NCIA/ACQ/2018/1596

09 October 2018

Market Survey Request for RFI on

Key Management System and High Assurance Certification Authority

NCI Agency Ref: MS-CO- 14892 -KMSHACA

The NATO Communications and Information Agency (NCI Agency) is seeking inputs from Nations and their Industry regarding their capacity in providing support to the implementation of the future NATO Key Management and Distribution System.

Market Survey Point of Contact: Ms. Gloria Paridi

E-mail: Gloria.Paridi@ncia.nato.int

To: See Distribution List

Subject: **Request for Vendors for NCI Agency Market Survey Request**

Key Management System and High Assurance Certification Authority

1. The NATO Communication and Information Agency (NCI Agency) is seeking inputs from Nations and their Industry regarding their capacity in providing support to the implementation of the future NATO Key Management and Distribution System. As implementation of this capability will rely on the establishment of a number of High Assurance Certification Authorities for NATO, which are to be procured separately from the remaining components of the system, separate information is requested on the availability of these Certification Authorities and the remaining system components.

2. The purpose of this Market Survey is to understand the capability of the supplier in providing answer to the implementation of the future NATO Key Management and Distribution System.

3. A list of potential firms, already identified, is included as Annex C. In addition to the firms noted, the broadest possible dissemination by Nation of this Market Survey to their qualified and interested industrial base is requested.

4. Respondents are requested to reply via the questionnaire in annex A. Other supporting information and documentation (technical data sheets, non-binding product pricing, marketing brochures, descriptions of existing installations, etc.) is desired.

5. The NCI Agency reference for this Market Survey Request is **MS-CO- 14892 - KMSHACA** and all correspondence and submissions concerning this matter **must** reference this number within the documentation and email or postal subject line.

6. Responses may be issued to NCI Agency directly from Nations or from their Industry. Respondents are invited to carefully review the Introduction within Annex A to determine interest.

7. Responses shall in all cases include the name of the firm, telephone number, e-mail address, designated Point of Contact, and a NATO UNCLASSIFIED description of the capability available and its functionalities. This shall include any restrictions (e.g. export controls) for direct procurement of the various capabilities by NCI Agency.

8. Responses are due back to NCIA no later than **close of business 10 December 2018**.

9. Please send all responses either via post/courier or email to the following NCI Agency contact:

   For Attention of:

   Ms Gloria Paridi
   Senior Contracting Assistant
   Email: Gloria.Paridi@ncia.nato.int

10. Product demonstrations or face-to-face briefings/meetings with industry are not foreseen during this initial stage. Respondents are requested to await further instructions after their submissions and are requested not to contact any NCI Agency staff directly other than the POC identified above in Para 8.

11. Any response to this request shall be provided on a voluntary basis. Negative responses shall not prejudice or cause the exclusion of companies from any future procurement that may arise from this Market Survey. Responses to this request, and any information provided within the context of this survey, including but not limited to pricing, quantities, capabilities, functionalities and requirements will be considered as indicative and informational only and will not be construed as binding on NATO for any future acquisition.

12. The NCI Agency is not liable for any expenses incurred by firms in conjunction with their responses to this Market Survey and this Survey shall not be regarded as a commitment of any kind concerning future procurement of the items described.

13. Your assistance in this Market Survey request is greatly appreciated.

FOR THE DIRECTOR OF ACQUISITION:

Rebecca Benson
Digitally signed by Rebecca Benson
Date: 2018.10.10 09:50:28 +02'00'

Rebecca Benson
Principal Contracting Officer

Attachment(s):

- Annex A – Summary of requirements
- Annex B – Questionnaire
- Annex C – Market Survey Industrial Recipients

ANNEX A
Summary of Requirements
Project ID 2017/0IS03007 & 2017/0IS03008, CP9C0122

Introduction

A detailed description of the procurement approach for the future NATO Key Management and Distribution System can be found in IMSWM-0709-2016(INV) - "Proposal for the Procurement of the NATO Key Management and Distribution Capability", dated 18 January 2017. Figure 1 provides a basic depiction of the design for the new capability that is to be procured under CP 9C0122.

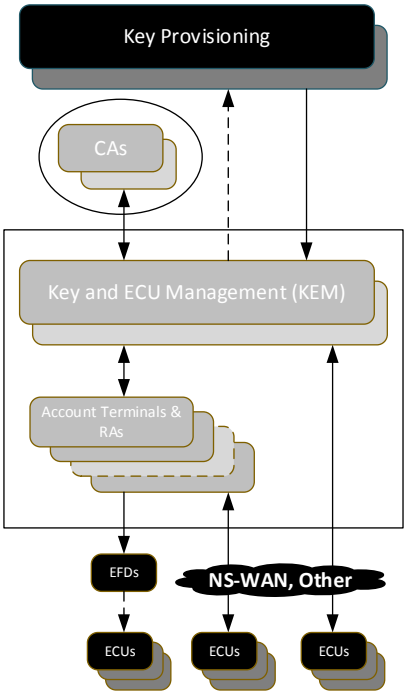

Figure 1 Schematic Overview of the NATO Key Management and Distribution Capability

The main components are the Key and ECU Management (KEM) system, which acts as the core system, and the Account Terminals and Registration Authorities (RAs) (either combined into a single terminal, or deployed individually). These components provide most of the overall system functionality and interface with the Key Provisioning system(s), Certification Authorities (CAs), Electronic Fill Devices (EFDs) and with End Crypto Units (ECUs) that implement the NATO Key Management (KM) Interoperability Specification (ISpec). The expectation is that each Account Terminal will have its own high assurance cryptographic module available in order to allow it to function as a Management Centre as defined in the NATO KM ISpec.

Certificate Management within the capability will be driven by a number of high assurance Certification Authorities, both for infrastructure operations and the provisioning of mission certificates for End Crypto Unit operations, which will be procured separately from the

KEM and Account Terminals/RAs. These CAs will be subordinate to an already existing NATO Root CA, hosted elsewhere in NATO. The KEM will have to interface with the new non-root CAs, which requires the interface specification to these CAs to be made available to the NCI Agency and the vendor providing the KEM.

As the combination of KEM and Account Terminals/RAs and the Certification Authorities will respectively be procured under separate Invitation for Bids (IFBs) (currently estimated to be sent out mid 2019 (CAs) and early 2020 (Key Management System), a separate list of questions is provided for both of these capability components.

Key Management System

The KEM and Account Terminals/RAs, hereafter referred to as the 'Key Management System', are expected to communicate keying material according to the parameters as defined in the NATO KM ISpec, both internally between system components (with the exception of communication with the CAs) and externally with EFDs and ECUs. Legacy interface descriptions based on various existing US EKMS standards will need to be followed in order to receive keying material through the Key Provisioning interface. This interface point should however also implement additional functionality in order to allow for full two-way interaction through the Key Provisioning interface in the future in line with the NATO KM ISpec requirements. Additional information on the precise interface requirement will be provided in the IFB.

The Key Management System will also be expected to incorporate full accounting and auditing of key- and crypto material transfer transactions between accounts, acting as a full replacement for NATO's COMSEC accounting system.

High Assurance Certification Authority

The "Converged NATO PKI and NATO High Assurance PKI Certificate Policy" [AC/322-WP(2017)0051-REV1, dated 18 January 2018] states the high-level requirements for any High Assurance (HA) Certification Authority (CA). This capability is intended to be an automated facility that after initial configuration is able to receive signed certification requests from the KEM, verify the signature, and return either a completed and signed certificate or an error message.

Whether the authorization checks for signatures, combined with the intended certificate scope, will occur within the Key Management System (KEM and Account Terminals/RAs), or within the HA CAs themselves depends on the anticipated granularity of the HA CAs expected to become available on the market at the time of IFB. If it is expected that no (suitable) Certification Authority will be available at the time of IFB, the NCI Agency may consider offering a development contract for this capability. Given such a contract, the selected vendor would be granted a given amount of time in order to modify its existing equipment in order to have it meet the full set of requirements as specified in the IFB, followed by (an updated) SECAN evaluation for the modified product.

ANNEX B
Questionnaire

Organisation name: _____

Contact name & details within organisation: _____

Notes

- Please **DO NOT** alter the formatting. If you need additional space to complete your text then please use the 'Continuation Sheet' at the end of this Annex and reference the question to which the text relates to.
- Please feel free to make assumptions, *HOWEVER* you must list your assumptions in the spaces provided.
- Please **DO NOT** enter any company marketing or sales material as part of your answers within this market survey. But please submit such material as enclosures with the appropriate references within your replies. If you need additional space, please use the sheet at the end of this Annex.
- Please **DO** try and answer the relevant questions as comprehensively as possible.
- All questions within this document should be answered in conjunction with the summary of requirements in Annex B.
- All questions apply to Commercial or Government respondees as appropriate to their Commercial off the Shelf (COTS) or Government off the Shelf (GOTS) product.
- Cost details required in the questions refer to Rough Order of Magnitude (ROM) Procurement & Life Cycle cost, including all assumptions the estimate is based upon:
    - Advantages & disadvantages of your product/solution/organisation,
    - Any other supporting information you may deem necessary including any assumptions relied upon.

1. Key Management System

a. Does your company provide any
(1) Cryptographic hardware modules/key processors,
(2) COMSEC accounting systems, or
(3) Other key management related equipment (excluding legacy EFDs supporting only EKMS308F-based communication)?

If so, please elaborate and specify your answers to the questions below based on applicability to the listed equipment. The assumption is that any offered Key Management System will be based on a combination of (evolutions of) these components.

For the components and systems expected to become available at the time of IFB:

b. What is the level and scope of the automation and scheduling of transactions provided?

c. Could you describe the (COMSEC) accounting capabilities provided by the system?

d. What level of backward interoperability is provided with legacy equipment?

e. Could you provide some information on the component registration procedure used in order to introduce cryptographic components to the key management system?

f. Will the system incorporate a Key Ordering mechanism for sub-accounts to order keying material through higher tier accounts? If so, could you elaborate on the level and scope of this capability?

g. Does the system incorporate a mechanism for the transfer of accounting and auditing information from local accounts to a central repository?

h. What kind of security and monitoring capabilities does your system provide?

i. Is the system ready for integration of log and event management with a SIEM?

j. What auditing mechanisms does the system support?

k. Does the system support protected key transfer between accounts (including the required accounting and auditing)?

l. What mechanisms does the system provide for the issuance of keys or crypto equipment to hand receipt holders (who typically are not to maintain a full crypto custodian account):

(1) In terms of limited functionality access for hand receipt holders,
(2) In terms of key- or crypto device transfer/assignment to a hand receipt holder within the system itself, and
(3) In terms of hand receipt holder key retrieval?

m. In terms of redundancy, does the system support
(1) Redundant communication paths between the KEM and Account Terminals/RAs?
(2) Fail-over in case of KEM instance failure?
(3) Short-term recovery in case of database corruption?

n. What kind of capacity and performance does the system provide:
(1) In terms of number of keys encapsulated/processed per minute,
(2) Maximum number of keys that can be stored in the system,
(3) Maximum number of Account Terminals supported?

o. Does the system support account-specific encryption and signatures (as mandated by the ISpec), also based on symmetric keys (KEKs and pre-shared symmetric signing keys)? Does the system support hybrid use of asymmetric and symmetric encryption and signatures?

p. Are the hardware tokens (if any) required in order to establish local accounts releasable to any non-NATO partner nations? If so, which?

q. Could you provide a rough cost estimate for the procurement (excluding deployment) of your key management system, based on delivery of the KEM and 90 Account Terminals/RAs? What would the expected additional cost per Account Terminal be if we were to procure additional ones shortly after completion of the procurement?

r. Could you provide a rough cost estimation for the development of an interface between the KEM and the Certification Authorities (all with identical interfaces), under the assumption that the main function of the interface would be to transfer (signed) certification requests and to receive the CA response?

NATO will in the near future start requiring all new equipment to implement NATO-approved quantum resilient algorithms, in particular for key establishment and the creation of digital signatures.

s. Does the equipment indicated earlier implement (possibly non-NATO approved) quantum resilient algorithms at the time of IFB?

(1) If so, which?
(2) Is the equipment able and does it come with sufficiently scaled hardware to update the included algorithms to NATO-selected quantum resilient algorithms in the future through a software/firmware update without loss of functionality (e.g. throughput speed, number of associations, etc)? Please clarify the current/expected situation as needed.
(3) Assuming that NATO will select public algorithms for key exchange and signature for Type B use and classified algorithms for key exchange and signature for Type A use, could you provide a rough cost indication for the provision of the required (software-based) equipment update?
(4) Is it possible to replace any embedded authentication signatures within the equipment at a future date, possibly through a limited hardware module replacement? If so, please clarify.

2. High Assurance Certification Authority

a. Is your company able to provide NATO with a High Assurance Certification Authority meeting the requirements in AC/322-WP(2017)0051-REV1 at the time of IFB? Is it expected that this CA will have passed SECAN evaluation at the time of IFB?

b. What algorithms can the CA support?

c. Is the CA able to work with an external root CA (which is not procured as part of the IFB)?

d. What technical and administrative controls does the CA provide in order to safeguard admin access to the CA?

e. What kind of hardware security modules does the CA embed or support?

f. Does the Certification Authority support automated authorization of signing requests in line with the description above? Please elaborate.
(1) If so, what level of authorization granularity can be defined within your CA?

g. Can you provide the NCI Agency with the interface description of the CA upon procurement in order to allow for integration with the KEM by the KEM contractor (based within one of the NATO nations)?

h. What kind of security and monitoring capabilities does the CA provide?

i. What auditing mechanisms will the system support?

j. Will the system be ready for integration of log and event management with a SIEM?

k. What is the anticipated selling price for the Certification Authorities, based on the procurement of 7 instances? Will there be a license fee per issued certificate or based on the number of registered accounts/devices? If so, could you provide an indication of the cost?

NATO will in the near future start requiring all new equipment to implement NATO-approved quantum resilient algorithms, in particular for key establishment and the creation of digital signatures.

l. Does the equipment indicated earlier implement (possibly non-NATO approved) quantum resilient algorithms?
- **(1) If so, which?**
- **(2) Is the equipment able and does it come with sufficiently scaled hardware to update the included algorithms to NATO-selected quantum resilient algorithms in the future through a software/firmware update without loss of functionality (e.g. throughput speed, number of associations, etc)? Please clarify the current/expected situation as needed.**
- **(3) Assuming that NATO will select public algorithms for key exchange and signature for Type B use and classified algorithms for key exchange and signature for Type A use, could you provide a rough cost indication for the provision of the required (software-based) equipment update?**
- **(4) Is it possible to replace any embedded authentication signatures within the equipment at a future date, possibly through a limited hardware module replacement? If so, please clarify.**

October 8, 2018 4:41 PM

Country	Vendor
BELGIUM	ATOS
	BE NETWORKS
	Brevco Services S.C.S.
	Computer Sciences Corporation
	ComputerLand S.L.M. S.A.
	Cybertrust Belgium NV
	Damovo Belgium NV/SA
	Dimension Data Belgium
	Ericsson sa/nv
	European Datacomm NV
	Getronics Belgium SA/NV
	Gillam-FEI
	NextiraOne
	Nijkerk Computer Solutions BeNeLux
	RHEA System S.A.
	SAIT
	Telenet C-Cure
	Telindus NV
	Thales Alenia Space Etca s.a.
	Thales Belgium S.A.
	Thales S.A.
	U2U Consult
	Uniskill NV
	Unisys Belgium S.A.
BULGARIA	KRISTANEA LTD.
	Lirex BG Ltd
	Telelink EAD
CANADA	ADGA Group Consultants, Inc.
	CloudMask
	General Dynamics Canada Ltd.
	Resul Control Systems Ltd.
CROATIA	CROZ d.o.o. za informaticku djelatnost
	INsig2 d.o.o.
CZECH REPUBLIC	Damovo Ceska republika s.r.o.
	Skill s.r.o.
DENMARK	Danoffice ApS
	Dencrypt A/S
	SAAB Danmark A/S
	Terma A/S
ESTONIA	Viking Security AS

October 8, 2018 4:41 PM

Country	Vendor
FRANCE	ASTRIUM SAS
	Airbus Defence and Space SAS
	Altran technologies_ASD Paris
	Bull SAS
	CS Systèmes d'Informations
	MARLINK SAS
	Sagem Defense Securite
GERMANY	Airbus Defence and Space GmbH(ex EADS GmbH)
	Bell Computer-Netzwerke GmbH
	CGI (Germany) Gmbh &Co.KG
	CSC Deutschland Solutions GmbH
	Cordsen Engineering Gmbh
	FREQUENTIS Deutschland GmbH
	GTSI Corp.
	IABG mbH
	OHB-System AG
	Roda Computer GmbH
	Rohde & Schwarz GmbH & Co. KG
	Secusmart GmbH
	T-Systems International GmbH
	Thales Electronic Systems GmbH
	XORTEC GmbH
GREECE	European Dynamics SA
	Hellenic Aerospace Industry (SA)
	Intracom Defense Electronics S.A.
	Space Hellas
HUNGARY	Fercom Ltd.
	Honvédelmi Minisztérium Elektronikai,Logisztikai és Vagyonkezelo zrt.
	Hubel Hungarian & Belgian Ltd.
	Synergon Information Systems plc- Synergon Integrator Kft
ITALY	Finmeccanica SpA
	Fondazione FORMIT
	Italtel
	NA.EL. SRL
LATVIA	DATI Group, LLC
	Datakom LTD
	SIA Fima
LITHUANIA	Blue Bridge
	JSC FIMA (UAB)
NETHERLANDS	Avensus Nederland BV

Annex C - Industry Recipients

Country	Vendor
NETHERLANDS	Compumatica Secure Networks B.V.
	Crosscheck Networks Nederland b.v.
	FOX-IT BV
	Gannexion B.V.
	Global Crossing
	PQR bv
	PointGroup BV
	Quint Wellington Redwood
	ROHDE & SCHWARZ BENELUX BV
	Sectra Communications BV
	Stork Fokker AESP BV
	SurCom International BV
	UNI Business Centre BV
	WBC Innovations BV
NORWAY	3D perception AS
	Atea Norge AS
	Evry
	Kongsberg Defence & Aerospace AS
	Saab Technologies Norway AS
	Umoe IKT
POLAND	Atende S.A.(prior ATM S.A.)
	Consortia Sp. z o.o.
	Enamor Sp. z.o.o
	MAW Telecom Intl SA
	Military Communication Institute
	Newind sp. z o.o.
	QUMAK S.A. (joint-stock company)
	S&T Services Polska Sp. z o.o.
	Siltec Sp. z.o.o.
	Unizeto Technologies SA
	WASKO S.A.
	Zbar Phu Mariusz Popenda
ROMANIA	ATOS Convergence Creators SRL
	Romsys SRL
	UTI Grup S.A.
SLOVAKIA	Aliter Technologies a.s
	Quadriq, a.s.
SPAIN	Alma Technologies s.a.
	Epicom S.A.
	Indra Sistemas S.A.
	Safelayer Secure Communications, S.A.
	Tecnobit S.L

Country	*Vendor*
SPAIN	
TURKEY	ASELSAN Elk. San ve Tic. A.S.
	C TECH Bilisim Tek. San ve Tic A.S.
	TUBITAK BILGEM
UNITED KINGDOM	Airbus DS Limited
	Audax
	Avanti Communications Group plc
	BAE Systems Applied Intelligence Ltd.
	Fujitsu
	GGR Communications Ltd UK
	General Dynamics United Kingdom Limited
	Info-Assure LTD.
	Rheatech Limited
	Secure Systems & Technologies Ltd. (SST)
	Software Box Ltd.
	Sopra Steria
	Spectra Group (UK) Ltd
	Thales UK Limited
	Ultra Electronics CIS Ltd.
	ViaSat UK
	Vocality International Ltd
	Voice Concepts Ltd.
UNITED STATES	AATD, LLC
	ADCI of Delaware, LLC
	ALTIMA GROUP INTERNATIONAL, INC. (AGI)
	AS GLOBAL
	AT&T Government Solutions, Inc.
	AVI Systems Inc.
	Advanced Programs Inc. (API)
	Affigent, LLC
	BAE Systems Information Solutions Inc.
	Comtech Mobile Datacom Corporation
	DRS Technical Services, Inc.
	EMW, Inc.
	Emerging Markets Communications (EMC)
	Equant
	Extreme Networks, Inc.
	Harris Corporation - RF CommunicationsDivision
	Honeywell Technology Solutions Inc.
	Hyperion, Inc.
	ISSTSPi
	Intelligent Waves LLC
	K3 Enterprises, Inc.
	L-3 National Security Solutions, Inc.
	LEIDOS Inc

October 8, 2018 4:41 PM

Country	*Vendor*
UNITED STATES	ManTech International Corporation
	Mutual Telecom Services Inc. d/b/a BlackBox Network Services Government Solution
	Pegasus Professional Services LLC
	PlanIT Group LLC
	Raytheon CompanyNetwork Centric Systems
	SAIC
	Spacenet Integrated Government Solutions
	Strategic Operational Solutions, Inc
	Systems Research and ApplicationsCorporation
	Technology and Management InternationalLLC (TAMI)
	TeleCommunication Systems, Inc.
	The Boeing Company
	URS Federal Services International Inc
	UXB Defense, Inc
	ViaSat, Inc.
	Vykin Corporation
	Wave Systems Corp.
	World Wide Technology Inc.
	XSAT USA
	XTec, Incorporated
Total :	**186**