Nabava sustava za upravljanje ključevima

Dopuna Poziva na istraživanje tržišta

Naručitelj je tijekom istraživanja tržišta zaprimio dodatna pitanja zainteresiranih subjekata te ovim putem objavljuje pristigla pitanja i odgovore, a u svrhu kvalitetnije pripreme odgovora na istraživanje tržišta. Naručitelj pitanja i odgovore objavljuje na hrvatskom i na engleskom jeziku.

1. Je li potrebno nuditi i QKD sustave?

2. Ako da, koje konfiguracije su potrebne? Sigurni način?

Odgovor: Ne, QKD sustavi će se nabavljati kroz drugu javnu nabavu koju će provoditi drugi projektni partner IRB (Institut Ruđer Bošković).

3. S kojim dobavljačima planirate povezati KMS? Je li potrebno povezivanje s QKD sustavima?

Odgovor: Dobavljač će biti poznat nakon provedbe postupka javne nabave koja će se izvršiti za nabavljanje QKD uređaja, ono što jest potvrđeno je da će te dvije komponente za komunikaciju koristiti ETSI standard (004 ili 014) za dohvat ključeva iz QKD sloja u KMS sloj.

4. Koja je procijenjena vrijednost nabave?

Odgovor: Procijenjena vrijednost nabave objavljena je u Planu nabave za 2024. godinu koji je javno dostupan na web stranicama EOJN RH i Naručiteljevim web stranicama.

5. Očekuje li se centralizirani ili decentralizirani sustav za upravljanje ključevima?

Odgovor: Očekujemo decentralizirani sustav, po jedan KMS uređaj na svakom čvoru.

6. Želimo li automatski rerouting?

Odgovor: Automatsko podešavanje ruta kojima će se prenositi kriptografski ključevi horizontalno između KMS sustava na različitim čvorovima trenutno nije nužna funkcionalnost. Važno je da KMS ima mogućnost bazičnog routinga i mogućnost povezivanja s SDN komponentama koje će biti dio QKD mreže u budućnosti.

7. Je li važno koji se protokol koristi za KMS-HSM komunikaciju?

Odgovor: Nije, PKCS#11 protokol smo izabrali jer je među najčešće korištenim kriptografskim aplikacijskim sučeljima.

8. Treba li KMS biti samostojeći, odvojen uređaj?

Odgovor: Da, jer se ostale komponente čvora nabavljaju zasebno te zato se KMS nabavlja zasebno na samostalnom odvojenom hardware-u (računalu).

9. Mogu li se javiti s partnerom i poslati jednu dokumentaciju za obje grupe?

Odgovor: Zajednica ponuditelja može podnijeti zajedničku ponudu. U Dokumentaciji o nabavi bit će detaljno raspisano na koji način se podnose ponude, međutim uobičajeno je da se za svaku grupu podnosi zasebna ponuda.

10. Imamo li specifikaciju kakvu enkripciju očekujemo pri usmjeravanju ključeva?

Odgovor: Očekujemo da je moguće ključ koji se treba usmjeravati kriptirati QKD ključem koristeći OTP (One Time Pad). Mogućnost konfiguracije ove stavke je poželjna, ali ne i nužna.

11. Kako će se spajati svi KMS uređaji između čvorova?

Odgovor: Za horizontalnu povezanost važno je da omogućuje prijenos ključa između čvorova.

12. Kakva se enkripcija očekuje? (za komunikaciju između KMS-ova na različitim čvorovima koja ne uključuje prijenos ključa)

Odgovor: Nije definirano u ovom trenutku.

13. Je li nužno da KMS uređaj bude tamper-proof (sadrži fizičku zaštitu od neovlaštenog rukovanja uređajem)?

Odgovor: Za KMS nam je jasno da trenutno nije dostupno takvo rješenje na tržištu pa takvo očekivanje stoga ne bi bilo realno.

14. Kakvu integraciju očekujemo? Očekuje li se da nešto razvijaju tijekom integracije?

Odgovor: Ne očekujemo da se razvijaju nova sučelja za komunikaciju s drugim komponentama (QKD uređaj, enkriptor i sl.) jer smo na razini projekta dogovorili da će sva komunikacija koju KMS ima s drugim komponentama slijediti ETSI standarde.

15. Što očekujemo za SDN?

Odgovor: SDN će biti uklopljen u našu QKD mrežu i čvorove u budućnosti, zato je trenutno jedino važno da KMS ima sučelje koje će služiti za komunikaciju s budućim SDN komponentama.

16. Očekujemo li kompatibilnost između različitih KMS vendora?

Odgovor: Ne, nabavljamo isto KMS rješenje za sve čvorove svoje mreže.

17. Je li funkcionalnost post-kvantnih algoritama nužna isključivo za HSM?

Odgovor: Da, za HSM je nužno da omogućuje upotrebu NIST PQC finalista (pohrana ključeva te njihovo korištenje u kriptografske svrhe), dok KMS ne mora imati implementiran PQC algoritam u nekom od svojih procesa.

18. Treba li KMS imati post-quantum funkcionalnost?

Odgovor: Poželjno je, ali nije nužno.

19. Koliko uređaja se nabavlja?

Odgovor: U Excel dokumentu (troškovnik) navedene su sve količine koje se planiraju nabaviti, za obje grupe.

CARNET has received additional questions from interested parties during the market research and hereby publishes the received questions and answers, in order to enable better preparation of the responses to the market research. The questions and answers are published in both Croatian and English.

1. Are the QKD systems required to be offered as well?

2. If so which configurations are needed? Secure mode?

Answer: No, the QKD systems will be procured through a separate public procurement procedure which will be carried out by another project partner - IRB (Ruđer Bošković Institute).

3. To which vendors do you plan the KMS to connect? if it is required to connect to QKD systems?

Answer: The choice of vendor for QKD systems depends solely on the public procurement procedure of the mentioned systems. What is confirmed is the interface for communication between the KMS and QKD component, we will be using the interface defined by the ETSI (004 or 014) standard for retrieving keys from the QKD layer to the KMS layer.

4. What is your estimated budget?

Answer: The estimated procurement value is published in the Procurement Plan for 2024, which is publicly available on the EOJN RH website and CARNET's website.

5. Is a centralized or decentralized key management system expected?

Answer: We expect a decentralized system, one KMS device on each node.

6. Do we want automatic rerouting?

Answer: Automatic adjustment of routes that will be used to transfer cryptographic keys horizontally between KMS systems on different nodes is currently not a necessary functionality. It is important that the KMS has the possibility of basic routing and the possibility of connecting with SDN components that will be part of the QKD network in the future.

7. Does it matter which protocol is used for KMS-HSM communication?

Answer: No, we chose the PKCS#11 protocol because it was one of the most used cryptographic interfaces on HSM devices.

8. Should KMS be a stand-alone, separate device?

Answer: Yes, because the other components of the node are purchased separately, and that is why the KMS is purchased separately on a separate separate hardware (computer).

9. Can I contact my partner and send one document for both groups?

Answer: A consortium of bidders may submit a joint bid. The procurement documentation will provide detailed instructions on how to submit bids; however, it is customary for a separate bid to be submitted for each group.

10. Do we have a specification of what kind of encryption we expect when routing keys?

Answer: We expect that it is possible to encrypt the key to be routed with a QKD key using OTP (One Time Pad). The ability to configure this process is desirable, but not necessary.

11. How will all KMS devices be connected between nodes?

Answer: For horizontal connectivity, it is important that it enables key transfer between nodes.

12. What kind of encryption is expected? (for communication between KMSs on different nodes that does not involve key transfer)

Answer: Not defined at this time.

13. Is it necessary for the KMS device to be tamper-proof?

Answer: For KMS, it is clear to us that such a solution is not currently available on the market, so such an expectation would therefore not be realistic.

14. What kind of integration do we expect? Are they expected to develop anything during the integration?

Answer: We do not expect new interfaces to be developed for communication with other components (QKD device, encryptor, etc.) because we agreed at the project level that all communication KMS has with other components will follow ETSI standards.

15. What do we expect for SDN?

Answer: SDN will be integrated into our QKD network and nodes in the future, so currently the only important thing is that KMS has an interface that will be used for communication with future SDN components.

16. Do we expect compatibility between different KMS vendors?

Answer: No, we procure the same KMS solution for all nodes of our network.

17. Is the functionality of post-quantum algorithms necessary only for HSM?

Answer: Yes, it is necessary for HSM to enable the use of NIST PQC finalists (storage of keys and their use for cryptographic purposes), while KMS does not have to have the PQC algorithms implemented in any of its processes.

18. Should KMS have post-quantum functionality?

Answer: Preferably, but not necessary.

19. How many devices will be purchased?

Answer: The Excel document (bill of costs) lists all the quantities that are planned to be procured, for both groups.