

Anexa la Anunțul de participare

Specificații tehnice

Lot 1. Echipament criptografic HSM pentru deservirea Complexului Protecție criptografică (Certificate Authority)

	Specificarea tehnică deplină solicitată de către autoritatea contractantă
1	Furnizorul de echipamente trebuie să asigure livrarea, instalarea și punerea în funcțiune a HSM-urilor cu următorii parametri în cantitate de 2 buc. (principal și de rezervă) cu furnizarea software-ului, licențelor și documentației tehnice necesare
2	HSM trebuie să vizeze următoarele sfere de aplicare: PKI, Root & SubRoot CA
3	HSM trebuie să fie proiectat pentru o perioadă de funcționare de cel puțin 7 ani
4	HSM trebuie să corespundă cerințelor de siguranță nu mai jos de: FIPS 140-2 nivelul 3
5	HSM trebuie să aibă încorporat Secure Key Storage
6	HSM trebuie să execute algoritmi de criptare asimetrică inclusiv, în mod obligator: RSA (nu mai puțin de, 8192 bits), DSA, ECC
7	HSM trebuie să execute algoritmi de criptare simetrică, inclusiv, în mod obligator: AES, Triple-DES, DES
8	HSM trebuie să execute funcții hash populare, inclusiv, în mod obligator: SHA-2 family
9	HSM trebuie să aibă încorporat Hardware Random Number Generator
10	Productivitatea HSM trebuie să corespundă următoarele valori: - RSA 2048 bits – nu mai puțin de 60 tps, - RSA 4096 bits – nu mai puțin de 10 tps, - ECC P-256 – nu mai puțin de 40 tps, - ECC P-384 – nu mai puțin de 12 tps
11	HSM trebuie să execute metoda de autentificare bazată pe Smartcard
12	HSM trebuie să fie capabil să accepte următoarele sisteme de operare (Client): MS Windows Server (2012, 2016) și versiuni ulterioare, Windows 7, 10 și versiuni ulterioare, Linux
13	HSM trebuie să accepte următoarele interfețe (API) - PKCS#11, Microsoft Cryptographic API (CAPI), Java (JCA/JCE)
14	PKI Vendor Compatibility: HSM trebuie să fie compatibili cu EJBCA (compania PrimeKey Solutions AB)
15	HSM trebuie să poată funcționa conectat în rețea și să poată interacționa în siguranță cu aplicațiile din medii locale și virtuale
16	HSM trebuie să accepte interfața de rețea: Ethernet, TCP/IP (IPv4, IPv6)
17	HSM trebuie să întrețină protocolul de comunicare securizat cu clientul
18	HSM trebuie să aibă următoarele dimensiuni: nu mai mult de 2U
19	HSM trebuie să aibă o sursă de alimentare dublă integrată, cu posibilitatea de a chimba una din sursele de alimentare “la cald”
20	HSM trebuie să aibă un ecran tactil propriu, sau posibilitatea de a conecta un monitor extern, tastatură și mouse fie ambele variante
21	HSM trebuie să aibă cel puțin 16 MB de memorie RAM
22	HSM trebuie să dispună de mijloace ce permit administrarea, monitorizarea și configurarea de la distanță prin intermediul unui canal de comunicare securizat

23	HSM trebuie să execute proceduri de copii de rezervă (backup and restore) pentru cheile criptografice și certificate utilizând un al doilea HSM (backup) de același tip
24	HSM trebuie să dispună de o caracteristică ce îi permite efectuarea automată a replicății bazei de date
25	Furnizorul de hardware trebuie să asigure posibilitatea utilizării în noile HSM (primare și de rezervă) a cheilor și certificatelor utilizate anterior în HSM scoase din exploatare
26	Furnizorul echipamentului trebuie să furnizeze Clientului informații de contact pentru cursurile de instruire ale producătorului pentru exploatarea acestui tip de HSM. Instruirea personalului se efectuează în conformitate cu un contract de instruire separat
27	Perioada de garanție pentru HSM trebuie să fie de cel puțin 1 an de la data punerii în funcțiune a echipamentului
28	Furnizorul de echipamente trebuie să ofere posibilitatea de a încheia contracte anuale pentru întreținerea post-garanție a HSM
29	Furnizorul de echipamente trebuie să ofere posibilitatea de a actualiza gratuit software-ul și licențele în perioada de valabilitate a unui acord separat pentru deservirea garanție sau post-garanție
30	Furnizorul de echipamente trebuie să asigure posibilitatea livrării rapide și a înlocuirii echipamentelor defecte în conformitate cu contractul actual pentru întreținere tehnică (garanție sau post-garanție) – în termen de o lună

Lot 2. Echipament criptografic HSM pentru deservirea proceselor de producere a documentelor de importanță statală

Specificarea tehnică deplină solicitată de către autoritatea contractantă	
1	Furnizorul de echipamente trebuie să asigure livrarea, instalarea și punerea în funcțiune a HSM-urilor cu următorii parametri în cantitate de 2 buc. (principal și de rezervă) cu furnizarea software-ului, licențelor și documentației tehnice necesare
2	HSM trebuie să vizeze următoarele sfere de aplicare: PKI, SSL/TLS, Code Signing, Certificate Signing and Validation, Document Signing, Transaction Processing, DB Encryption, Smart Card Issuance
3	HSM trebuie să fie proiectat pentru o perioadă de funcționare de cel puțin 7 ani în modul <i>non-stop</i> 24/365
4	HSM trebuie să corespundă cerințelor de siguranță nu mai jos de: FIPS 140-2 nivelul 3
5	HSM trebuie să aibă încorporat Secure Key Storage
6	HSM trebuie să execute algoritmi de criptare asimetrică inclusiv, în mod obligator: RSA (nu mai puțin de, 4096 bits), DSA, ECC
7	HSM trebuie să execute algoritmi de criptare simetrică, inclusiv, în mod obligator: AES, Triple-DES, DES
8	HSM trebuie să execute funcții hash populare, inclusiv, în mod obligator: SHA-2 family
9	HSM trebuie să aibă încorporat Hardware Random Number Generator
10	Productivitatea HSM trebuie să corespundă următoarele valori: <ul style="list-style-type: none"> - RSA 2048 bits – nu mai puțin de 1 200 tps, - RSA 4096 bits – nu mai puțin de 300 tps, - ECC P-256 – nu mai puțin de 2500 tps, - ECC P-384 – nu mai puțin de 1500 tps

11	HSM trebuie să execute metoda de autentificare bazată pe Smartcard
12	HSM trebuie să fie capabil să accepte următoarele sisteme de operare (Client): MS Windows Server (2012, 2016) și versiuni ulterioare, Windows 7, 10 și versiuni ulterioare, Linux
13	HSM trebuie să accepte următoarele interfețe (API) - PKCS#11, Microsoft Cryptographic API (CAPI), Java (JCA/JCE)
14	PKI Vendor Compatibility: HSM trebuie să fie compatibil cu EJBCA (compania PrimeKey Solutions AB)
15	HSM trebuie să poată funcționa conectat în rețea și să poată interacționa în siguranță cu aplicațiile din medii locale și virtuale
16	HSM trebuie să accepte interfața de rețea: Ethernet, TCP/IP (IPv4, IPv6)
17	HSM trebuie să întrețină protocolul de comunicare securizat cu clientul
18	HSM trebuie să aibă următoarele dimensiuni: nu mai mult de 2U
19	HSM trebuie să aibă o sursă de alimentare dublă integrată, cu posibilitatea de a chimba una din sursele de alimentare "la cald"
20	HSM trebuie să aibă un ecran tactil propriu, sau posibilitatea de a conecta un monitor extern, tastatură și mouse fie ambele variante
21	HSM trebuie să aibă cel puțin 16 MB de memorie RAM
22	HSM trebuie să dispună de mijloace ce permit administrarea, monitorizarea și configurarea de la distanță prin intermediul unui canal de comunicare securizat
23	HSM trebuie să execute proceduri de copii de rezervă (backup and restore) pentru cheile criptografice și certificate utilizând un al doilea HSM (backup) de același tip
24	HSM trebuie să dispună de o caracteristică ce îi permite efectuarea automată a replicăției bazei de date
25	Furnizorul de hardware trebuie să asigure posibilitatea utilizării în noile HSM (primare și de rezervă) a cheilor și certificatelor utilizate anterior în HSM scoase din exploatare
26	Furnizorul echipamentului trebuie să furnizeze Clientului informații de contact pentru cursurile de instruire ale producătorului pentru exploatarea acestui tip de HSM. Instruirea personalului se efectuează în conformitate cu un contract de instruire separat
27	Perioada de garanție pentru HSM trebuie să fie de cel puțin 1 an de la data punerii în funcțiune a echipamentului
28	Furnizorul de echipamente trebuie să ofere posibilitatea de a încheia contracte anuale pentru întreținerea post-garanție a HSM
29	Furnizorul de echipamente trebuie să ofere posibilitatea de a actualiza gratuit software-ul și licențele în perioada de valabilitate a unui acord separat pentru deservirea garanției sau post-garanție
30	Furnizorul de echipamente trebuie să asigure posibilitatea livrării rapide și a înlocuirii echipamentelor defecte în conformitate cu contractul actual pentru întreținere tehnică (garanție sau post-garanție) – în termen de 2 săptămâni