CLARIFICATION NO.3

EUSPA/OP/11/21

(EUSPA PKI)

Question 1: Which particular accreditation is mentioned in SoW document as "accreditation of the PKI System (defined mainly in the sections 2.1, 2.2 and 3.7 of this SoW and in the section 2.3 of CISL [AD-01])"?

Answer:

The accreditation of the PKI System will be performed according to the Security Accreditation and Certification documents that will be provided according rules defined in section 2.5.1 of the EUSPA PKI -Tender Specification

Question 2:

- How many "issuing certification authorities" will there be in level 3 of CA chain?

Although issuing authorities are not in scope of RFP, it may affect the processes

designed for those two superior levels in the authority chain.

- How many authorities are you considering on each level (on RCA level and SCA level)?

Answer:

Only one RCA will be implemented.

In the initial phase only one SCA and one ICA will be implemented for OSNMA service provisioning.

In the future other SCAs and ICAs for new services will be implemented.

For the future services, the expected number of new SCAs is < 5 and expected number of new ICAs is < 10.

Question 3: What is meant by OPER chain and VAL chain? Is VAL chain part of system dedicated to issuing of CRL and OCSP?

Answer:

The PKI OPE chain is the PKI system operated by PKI operators in order to support the service provisioning.
The PKI VAL chain is the PKI system used to validate new features and for training purpose and it is not directly involved in the service provisioning.
The functionality related to CRL has to be implemented by both PKI systems (PKI OPE chain and PKI VAL chain)

Question 4: Will the contractor be requested to deploy a testing platform?

Answer:

The OPE Chain shall be deployed at EUSPA GSC to be validated at QR milestone (RCA shall be shipped to EUSPA HQ after the qualification).

The VAL Chain shall be deployed at EUSPA HQ and EUSPA GSC to be validated at ORR milestone.

As mentioned in the Statement of Works, the Contractor shall be responsible for shipping any asset procured within the Contract that remains in their premises at the end of the Contract (e.g. development or factory qualification platform) to an EU location upon request of the Contracting Authority, or for the disposal of any item not requested to be transferred without additional cost.

Question 5: What are the requirements for registration authorities? What is the Process of requestor verification?

Answer: The PKI has to implement the functionalities of a registration authority (RA) in order to verify the identity of entities requesting the certificate signing request and to manage the certificate lifecycle (revocation). The bidder is expected to propose processes and procedures fitting with the purpose of the PKI.

Question 6:

- What should be a default validity of root certificates? (How many years?)
- What is your requirement regarding the cryptographic algorithms used and length of hashes etc? (RSA, ECC, SHA…)
- HSM:
  1. Is delivery of HSM part your requirements?
  2. Do you use HSMs now and what HSMs do you use?
  3. From the point of view of maintenance and operations, do you prefer to use HSM from one vendor?
  4. What are your requirements regarding HSM certifications?

Answer:
The detailed PKI requirements (validity of certificates, HSM,..) are specified in the document EUSPA-SEC-SREQ-A12887-RUE 1.2 that will be provided according rules defined in section 2.5.1 of the EUSPA PKI -Tender Specification.
Selected HSM should be a cryptographic product approved by the Secretary General of the Council (see List of Approved Cryptographic Products 5335/5/21)
HSM delivery is part of the procurement and from the point of view of maintenance and operations, the use of one type of HSM is preferable

Question 7: Is there a requirement for automated issuance of certificates? If so, which specific industry standard protocols shall be implemented (SCEP, ACME,..)?

Answer:
There is not a specific requirement for automated issuance of certificates

Question 8:
What types of CDPs (CRL distribution points) should be implemented in the system?
Should OCSP responder be a part of the delivery?

Answer:
The PKI System has to define and maintain a Certification Revocation List that has to be shared with the ICA and published in a web server for user consultation. In case the Online Certificate Status Protocol (OCSP) is implemented to check the revocation status of a digital certificate, OCSP responder has to be part of the delivery.

Question 9: What are EUSPA expectations concerning a certificate storage repository available to applications or users? (LDAP, ActiveDirectory, database, other..)

Answer:
The PKI system has to implement and maintain a database for storing the certification requests and security events. The PKI System has also to define and maintain a Certification Revocation List that has to be shared with the ICA and published in a web server for user consultation. Detailed PKI requirements are specified in the document EUSPA-SEC-SREQ-A12887-RUE 1.2 that will be provided according rules defined in section 2.5.1 of the EUSPA PKI -Tender Specification.

- End of document -