NCIA/ACQ/2025/07494
Tuesday, 11 November 2025

NCIA Request for Information (RFI)

To: **Industry Partners**

Subject: **NATO PUBLIC KEY INFRASTRUCTURE – THIRD PARTY TRUST**
RFI-424314-NPKI-TPT

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify qualified vendors and gather input on potential solutions to support the upcoming acquisition for publically trusted certificates for document signing, email signing and TLS support. To that end, we are issuing the attached Request for Information (RFI) 424314 to solicit feedback from capable and interested industry partners.

2. This RFI is issued for planning and budgeting purposes only and is not a request for bids. It is part of NCIA's effort to ensure it has a clear understanding of the marketplace, available capabilities, estimated costs and potential acquisition strategies.

3. We value your insight and invite you to:
   a. Share relevant corporate capabilities and experience;
   b. Review and comment on our draft requirements (Annexes A) with a view in providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during planning.

4. Submission instructions and additional details can be found in the enclosure to this RFI.

5. Only companies from a NATO member country can participate in or respond to this RFI (https://www.nato.int/cps/en/natohq/nato_countries.htm).

6. Should you have any questions or need clarification, please contact Leonora Alushani, Contracting Officer at RFI-424314-NPKI-TPT@ncia.nato.int.

7. We thank you in advance for your time and input, and we look forward to engaging with you as we shape this potential acquisition.

For the Chief of Acquisition:

Leonora Alushani
Contracting Officer

Enclosure:

- Request for Information with Annexes A
- Distribution List

Distribution List

1. NATO Delegation (Attn: Infrastructure Adviser)

1. Albania	**12.** Greece	**23.** Poland
2. Belgium	**13.** Hungary	**24.** Portugal
3. Bulgaria	**14.** Iceland	**25.** Romania
4. Canada	**15.** Italy	**26.** Slovakia
5. Croatia	**16.** Latvia	**27.** Slovenia
6. Czechia	**17.** Lithuania	**28.** Spain
7. Denmark	**18.** Luxembourg	**29.** Sweden
8. Estonia	**19.** Montenegro	**30.** Türkiye
9. Finland	**20.** Netherlands	**31.** United Kingdom
10. France	**21.** North Macedonia	**32.** United States
11. Germany	**22.** Norway	

2. All NATEXs

Table of Contents

NATO Communications and Information Agency

REQUEST FOR INFORMATION

A. Introduction

1. The NATO Communications and Information Agency (NCIA) is conducting market research to identify potential sources and gather information regarding industry capabilities to support the issuance of publically trusted certificates, for a) document signing, b) email signing, c) web sites/web services (TLS). This Request for Information (RFI) is issued solely for informational and planning 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, budget planning and shaping the strategy for any future solicitation.

C. Background

1. NATO has operated its own internal NATO Public Key Infrastructure (NPKI) for several years, providing digital certificates and related trust services for internal authentication, encryption, and document signing. Over this period, multiple smart card technologies have been deployed across the enterprise, including IDEMIA cards for X.509-based credentials and YubiKey and Thales Gemalto cards for PIV-compatible certificates.
2. While this infrastructure continues to serve effectively internal needs, it is not currently publicly trusted or recognized across external ecosystems. To support expanding digital transformation initiatives and ensure interoperability with external entities, NATO is now exploring options for publicly trusted and qualified trust services.
3. Through this RFI, NCIA aims to assess potential solutions, partnerships, and operating models that enable the establishment of a publicly trusted, compliant, and interoperable trust service model.
4. The target outcome is to use the information collected to develop our acquisition strategy for an upcoming procurement. The procurement will aim to establish or collaborate with a Qualified Trust Service Provider (QTSP) or equivalent partner, to support qualified signatures, secure communications, and centralized trust governance, across multiple domains and use cases:
    a. Qualified and Legally Recognized Digital Signatures
        - Establishment or partnership with a QTSP under the EU eIDAS Regulation (EU) No 910/2014/ (EU) 2024/1183.
        - Capability to issue and manage Qualified Electronic Signatures (QES) that are legally recognized within the EU/EEA, and other jurisdictions with aligned frameworks.
        - Enablement of digitally signed documents that can be validated by external relying parties through common environments, such as Adobe Acrobat (AATL) and European Union trust lists.
    b. Publicly trusted Email signatures
        - Utilization of qualified certificates, where appropriate, for email signing (S/MIME) to ensure message authenticity and integrity.

- Assurance of interoperability and trust validation across major email clients (e.g., Microsoft Outlook, Apple Mail, Mozilla Thunderbird) and external recipients.
- Assessment of the technical feasibility and eIDAS policy implications of using qualified certificates within the S/MIME ecosystem.

c. Client Authentication Certificates (Enterprise Use)
- Enable issuance and management of certificate-based authentication credentials for internal use.
- Support storage of client authentication certificates on the same smart card or token as QES certificates.
- Ensure compatibility with enterprise operating systems (Windows, macOS, Linux) and identity management systems, including cloud identity providers.
- Clarify options for internal CA issuance versus QTSP issuance, and integration with existing PKI infrastructure.

d. Public-Facing TLS Certificates for Websites and Services
- Continued procurement of commercially trusted TLS/SSL certificates from globally recognized Certification Authorities (CAs).
- Introduction of a centralized governance and lifecycle management model for TLS certificates, enabling NATO to:
    a. Standardize certificate issuance and renewal processes,
    b. Maintain visibility over all externally facing digital certificates, and
    c. Ensure consistent compliance and auditability across multiple domains and systems.

4.2. The number of users that shall be provided with certificates for document and email signing is roughly twenty thousand (20.000). The number of TLS certificates is in the range of 300-500 certificates.

4.3. NCIA is particularly interested in understanding three main models for providing qualified trust services (other possible options, if exist, are also welcome). Respondents are requested to describe their capabilities, approaches, and experience (i.e. market examples/references) for each model.

Option	Name	Description	RA Function	CA Ownership / Operation
Option 1	NATO procures services from an existing QTSP CA	Certificates are purchased directly from a compliant QTSP. Certificate issuance and trust management are primarily handled by the vendor.	Handled by vendor or delegated to NATO.	NATO does not operate the root or issuing CAs. NATO accepts the provider's existing Certificate Policy and Certificate Practice Statement.
Option 2	Vendor deploys a CA Infrastructure on behalf of NATO	Vendor establishes a dedicated CA infrastructure for NATO, including	Handled by vendor or delegated to the NATO.	NATO does not operate the root or issuing CAs. However,

	(infrastructure to be hosted on vendor's premises)	Root CA, intermediate/sub-CAs, and management systems. Vendor ensures that the CIS is eIDAS compliant and is maintained in this way.		NATO has a deeper visibility into the audits of the CA and can influence the Certificate Policy and Certificate Practice Statements.
Option 3	NATO deploys and operates the CA. Vendor provides advisory/support	NATO fully owns and operates the CA hierarchy (Root, Intermediate and Issuing CAs, and the management aspects).	NATO manages RA, certificate issuance, and lifecycle independently.	The vendor provides advisory, implementation guidance, and compliance support but does not operate or host the CA.

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 **05 January 2026**.

b. Responses should be submitted in PDF or Word format and must not exceed **20 pages**, including:

i. Responses to Annex A

excluding:

i. Cover page
ii. Company brochures or product literature (if included)
iii. Attachments such as past performance references (optional)

c. Use the following subject line for submission

i. "Response to RFI [424314-NPKI-TPT] – [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

2. RFI-424314-NPKI-TPT@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. Responses to the following RFI Questions:

2. **Requested Technical Support**

2.1. Qualified Electronic Signatures (QES)

For each option, provided in the **C. Background section** (Option 1 – Managed QTSP, Option 2 – Vendor-Hosted CA, Option 3 – Organization-Operated CA), please provide the following (if the answers are irrelevant to the deployment model, answers may be consolidated/skipped):

i. CA Infrastructure Deployment
   i. Describe the high-level technical architecture (Root CA, Intermediate/Sub-CAs, Hardware Security Module (HSM), Qualified Signature Creation Devices (QSCDs)).
   ii. Specify hosting options supported (cloud, vendor premises, on-site at customer).
   iii. Outline security measures, key management, and operational best practices.
   iv. Describe whether the CA operators can be NATO cleared personnel or not.
   v. Confirm compliance with eIDAS requirements and any other applicable regulations.
   vi. Describe how you will address the liability requirements for Trust Service Providers (as per eIDAS), for Options 1 & 2.

ii. Certificate lifecycle management
   i. Describe how Registration Authority (RA) functions are performed in this model.
   ii. Explain identity vetting workflows (local desk, online/eIDAS-compliant, delegated RA).
   iii. Explain how the identity information can be obtained from authoritative sources (e.g. manual creation for each record, integration with existing HR database systems etc.)
   iv. Confirm compliance with eIDAS requirements and any other applicable regulations.
   v. Describe how the tokens can be issued (e.g. issuance at a local desk, shipping by mail after registration etc.)
   vi. Describe the revocation process

iii. Integration and Interoperability

i. Explain integration/interoperability capabilities with document signing /verifying platforms (e.g., Adobe AATL, Microsoft, Apple)

iv. Advisory and Compliance Support
   i. Describe any guidance services for building or operating an eIDAS compliant CA infrastructure.
   ii. Recommendations for achieving QTSP compliance and registration in trust lists (EUTL, AATL).
   iii. Describe how the legal liability requirements (Article 13 of EU Regulation No 910/2014) can be met and provide recommendations

v. Pros and Cons
   i. Provide observed advantages and limitations for this model, including:
   ii. Operational complexity,
   iii. Compliance and audit burden,
   iv. Cost and scalability,
   v. Legal and technical risks.

2.2. Email Signing (S/MIME)

For each deployment model (Option 1 – Managed QTSP, Option 2 – Vendor-Hosted CA, Option 3 – Organization-Operated CA), vendors are requested to provide information on the following (if the answers are irrelevant to the deployment model, answers may be consolidated/skipped):

vi. Use of QES for Email Signing
   i. Indicate whether the QES certificate solution can be used for trusted S/MIME email signing.
   ii. If not feasible, describe alternative approaches to achieve publicly trusted email signing.

vii. Integration and Practical Considerations
   i. Highlight any limitations, interoperability issues, or additional steps required to ensure trust validation across major email clients (Outlook, Apple Mail) and platforms (Windows, macOS, Linux, mobile).
   ii. Describe whether the same RA or identity validation process used for QES can be leveraged for trusted email certificates

viii. Pros and Cons
   i. Provide observed advantages and limitations of each approach for email signing and encryption, including operational complexity, compliance, and interoperability considerations.

2.3. Client Authentication Certificates (Enterprise Use)

NATO is exploring the possibility of storing client authentication certificates on the same smart card or token as Qualified Electronic Signature (QES) certificates. Respondents are requested to provide guidance and technical details regarding this scenario.

ix. Certificate Model and Issuance Options
   i. Indicate whether the QES certificates can be used for client authentication for Windows OS login (on-prem and Entra ID) with Microsoft's strong binding requirements between the identity and its certificates. If this is not feasible:
   ii. Indicate whether a client authentication certificates can be issued from a QTSP CA and stored on the same token as QES certificates. If this is not feasible:
   iii. Describe how a separate CA could be used to issue client authentication certificates that coexist with QES certificates on the same token. In such case:

1. Clarify whether NATO's existing internal CA can be leveraged for client authentication certificates or it would require the establishment of a new CA by the vendor that provides the QTSP CA.

x. Describe technical approaches for coexistence of certificates from two CAs on the same token, including:
- **i.** Key management and slot allocation,
- **ii.** Token initialization and personalization,
- **iii.** Middleware or driver requirements for applications (e.g., Windows logon, VPN, cloud identity).

xi. Explain how enrolment, renewal, and revocation would be handled when two CA hierarchies are involved.

xii. Outline any policy or security implications, including compliance with eIDAS.

xiii. Pros and Cons
- **i.** Provide observed advantages and limitations of using the same token for QES and client authentication certificates, including operational complexity, compliance, and end-user experience.
- **ii.** Describe lessons learned from similar deployments, if available.

2.4. Public-Facing TLS Certificates

NATO is seeking information on solutions and services for procuring and managing publicly trusted TLS/SSL certificates for websites, APIs, and other externally accessible services. This is separate from any qualified certificate or QTSP use case for user certificates.

xiv. Procurement and Issuance
- **i.** Describe your approach for providing publicly trusted TLS/SSL certificates for external domains and services.
- **ii.** Indicate participation in major root programs (Microsoft, Apple, Google, Mozilla) and adherence to CA/B Forum Baseline Requirements.
- **iii.** Explain supported certificate types (DV, OV, EV, wildcard, SAN/multi-domain) and issuance timelines.
- **iv.** Describe any automation options for certificate lifecycle management (e.g., ACME protocol, API integrations).

xv. Governance and Lifecycle Management
- **i.** Outline capabilities for centralized management of TLS certificates, including:
  1. Inventory and discovery of existing public facing website certificates,
  2. Renewal and revocation management,
  3. Reporting and compliance tracking.
  4. Monitoring of Certificate Transparency (CT) logs to detect unauthorized or unexpected certificate issuance.
- **ii.** Describe alerting and reporting mechanisms tied to certificate expirations, revocations, and CT log events.
- **iii.** Describe integration options with enterprise certificate lifecycle management (CLM) tools or PKI platforms, including support for automated provisioning across web servers, load balancers, and cloud services.

xvi. Pros and Cons
- **i.** Provide observed advantages and limitations of your solution for TLS certificate lifecycle management, including operational complexity, automation, scalability, and cost.

3. Costing and Pricing Models

Respondents are requested to provide information on rough costs and pricing models for each deployment model (Option 1, 2 and 3) and each use case (QES, Email/S-MIME, Client Authentication certificates, TLS certificates). The following tables are provided to facilitate the costing/pricing. However, respondents are welcome to modify these tables or provide rough order of magnitude estimates based on their own cost/pricing methods.

When you submit your reply to Annex A, please include a separate excel sheet for your ROM costing/pricing either by using the table provided below as model or by providing your own cost/pricing model.

i. Setup/Initial Costs

Cost Item	Description	One-Time Cost (Year 0)	Notes / Assumptions	Key cost drivers
CA Infrastructure Deployment	Root/Intermediate CA setup, HSMs, QSCDs			
RA/Enrolment Setup	Registration desk, identity vetting systems, integration			
Middleware / Token Provisioning	Smart card or token personalization			
Advisory / Consulting	eIDAS compliance, QTSP onboarding, audit support			
Integration with Enterprise Systems	Document signing, email, authentication systems			
Other	Specify			

ii. Recurring Operational Costs

Cost Item	Description	Annual Cost (Year 1–5)	Notes / Assumptions	Key cost drivers
CA Operation	Hosting, key management, maintenance			
RA Operations	Delegated RA, identity verification			
Support & Monitoring	Helpdesk, incident response, alerting, CT monitoring			
Lifecycle Management	Renewal, revocation, reporting			
Software Licenses	Middleware, CLM tools, HSM software			
Other	Specify			

iii. Per-certificate Costs

Certificate Type	Volume / Year	Cost per Certificate	Total Cost / Year	Notes / Assumptions	Pricing tiers or packages?
QES / QSeal					
Email / S-MIME					
TLS / SSL					
Client Authentication					

iv. Lifecycle Extension / Renewal Costs

Cost Item	Description	Cost Over 5 Years	Cost Over 10 Years	Notes / Assumptions
Certificate Renewal	Per-certificate renewal fees			
Token / QSCD Replacement	Hardware refresh / re-personalization			
RA Operations	Identity re-validation / enrolment			
Other	Specify			

v. Optional / Value-Added Services

Service	Description	Cost (One-Time or Annual)	Notes / Assumptions	Key cost drivers
Certificate Transparency (CT) Monitoring	Alerting and reporting on CT logs			
Automated TLS Management	API or ACME integration			
Reporting / Dashboards	Certificate inventory, compliance reports			
Premium Support	SLA, response times, dedicated support			
Other	Specify			

4. Supplementary questions

i. Describe your roadmap for PQC. When do you expect to be able to issue PQC certificates to meet the aforementioned use cases? Considering that the initial deployment will use non-quantum resistant (classical) cryptography, what would be your recommendation for transitioning from classical to PQC, in the context of the services requested in this RFI?

ii. For Options 1 & 2, describe how you would address a new vulnerability/weakness affecting the crypto components (algorithms, ciphers, hash functions, or the tokens etc.) used as part of the service.

iii. For Options 1 & 2, provide the SLA that you can offer for these services.