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 hardverskog sigurnosnog modela kao komponentu 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 5. prosinca 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.

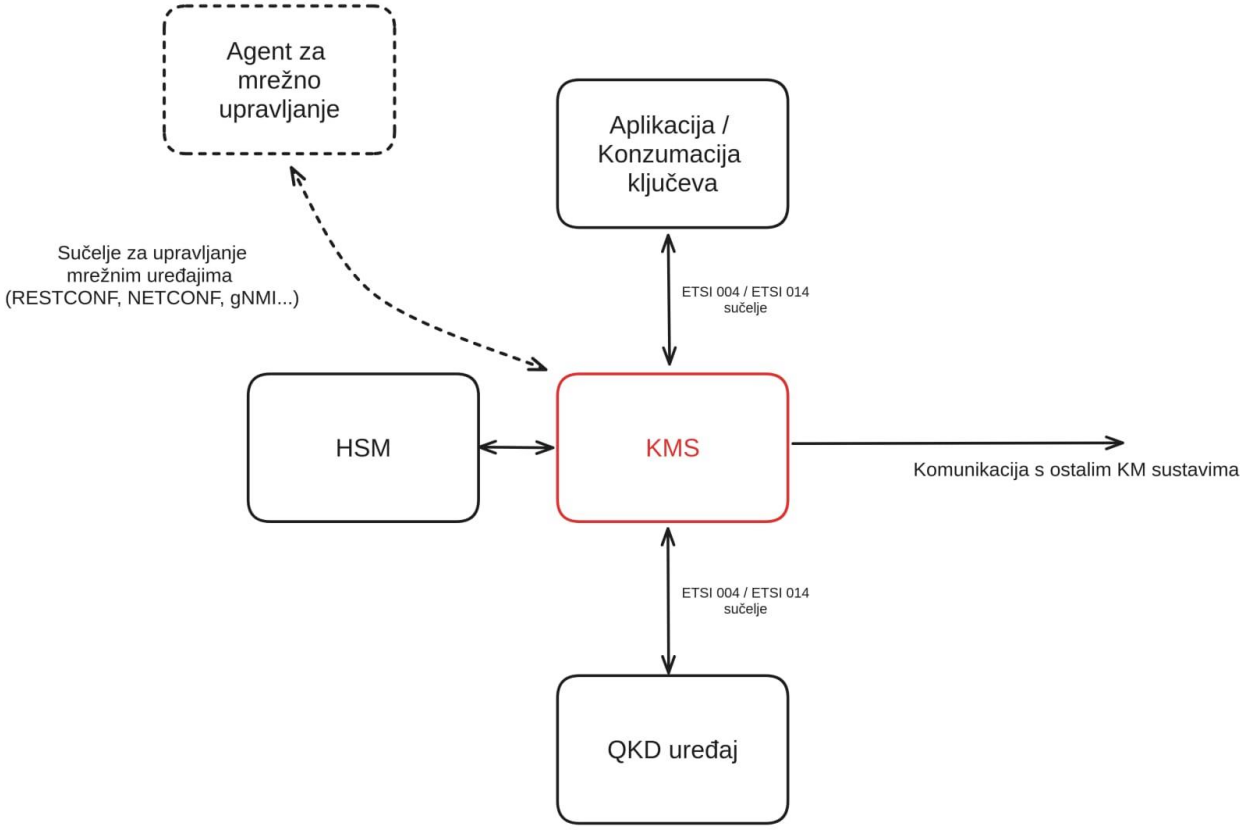
Cilj projekta je implementacija eksperimentalnih kvantnih komunikacijskih sustava i mreže, nadopunjenih i integriranih s rasponom klasičnih sigurnih komunikacijskih tehnologija.

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 HSM uređaja u CroQCI arhitekturi

Radi jasnijeg razumijevanja smještaja sustava za upravljanje ključevima, 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.

3. Predmet nabave

Predmet nabave je hardverski sigurnosni modul (HSM) koji će biti dio sustava za upravljanje ključevima koji uz hardverski sigurnosni modul sadrži i glavni uređaja za upravljanje ključevima (KMS) koji neće biti predmet nabave.

Opis predmeta nabave

Hardverski sigurnosni modul (HSM) bit 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:

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 5 članova projekta Naručitelja)
5. Tehnička podrška
6. Jamstvo za otklanjanje nedostataka u jamstvenom roku na uređaj u trajanju od minimalno 2 godine

4. Demo testiranje

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

Scenariji koji se planiraju provesti kroz demo testiranje su opisani u priloženom dokumentu Demo testiranje.

5. Faze izvedbe

Očekuje se isporuka predmeta nabave kroz faze:

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

1. Aktivnost - Isporuka HSM uređaja na lokacije koje definira Naručitelj
2. Aktivnost - Postavljanje i konfiguracija HSM uređaja sukladno potrebama Naručitelja
3. Aktivnost - Testiranje HSM 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 2 godine

6. Zahtjevi od gospodarskog subjekta

Od zainteresiranog gospodarskog subjekta očekuje se da:

1. Ispuni priloženi Troškovnik (Prilog 1 - Troškovnik). Pod jediničnom cijenom uređaja trebaju biti obuhvaćeni i ostali troškovi izvedbe kao što je instalacija, jamstvo, tehnička podrška i edukacija;
2. Dostavi informaciju o trajanju jamstva na isporučenu opremu;
3. Dostavi ispunjenu tablicu s tehničko-funkcionalnim zahtjevima koja je priložena objavi (Prilog 2 - Tehničko-funkcionalni zahtjevi - HSM) te označi koje od traženih funkcionalnosti zadovoljava uređaj;
4. Dostavi funkcionalnosti uređaja u obliku dokumenta (tehnička specifikacija, funkcionalna specifikacije, tzv. white paper, i sl.) u kojima su potkrijepljene tvrdnje o traženim funkcionalnostima u tablici s tehničko-funkcionalnim zahtjevima;
5. Dostave referentu listu projekata u kojima su proveli implementaciju predmeta nabave;
6. Daju prijedloge ili komentare na scenarije koji su opisani u dokumentu o demo testiranju (Prilog 3 - Demo testiranje);
7. Dostavi ostale prijedloge i komentare.

Od zainteresiranog gospodarskog subjekta očekuju se i informacije o:

- Minimalnom roku u kojem će se 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 5.12.2024. na adresu elektroničke pošte nabava@carnet.hr.

CARNET će sve informacije koje nastanu temeljem dodatnih pitanja javno objaviti na mrežnim stranicama na isti način kao i ovu obavijest.