or a database), or explicitly defined (e.g. as a schema definition)

Requirement ID: SRS-1663

•E-NPKI shall preserve structured and unstructured data for future analysis

Requirement ID: SRS-1664

•E-NPKI shall preserve the logical structure of datasets as well as syntax and semantics of elements within the dataset.

Requirement ID: SRS-1665

•E-NPKI shall preserve data types and data structures.

4.4.4.1.2 Web archive

The web archive type concern the archival of entire web sites, portals, or parts of them. While some information might be contained in static web pages and is therefore easy to capture, other parts might be dynamically rendered.

Web archives typically contain structured textual descriptions as well as still and moving images.

Requirement ID: SRS-1715

•E-NPKI shall preserve the structure and content of the web, including any script.

Requirement ID: SRS-1716

•E-NPKI shall include any necessary external content.

Requirement ID: SRS-1717

•E-NPKI shall preserve all metadata associated with web content.

It will be taken into account that dynamic/interactive or user-specific content is problematic towards its preservation.

Requirement ID: SRS-1719

•The format for archiving web sites and/or portal shall be any of the following:

•ISO 28500:2009, Information and documentation -- WARC file format.

•IETF RFC 2557, MIME Encapsulation of Aggregate Documents, such as HTML (MHTML)

4.4.5 Data Definition

Requirement ID: SRS-1721

•If the Content consists of structured data, a separate Data Definition shall be included to describe the logical structure of the Content. This is primarily applicable to Content of the following types:

•Data Set

•Geospatial

•Web Archive

Requirement ID: SRS-1722

•The format of the Data Definition shall be XML Schema 1.1.

4.4.6 Metadata

Requirement ID: SRS-1724

•All content in E-NPKI for long-term preservation shall be accompanied by descriptive and administrative metadata, following a set of metadata elements.

Requirement ID: SRS-1725

•The SIP metadata shall follow the NATO Core Metadata Specification (NCMS) [AC/322-

•D(2014)xxxx, 2014] and the NATO Labelling Specification [AC/322-D(2014)yyyy/zzz, 2014].

Visualization

Optionally, a human readable representation or visualization of the E-NPKI Content in its original context can be included as an optional item. E.g., screenshots or diagrams that illustrate the environment in which the Content was used.

Requirement ID: SRS-1728

•The format used for the context information shall be one of those listed for the various types of Content.

4.4.7 Packaging

Requirement ID: SRS-1730

•E-NPKI shall package the Content, Data Definition and Visualization information into a single digital object.

Requirement ID: SRS-1731

•E-NPKI documentation related to information of permanent value shall be maintained and shall be included as part of the package submitted for long-term preservation

4.4.8 Authentication

Authentication is defined as the verification of the identity of the subscriber or consumer of a service or application

4.4.8.1 General

4.4.8.2 Authentication Processing

Requirement ID: SRS-1598

•E-NPKI shall uniquely Identify and strongly Authenticate (I&A) subscribers.

Requirement ID: SRS-1599

•E-NPKI shall allow an authorised subscriber (i.e. E-NPKI Admin) to manage (create, update, delete) E-NPKI subscriber Accounts, password details, and assign subscriber Roles to subscriber Account and manage general access privileges of individual subscriber Accounts.

Requirement ID: SRS-1602

•When a subscriber is authenticated in E-NPKI, the subscriber shall be assigned with the Roles for that subscriber.

Requirement ID: SRS-1603

•If a subscriber has more than one Basic Role, the subscriber shall be prompted to choose one of the Basic Roles in E-NPKI for that session.

Requirement ID: SRS-1605

•E-NPKI shall integrate with existing users management systems from the Bi-SC AIS: NATO Enterprise Directory Service.

Requirement ID: SRS-1607

•E-NPKI shall implement an authentication service that requires the subscriber to authenticate using their E-NPKI credentials.

Requirement ID: SRS-1610

•E-NPKI shall provide privileged E-NPKI accounts (e.g., RA and CA administrator accounts).

Requirement ID: SRS-1611

•Within E-NPKI an authorised subscriber shall have a set of access rights (data and applications) such that these rights can be maintained.

Requirement ID: SRS-1612

•The interval for password change in E-NPKI shall be configurable.

Requirement ID: SRS-1613

•E-NPKI shall allow authenticated subscribers to manage their password and information from their subscriber profile for which E-NPKI is the authoritative data source.

Requirement ID: SRS-1614

•E-NPKI shall provide help texts to support the login process together with links to recover lost password and login details.

4.4.9 Authorisation

Authorisation consists of ensuring that the consumer is able to perform a particular action on a resource.

Requirement ID: SRS-1618

•The term 'authorised subscriber' as used within this E-NPKI document shall be interpreted as authenticated subscribers specifically authorised to view the relevant information or perform the relevant function.

Requirement ID: SRS-1619

•If an (authenticated) E-NPKI subscriber is a member of more than one Organization (i.e. Organizational Node), the subscriber shall be prompted to select the Organization to be used during that session.

Requirement ID: SRS-1621

•E-NPKI shall allow two or more subscribers to have the same Role simultaneously.

4.5 Computer Resource Requirements

4.5.1 Hardware and Software Components

Requirement ID: SRS-1740

•E-NPKI shall support the following environment configuration for the client workstation:

•Operating System: Microsoft Windows 7 and later including 32-bit and 64-bit editions

•Components: Microsoft .NET Framework version 4.5 or later.

Requirement ID: SRS-2804

•The client OS version shall be decided as close as possible to BLAT milestone.

Requirement ID: SRS-1741

•E-NPKI shall support the following environment configuration for the server components:

•Operating System: Microsoft Windows Server 2012 and later.

•Web Server: Internet Information Services (IIS) version as per OS used.

• (Use of TOMCAT or JETTY can be approved upon request)

Requirement ID: SRS-2805

•The server OS version shall be decided as close as possible to BLAT milestone.

Requirement ID: SRS-1742

•E-NPKI shall work nominally with the following hardware configuration for the standalone and client applications:

•Workstation: Desktop or Laptop

•CPU: Intel Core 2 Duo E8200 or equivalent

•RAM Internal Memory: 2GB

•Available Hard Disk Space: 4GB

•Graphics card: Integrated Graphics Intel 4000HD or equivalent

•Monitor: 15" screen with a resolution of 1280x1024.

Requirement ID: SRS-1744

•The infrastructure requirements of a service or application shall not be designed and deployed with a “per service, per application” approach but shall be covered through a harmonized “infrastructure services” approach applicable to all services and applications making use of the infrastructure services.

Requirement ID: SRS-1745

•The Contractor shall identify the requirements from the infrastructure services NOT in terms of component specifications, but in terms of service parameters such as:

•Virtual Machine units of specified CPU, Memory, Disk Capacity, Disk I/O, Network Bandwidth and Network I/O parameters.

•Number of Virtual Machine units

•Security Classification of the targeted Network

•Cross Domain Information Exchange Requirements

Requirement ID: SRS-1746

•The Virtual Machine Performance Parameters shall be scaled NOT TO EXCEED 30% LOAD on average in 24 hours.

Requirement ID: SRS-1748

•The E-NPKI software shall be compatible with the native file system of NATO Server Baseline.

Requirement ID: SRS-1749

•The E-NPKI software shall not have any direct dependency to the physical parameters of the storage environment (such as disk type, connection type, SAN topology, SAN protocol).

Requirement ID: SRS-1750

•The E-NPKI software shall not have any hard coded UNC, File Path, Drive Letter or similar storage location settings.

Requirement ID: SRS-1751

•All UNC, File Path, Drive Letter or similar storage location settings shall be parametric, configurable, and possible to automate for unattended installation, backup, recovery.

Requirement ID: SRS-1752

•The E-NPKI software shall not have any hard coded URL, DNS or IP Address settings. All URL, DNS, IP Addressing and similar network settings shall be parametric, configurable, and possible to automate for unattended installation, backup, recovery.

Requirement ID: SRS-1753

•The server deployment package (virtual appliance or installation package) shall be tested against the following hypervisors, configured in accordance with NATO Security Settings:

•VMWare ESXi 4.0 and later

•Microsoft Hyper-V 2008 and later

Requirement ID: SRS-1754

•E-NPKI Client functionality shall be tested against NATO Desktop Baseline.

Requirement ID: SRS-1755

•E-NPKI SMC integration shall be tested against NATO EMS.

4.5.2 Configuration Management Tools

Requirement ID: SRS-1757

Requirement deleted.

4.6 Interoperability

Interoperability is defined as the capability of the software product to interact with one or more specified systems.

4.6.1 General

Requirement ID: SRS-1764

•For each specified interface (i.e., inputs and outputs to E-NPKI and between E-NPKI and another systems), E-NPKI shall be equipped with an Interface Control

Document (ICD) describing the interface. The content shall include, where applicable, the following information:

•A list of the applicable technical standards

•A catalogue of the services and interfaces exposed by E-NPKI

•A detailed description of the interfaces, including diagrams, data elements, data formats, performance values, communication protocols, security settings, etc.

•Descriptions of data elements

•units of measure required for the data element, such as seconds, meters, kilohertz, etc.,

•limit/range of values required for the data element (for constants provide the actual value),

•accuracy required for the data element,

•precision or resolution required for the data element in terms of significant digits,

•frequency at which the data element is calculated or refreshed, such as 10 KHz or 50 Msec,

•legality checks performed on the data element,

•data type, such as integer, ASCII, fixed, real, enumerated, etc.

•data representation/format,

•priority of the data element,

•Service Descriptors, identifying the services endpoints, a detailed description of the of the service operations and service parameters.

•All related artefacts such as WSDL, schema files and descriptors.

•Message descriptions,

•Interface priority,

•Communications protocol.

4.6.2 Interface Mechanisms

Requirement ID: SRS-1766

- The following interface mechanisms shall be used in E-NPKI:

•Web Services

•File exchange,

•Direct database and file access,

•API.

•Simple Certificate Enrolment Protocol (SCEP)

•PKIX CMP

•LDAP

•LDAP over SSL (LDAPS)

•EST

4.6.2.1 Web Services

4.6.2.1.1 General

Web Services are intended to provide self-describing, self-contained, modular units of software application logic that provide defined business functionality. Web Services are consumable software services that typically include some combination of business logic and data. Web Services can be aggregated to establish a larger workflow or business transactions. Inherently, the architectural components of web services support messaging, services description, registries and loosely coupled interoperability.

E-NPKI support for Web Services is required to enable applications to streamline the sharing of data across different functional services, support integration, and reduce development time of new capabilities.

Requirement ID: SRS-1772

•E-NPKI shall provide an implementation supported by Extensible Mark-up Language (XML) technology for all external interfaces.

Requirement ID: SRS-1773

•All Web Services published by E-NPKI shall adapt a single, consistent exception handling and reporting mechanism.

Requirement ID: SRS-1775

•E-NPKI shall avoid the practice, as both a publisher and consumer, of treating web services as a high frequency, poll-able call.

Requirement ID: SRS-1776

•E-NPKI shall observe the best practice of preferring primitive types for web service parameters.

Requirement ID: SRS-1777

•E-NPKI shall consider the best practice of avoiding long running web services to be a design goal.

Requirement ID: SRS-1778

•E-NPKI shall observe best practice and prefer message-based interactions over the remote procedure call (RPC) style while implementing web services.

4.6.2.1.2 Web Service Standards

Requirement ID: SRS-1784

•E-NPKI shall use World Wide Web Consortium (W3C), Web Services Interoperability Organization (WS-I), Internet Engineering Task Force (IETF) and Organization for the Advancement of Structured Information Standards (OASIS) ratified standards (WS-* and otherwise) in the implementation of Web Services.

Requirement ID: SRS-1785

•E-NPKI shall specify the syntax of the XML documents it accepts and produces.

Requirement ID: SRS-1787

•E-NPKI shall provide W3C XML schemas to express all XML file formats.

Requirement ID: SRS-1788

•E-NPKI shall validate all received XML files against the schemas published by the suppliers.

Requirement ID: SRS-1789

•E-NPKI shall use the SOAP XML format to exchange information between the service provider and the service requester.

Requirement ID: SRS-1791

•E-NPKI shall use the Web Service Description Language (WSDL) XML format to describe the web services provided.

Requirement ID: SRS-1795

•E-NPKI Web Services shall be compliant with the Web service security standards in reference [WS-Security].

Requirement ID: SRS-1796

•E-NPKI Web Services shall be compliant with the digital signature standards in reference [XML-DigitalSignature].

Requirement ID: SRS-2737

•E-NPKI Web Services shall be compliant with the encryption standards in reference [XML-Encryption].

Requirement ID: SRS-1797

•E-NPKI Web Services shall be compliant with the SAML standards in reference [WS-SAML].

Requirement ID: SRS-1798

•E-NPKI Web Services shall be compliant with the X509 Token standards in reference [WS-X509].

4.6.2.1.3 Web Service Security

Requirement ID: SRS-1815

•E-NPKI Web Services shall be demonstrated to meet the non-functional security requirements specified in this document to include authentication, authorisation, confidentiality, integrity and non-repudiation.

Requirement ID: SRS-1816

•E-NPKI web services shall be compliant with OASIS WS-Security set of specifications for publishing and consuming web services.

Requirement ID: SRS-1817

•E-NPKI Web Services shall support auditing and non-repudiation.

Requirement ID: SRS-1818

•E-NPKI Web Services shall support point-to-point integrity.

Requirement ID: SRS-1819

•E-NPKI Web Services shall support point-to-point confidentiality.

Requirement ID: SRS-1820

•E-NPKI Web Services shall incorporate authorisation according to the Role-based Access mechanisms.

Requirement ID: SRS-1821

•E-NPKI Web Services shall incorporate authentication.

Requirement ID: SRS-1822

•E-NPKI shall implement role based access to access external services and service operations.

Requirement ID: SRS-1823

•E-NPKI shall use approved X.509 certificates produced by the responsible E-NPKI Trusted Role

Requirement ID: SRS-1824

•E-NPKI shall sign a validated service request to external services using its Bi-SC AIS credentials defined in its X.509 certificate.

Requirement ID: SRS-1825

•E-NPKI shall only accept data signed by external services with valid X.509 certificates.

4.6.2.1.4 Web Interface Requirements

Requirement ID: SRS-2742

•The E-NPKI system shall provide web interfaces to support Registration Authority activities defined within this SRS including but not limited to user provisioning, CSR approvals, key recovery, certificate revocation, and password resets.

Requirement ID: SRS-2743

•The E-NPKI system shall provide the user with a self-service kiosk to support common user functionality defined within this SRS including but not limited to certificate requests, rekey, and password recovery,

Requirement ID: SRS-2744

•The E-NPKI system shall provide sponsors with a web service interface to support common device functionality defined within this SRS including but not limited to certificate requests, CSR uploading, certificate downloading, and certificate revocation.

4.6.2.2 File Exchange

Requirement ID: SRS-1839

•File exchange shall be required, in some instances, to enable the exchange of information between systems for reasons of legacy, security, connectivity, capability or efficiency. Bespoke file formats, where possible, shall use XML as the primary mechanism for file-level information exchange.

Requirement ID: SRS-1840

•E-NPKI shall provide adequate documentation for the content and meaning of the file formats it produces or accepts. An adequate definition is one that enables a programmer or subscriber to understand the meaning of the data and determine whether it is suitable for its intended use. E-NPKI shall supply a definition for every element, attribute, and enumeration value defined in the file format.

Requirement ID: SRS-1841

•E-NPKI shall, to the extent possible, validate the format and contents of all incoming and outgoing files according to the documented format.

4.6.2.3 Direct Database and File Access

Requirement ID: SRS-1845

•E-NPKI shall not allow external direct access to the database supporting the E-NPKI capability.

Requirement ID: SRS-1846

•In E-NPKI, the direct database access mechanism shall limit access of authenticated and authorised Users/Systems to information items (e.g., records,

files) and structures (e.g., tables, directories) required to perform the authorised function.

Requirement ID: SRS-2736

•The E-NPKI shall be capable of direct database connectivity to external Physical Access Control systems via an ODBC compliant interface.

4.6.3 Interfaces

4.6.3.1 General

4.6.3.2 Bi-SC AIS Program Components

4.6.3.2.1 General

Requirement ID: SRS-1865

•Data sharing with external systems shall be established according to Interface Agreements made with the controlling authority for each external system.

Requirement ID: SRS-1866

•E-NPKI shall support the automated exchange of information between related systems in order to improve the timeliness and accuracy of the information and to reduce the manual data capture, management, and presentation workload of planning personnel using their respective systems.

Requirement ID: SRS-1867

•E-NPKI shall interface and function correctly with the NGCS network and security infrastructure.

Requirement ID: SRS-1868

•E-NPKI shall, as a design goal, minimise the number of different types of interfaces supported to meet interoperability requirements.

4.6.3.2.2 Bi-SC AIS Core Services

4.6.3.2.2.1Directory services

Requirement ID: SRS-2190

•E-NPKI shall integrate with NATO Enterprise Directory Service (NEDS) for the retrieval and storage of data.

Requirement ID: SRS-2191

•E-NPKI shall publish the following artefacts to NEDS:

• - CA Certificates;

• - End-entity certificates;

• - CRLs;

- - ARLs

Requirement ID: SRS-2192

•E-NPKI shall be compliant with the latest ratified version of ACP 133 (See REF: SOW 2.1.4.5).

4.6.3.2.2.2 Enterprise Management System

Requirement ID: SRS-1882

•Errors and suggested corrective actions in E-NPKI shall be reported to the Bi-SC AIS Enterprise Management Services (EMS) automatically.

4.6.3.2.2.3 E-mail Services

Requirement ID: SRS-1884

•E-NPKI shall be integrated with the Bi-SC AIS E-mail Services based on MS Exchange.

Requirement ID: SRS-1885

•E-NPKI shall be compatible with Bi-SC AIS E-mail services and protocols

Requirement ID: SRS-1886

•E-mail messages produced by E-NPKI to be provided to the Bi-SC AIS E-mail Services shall be compatible with the formats used in the Bi-SC AIS (e.g., classification header).

4.6.3.2.2.4 Security Services

Requirement ID: SRS-1889

•E-NPKI shall coexist (i.e., work correctly and not adversely impact other applications) with the current NATO security settings for Client and Server.

Requirement ID: SRS-2598

•The set of NATO security settings against which E-NPKI shall comply will be identified by the Purchaser during the Design Stage.

Requirement ID: SRS-1890

•E-NPKI shall work without change to the NATO security settings. Any changes to the standard security settings shall be submitted for approval to the Purchaser not later than the Design Stage.

Requirement ID: SRS-1891

•E-NPKI shall coexist (i.e., work correctly and not adversely impact other applications) with Bi-SC AIS standard anti-virus software during installation and operation.

Requirement ID: SRS-1893

•E-NPKI shall ensure that no security warnings are generated in the applicable system log as a result of normal E-NPKI operation.

4.6.3.2.2.5 Collaboration Services

Requirement ID: SRS-1896

•E-NPKI shall be integrated with the Bi-SC AIS Collaboration Services.

Requirement ID: SRS-1897

•E-NPKI shall be compatible with Bi-SC AIS Collaboration services and protocols (e.g., SIP).

4.6.3.2.2.6 Infrastructure Services

4.6.3.2.2.6.1 DNS

The Domain Name System (DNS) allows the Fully Qualified Domain Names (FQDN) of hosts to be resolved to IP addresses.

Requirement ID: SRS-2193

•E-NPKI shall integrate with the existing DNS infrastructure.

Requirement ID: SRS-2194

•E-NPKI shall use FQDNs for identifying all hosts, unless specifically requested not to.

4.6.3.2.2.6.2 Load Balancing

Load Balancing allows requests to services to be assigned to different instances of those services, transparently to the subscriber. There are a number of different mechanisms for implementing Load balancing, including DNS and hardware-based load balancing.

4.6.3.3 Communication Interface

Requirement ID: SRS-1908

•E-NPKI shall provide an interface with write-once ISO CDFS as an alternate communication interface (input and output), according to NATO Policy on CD-ROM.

Requirement ID: SRS-1909

•E-NPKI shall provide a mechanism for exchange of information with other Institutions and this mechanism shall be compliant with Information Exchange Gateway (IEG).

4.7 Applicable Standards

This section describes by reference all standards and the specific sections of any such standards, which apply to E-NPKI.

Requirement ID: SRS-1919

•E-NPKI shall be compliant with ADatP-34 base standards and profiles for XML implementation.

Requirement ID: SRS-1920

•E-NPKI shall be compliant with ADatP-34 base standards and profiles for information exchange

4.7.1 Technical Standards

Requirement ID: SRS-1922

•E-NPKI shall comply with the applicable Technical Standards. Any variations from the Technical Standards shall be approved by the Purchaser.

4.7.1.1 Document Format Standards

PDF ISO 32000-1:2008

Document Management - Portable Document Format - Part 1: PDF 1.7

PDF/A ISO 19005-1:2005

Document Management - Electronic document file format for long-term preservation - Part 1:

Use of PDF 1.4 (PDF/A-1)

ISO 19005-2:2011

Document Management - Electronic document file format for long-term preservation - Part 2:

Use of ISO 32000-1 (PDF/A-2)

ISO 19005-3:2012

Document Management - Electronic document file format for long-term preservation - Part 3:

Use of ISO 32000-1 with support for embedded files (PDF/A-3)

RTF Rich Text Format (RTF), Microsoft Specification, Version 1.5,

Microsoft Application Note GC0165:1997

DOCX ISO/IEC 29500:2008

Information technology - Office Open XML File Formats

XSLX ISO/IEC 29500:2008

	Information technology - Office Open XML File Formats
PPTX	ISO/IEC 29500:2008
	Information technology - Office Open XML File Formats

4.7.1.2 XML Standards

XML	W3C - eXtensible Markup Language (XML) Version 1.0 (Fifth Edition),
	W3C REC-xml-20081126
XSD	W3C - XML Schema Definition Language (XSD)
	W3C REC-xmlschema11-1-20120405
XSL	W3C - eXtensible Stylesheet Language (XSL) 1.1
	W3C REC-xsl11-20061205
XML NS	W3C - Namespaces in XML 1.0 (Third Edition)
	W3C REC-xml-names-20091208
XSLT 2.0	W3C - eXtensible Stylesheet Language Transformations (XSLT)
	W3C REC-xslt20-20070123
XMLENC	W3C - XML Encryption Syntax and Processing
	W3C REC-xmlenc-core-20021210
XMLDSIG	W3C - XML Signature Syntax and Processing (Second Edition)
	W3C REC-smldsig-core-20080610
RDF	Resource Description Framework
	www.w3c.org/RDF
XQuery	W3C - An XML Query Language 1.0 (Second Edition)
	W3C REC-xquery-20101214
XPath	W3C - XML Path Language 2.0 (Second Edition)
	W3C REC-xpath20-20101214

4.7.2 Quality Standards

Requirement ID: SRS-1942

•E-NPKI shall comply with the applicable Quality Standards. Any variations from the Quality Standards shall be approved by the Purchaser.

4.7.3 Programming Standards

Requirement ID: SRS-1944

•E-NPKI shall comply with the applicable Programming Standards. Any variations from the Programming Standards shall be approved by the Purchaser.

4.8 Deployable Systems

See program-level formal module "DCIS Requirements"

4.9 Information Exchange Requirements (IERs)

Requirement ID: SRS-1948

•E-NPKI shall exchange information with IEG C to cross from NATO Secret to Mission Secret Security domains

4.9.1 Information Products

Requirement ID: SRS-1955

•The Bi-SC AIS NEDS service shall be the trusted data source of enterprise directory data sets.

Requirement ID: SRS-2808

•E-NPKI shall interface with NEDS according to “NEDS Agreements” to be established in coordination with NEDS project.

Requirement ID: SRS-1956

•E-NPKI shall retrieve subscriber Profile information from NEDS

Requirement ID: SRS-1957

•E-NPKI shall store subscriber Profile information in NEDS

Requirement ID: SRS-1962

•E-NPKI shall retrieve specific directory information from NEDS

Requirement ID: SRS-1963

•E-NPKI shall store specific directory information in NEDS

Requirement ID: SRS-2809

•Where NEDS does not provide directory services in support of specific E-NPKI communities, alternate "Directory Agreements" shall be established in coordination with the appropriate directory service system.

4.9.2 Interfaces

4.9.2.1 LDAP / LDAP over SSL

Requirement ID: SRS-1996

•The E-NPKI Certificate Authorities shall interface with the NATO Enterprise Directory Service (NEDS) via LDAP over SSL for all information read from and written to the NEDS.

Requirement ID: SRS-2746

•The E-NPKI Registration Authorities shall interface with the NATO Enterprise Directory Service (NEDS) via LDAP over SSL for all information written to the NEDS.

Requirement ID: SRS-2747

•The E-NPKI system shall support LDAP for reading information from the NEDS.

4.9.2.2 PKIX CMP

Requirement ID: SRS-2748

•The E-NPKI system shall support PKIX CMP as described in RFC4210 for cryptographic key generation and certificate signing between end entity and the Certificate Authority.

4.9.2.3 Key and Certificate data structures

Requirement ID: SRS-2752

•E-NPKI shall support software key and certificate data structures including the following:

Requirement ID: SRS-2753

•PKCS#12 including encryption of keys

Requirement ID: SRS-2754

•PKCS#10

Requirement ID: SRS-2755

•PKCS#7

Requirement ID: SRS-2756

•Binary and PEM encoded Certificates

Requirement ID: SRS-2757

•PEM encoded key files (both clear and encrypted key material)

4.9.2.4 Smart Card Interfaces

Requirement ID: SRS-2751

•E-NPKI System shall support multiple smartcard, HSM, and TPM interfaces across the full range of operating systems and applications within NATO; to include Personal Computer/Smart Card (PC/SC), PKCS#11, and FIPS 201 PIV-(C).

Requirement ID: SRS-2824

•E-NPKI System including the LACS CMS shall support the existing deployed base of approved elliptic curve smartcards including but not limited to the Gemalto IDPrime PIV card v2.0 (with a Mifare DESFire chip for PACS) and the Safenet SC650 across the full range of operating systems and applications within NATO.

4.9.2.5 OCSP

Requirement ID: SRS-2750

•E-NPKI OCSP servers shall implement services in accordance with RFC6960.

4.9.2.6 Timestamp

Requirement ID: SRS-2749

•E-NPKI Timestamp servers shall implement services in accordance with RFC3161.

4.9.2.7 Simple Certificate Enrolment Protocol (SCEP)

Requirement ID: SRS-2768

•The E-NPKI shall provide a SCEP interface As defined in Simple Certificate Enrolment Protocol draft-gutmann-scep-01.txt including a Registration Authority workflow to validate the certificate request.

4.9.2.8 Enrolment Over Secure Transport (EST)

Requirement ID: SRS-2807

•The E-NPKI shall provide an EST interface as defined in RFC 7030 including a Registration Authority workflow to validate the certificate request.

4.9.2.9 SMTP

Requirement ID: SRS-2770

•The E-NPKI shall include an SMTP interface to interconnect with internal mail servers to communicate with E-NPKI subscribers.

4.9.2.10 External Audit Logging Interfaces

Requirement ID: SRS-2007

•E-NPKI shall interface with NCIRC using NCIRC ICD.

4.10 Integration with existing systems and applications

The following list provides an indication (but not a complete list) of the types of PKI enabled applications to be supported by E-NPKI.

Requirement ID: SRS-2771

•The E-NPKI shall support the full complement of existing PKI enabled applications within NATO.

Requirement ID: SRS-2758

•The E-NPKI system shall provide auto-enrolment of Windows Devices (both software and TPM storage of keys), including a Registration Authority workflow to validate the certificate request.

Requirement ID: SRS-2759

•The E-NPKI system shall provide Smart Card Logon for all fielded servers and workstations based on the Windows family of operating systems.

Requirement ID: SRS-2764

•The E-NPKI system shall be integrated with 802.1X authentication (including smart card authentication for users and TPM based machine authentication for devices) for all existing servers and workstations based on the Windows family of operating systems.

Requirement ID: SRS-2767

•802.1X authentication shall be implemented for WIFI authentication, Network Access Control (NAC), and Network Access Protection (NAP)

Requirement ID: SRS-2765

•The E-NPKI system shall be integrated with 802.1X authentication for the existing smartphones based on Windows, Apple IOS, and Blackberry OS.

Requirement ID: SRS-2761

•The E-NPKI system shall integrate encryption and digital signatures for the deployed versions of Microsoft Office.

Requirement ID: SRS-2762

•The E-NPKI system shall integrate timestamping, encryption, and digital signatures for the deployed version of Microsoft Outlook, and Outlook Web Access systems within NATO.

Requirement ID: SRS-2763

•The E-NPKI system shall integrate timestamping, encryption, and digital signatures for the deployed version of Adobe Acrobat Reader, and Acrobat Professional systems within NATO.

Requirement ID: SRS-2769

•The E-NPKI system shall integrate with existing Mobile Device Management products including MobileIron, AirWatch and Blackberry Enterprise.

Requirement ID: SRS-2773

•The E-NPKI system shall integrate with all existing Web Server technologies within NATO; to include IIS, Apache, Apache Tomcat, Jetty.

Requirement ID: SRS-2774

•The E-NPKI system shall interoperate with all existing appliances implementing SSL management interfaces based on JAVA and OpenSSL.

Requirement ID: SRS-2775

•The E-NPKI system shall interoperate with all existing SSL and IPSEC VPN systems in NATO; including but not limited to Cisco, Juniper,

Requirement ID: SRS-2783

•The E-NPKI system shall interoperate with applications providing code signing (based on PKCS#7 data structures); including JAVA, Authenticode, and .NET.