ANNEX II + III: TECHNICAL SPECIFICATIONS + TECHNICAL OFFER

Contract title: Supply of IT equipment and software for the establishment of a single "National centralized criminal intelligence system" (NCIS)

Publication reference: EuropeAid/139498/DH/SUP/RS

LOT 4 – Supply of SOA rack mountable network XML appliance, application instance for KOS/NCIS system

Columns 1-2 should be completed by the Contracting Authority
Columns 3-4 should be completed by the tenderer
Column 5 is reserved for the evaluation committee

Annex III - the Contractor's technical offer

The tenderers are requested to complete the template on the next pages:

- Column 2 is completed by the Contracting Authority shows the required specifications (not to be modified by the tenderer),
- Column 3 is to be filled in by the tenderer and must detail what is offered (for example the words “compliant” or “yes” are not sufficient)
- Column 4 allows the tenderer to make comments on its proposed supply and to make eventual references to the documentation

The eventual documentation supplied should clearly indicate (highlight, mark) the models offered and the options included, if any, so that the evaluators can see the exact configuration. Offers that do not permit to identify precisely the models and the specifications may be rejected by the evaluation committee.

The offer must be clear enough to allow the evaluators to make an easy comparison between the requested specifications and the offered specifications.

Unless otherwise specified, the requirements in these Technical Specifications are presented as a minimum standard which the offered goods must meet in order to be compliant. Tenderers may not submit a variant solution for the items required in these Technical Specifications. The tenderer is expected to submit documentary evidence (brochures, technical data sheets etc.) of the technical compliance of his offer.

Provided documentation must be tidy organized, and all items in respective documentation must be clearly identified (highlighted and indicated by "Item Number").

The documentation's page numbers where the information could be found must be clearly stated in the "Notes, remarks, ref to documentation" column of the offer.

EU Visibility: All supplies shall comply with the visibility Manual for EU External Actions (https://ec.europa.eu/europeaid/communication-and-visibility-manual-eu-external-actions_en) as well as the EU Visibility Manual produced by the EU Delegation to Serbia.

Stickers should be placed on the supplies with a clearly visible EU flag and the phrase "Provided with the support of the EU" in the operational language of the EU programme and in the Serbian language.

A visibility event should be foreseen and financed by the contractor and organised in conjunction with the Contracting Authority.

Abbreviations

The following abbreviations are used consistently throughout the document:

AC	Alternating current
CE	Conformité Européenne
EU	European Union
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KOS	National Integrated Criminal Intelligence System
MoI	Ministry of Interior
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SSL	Secure Sockets Layer
UDDI	Universal Description, Discovery, and Integration
URL	Uniform Resource Locator
WSDL	Web Services Description Language
XML	Extensible Markup Language
XSD	XML Schema Definition

Project scope:

The delivery includes psychical installation of the hardware and installation of the appropriate system and application software in order to be provided all prerequisites for the further project deliveries:

- Installation and configuration of equipment
- SSL/network links configuration between the KOS extranet and MoI network
- Maintenance and support during the warranty period (12 months).

Prerequisite:

The delivery of SOA rack mountable network XML appliance with additional advanced operations for centralized troubleshooting compatible with existing IBM DataPower device with security module and IBM DataPower Operations Dashboard is in line with the National action plan for Chapter 24, Recommendation 2 "Prepare for the establishment of a single centralised criminal intelligence system and a safe platform for communicating between law enforcement bodies." and activity 6.2.2.4. It is required because it provides single centralised safe platform for communicating between law enforcement bodies. In addition, it is required because the beneficiary:

- Has developed already specific software for running KOS-like Extranet applications at MoI
- Has ensured security by splitting physically two systems (internal system, separated from the external)
- Has provided single centralised safe platform for communicating between law enforcement bodies as it is single point of authorisation for the systems at MoI
- Allows to control secured and optimised access via ESB-like interface (Activity 6.2.2.2) for shared data at MoI, serving them to the other enforcement bodies

The new device has to be compatible with existing IBM DataPower currently is running at MoI site and the authorisation process has to be based on centralised safe single point of authorisation for all systems at MoI. It has to work together with IBM Data Power device. The new device also has to cover optimised SOA data exchange. It is based on XSD schema / XML data, which is in line with Activity 6.2.2.2 from the action plan for standards of data exchange. Now the authorisation procedure is integrated into device and all running applications including current Extranet are considering this availability.

The new device has to work in parallel for the new KOS system in line with existing for Extranet system IBM Data Power. Extranet is internal system at MoI and it relies on existing IBM Data Power. The Extranet system is fully developed and operational. It is heavily used, being proven to be stable and reliable. The development of the system was completed by MoI IT department in-house within 3 years. The system is maintained by MoI staff on daily basis. For its systems, MoI is using IBM DataPower as single point of authorisation and it provides controlled and optimised access to the MoI databases. Since 2015, Extranet is running successfully inside and outside MoI for registered number of users, providing more than 10000 requests per month to various public authorities.

The new KOS system will be based on developed Extranet system. KOS system will decrease the number of users restricting them to law enforcement bodies only, but it will increase the list of the provided type of data, following protection of personal information. The current functionality will be kept while the data model will be extended. Single point of registration shall be kept. MoI invest in Extranet system own experts' time and significant financial resource. The new device for KOS system has to be fully compatible with existing equipment and the developed software for Extranet system.

New appliance has to be compatible with IBM DataPower Gateway with HSM Card Appliance - D1AT1LL

New application instance has to be compatible with IBM DataPower Operations Dashboard Single Gateway Application Instance - D1NAWLL

Both of the items have to be delivered with 12 months subscription and support

The Beneficiary owns all server and client licenses, data models and source code for the developed application software that is used for performing of the already completed tasks, and could be used by new redesigned models. The completed list of all licenses is provided in Table 1. Adoption of these particular software licenses for the tendered appliances is however not compulsory.

The Bidder may decide to reuse in its proposal these licenses. If the reuse of existing licenses is selected, then in the offer these licenses shall be delivered in its last version with option to downgrade to existing one accordingly.

The Bidder may choose also to use different licenses and appliances. In this case the Bidder shall deliver in addition to requested also replacement of existing appliances with their corresponding licenses for both existing and extended KOS system, and shall assure and deliver full redesign and redevelopment of existing applications and data models, triggers and stored procedures that are currently in use, assuring with it full compatibility with other existing systems and applications.

Delivery summary

Lot 4: Supply of SOA rack mountable network XML appliance, application instance for KOS/NCIS system		
No.	**Item(s)**	**Quantity**
1.	SOA rack mountable network XML appliance	1
2.	Application Instance for SOA rack mountable network XML appliance advanced operations for centralized troubleshooting	1

General requirements for hardware and system software:

Regarding safety requirements, equipment must have necessary operational warnings as well as mechanical interlocks on the equipment operating/generating more than 30 Volts AC or DC, in accordance with current IEC and EU standards.

Software must be licensed to the Beneficiary in order to allow trained personnel of the Beneficiary to perform software installation, update/upgrade, repair/debug and/or diagnosis/report activities without Tenderer assistance.

Equipment allowing capacity upgrading must be provided in a way that upgrades can be performed by installing additional capacity, without discarding the already installed capacities.

Equipment delivery, including final installation must include all miscellaneous but needed items for equipment delivery and installation in order that the supplies are left in place fully operational and ready for use. Consumables used during delivery, installation and during testing time before provisional acceptance, must be anticipated and calculated in the offer. It shall be the sole responsibility of the Tenderer to check all site dimensions for completeness of equipment delivery before the commencement of delivery.

The Tenderer must provide necessary measures to prevent any damage during any/all delivery and installation stage(s). If damage occurs, it must be rectified in an appropriate way by the Tenderer, which must keep the work site clean and safe against fire and/or other hazards during any/all delivery and installation stage(s) until formal acceptance.

Equipment must conform and/or be compatible with any standards, or with the commonly accepted best production practices currently in force, including any ISO, IEC or other relevant standards that may apply to each specific category of equipment. The Tenderer must deliver a certificate of conformity (issued by a quality control independent regulatory agency of recognized competence) for each equipment item or group of items.

Equipment must conform to the relevant CE regulation; all equipment must be CE compliant and fully authorised for use in Europe.

Mains power supply should operate on 220V − 20V, 50Hz - 60Hz, and be suitable for direct connection to the standard power outlets in Beneficiary country.

Items to be delivered

1. Item Number	2. Specifications Required		3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
1.	**SOA rack mountable network XML appliance**	**Quantity: 1**			
	Manufacturer's name:				
	Product type, model:				
1.1.	SOA rack mountable network XML appliance, compatible with IBM DataPower Operations Dashboard Single Gateway Application Instance License + SW Subscription & Support 12 Months (D1NAWLL)				
1.2.	The requested device is XML Gateway, a dedicated network device designed to provide protection for all protocols using XML data format (SOAP / Web Service).				
1.3.	The device must provide a graphical way of configuring the processing flow for each of the Web services that it protects. The processing flow should support an architectural style known as Pipes and Filters: http://www.enterpriseintegrationpatterns.com/patterns/messaging/PipesAndFilters.html). Configuring the processing flow should support the so-called "drag and drop" method of inserting process components (filters). The basic process components that the device needs to perform on the message (both when accepting an incoming message and when returning the response) are encryption and decryption, content checking, protection against all XML attack types, digital signing and signature verification, content transformation, authentication and authorization sender, journalism, flow control. All these filters should be provided in the device, and the configuration of the filters themselves in a specific scenario (for example, the location of the authentication and authorization data repositories) should be simple and intuitive.				
1.4.	The device must be tamper-proof (i.e. automatically shut off in case of opening), manufactured by the manufacturer as an integrated system with specialized				

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	hardware, adapted with the appropriate firmware and built-in OS (operating system).			
1.5.	The device must have an HSM (Hardware Security Module) installed for private keys protection.			
1.6.	The device must have a strictly controlled way of accessing all the data contained therein, it may not have unnecessary ports.			
1.7.	The device must prevent the installation of an interpreter of any programming language.			
1.8.	The device must be Rack-mountable network device designed to fit into the standard industrial rack. Network connectivity is via Ethernet interface.			
1.9.	The device must support any-to-any data transformation between a wide range of data formats, including XML, text and binary formats.			
1.10.	The device must protect against attacks such as XML Denial of Service (XDoS), buffer overflow, or vulnerability to deliberately or inadvertently created malicious XML documents.			
1.11.	The device should have the ability to act as a point of implementation of the rules, or as a central subsystem that will control all defined policies - (authentication, authorization, validation, timestamping, etc.).			
1.12.	The device must support at least this encryption method: XKMS, RSA, 3DES, DES, AES, SHA, X.509, PKCS, CRLs, OCSP, XML digital signature, time stamp and undeniability, SSL.			
1.13.	The device must support encryption / signing at both field level and document level.			
1.14.	The device must support various access control mechanisms, including XACML, Security Assertion Markup Language (SAML), SSL, LDAP, RADIUS, and a simple client / URL tables.			

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
1.15.	The device must support all WS- * standards.			
1.16.	The device must support WS-Policy Framework and WS-Policy Attachment. The device should automatically insert WS-Policy metadata into WSDL so that customers can automatically generate requests that match the given policies.			
1.17.	The device must support SAML versions 1.0, 1.1 and 2.0.			
1.18.	To verify the identity of users, the device should provide the ability to verify users by validating the certificate, extracting identities from different security tokens in the message header / protocol, and checking external (e.g. LDAP) or internal (high-security) identity repositories.			
1.19.	The device must provide the ability to validate the input that is used by comparing data in the WSDLs XML Schema, XSLT can also be used.			
1.20.	The device must provide the functionality of external configurable auditing.			
1.21.	Administrative access to the device must be provided via SSL.			
1.22.	The device must support the ability to upgrade firmware in an easy way (the ability to download firmware and upgrade to the device, with all the configurations being saved).			
1.23.	The device must support an active-active fail-over configuration. The device must provide redundant network ports for fail-over functionality.			
1.24.	The device must support SNMP traps for system management.			
1.25.	The device must provide a wide range of diagnostics and troubleshooting options, including basic network connectivity tests (ping, access to a specific remote port, etc.), and the ability to monitor and correct errors in data flows. This device should provide the ability to capture packages that will help detect problems at the network level.			
1.26.	The device must support execution priorities (the ability to design or speed up			

1. Item Number	2. Specifications Required		3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	traffic to maintain SLA's).				
1.27.	The device must support integration with any UDDI products.				
1.28.	The device must provide the ability to use the off-load of a Web service that protects it by running XPath routing, depending on the number of messages.				
1.29.	The device must provide the ability to control the flow of messages to a particular Web service, as well as to control the forwarding of messages that come from a specific client or from a particular network segment.				
2.	**Application Instance for SOA rack mountable network XML appliance advanced operations for centralized troubleshooting**	**Quantity: 1**			
	Manufacturer's name:				
	Product type, model:				
2.1.	Application Instance for SOA rack mountable network XML appliance advanced operations for centralized troubleshooting, compatible with IBM DataPower Operations Dashboard Single Gateway Application Instance License + SW Subscription & Support 12 Months (D1NAWLL)				
2.2.	Softer for providing the advanced operations for real-time visibility of transactions and centralized operations for offered XML Gateways,				
2.3.	Deep operational insight into offered XML Gateways for quicker problem determination and operational resiliency.				
2.4.	Full-text search across transactions and service configuration.				
2.5.	Change audit to review changes: - Ensure production consistency - Track administrative changes and correlate them to changes in the				

1. Item Number	2. Specifications Required	3. Specifications Offered	4. Notes, remarks, ref to documentation	5. Evaluation Committee's notes
	behaviour of services.			
2.6.	Self-service console to provide developers controlled access to transactions.			
2.7.	Easy creation of automated reports from transactions for compliance and audit requirements.			
2.8.	Detect security errors from transactions, expired certificates and invalid login to administrative console.			
2.9.	Comprehensive transaction details including payload and system log entries.			

Annex 1 - Delivery Locations

No.	Location	Address	Contact person	Contact e-mail	Contact phone
1	Ministry of Interior	Kneza Miloša 101, 11000 Beograd			