Anexă la Anunțul de participare

Cerințe și specificații tehnice pentru
Echipamentele criptografice HSM pentru deservirea Autorităților de certificare

1.	Furnizorul trebuie să asigure livrarea, instalarea, configurarea, punerea în funcțiune, migrarea cheilor securizate și asistența tehnică pentru echipamentele criptografice HSM
2.	HSM trebuie să fie orientat spre următoarele domenii de aplicare: PKI, Root & SubRoot CA.
3.	Echipamentul HSM trebuie să respecte următoarele cerințe și criterii ale securității informaționale: (a) FIPS 140-2 nivelul 2 și nivelul 3; (b) Common Criteria EAL4+; (c) eIDAS; (d) IPv6 și compatibilitate cu USGv6
4.	HSM-ul trebuie să fie pe deplin compatibil cu arhitectura *nShield Security World*, care este utilizată de ASP ca arhitectură de bază pentru stocarea cheilor securizate de lungă durată
5.	HSM trebuie să fie compatibil cu produsul program EJBCA, care este utilizat în ASP ca platformă pentru crearea și gestionarea Centrelor de certificare. Menționarea modelului HSM propus trebuie să se regăsească în lista modulelor criptografice hardware cu care interacționează EJBCA: ***https://doc.primekey.com/ejbca/ejbca-integration/hardware-security-modules-hsm***
6.	HSM trebuie să interacționeze cu următoarele sisteme de operare și platforme: sisteme de operare Windows și Linux, inclusiv distribuțiile RedHat, SUSE.
7.	HSM trebuie să posede următoarele interfețe de programare a aplicațiilor (API): (a) OpenSSL, (b) PKCS#11, (c) Java (JCE), (d) Microsoft CAPI/CNG.
8.	Interfața de rețea: Ethernet, TCP/IP (IPv4, IPv6).
9.	HSM trebuie să dispună port serial (COM-PORT) pentru interacțiunea cu dispozitivele și sistemele externe
10.	Performanță. Furnizorul trebuie să ofere un model de bază cu o capacitate suficientă pentru deservirea Centrelor de certificare.
11.	Posibilitatea de monitorizare și administrare a HSM (cerințe minime): (a) mecanism securizat de jurnalizare și audit; (b) monitorizare cu utilizarea protocolului SNMP.
12.	Echipamentul HSM trebuie să posede următorii algoritmi criptografici pentru criptarea asimetrică: (a) RSA; (b) Diffie-Hellman; (c) DSA; (d) El-Gamal; (e) ECMQV, ECDSA, ECDH

13.	Echipamentul HSM trebuie să posede următorii algoritmi criptografici pentru criptarea simetrică: (a) AES; (b) DES, 3DES; (c) MD5; (d) SHA – 1 (224, 256, 384, 512) HMAC
14.	HSM trebuie să posede următoarele funcții hash : (a) MD5 (b) SHA-1 (c) SHA-2 (224, 256, 384, 512 bit)
15.	Alimentarea de la o sursă de curent alternativă cu o tensiune de 230 V și o frecvență de 50 Hz.
16.	HSM-ul trebuie să fie alimentat din 2 surse de alimentare, cu posibilitatea de înlocuire a unității defecte fără întrerupere. Setul trebuie să includă 4 surse de alimentare rezervă, câte 2 pentru fiecare modul.
17.	Dimensiuni HSM: nu mai mult de 2U. Dimensiunile HSM trebuie să permită instalarea acestuia într-un rack standard.
18.	Fiabilitatea HSM: Timpul mediu de bună funcționare ***(MTBF)*** - cel puțin 10 ani.
19.	Modelul HSM propus trebuie să aparțină unei noi generații de dispozitive, pentru care perioada de suport a producătorului este de cel puțin 5-6 ani din momentul livrării.
20.	Setul HSM obligator trebuie să includă: (a) Echipamente criptografice HSM - 2 bucăți; (b) Surse de alimentare rezervă - 2 x 2 module, total - 4 bucăți; (c) Componente constructive de rezervă (în cazul în care sunt prevăzute) - 2 seturi; (d) Produsul program integrat HSM - 2 seturi; (e) Module software suplimentare pentru extinderea funcționalității - 2 seturi. (f) Licențe pentru clienți - cel puțin 6 per modul, total - cel puțin 12 licențe ; (g) Smart card-uri pentru organizarea accesului la HSM – minim 45 bucăți < (h) Reader pentru lucru cu Smart carduri la distanță - 1 buc.
21.	Furnizorul va asigura instalarea HSM-urilor (primare și de rezervă), inclusiv și integrarea acestora în arhitectura existentă *nShield Security World* în cadrul infrastructurii Autoritatii contractante.
22.	Furnizorul trebuie să asigure posibilitatea de funcționare a echipamentelor HSM cu cheile securizate stocate în *nShield Security World*.
23.	Furnizorul trebuie să asigure mentenanța echipamentului pe parcursul perioadei de garanție. Perioada de garanție minim **24 luni** din momentul activării echipamentului.