NCIA/ACQ/2017/2096
06 November 2017

Notification of Intent to Invite International Competitive Bids

Provision of Service Oriented Architecture & Identity Management Platform (SOA & IdM)

Project Reference: 2014/0IS03094

Estimated Project Value: 10,440,458 EUR

The project is intended to provide the underlying SOA & IdM Platform that will enable NATO to rapidly deliver integrated information systems. The platform will allow other projects to use consistent, coherent and proven solutions to common problems.

NCI Agency Principal Contracting Officer responsible for this solicitation is Mr. Giacomo Piliego; all correspondence regarding this IFB should solely be addressed to:

Mr. Curtis Day
E-mail: Curtis.Day@ncia.nato.int

To: Distribution List

Subject: **Notification of Intent to Invite International Competitive Bids for the Project: Service Oriented Architecture & Identity Management Platform (SOA & IdM) IFB-CO-14176-SOA-IDM**

Reference(s) :

A. AC/4-D/2261 (1996 Edition)
B. AC/4-D/2261-ADD2 (1996 Edition)
C. AC/4-D(2008)0002-REV2
D. SOA & IdM TBCE - NCIA/EM/NLO/2014/03202, dated 31 October 2014
E. AC/4(PP)D/27047-ADD2, dated 7 September 2015
F. AC/4-DS(2015)0024, dated 18 December 2015
G. AC/4(PP)D/27047-ADD3 dated 3 July 2017
H. AC/4-DS(2017)0017

1. In accordance with References A through H, notice is given of the intent of the NATO Communications and Information Agency (NCI Agency), as the Host Nation, to issue an Invitation for Bid (IFB) for the provision of Service Oriented Architecture and Identity Management (SOA & IdM) Platform.

2. The project is intended to deliver the underlying SOA & IdM Platform that will enable NATO to more rapidly implement and deliver integrated information systems. The Platform will allow future projects to use consistent, coherent and proven solutions to common problems thereby allowing them to focus on delivering business value.

3. Together with the Infrastructure as a Service capability being delivered through IT Modernization project (ITM), the Platform will change the way NATO builds and procures FS (Functional Service) applications by allowing reuse of common functionality to reduce stove pipe solutions and more readily share data.

4. Specifically, this project will provide:

   4.1. A middleware platform in the form of a common set of Web Services that are responsible for security, integration, registry & repository, service management, information discovery and hosting;

   4.2. Refined Identity Management (IdM) business processes with a set of IdM services to FSs and other Core Services;

   4.3. Additional security services and control mechanisms;

   4.4. Integration with NPKI (NATO Public Key Infrastructure) to support strong authentication;

   4.5. Interfaces with other current and future IdM-related systems;

   4.6. The Alliance Replication Hub (ARH) as the directory interface between NATO and Nations.

5. Attached to this letter at Annex A is a summary of the project requirements. These requirements are being further refined and will be detailed as part of the upcoming SOA & IdM Platform Invitation for Bid (IFB).

6. The reference for the Invitation for Bid is IFB-CO-14176-SOA-IDM, and all correspondence concerning the IFB should reference this number.

7. The intention is to place an initial contract for Wave 1, with 3 additional Options which will be Costed and Evaluated Options, for Wave 1 O&M (Operation and Maintenance), Wave 2 and Wave 2 O&M.

8. The estimated investment cost for the services and deliverables included within the scope of the intended Wave 1 contract is 10,440,458 euros (125% Best Value celling amount).

The following phases are Costed and Evaluated options:

	Status	Cost (100%, No CR)	BV ceiling (125%)
Wave 1 O&M	Costed & Evaluated Option	€ 7,122,885	€ 8,903,606
Wave 2	Costed & Evaluated Option	€ 12,357,380	€ 15,446,725
Wave 2 O&M	Costed & Evaluated Option	€ 11,347,043	€ 14,183,804

Funding for this project is provided by the Investment Committee "at 28".

9. No partial bidding will be allowed, Bidders must provide a proposal for both Wave 1 (one) and all three of the Costed and Evaluated Options.

10. The NCI Agency has been authorised to use the International Competitive Bidding (ICB) Best Value (BV) procedures. The successful bid pursuant to this IFB will be that bid which is deemed to offer the best value for money in accordance with predefined bid evaluation criteria which will be detailed in the IFB as prescribed by the Reference C

11. Agreed Top level criteria for evaluation are (40%) Price and (60%) Technical. The second level Technical sub-criteria for evaluation are Engineering (50%), Management (20%), Supportability (20%) and Risk (10%).

12. The evaluation of the bids will be undertaken equally on the basis of Wave 1 Cost plus three Optional phases.

13. The formal IFB is planned to be issued in the Q4 2017. The Bid Closing Date will be in Q1 2018. Contract award is anticipated to be in Q1 2019.

14. National responsible authorities are kindly requested, to provide the NCI Agency with Declarations of Eligibility, no later than **4th December 2017** with the details of qualified and certified firms which are interested in bidding for this project. In addition to the certification of the firm's security clearances required under this NOI, the Declarations of Eligibility should include the following information for each of the nominated firms: **Name of the Firm, Telephone number, Fax number, E-mail address and One (1) Point of Contact**. This information is critical in order to enable prompt and accurate communication with prospective Bidders and should be sent to the following address:

NATO CI Agency
Boulevard Leopold III
1110 Brussels, Belgium

NCI Agency Contracting Officer responsible for this solicitation is Mr. Giacomo Piliego; all correspondence regarding this IFB should solely be addressed to: Mr. Curtis Day
E-mail: Curtis.Day@ncia.nato.int

15. It must be emphasised that requests for participation in this competition received directly from individual firms cannot be considered.

16. Bidders will be required to declare a bid validity period of twelve (12) months from the closing date for receipt of bids. This must also be supported by a Bid Guarantee of EUR 300,000 (three hundred thousand Euro). Should the selection and award procedure exceed the Bid Closing Date by more than twelve (12) months, firms will be requested to voluntarily extend the validity of their bids and the Bid Guarantee accordingly. Bidders may decline to do so and withdraw their bid and thereby exclude themselves from the bidding process without penalty.

17. National authorities are advised that the IFB package is anticipated to be NATO UNCLASSIFIED; however, the bidding and the contractual documents are expected to contain references to other NATO documents classified as "NATO RESTRICTED". Bidders must therefore have a personnel security clearance of "NATO RESTRICTED" or above in order to be eligible to review the applicable referenced documents.

18. The successful Bidder will be required to handle and/or store classified information up to the level of "NATO SECRET" during the execution of the Contract. In addition, Contractor's personnel will be required to work unescorted in Class II and Class I Security Areas. Access to these areas can only be permitted to cleared individuals holding individual clearances of "NATO SECRET". Only companies maintaining such cleared facilities and the appropriate personnel clearances will be able to perform the resulting contract.

19. Please note that it is anticipated that the IFB at the time of its issuance will contain an Organizational Conflict of Interest (OCI) provision to exclude any Bidder who is deemed to be in a position to unfairly influence the IFB as a result of being selected for the work performed or to be performed under other Contracts with NATO. This project is listed in the Excluded Project List under reference NCIA/EM/NLO/2014/03155 dated 22 July 2014.

20. Your assistance in this procurement is greatly appreciated.

FOR THE GENERAL MANAGER:

Giacomo Piliego
Principal Contracting Officer

Attachment(s):

Annex A: Summary of Requirements (NOI)

Annex A - Summary of the Requirements
NOI

1. Introduction

1.1. Historically, NATO capabilities have been delivered as a collection of self-contained, individual systems. Separate projects procured all the necessary hardware, software and services required to implement a required capability, which operated within its own system and information silo. These systems rarely shared information between themselves, and certain features and functionality were recreated time and again. These characteristics of systems do not take advantage of economies of scale or the rationalisation of Information Technology (IT) infrastructure that NATO is capable of leveraging.

1.2. NATO is now changing the way it delivers its Information Technology (IT) and Communications infrastructure and applications. Under the banner of "IT Modernisation", it is shifting from an independent, stove-piped approach to a more granular set of loosely coupled services that can be quickly and easily composed to deliver agile and cost-effective support to operations.

1.3. Future systems within NATO will adapt to the architectural paradigms adopted in modern Cloud Computing solutions, as originally outlined in the NATO Network Enabled Capability (NNEC) Feasibility Study and which have been broadly and successfully implemented in militaries and industries across the NATO Nations.

1.4. The IT infrastructure of the future will be consolidated into a limited number of data centres, based on a common hardware platform and with a centralised Operations & Maintenance environment. All of this will be delivered as a service (known in Cloud Computing terms as "Infrastructure-as-a-Service", or IaaS).

1.5. At the applications/systems level, the IT platform of the future will provide the environment to enable systems developers to rapidly implement and deploy new capabilities and reuse existing capabilities into the NATO functional landscape. In Cloud Computing terms this is known as "Platform-as-a-Service" or PaaS.

1.6. PaaS is a category of Cloud Computing services that provides a platform allowing for the development, execution, and management of applications without the cost and complexity of building and maintaining the underlying common services necessary for almost all applications.

1.7. Providing the NATO Enterprise with a robust, secure PaaS environment is the primary role of the SOA & IdM Platform.

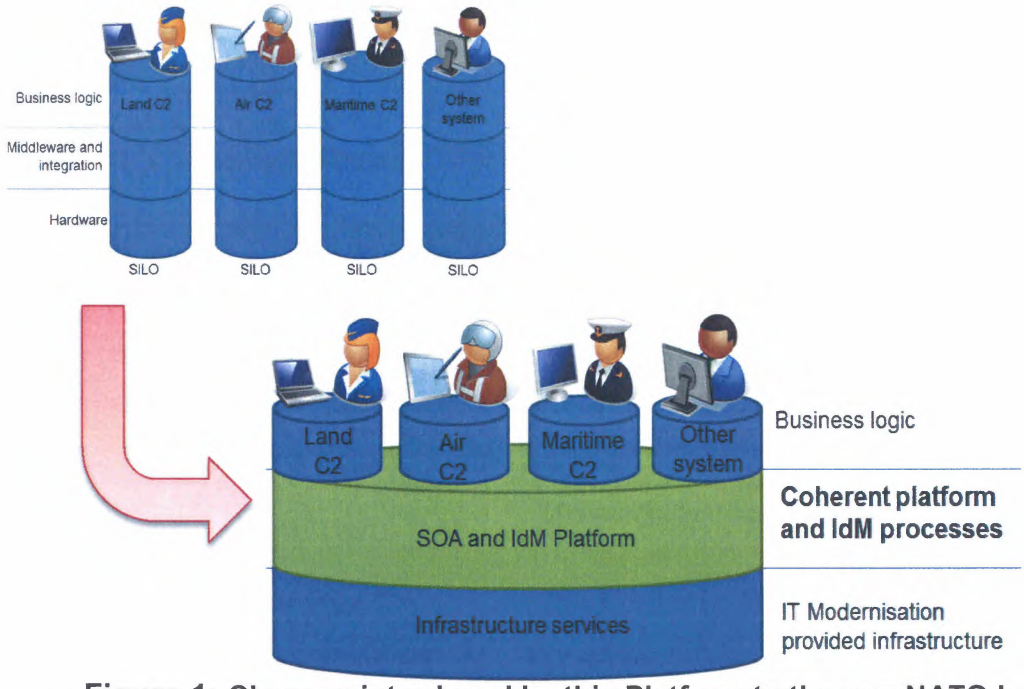

Figure 1: Changes introduced by this Platform to the way NATO builds software

2. Project scope

2.1. The SOA & IdM Platform services will be installed and operated on the Operational Network (ON) which operates up to NATO SECRET level, and on the NATO Enterprise Protected Business Network (PBN) which operates at the NATO RESTRICTED and at the NATO UNCLASSIFIED levels.

2.2. The Platform will be implemented across the NATO Enterprise on computing nodes (Data Centres) which are to be provided by the related IT Modernisation (ITM) project.

2.3. A complete suite of the SOA & IdM Platform services will be provided at each Data Centre.

2.4. The Platform services will be provided for:

2.4.1. a Testbed and a Reference environment,

2.4.2. Training and Mission preparation environments

2.5. 2.5 The services to be provided by the Platform are outlined in the picture below. Their provision will be split into two (2) Waves.

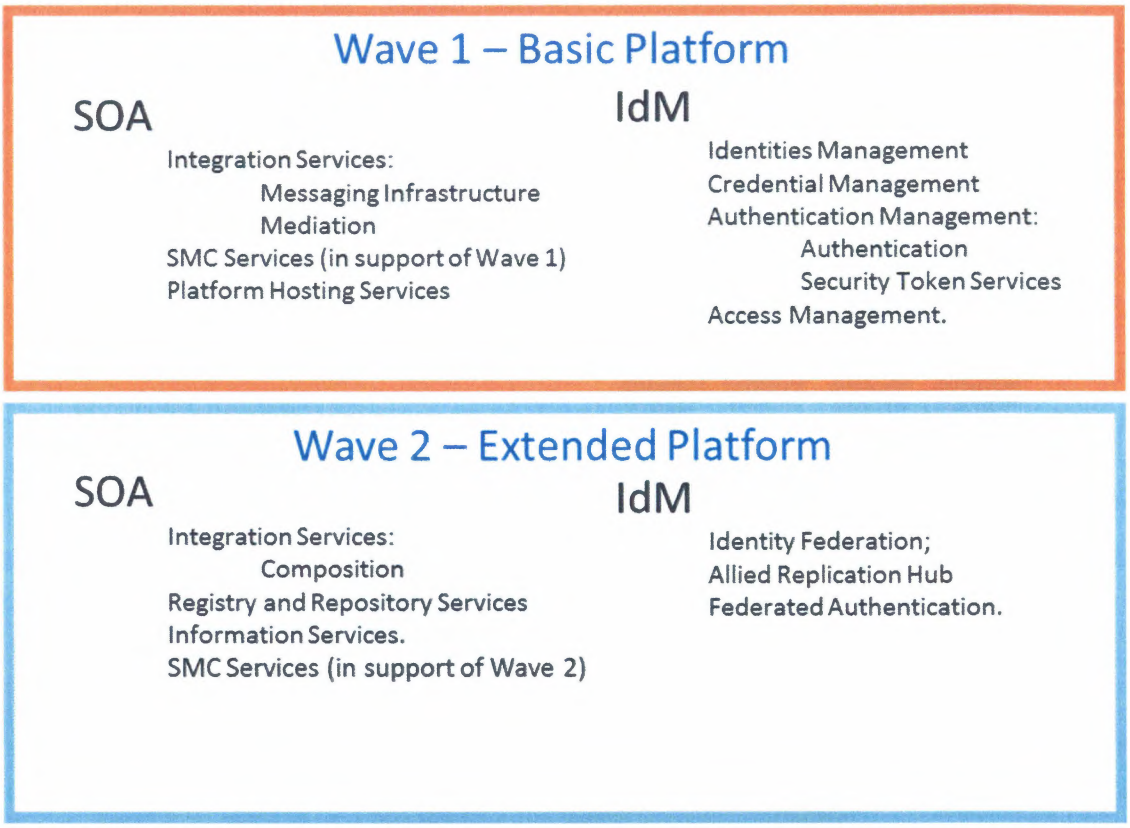

Figure 2: Waves description

2.6. The project scope will include:

2.6.1. Project management

2.6.2. Requirement analysis, system engineering / design, testing, site surveys

2.6.3. Security accreditation

2.6.4. Site implementation

2.6.5. Integrated Logistics Support (ILS)

2.6.6. 5-year Operation and Maintenance (O&M) support as contract options

3. Notional architecture

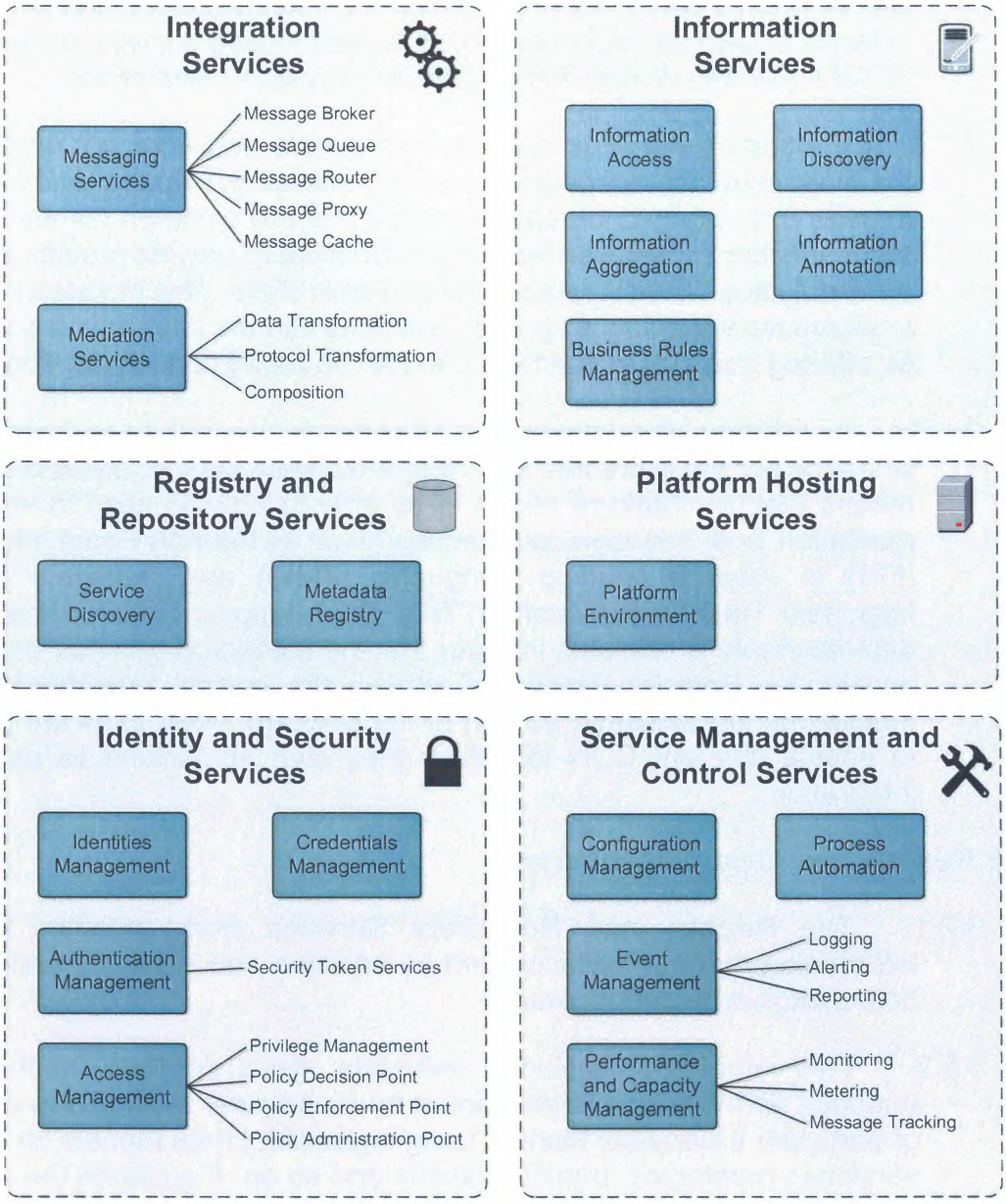

Figure 3: Platform Services

3.1. Integration Services

3.1.1. One of the primary functions of the Platform is to provide interoperability between systems or system components, in order that data from one system can be easily and efficiently distributed with others regardless of the data payload (images, text, video etc.).

3.1.2. The Integration Services provide the key information exchange capabilities of the SOA Platform. They provide the connections between different service providers and consumers in a transparent, easy to use and reliable way (Messaging). They are data agnostic, though they can be configured to support different outcomes according to values or structures

within the data, including prioritisation of critical messages (Routing). Likewise, they can perform mediation between providers and consumers, in terms of data structures or protocols, seamlessly allowing the exchange of data between diverse heterogeneous systems (Mediation).

3.1.3. Integration Services support both simple and complex modelling of the interactions, leveraging the use of Messaging, Routing, and Mediation in order to produce compound services that are common combinations of other services. These can be further combined to provide greater and more powerful capabilities in more rapid and agile ways. This includes the ability to incorporate existing proprietary services into the information ecosystem by offering a standard interface that can be easily consumed (Proxying).

3.1.4. In addition, the consumers of services are not necessarily known when the service is created and there are always unanticipated users. This means that the Platform needs to be able to provide easy to implement mediation, both between data formats (such as Friendly Force Information (FFI) to Keyhole Markup Language (KML)) and protocols (FTP to Hypertext Transfer Protocol (HTTP)). The mapping between the various data elements is reusable in order that the mediation services are able to access the Registry directly to retrieve the correct stylesheets. Some mediations are delivered as part of the platform, while tools are provided to enable different COIs to deliver their own mediations as part of FS integration.

3.2. Registry and Repository Services

3.2.1. The Registry and Repository Services work together to store information that can be accessed by services and service developers at both design time and runtime.

3.2.2. This information includes metadata about services, such as the endpoint and interface implemented by a particular service, the schemas of particular eXtensible Markup Language (XML) data models (in different versions), ontologies, transformations and so on. It supports the advance and dynamic discovery of services and information sources.

3.3. Service Management and Control (SMC) Services

3.3.1. In order to optimise the efficiency and availability of services, it is important that their status is continuously monitored, not only at the machine level, but also at the service level. Therefore the Platform is integrated with the SMC system that is in place across NATO. This is also linked to other services, such as the Registry, to allow the dynamic allocation of service endpoints based on current service performance. The monitoring of services also supports meeting Service Level Agreement (SLA) targets, and – if necessary – the metering (and charging) of services.

3.3.2. The Platform's SMC Services provide a suite of capabilities needed to ensure that SOA services are up and running, accessible and available to users, protected and secure, and that they are operating and performing within agreed upon Quality of Service and SLA parameters.

3.4. Platform Hosting Services

3.4.1. Platform Hosting provides environments which can be used for developing, testing, deploying and operating web applications and services.

3.5. Information Services

3.5.1. NATO systems provide vast amounts of information, which are usually only available within specific COIs or in formats that are not immediately accessible to, or exchangeable with, the data stores of other systems. The Platform provides the mechanisms to make information sources discoverable and accessible by FSs, business applications or human users, across organisational boundaries and communities of interest.

3.5.2. The Information Services provide capabilities to the NATO Enterprise required to manage the enterprise information sphere. They provide a uniform way of representing, accessing, maintaining, managing, analysing, and integrating data and content across heterogeneous information sources. It includes information access, discovery, aggregation and annotation, as well as business rules engines.

3.6. Identity and Security Services

3.6.1. The overall capability of Identity and Access Management (IAM) is a framework that facilitates the management of electronic identities, and the assignment of their rights and privileges. It is described as "the security discipline that enables the right individuals to access the right resources at the right times and for the right reasons".

3.6.2. The Platform increases the use of a common, centralised security framework. This improves the time to deliver systems, through more streamlined accreditation processes, while at the same time hardening the security posture.

3.6.3. Administrators do not have to constantly be provisioning and de-provisioning accounts. Instead, the number of identities required by individuals to perform their duties is reduced, by implementing enhanced IAM processes and centralised access control as well as by applying Single-Sign-On (SSO) solutions that leverage new federation capabilities in the NATO Enterprise. The identity information is passed through different systems and services, delivering true, end to end authentication. Access control is again centralised, and based on policy, thus widening the availability of potential consumers ("responsibility to share") while at

the same time ensuring only those with the "need to know" can perform action on the data.