NATO KEY MANAGEMENT INTEROPERABILITY SPECIFICATION

REQUEST FOR INFORMATION (RFI)
NCSC
424283

RFI Issue Date: 15 July 2025
Response Due Date: 19 August 2025

Table of Contents

REQUEST FOR INFORMATION

A. Introduction

1. The NATO Communications and Information Agency (NCA) is conducting market research to identify potential sources and gather information regarding industry capabilities to support NCIA NATO Cyber Security Center. This Request for Information (RFI) is issued solely for informational purposes and does not constitute a Request for Proposal (RFP), Request for Quotation (RFQ), or invitation for bid.

B. Purpose

1. The purpose of this RFI is to obtain Rough Order Magnitude price quote for performing the work described under the Statement of Work (SOW) in Annex B. This will help NCIA planning for an appropriate amount of funding.
2. Companies are also requested to comment on the provided statement of work. Responses to this RFI will assist in refining requirements, identifying capabilities, and shaping the strategy for any future solicitation.

C. Background

1. The NATO Key Management Interoperability Specification (NKMIS) aims to standardize cryptographic key management interactions within the NATO Alliance.

D. Submission Instructions

1. Interested parties are invited to respond in accordance with the instructions below:

   a. Submit responses via the email address in section G no later than **12:00 hours Central European Time (CET)** on **19 August 2025**.

   b. Responses should be submitted in PDF or Word format and must not exceed **15 pages**, including:
      - **i.** Responses to Annex A and comments on Annex B excluding:
      - **i.** Cover page
      - **ii.** Company brochures or product literature (if included)
      - **iii.** Attachments such as past performance references

   c. Use the following subject line for submission
      - **i.** “Response to RFI [RFI Number] – [Company Name]”

   d. All responses should address the items listed in Annex A – Requested Information.

   e. Respondents are also encouraged to review and comment on the draft requirements in Annex B – Draft Statement of Work (SOW)/Performance Work Statement (PWS).

E. Disclaimer

1. This RFI is for planning and informational purposes only and shall not be construed as a solicitation or obligation on the part of the NCIA. The NCIA does not intend to award a contract based on responses to this RFI. Respondents are solely responsible for all costs incurred in responding to this RFI. The NCIA will consider and analyse all

information received from this RFI and may use these findings to develop a future solicitation. The NCIA will consider all responses as confidential commercial information and will protect it as such.

2. NCIA reserves the right, at any time, to cancel this informal market survey, partially or in its entirety. No legal liability on the part of NCIA for payment of any sort shall arise and in no event will a cause of action lie with any prospective participant for the recovery of any costs incurred in connection with the preparation of documentation or participation in response hereto. All effort initiated or undertaken by prospective informal market survey participants shall be done considering and accepting this fact.

F. Use of Information Provided through Responses

1. Confidentiality of Responses

The NCIA may incorporate industry comments and responses, in part or in whole, into a future release of a solicitation. Should respondents include proprietary data in their responses that they do not wish to be disclosed to the public for any purpose, or used by NCIA (except for internal evaluation purposes), they must:

a. Mark the title page with the following legend:

This document includes data that shall not be disclosed outside NATO and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than for NCIA internal evaluation purposes, unless otherwise expressly authorised by [insert company name]. This restriction does not limit the NCIA's right to use information contained in this data without restriction if it is obtained from another source. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]

b. Mark each sheet of data it wishes to restrict with the following legend:

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

G. RFI Point of Contact

1. Leonora Alushani, Contracting Officer

2. RFI-424283-NKMIS@ncia.nato.int

Annex A – Requested Information

1. Respondents are encouraged to provide the following information in their response:

   a. **Company Information**
      i. Legal Business Name
      ii. Address
      iii. Website
      iv. Primary Point of Contact
      v. Email address

   b. **Technical Capability**
      i. Summary of relevant capabilities and past performance

   c. **Feedback and Recommendations**
      i. Comments on the draft Statement of Work (SOW)
      ii. Innovations or alternatives
      iii. Rough Order Magnitude (ROM), including any assumptions upon which they are based

   d. **Questions or Concerns**
      i. Risks, concerns, or barriers
      ii. Suggestions for risk mitigation or enhancing competition

Annex B – Draft Requirements / Statement of Work (SOW/PWS)

Note: This is a DRAFT and subject to change. The NCIA is seeking industry feedback.
In the following draft SOW we ask for full source code. If this represents a challenge for you, please include ROM pricing for closed source contributions as well.

STATEMENT OF WORK

1. INTRODUCTION

The NATO Key Management Interoperability Specification (NKMIS) aims to standardize cryptographic key management interactions within the NATO Alliance. After several years of consultations and designs, the DPC has recently approved Version 2.0 of the NKMIS (AC/322-D(2024)0030, NATO Key Management Interoperability Specification (NKMIS) V2.0, 31 May 2024). NCIA is seeking expertise to design, develop and deliver a Conformance Test Tool that will serve as the single independent Reference Implementation and Conformance Test Tool for the NKMIS.

2. . SCOPE

The selected Contractor shall design and deliver a system sufficiently mature and automated so that it function as the Conformance Test Tool for the implementation of the NKMIS in industry products.
For the purpose of this SOW, only the KM-2 and KM-3 interfaces and the NATO Type B cryptographic algorithm suites detailed in the NKMIS are in scope. However, the tool should have a modular design that allows for the addition of modules implementing Type A cryptographic algorithms in the future.
The tool shall be to verify/identify conformance for the following NKMIS conformance indicator markings (as defined in para 23-26 in the NKMIS):

- M2;
- M3;
- E2;
- E3;
- ME2, and
- ME3.

3. TASK DESCRIPTION

3.1. Overall expectations

The intended beneficiaries of the Conformance Test Tool include:

a. NCIA regulatory and technical and authorities
b. National Authorities
c. Product developers and System Integrators
d. Government and International Certification bodies
e. Testing and Accreditation Laboratories

It is critical that the delivered tool does not place undue restrictions on its operating environment (e.g. the use of a niche programming language or dependency on a proprietary compilation- or interpretation platform). More specifically, the tool is expected to be developed with a widely used programming- or scripting language that comes with a freely available and well-maintained development framework (e.g. C, Java, Python, or a comparable language). Moreover, it must be compatible with a widely available and accessible Operating System.
The tool shall be able to automatically run a series of tests to identify if the subject system (e.g. MC, ECU) passes or fails any testable NKMIS requirements related to the NKMIS conformance indicators. Failed results shall be accompanied with a short description of what portion of the test failed in order to provide insight into the deficiency. Some requirements in

the NKMIS are optional and the tool shall be able to enable or disable testing of these requirements individually and as a grouped feature set where appropriate.
To implement the security mechanisms required by the specifications, the tool must verify the correct implementation of the Key Management Data Structure (KMDS). This includes ensuring that the KMDS adheres to the NKMIS and is encoded with the Abstract Syntax Notation One (ASN.1), as outlined in the NKMIS. Accurate implementation of the KMDS with ASN.1 encoding is critical for achieving interoperability, secure communication, and compliance with the defined security framework.
Furthermore, the Cryptographic Message Syntax (CMS) must be properly utilized as part of the implementation to handle the secure transmission of cryptographic messages. CMS provides a standardized structure for digitally signing, encrypting, and authenticating messages, ensuring the integrity and confidentiality of the data exchanged. The tool must validate that CMS is correctly integrated with the KMDS to ensure seamless operation.
Additionally, the implementation must meet the NKMIS requirements specified for Trust Anchors (TA), which serve as the foundational elements for establishing trust in the cryptographic ecosystem. The CTT must validate that the Trust Anchors are correctly defined, handled, securely stored, and properly integrated within the KMDS. This ensure a robust chain of trust and adherence to the specifications outlined in the reference document.
It should be noted that the NKMIS will continue to evolve even after its adoption as a NATO standard and that the aim is to keep the developed tool synchronized with the most current official version of the standard. Following satisfactory performance, there is therefore a potential for future follow-on contracts for the selected Contractor.

3.2. Deliverables

The Contractor is to provide the following deliverables before conclusion of the contract:

- A tool meeting the in-scope requirements and specifications of the NKMIS and this SOW;
- The Contractor must demonstrate how each requirement within the scope is met by completing the following:
    - providing a detailed written description; and
    - delivering a demonstration using the in-scope use cases outlined in the NKMIS;
- A detailed Test Plan and the corresponding Final Test Report;
- Well-documented source code;
- Documentation on any deviations of (or additions to) the implementation with respect to this SOW and the NKMIS; and
- End user documentation (e.g. installation instructions, basic user guide, implementation roadmap, etc.).

All deliverables will transfer to full customer ownership (NATO Owned – NATO Operated) upon delivery and may not rely upon any proprietary/not freely available components.

3.3. Work execution

The development can be executed on any development environment.
Final testing (Site Acceptance Test) of the proof of concept shall happen on NATO premises (The Hague, Netherlands).