

PRILOG 3

Demo testiranje sustava za upravljanje ključevima

SADRŽAJ:

[Uvod 2](#_Toc1168589849)

[Testiranje HSM uređaja 3](#_Toc508129400)

[Definiranje i postavljanje demo okoline na lokaciji Naručitelja 3](#_Toc1631714606)

[Testiranje scenarija spremanja i dohvaćanja postkvantnih ključeva 3](#_Toc1199643540)

[Testiranje scenarija spremanja i dohvaćanja simetričnih kriptografskih ključeva 3](#_Toc1721957090)

# Uvod

Sukladno članku 268. st. 1. točka 13. Zakona o javnoj nabavi (NN 120/16, 114/22 dalje u tekstu ZJN 2016) Naručitelj će provesti Demo testiranje ponuđene opreme.

Ponuđena oprema mora imati sve karakteristike propisane u Tehničkoj specifikaciji.

Naručitelj će prije donošenja Odluke o odabiru pozvati Ponuditelja čija ponuda bude ekonomski najpovoljnija da se na ponuđenoj opremi izvrši demo testiranje. Kao dokaz ispunjavanja predmetne sposobnosti prihvaća se popunjeni Zapisnik o provedenom testiranju.

Demo testiranje je javno. Naručitelj provodi javno demo testiranje postupajući u skladu sa člankom 4. ZJN 2016, a posebno uzimajući u obzir načelo transparentnosti. S obzirom na to da je predmet nabave roba velike vrijednosti Naručitelj smatra da nije razmjerno da robu zadržava kao uzorak, ali tijekom demo testiranja omogućava zainteresiranim gospodarskim subjektima da imaju uvid u provjeru sukladnosti ponuđene robe s tehničkom i funkcionalnom specifikacijom. U skladu s načelom transparentnosti ponuditelj će snimiti postupak demo testiranja robe.

CARNET će najkasnije 48 sati prije održavanja demo testiranja na svojim mrežnim stranicama objaviti mjesto i vrijeme održavanja demo testiranja te adresu elektroničke pošte na koju zainteresirani subjekti mogu poslati obavijest o prisustvovanju demo testiranju.

Demo testiranje će se provesti na lokaciji koju će osigurati Naručitelj. Ponuditelj prije demo testiranja ima pravo provjeriti prostorije Naručitelja i ostale tehničke uvjete.

Naručitelj ostavlja mogućnost Ponuditelju da demo testiranje provede i na lokaciji po vlastitom izboru u Zagrebu.

Naručitelj će poziv uputiti Ponuditelju čija ponuda bude ekonomski najpovoljnija putem EOJN RH s prijedlogom datuma demo testiranja. U slučaju da se Ponuditelj u roku od 5 dana od zaprimanja poziva ne odazove, njegova ponuda smatrat će se nepravilnom i odbit će se sukladno čl. 295. st. 1 ZJN 2016. Predloženi datum demo testiranja neće biti prije isteka roka od 5 dana od dana zaprimanja poziva. Ako Ponuditelj iz opravdanih objektivnih razloga nije u mogućnosti provesti demo testiranje na predloženi datum, Ponuditelj može Naručitelju uputiti zahtjev za promjenom datuma demo testiranja putem EOJN RH.

Sve stavke specifikacije demo testiranja moraju biti uspješno izvršene te predstavljaju minimalne tražene zahtjeve. U slučaju neuspješnog ispunjenja jedne od stavaka ponuda Ponuditelja smatrat će se nepravilnom i odbit će se sukladno čl. 295. st. 1 ZJN 2016, a Naručitelj će uputiti poziv za demo testiranje onom Ponuditelju čija je ponuda sljedeća ekonomski najpovoljnija.

Prije početka testiranja Ponuditelj je dužan osigurati svu traženu opremu te podići sve potrebne servise kako bi se provelo testiranje.

Pravo aktivnog sudjelovanja na testiranju imaju samo članovi stručnog povjerenstva Naručitelja i ovlašteni predstavnici Ponuditelja koji su u postupku nabave predali ponudu.

Ovlašteni predstavnici Ponuditelja dužni su prije početka testiranja predati ovlaštenje ovlaštene osobe Ponuditelja da u ime Ponuditelja prisustvuju testiranju.

Za vrijeme demo testiranja opreme moraju biti prisutni predstavnici Ponuditelja.

Demo testiranje može trajati maksimalno dva dana po osam sati (16 sati). Definirana dva dana za demo testiranje moraju biti uzastopni dani.

Vrijeme trajanja testiranja moguće je prema potrebi produžiti ako za to postoje objektivno opravdani razlozi za koje krivnja nije na strani Ponuditelja.

Za potrebe provođenja demo testiranja Ponuditelj smije instalirati isključivo opremu koju je ponudio i koja je specificirana unutar tehničke specifikacije ponude Ponuditelja te je dužan osigurati popis opreme koja će se koristiti u testu, koji je Ponuditelj dužan dostaviti Naručitelju uz odgovor na poziv za demo testiranje.

Nakon provedenog Demo testiranja Naručitelj i Ponuditelj potpisat će Zapisnik o provedenom Demo testiranju. Popis opreme će biti u prilogu potpisanog zapisnika nakon izvršenih testiranja.

# Testiranje HSM uređaja

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

Aktivnost 1 - Definiranje i postavljanje demo okoline na lokaciji Naručitelja

* demo okolina mora sadržavati dovoljne komponente da se mogu demonstrirati aktivnosti 2. i 3. - klijent (klijentska aplikacija) koja može putem PKCS#11 sučelja na HSM-u slati odgovarajuće zahtjeve i zaprimati odgovore

Aktivnost 2 - Testiranje scenarija spremanja i dohvaćanja postkvantnih ključeva

* kriptografski klijent se autentificira na HSM
* kriptografski klijent sprema PQC kriptografski ključ na HSM
* kriptografski klijent dohvaća PQC kriptografski ključ sa HSM-a

Aktivnost 3 - Testiranje scenarija spremanja i dohvaćanja simetričnih kriptografskih ključeva

* kriptografski klijent se autentificira na HSM
* kriptografski klijent sprema simetrični kriptografski ključ i njegove metapodatke na HSM
* kriptografski klijent dohvaća simetrični kriptografski ključ i njegove metapodatke sa HSM-a

Aktivnost 4 - Potpisivanje zapisnika o provedenom demo testiranju

Nakon provedeog testiranja Ponuditelj i Naručitelj potpisuju Zapisnik o provedenom demo testiranju.

# Test 1 - Definiranje i postavljanje demo okoline na lokaciji Naručitelja

Test 1.1 - Provjera testne okoline

|  |  |  |  |
| --- | --- | --- | --- |
| Cilj testa | Provjera odgovara li testna okolina zahtjevima daljnjih aktivnosti | | |
| Početni uvjeti | Testna okolina je postavljena sa svim svojim komponentama koje su mrežno povezane. | | |
| Postupak testiranja | | | Očekivani rezultati |
| 1. Provjera sadržava li testna okolina testnu aplikaciju koja ima ulogu kriptografskog klijenta za ključeve. | | | 1. Testna aplikacija ima funkcionalnost komunikacije s PKCS#11 sučeljem na HSM uređaju. |
| Rezultat testa | |  | |
| Komentar | |  | |
| Datum | |  | |
| Test započeo (sat i minuta) | |  | |
| Test završio (sat i minuta) | |  | |
| Test proveo | |  | |

# Test 2 - Testiranje scenarija spremanja i dohvaćanja postkvantnih ključeva

|  |  |  |  |
| --- | --- | --- | --- |
| Cilj testa | Provjera sadrži li HSM kriptografske funkcionalnosti spremanja i dohvaćanja postkvantnih kriptografskih ključeva. | | |
| Početni uvjeti | Pripremljena testna okolina koja je zadovoljila uvjete ispitane u aktivnosti "Definiranje i postavljanje demo okoline na lokaciji Naručitelja". | | |
| Postupak testiranja | | | Očekivani rezultati |
| 1. Testna klijentska aplikacija se autentificira kao kriptografski korisnik na HSM uređaj.  2. Testna klijentska aplikacija pohranjuje PQC ključ (CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, SPHINCS+) na HSM uređaj.  3. Testna klijentska aplikacija dohvaća PQC ključ (CRYSTALS-KYBER, CRYSTALS-Dilithium, FALCON, SPHINCS+) sa HSM uređaja. | | | 1. HSM bilježi autentifikaciju u odgovarajuću log datoteku.  2. HSM sprema PQC ključ i odgovarajuće metapodatke.  3. HSM poslužuje odgovarajući PQC ključ koji odgovara zahtjevu klijenta. |
| Rezultat testa | |  | |
| Komentar | |  | |
| Datum | |  | |
| Test započeo (sat i minuta) | |  | |
| Test završio (sat i minuta) | |  | |
| Test proveo | |  | |

# Test 3 - Testiranje scenarija spremanja i dohvaćanja simetričnih kriptografskih ključeva

|  |  |  |  |
| --- | --- | --- | --- |
| Cilj testa | Provjera sadrži li HSM kriptografske funkcionalnosti spremanja i dohvaćanja simetričnih kriptografskih ključeva. | | |
| Početni uvjeti | Pripremljena testna okolina koja je zadovoljila uvjete ispitane u aktivnosti "Definiranje i postavljanje demo okoline na lokaciji Naručitelja". | | |
| Postupak testiranja | | | Očekivani rezultati |
| 1. Testna klijentska aplikacija se autentificira kao kriptografski korisnik na HSM uređaj.  2. Testna klijentska aplikacija pohranjuje simetrični (AES256).  3. Testna klijentska aplikacija dohvaća simetrični ključ (AES256) sa HSM uređaja. | | | 1. HSM bilježi autentifikaciju u odgovarajuću log datoteku.  2. HSM sprema simetrični ključ i odgovarajuće metapodatke. Proces bilježi u odgovarajuću log datoteku.  3. HSM poslužuje odgovarajući simetrični ključ koji odgovara zahtjevu klijenta. Proces bilježi u odgovarajuću log datoteku. |
| Rezultat testa | |  | |
| Komentar | |  | |
| Datum | |  | |
| Test započeo (sat i minuta) | |  | |
| Test završio (sat i minuta) | |  | |
| Test proveo | |  | |