PUBLIC KEY INFRASTRUCTURE (PKI)

REQUEST FOR INFORMATION (RFI)
NATO CYBER SECURITY CENTER (NCSC)
424282

RFI Issue Date: 02 July 2025
Response Due Date: 25 August 2025

Table of Contents

REQUEST FOR INFORMATION

A. Introduction

1. As part of our strategic review of Public Key Infrastructure (PKI) service delivery, we are evaluating the availability and technical capabilities in the market to provide a comprehensive PKI solution based on EJBCA platform. 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 input from industry to help inform the NCIA's acquisition planning. Responses to this RFI will assist in refining requirements, identifying capabilities, and shaping the strategy for any future solicitation.

C. Background

1. In order to meet NATO 2030 goals, NCIA is looking for a new PKI solution that will meet the modern coalition PKI needs and enable critical mission success by demonstrating advanced technical capabilities, supporting modern infrastructure requirements and proving its readiness for next generation cryptography.

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 **25 August 2025**.

   b. Responses should be submitted in PDF or Word format and must not exceed **15 pages**, including:
      i. Responses to Annex A

      excluding:
      i. Cover page
      ii. Company brochures or product literature (if included)

   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. 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-424282-PKI@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

   Related to the following fields, Vendors will provide and/or explain:

2. Licensing and Subscription Model

Clear and comprehensive information about available EJBCA licensing models, including subscription-based options, any minimum required license quantities, and scalability options (e.g., licensing based on the number of issued certificates, users, or devices). Transparency in cost structure will support total cost of ownership (TCO) evaluation.

3. Integration with Thales Network HSMs

How the solution supports native and officially documented integration with Thales Network HSMs. Vendors must provide detailed guidance for configuring multi-partition environments and ensuring compliance with high-assurance key management practices.

4. Role Separation and Two-Person Control

How the solution enforces strong role-based access control (RBAC) and mandatory separation between Certification Authority (CA) and Registration Authority (RA) roles, and how it supports dual-control approval workflows to comply with two-person integrity and audit requirements.

5. Integration with Card Management Systems (CMS)

How the proposed solution allows for flexible integration with CMS platforms for the issuance and enrolment of smart cards and hardware tokens (e.g., YubiKeys). Vendors must describe the integration mechanism, lifecycle management capabilities, and adherence to security policies. No specific CMS vendor should be assumed.

6. Deployment Model

How the system supports flexible deployment options, including on-premise, hybrid, and public cloud models, and how it provides certificate-based authentication and identity management for use cases such as IaaS, PaaS, multi-cloud landing zones, IoT, and workload authentication. Availability of a dedicated hardware appliance should also be noted. Single Sign-On (SSO) support is expected to be explained.

7. High Availability, Load Balancing and Data Replication

How the architecture is designed for high resiliency, supporting real-time data replication across geographically distributed sites. Load balancing, fault tolerance, and failover capabilities should be explicitly documented.

8. Backup and Disaster Recovery

Robust backup and disaster recovery procedures, including point-in-time recovery options, offline backups, and clear restoration processes it should include data and configuration.

9. Standard Protocol and Interface Support

How the system supports standard protocols and interfaces including OCSP, REST API, EST, SCEP, and others. All interfaces should be well documented to ensure interoperability and ease of integration.

10. Migration from Existing Entrust PKI Environment

Their approach to migrating existing user and device certificates from an Entrust CA, including certificates issued manually. Additionally, vendors should propose a method for transitioning from Entrust EIE v13 to a new CMS without service disruption.

11. PQC and Cryptographic Agility

How the platform they propose supports cryptographic agility and readiness for post-quantum cryptography (PQC). This includes the ability to implement, test, and manage hybrid and quantum-safe certificates as standards evolve.

12. Developer and DevOps Friendliness

How they will ensure a developer-friendly environment through a rich, publicly documented REST API and CLI tools. These tools should facilitate automation, integration, and testing within CI/CD pipelines and other DevOps workflows.

13. Database Management

How the system supports operation in a clustered database environment and its capability of performing updates without downtime and support efficient data retrieval from relational database management systems (RDBMS).

14. Support Model

How they will ensure 24/7/365 technical support and provide details on support tiers, response times, and escalation paths.

15. System Updates

How the solution supports offline updates for environments not connected to the public internet and how they will ensure a clear update process and timeline for critical patches and feature releases.

16. FIPS Compliance

How the solution is compliant with applicable Federal Information Processing Standards (FIPS), particularly in line with NIST requirements for cryptographic modules and practices.

Responses to the topics listed above will be used to assess market capabilities and help shape the procurement documentation. Vendors are encouraged to provide detailed, transparent, and technically sound responses aligned with industry best practices.

Your support in this RFI is greatly appreciated!

For the Chief of Acquisition,

Leonora Alushani

Contracting Officer