Príloha č. 1 Výzvy: Opis predmetu zákazky

Predmetom zákazky je dodanie hardvérových komponentov v špecifikácii, počte a rozsahu uvedenom v tabuľkách nižšie vrátane poskytnutia súvisiacich služieb dodania tovaru do miesta dodania, vyloženia tovaru v mieste dodania, odberu a ekologickej likvidácia spotrebného materiálu/obalov, ako aj poskytnutie súčinnosti pri inštalácii a konfigurácii, inštalácii ovládačov, poskytnutia telefonickej podpory a záruky na mieste v trvaní uvedenom pri jednotlivých položkách predmetu zákazky.

Hardvérové komponenty

Hardware Security Module

Technické vlastnosti	Minimálne požadované parametre
Výrobca/model	
Typ:	Sieťový HSM modul
Základné požiadavky	Generovanie symetrických a asymetrických kryptografických kľúčov Poskytnutie fyzickej a logickej ochrany kryptografických kľúčov Riadenie prístupu ku kryptografickým kľúčom Akcelerácia operácií s využitím kryptografických kľúčov Záloha a obnova kryptografických kľúčov Podpora redundantnosti, vyrovnávania záťaže a HA (High availability)
Certifikácia	Musí mať certifikáciu na úrovni FIPS-140-2 Level3 alebo zodpovedajúcej, uznáva sa aj certifikácia samotného HSM modulu sieťového zariadenia. Musí mať EIDAS CC EAL4+ (AVA_VAN.5 and ALC_FLR.2) - Protection Profile 419221-5 *
Výkon	Musí spĺňať minimálne parametre na performance (transaction per second): - RSA 2048 bitov minimalne 5000 tps - ECC P256 bitov minimalne 10000 tps - AES-GCM small packet encryption minimalne 10000 tps Musí podporovať minimálne 20 nezávislých, kompletne oddelených zákazníkov alebo ich systémov s prístupom cez sieť. Každý nezávislý tenant musí mať kompletné práva na kryptooperácie (správa tokenov), ako aj definiciu bezpečnostných politík, uzívateľov a rolí, klientov a správu vlastných záloh bez ovplyvnenia ostatných tenantov s rovnakymi právami.
Kryptografia	Kryptografické kľúče musia byť uložené v HSM zariadeniach • symetrické šifrovanie: AES, DES, Triple DES, ARIA, SEED, RC2, RC4, RC5, CAST • asymetrické šifrovanie: RSA, DSA, Diffie-Hellman, Eliptické krivky • hash funkcie: SHA2 (SHA-224, SHA-256, SHA-384, SHA-512)" , SM3 • Cryptography (ECDSA, ECDH, Ed25519, ECIES) s mennými, užívateľom definovanými a Brainpool krivkami, KCDSA, a ďalšie • Odvodenie kľúča: SP800-108 Counter Mode • Zapuzdrenie kľúča: SP800-38F • Generátor náhodných čísel: navrhnutý pre legislatívnu zhodu s AIS • 20/31 až po DRG.4 využitím hardvérového zdroja skutočného šumu • a CTR-DRBG zhodné s odporúčaním NIST 800-90A • Enkrypcia digitálne peňaženky: BIP32
Podpora OS a API	Podpora pre Windows, Linux, Solaris, AIX Virtual: VMware, Hyper-V, Xen, KVM Musí poskytovať REST API na integráciu do komplexných riešení Musí obsahovať súpravu vývojových nástrojov (SDK) pre platformy Win64 a Linux (RH) 64 PKCS#11, Java (JCA/JCE), Microsoft CAPI a CNG, OpenSSL
Licencovanie	Licencie musia byt perpetuálne a podpora na obdobie min. 3 roky
HW a Systémové požiadavky	2x HW appliance HSM zapojená v HA HW musí byť vo vyhotovení pre inštaláciu do štandardizovanej 19" skrine, max. výška 1U, s dvoma nezávislými napájacími zdrojmi s možnosťou výmeny počas behu zariadenia Musí mať min. 4 Gigabit Ethernet porty s možnosťou spájania do zväzkov Zhoda s bezpečnostnými a environmentálnymi normami UL, CSA, CE, FCC, CE, VCCI, C-TICK, KCMark, RoHS2, WEEE, TAA
Zálohovanie	Je potrebné zabezpečiť zálohovanie pre celé HSM na diaľku
Podpora	8x5 počas 3 rokov poskytovaná výrobcom
Počet HSM	2

Key Management System

Technické vlastnosti	Minimálne požadované parametre
Výrobca/model	
Typ:	Systém správy kľúčov (KMS)
Základné požiadavky	Systém musí ponúkať možnosti správy kryptografických kľúčov počas ich životného cyklu vrátane generovania kľúčov, importu a exportu kľúčov a rotácie kľúčov. Všetky kryptografické kľúče musia byť uložené v centralizovanom, spevnenom hardwarovom zariadení, aby sa zjednodušila správa a zaistila prísna bezpečnosť. Bezpečnosť bude zabezpečená z HSM. Podpora redundantnosti HA (High availability)
Systémové požiadavky	Systém musí byť schopný vykonávať minimálne tieto operácie : - správa šifrovacích kľúčov počas celého životného cyklu - generovať symetrické a asymetrické kryptografické kľúče, ako aj tajné údaje a certifikáty X.509 - distribúcia kľúčov, deaktivácia a vymazanie - automatizované operácie založené na policies musia zjednodušovať úlohy vypršania platnosti a rotácie kľúčov - zabezpečiť kontrolu prístupu ku kľúčom - zálohovanie a obnova kryptografického obsahu a konfigurácie
Ďalšie požiadavky	• systém musí byť schopný integrácie s hardvérovým bezpečnostným modulom (HSM) certifikácie FIPS 140-2 Level3 alebo vyššou na ochranu šifrovacích kľúčov. • Riešenie musí byť schopné uložiť najmenej 1.000.000 kryptografických kľúčov • Riešenie musí podporovať viac serverov a aplikácií z viacerých umiestnení v sieti. Toto riešenie musí byť schopné podporovať až 100 000 pripojení súčasne • Riešenie by malo umožňovať vzdialenú správu cez WebUI, CLI a REST API. • Systém KMS musí poskytovať integráciu prostredníctvom nasledujúcich rozhraní API / rozhraní: NAE-XML, KMIP, REST API. Riešenie by malo ponúkať možnosti správy kľúčov, ktoré je možné integrovať do rôznych komerčných šifrovacích produktov. Podporované technológie musia obsahovať: - šifrovanie aplikácií (integrácia cez API), - šifrovanie databázy vrátane natívneho šifrovania databázy (napr. transparentné šifrovanie údajov dostupné v serveroch MS SQL Server a Oracle Database), - riešenia šifrovania na úrovni súborov a úložísk - výrobky podporujúce štandard protokolu OASIS Key Management Interoperability Protocol (KMIP), - rotácia kľúčov bez výpadku - štruktúrované dáta MS SQL a Oracle Zariadenie musí byť vybavené príslušnými licenciami na správu kľúčov 2 inštancií databázy podporujúcich mechanizmus transparentného šifrovania údajov. Systém musí byť schopný objednávať licencie on demand priamo u výrobcu podľa aktuálnych potrieb objednávateľa..
Licencovanie	Licencie musia byt perpetuálne a podpora na obdobie min. 3 roky
Manažment	Riešenie musí podporovať operácie naprieč viacerými nasadeniami a produktmi šifrovania a zároveň zabezpečiť, aby správcovia mali obmedzené roly definované pre ich rozsah zodpovednosti z konzoly centralizovanej správy. KMS musí využívať existujúce adresáre LDAP alebo AD na mapovanie administratívneho a kľúčového prístupu pre aplikáciu a koncových používateľov (integrované aplikácie)
Vysoká dostupnosť a vyvažovanie záťaže	KMS je možné nasadiť v klastrovanej konfigurácii s replikáciou kľúčov, zásad a konfiguračných informácií v reálnom čase vo viacerých inštanciách - čo umožňuje úplné zotavenie po katastrofe a kontinuitu podnikania. KMS s dodávaným softvérom musia byť schopné pracovať v režime vysokej dostupnosti. V prípade viacerých riešení šifrovania integrovaných do KMS musia byť kľúče spravované centrálne bez toho, aby to malo citeľný vplyv na výkon systému.
Zálohovanie a obnovenie	Riešenie musí umožňovať zálohovanie a obnovu kryptografického obsahu a konfigurácie - Zálohovanie musí byť chránené (aspoň pomocou prístupovej fázy). - Riešenie musí vykonávať zálohy na požiadanie a podľa harmonogramu
Počet KMS	2