CLARIFICATION NO.6

EUSPA/OP/11/21

(EUSPA PKI)

Question 1:

a) Regarding the requirement "PKI-SOW-0130" described in the SoW document ("Annex I.1_EUSPA-SEC-SREQ-SOW-A13466_1.0_PKI_SOW.pdf"):

"*PKI-SOW-0130: Internal Penetration test*
*After successful qualification and final deployment of the PKI System at EUSPA Headquarter in Prague and at EUSPA GSC site in Madrid, the PKI System shall be subject to an Internal penetration test carried out by a specialised company contracted by the contracto*r."
Could you please confirm that is a mandatory requirement to include an external company (subcontractor or member of the consortium) in the offer and that it is not possible to meet the requirement with the main contractor's own capabilities and considering a COTS PKI system with high security certifications (e.g. Common Criteria EAL4+)?

b) Could you please clarify if the above applies also to requirement "PKI-SOW-0140":

"*PKI-SOW-0140: Support of Execution of independent penetration tests*

After successful qualification and final deployment of the PKI System in EUSPA Headquarter in Prague and EUSPA GSC site in Madrid, the PKI System may be subject to independent penetration test by Contracting Authority. During that period contractor shall support the Contracting Authority as identified in the section 3.8."

Answer:

a) PKI-SOW-0130 is relevant to the internal penetration test to be performed by a specialized company contracted by the contractor. This activity may be also performed by main contractor in case this has the capabilities and may assure the independency in conducting this task.
b) The PKI-SOW-0130 does not apply to the PKI-SOW-0140 since the PKI-SOW-0140 is relevant to the penetration test performed by the Contracting Authority and the Contractor shall support the Execution of independent test providing required information.

Question 2: We need to confirm that in the case of proposing a COTS solution developed by the prime Contractor, in terms of intellectual property, what is described in section 17.1.2 of the Annex II Draft Contract (copied below) is applicable:

"Where Commercial Off-the-Shelf (COTS) products are concerned and the standard license terms of the third-party apply vendor, such license shall grant to the Agency/Commission the right and

license to use such COTS products for the purpose of this Contract and for the purpose of operating the PKI, excluding any rights of sub-licence."

Answer: Yes

Question 3: In relation to the "Threat Scenario Coverage (as-designed and as-built)" requirement, described in "Annex I.1_EUSPA-SEC-SREQ-SOW-A13466_1.0_PKI_SOW.pdf" and "EUSPA-SEC-SREQ-DCG-A13468_1.0_EUSPA PKI DCG_CLEAN.pdf" documents, if the proposal is based on COTS, would it need to be carried out both as-designed and as-built or only as-built?

Answer: If the proposal is based on COTS, the delivery of Threat Scenario Coverage as-designed can be substituted by Threat Scenario Coverage as as-built.

Question 4: If providing an OCSP service is valuable, in order to properly size the environments, could you please clarify whether there are performance requirements such as validation requests processing (requests per second) or response times (maximum, average, etc.).

Answer: In case OCSP is implemented, the Contractor shall define and justify performance requirements for OCSP service.

Question 5: Regarding the training requirements described in "Annex I.1_EUSPA-SEC-SREQ-SOW-A13466_1.0_PKI_SOW.pdf":

1. "*PKI-SOW-1325: PKI System operations team training. The contractor shall provide training sessions (including training material for the course) for trainers, maintainers, administrators and operations team members at the GSC site for Sub CA and at EUSPA HQ for RCA*." Should physical training sessions be considered at the GSC site and EUSPA HQ or will it be acceptable to propose that the training sessions take place at one of the two locations and the students of the other connect remotely? In that case, where would the physical training take place?

2. "*PKI-SOW-0180: Operational and validation PKI System chains*" *"... The VAL Chain equipment shall be transportable for training purposes*.". We would be interested in confirming that it will be necessary to transport both the RCA and the SCA and to which locations.

Answer:

1. The physical training sessions shall be provided at the GSC site and at EUSPA HQ
2. The RCA and the SCA for the VAL chain shall be transportable in other locations within the Site they are located (RCA in the EUSPA HoQ and GSC in EUSPA GSC)

- End of document -