Nabava sustava za upravljanje ključevima

Obavijest gospodarskim subjektima s ciljem istraživanja tržišta

Sadržaj

1. Uvod

Općenito o nabavi

Hrvatska akademska i istraživačka mreža – CARNET planira započeti postupak javne nabave sustava za upravljanje ključevima, a sve u sklopu projekta „Hrvatska kvantna komunikacijska infrastruktura – CroQCI".

Krajnji korisnici ovog projekta su ustanove partneri u projektu.

Sukladno Zakonu o javnoj nabavi (NN 120/16, NN114/22) sa svrhom pripreme nabave i informiranja gospodarskih subjekata o svojim planovima i zahtjevima u vezi s nabavom, u nastavku obavijesti, CARNET objavljuje zahtjeve vezane za nabavu sustava za upravljanje ključevima.

Radi daljnjeg planiranja i provedbe postupka nabave te izrade Dokumentacije o nabavi molimo sve zainteresirane gospodarske subjekte da dostave prijedloge i primjedbe zajedno s procijenjenom vrijednosti svih troškovničkih stavki koristeći priloženi troškovnik sukladno danim zahtjevima te ostale stavke navedene u točci 6. Zahtjevi od gospodarskog subjekta, najkasnije do 04. srpnja 2024. godine, na adresu elektroničke pošte nabava@carnet.hr.

Prilikom provođenja istraživanja tržišta CARNET će postupati na način da svojim postupcima ne narušava tržišno natjecanje niti krši načela zabrane diskriminacije i transparentnosti.

Rezultati provedenog istraživanja ne obvezuju CARNET niti se stvara bilo kakav pravni posao ili odnos s gospodarskim subjektima koji sudjeluju u istraživanju.

Općenito o projektu CroQCI

Republika Hrvatska prepoznala je važnost inicijative Europske kvantne komunikacijske infrastrukture (EuroQCI) te je 2019. godine potpisala Deklaraciju o europskoj kvantnoj komunikacijskoj infrastrukturi čime se obvezala na provedbu aktivnosti na izgradnji sigurne kvantne komunikacijske infrastrukture koja će obuhvatiti cijelu Europsku uniju.

CroQCI konzorcij čine ključne istraživačke i znanstvene institucije, ustanove visokog obrazovanja, javne ustanove i javna poduzeća ovlaštena od strane Ministarstva znanosti i obrazovanja za razvoj nacionalne QCI mreže te pripremu i provedbu nacionalnog projekta Hrvatska kvantna komunikacijska infrastruktura – CroQCI.

Nositelj odnosno koordinator projekta jest Hrvatska akademska i istraživačka mreža – CARNET.

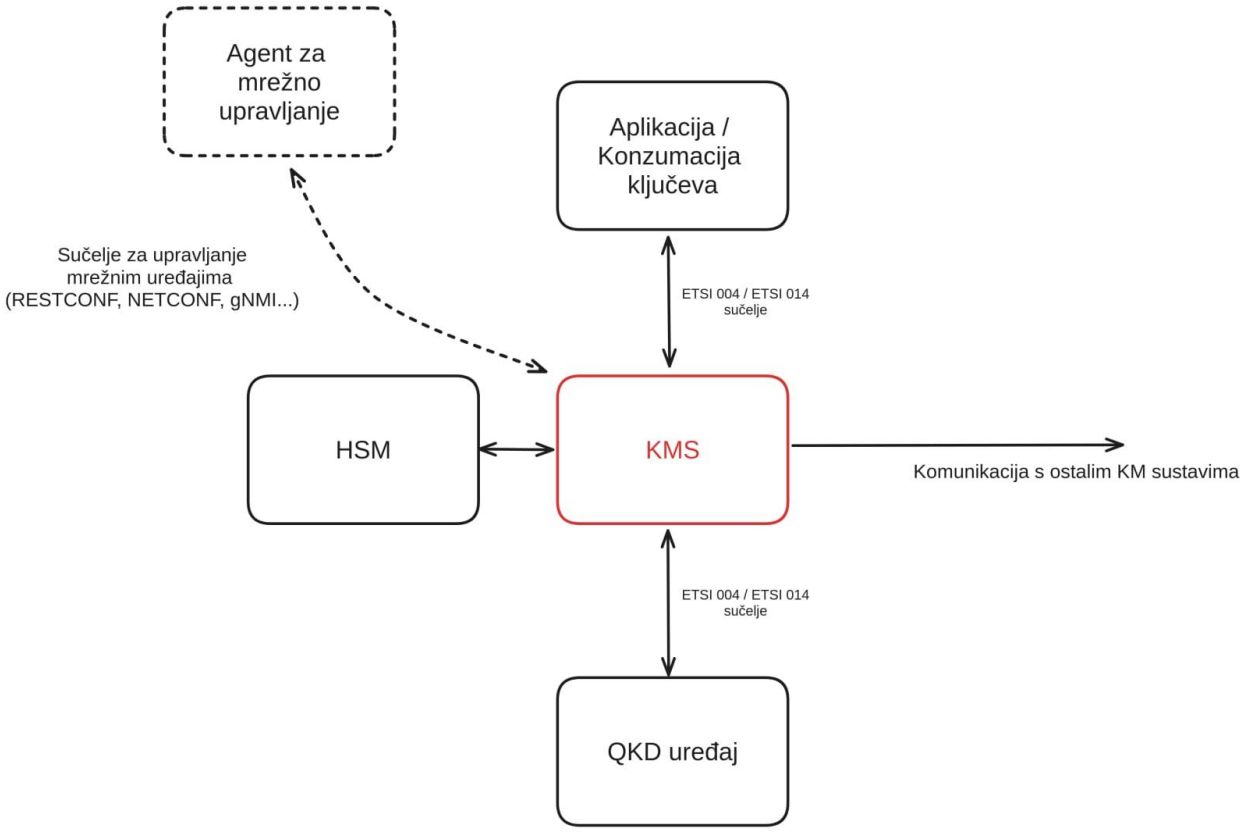
Cilj projekta je implementacija eksperimentalnih kvantnih komunikacijskih sustava i mreže, nadopunjenih i integriranih s rasponom klasičnih sigurnih komunikacijskih tehnologija.

To uključuje izgradnju i testiranje uređaja i sustava koji kombiniraju najbolje od kvantnih, postkvantnih klasičnih i kvantno unaprijeđenih rješenja.

Više o projektu možete pronaći na poveznici: https://www.carnet.hr/projekt/croqci/

2. Logički prikaz KMS i HSM uređaja u CroQCI arhitekturi

Radi jasnijeg razumijevanja smještaja sustava za upravljanje ključevima koji je predmet nabave kroz dvije grupe, prikazat će se logički prikaz smještaja KMS i HSM uređaja.



Slika 1. - Logički prikaz smještaja KMS i HSM uređaja u CroQCI arhitekturi

Arhitektura predviđa da sloj za upravljanje ključevima sadrži dvije komponente: sustav za upravljanje ključevima (KMS) i hardverski sigurnosni modul (Hardware Security Module – HSM). KMS ima zadaću zahtijevati ključeve od kvantnog sloja (od samostalnog QKD uređaja preko sučelja definiranog ETSI 004 i/ili ETSI 014 standardnom) te na zahtjev predavati ključ aplikacijama, a HSM bi služio kao arhiva ključeva koja, uz softversku zaštitu, sadrži i hardversku zaštitu protiv neovlaštenog rukovanja opremom.

KMS bi trebao imati opciju mrežnog upravljanja putem nekog od standardnih protokola za upravljanje udaljenim mrežnim objektima - RESTCONF, NETCONF ili gNMI.

3. Predmet nabave

Predmet nabave je sustav za upravljanje ključevima koji se sastoji od glavnog uređaja za upravljanje ključevima te uređaja koji predstavlja hardverski sigurnosni modul.

Predmet nabave podijeljen je u dvije grupe prema namjeni i specifičnosti opreme.

Grupa 1: Uređaj za upravljanje ključevima (KMS)

Opis predmeta nabave

Radi se o sustavu za upravljanje ključevima na dediciranom hardveru. KMS će biti ugrađen u čvorove mreže kvantne distribucije ključa zbog čega mora moći komunicirati s ostalim funkcionalnim elementima čvora.

KMS preuzima simetrične AES ključeve (minimalno duljine 256) iz kvantnog sloja putem ETSI standardiziranog sučelja (ETSI 004 i/ili ETSI 014) te bi trebao sadržavati komponentu koja može komunicirati s tim sučeljem na kvantnom sloju te preuzimati kriptografske ključeve i njihove metapodatke.

KMS treba imati mogućnost pohraniti ključeve (ovisno o konfiguraciji) ili u lokalnoj bazi ili na hardverskom sigurnosnom modulu (HSM). Zbog navedene funkcionalnosti, KMS treba imati agenta koji može komunicirati s HSM-om putem nekog od standardiziranih sučelja (npr. PKCS#11).

KMS treba sadržavati sučelje putem kojeg može poslužiti ključeve pohranjene u njegovoj lokalnoj bazi ili na HSM-u aplikacijama koje zahtijevaju kriptografske ključeve putem ETSI standardiziranog aplikacijskog sučelja (prema ETSI 004 i/ili ETSI 014 standardu).

Na svakom čvoru mreže kvantne distribucije ključa nalazit će se jedan KMS, svi KMS-ovi trebaju imati mogućnost usmjeravanja između čvorova. Svaki KMS bi trebao imati informaciju o tome koji su čvorovi izravno povezani te na osnovu toga odabrati rutu kojom bi se mogla uspostaviti komunikacija između dva čvora koji nisu izravno povezani kvantnim linkom.

KMS treba brinuti o životnom ciklusu kriptografskog ključa te sve radnje nad ključem, tj. njegove životne faze pratiti i zapisivati u log datoteke: dohvaćanje, pohrana, distribucija, rotacija, nadzor nad ključevima i uklanjanje.

KMS treba imati upravljačko sučelje putem kojeg ovlaštena osoba može nadzirati podatke o ključevima i podešavati i odabirati postavke putem kojih može zadati željene sigurnosne politike poput rotacije ključa, dozvola pristupa ključu, mjesto pohrane ključa, vremenski period nakon kojeg se ključ uklanja, itd.

KMS treba moći razlikovati dva načina rada: prvi u kojem konstantno preuzima ključeve iz kvantnog sloja (sve dok se ne zadovolji definirani broj spremljenih ključeva), te drugi u kojem KMS tek na zahtjev aplikacije preuzima ključ iz kvantnog sloja i prosljeđuje ga aplikaciji.

Aktivnosti Grupe 1:

1. KMS uređaj
2. Isporuka, postavljanje, konfiguracija i testiranje uređaja
3. Izrada uputa za isporučenu opremu (u elektroničkom obliku) na hrvatskom ili engleskom jeziku
4. Provedba edukacije o korištenju i administriranju uređaja (minimalno 3 člana projekta Naručitelja)
5. Tehnička podrška
6. Jamstvo za otklanjanje nedostataka u jamstvenom roku na uređaj u trajanju od minimalno 6 godina

Grupa 2: Hardverski sigurnosni modul (HSM - Hardware Security Module)

Opis predmeta nabave

Hardverski sigurnosni modul (HSM) biti će ugrađen u čvorove mreže kvantne distribucije ključa. Imat će dvojaku ulogu, ulogu sigurne pohrane kriptografskih simetričnih ključeva nastalih u kvantnom sloju i ulogu pružanja sučelja koje omogućuje korištenje post-kvantnih kriptografskih algoritama.

Simetrični ključevi iz kvantnog sloja mreže kvantne distribucije ključa će biti preuzeti od strane KMS sustava koji ih zatim pohranjuje na HSM. Za tu funkciju, HSM treba omogućiti standardizirano sučelje (npr. PKCS#11) putem kojeg će KMS moći izvršiti navedenu radnju te kasnije (po zahtjevu aplikacije) preuzeti ključ (putem istog sučelja) iz HSM-a.

HSM također treba sadržavati (uz klasične kriptografske algoritme) post-kvantne algoritme te omogućiti aplikacijama da ih koriste, pohranjuju post-kvantne asimetrične ključeve na HSM-u te ih dohvaćaju na zahtjev. Navedene radnje se također trebaju odvijati putem standardnog kriptografskog aplikacijskog sučelja.

Aktivnosti Grupe 2:

1. HSM uređaj
2. Isporuka, postavljanje, konfiguracija i testiranje uređaja
3. Izrada uputa za isporučenu opremu (u elektroničkom obliku) na hrvatskom ili engleskom jeziku
4. Provedba edukacije o korištenju i administriranju uređaja (minimalno 3 člana projekta Naručitelja)
5. Tehnička podrška
6. Jamstvo za otklanjanje nedostataka u jamstvenom roku na uređaj u trajanju od minimalno 6 godina

4. SDN komponenta

Ova komponenta potrebna je samo za predmet nabave Grupe 1.

SDN (Software Defined Network) je komponenta koja treba pomoći u nadzoru i udaljenom upravljanju čvorovima kvantne mreže distribucije ključa (i njihovim komponentama). Funkcionira na principu agenata i kontrolera. Za ulogu SDN-a u mreži kvantne distribucije ključa relevantan je standard ETSI 015. KMS bi trebao ili sadržavati SDN funkcionalnosti ili imati mogućnost kasnije nadogradnje s istima. KMS treba sadržavati sučelje za SDN funkcionalnost, a za komunikaciju bi trebao koristiti jedan od standardnih protokola kao što su NETCONF, RESTCONF i gNMI.

5. Demo testiranje za Grupu 1

Kao dio postupka odabira Ponuditelja izvršit će se demo testiranje KMS uređaja koje će se sastojati od sljedećih aktivnosti:

1. Aktivnost - Definiranje i postavljanje demo okoline na lokaciji Naručitelja
2. Aktivnost - Testiranje scenarija direktnog dohvaćanja ključeva na zahtjev i pohrana ključeva
3. Aktivnost - Testiranje scenarija periodičkog dohvaćanja ključeva i pohrana ključeva
4. Aktivnost - Potpisivanje zapisnika o provedenom demo testiranju

6. Demo testiranje za Grupu 2

Kao dio postupka odabira Ponuditelja izvršit će se demo testiranje HSM uređaja koje će se sastojati od sljedećih aktivnosti:

1. Aktivnost - Definiranje i postavljanje demo okoline na lokaciji Naručitelja
2. Aktivnost - Testiranje scenarija spremanja i dohvaćanja postkvantnih ključeva
3. Aktivnost - Testiranje scenarija spremanja i dohvaćanja simetričnih kriptografskih ključeva
4. Aktivnost - Potpisivanje zapisnika o provedenom demo testiranju

7. Faze izvedbe za Grupu 1

Očekuje se isporuka predmeta nabave iz Grupe 1 kroz faze:

FAZA 1 Isporuka, postavljanje, konfiguracija i testiranje KMS uređaja

1. Aktivnost - Isporuka KMS uređaja na lokacije koje definira Naručitelj
2. Aktivnost - Postavljanje i konfiguracija KMS uređaja sukladno potrebama Naručitelja
3. Aktivnost - Testiranje KMS uređaja scenarijima zadanim od strane Naručitelja
4. Aktivnost - Potpisivanje zapisnika o primopredaji

FAZA 2: Izrada uputa za isporučenu opremu (u elektroničkom obliku) na hrvatskom ili engleskom jeziku

5. Aktivnost - Dostava uputa na hrvatskom i/ili engleskom jeziku u elektroničkom obliku

FAZA 3: Edukacija

6. Aktivnost - Provedba edukacije o korištenju i administriranju uređaja (minimalno 3 člana projekta Naručitelja)

FAZA 4: Tehnička podrška

7. Aktivnost - Tehnička podrška za vrijeme trajanja projekta (do 30.6.2025.)

FAZA 5: Jamstvo

8. Aktivnost - ispravljanje i otklanjanje svih nedostataka uključivo nužne i sigurnosne nadogradnje sustava (uključujući softver bilo koje komponente sustava) koje su potrebne da bi se otklonili nedostatci u funkcioniranju opreme i sustava te sigurnosne ranjivosti na period od minimalno 6 godina

Ugovorna obveza za završnu konfiguraciju predmeta nabave iz Grupe 1 ovisi o Ugovoru o javnoj nabavi za Grupu 2 jer se uređaj iz Grupe 2 treba povezati s uređajem iz Grupe 1. Obzirom da se radi o inovativnom sustavu za upravljanje ključevima odabrani Ponuditelj iz Grupe 1 mora biti prisutan prilikom implementacije predmeta nabave iz Grupe 2.

8. Faze izvedbe za Grupu 2

Očekuje se isporuka predmeta nabave iz Grupe 2 kroz faze:

FAZA 1: Isporuka, postavljanje, konfiguracija i testiranje HSM uređaja

9. Aktivnost - Isporuka HSM uređaja na lokacije koje definira Naručitelj
10. Aktivnost - Postavljanje i konfiguracija HSM uređaja sukladno potrebama Naručitelja
11. Aktivnost - Testiranje HSM uređaja scenarijima zadanim od strane Naručitelja
12. Aktivnost - Potpisivanje zapisnika o primopredaji

FAZA 2: Izrada uputa za isporučenu opremu (u elektroničkom obliku) na hrvatskom ili engleskom jeziku

13. Aktivnost - Dostava uputa na hrvatskom i/ili engleskom jeziku u elektroničkom obliku

FAZA 3: Edukacija

14. Aktivnost - Provedba edukacije o korištenju i administriranju uređaja (minimalno 3 člana projekta Naručitelja)

FAZA 4: Tehnička podrška

15. Aktivnost - Tehnička podrška za vrijeme trajanja projekta (do 30.6.2025.)

FAZA 5: Jamstvo

16. Aktivnost - ispravljanje i otklanjanje svih nedostataka uključivo nužne i sigurnosne nadogradnje sustava (uključujući softver bilo koje komponente sustava) koje su potrebne da bi se otklonili nedostatci u funkcioniranju opreme i sustava te sigurnosne ranjivosti na period od minimalno 6 godina.

Ugovorna obveza za završnu konfiguraciju predmeta nabave iz Grupe 2 ovisi o Ugovoru o javnoj nabavi za Grupu 1 jer se uređaj iz Grupe 1 treba povezati s uređajem iz Grupe 2. Obzirom da se radi o inovativnom sustavu za upravljanje ključevima odabrani Ponuditelj iz Grupe 2 mora biti prisutan prilikom implementacije predmeta nabave iz Grupe 1.

9. Zahtjevi od gospodarskog subjekta

Od zainteresiranog gospodarskog subjekta za Grupu 1 i Grupu 2 očekuje se da:

1. Ispuni priložene Troškovnike;
2. Dostavi informaciju o trajanju jamstva na isporučenu opremu;
3. Dostavi informaciju o proizvođaču i modelu predloženih uređaja za Grupu 1 i Grupu 2
4. Dostavi ostale prijedloge i komentare.

Od zainteresiranog gospodarskog subjekta za Grupu 1 i Grupu 2 očekuju se i informacije o:

- Minimalnom roku u kojem se može provesti demo testiranje;
- Minimalnom roku u kojem se oprema može isporučiti, postaviti, konfigurirati i testirati na lokacijama koje definira Naručitelj.

Sve lokacije Naručitelja nalaze se u Republici Hrvatskoj, u Zagrebu.

Radi daljnjeg planiranja i provedbe postupka nabave te izrade Dokumentacije o nabavi molimo sve zainteresirane gospodarske subjekte da dostave prijedloge i primjedbe prema traženim informacijama i s troškovnikom najkasnije do 04. srpnja 2024. na adresu elektroničke pošte nabava@carnet.hr.