

PRIMEKEY EJBCA PKI

PKI rešenje mora da ima sve komponente potrebne za uspešnu implementaciju i rad infrastrukture javnih ključeva (PKI). To uključuje kompletan sistem za izdavanje digitalnih sertifikata (CA, Certification Authority), registraciono telo (RA Registration Authority) i sistem za validaciju. (VA Validation Authority).

Rešenje mora nuditi mogućnost implementacije kroz virtuelni sistem (*virtual appliance*).

Mora da postoji više modela koji variraju od XS, koji se koristi npr. kao CA root, do XL modela koji se koristi u velikim sistemima koje zahtevaju visoke performanse i na ovaj način omogućavaju jednostavno skaliranje u odnosu na broj korisnika.

Rešenje mora da nudi *web-based* interfejs, uključujući sve funkcije koje su potrebne za jednostavnu instalaciju i operaciju.

Rešenje mora da ima mogućnost podizanja neograničenog broja sertifikacionih tela (CA)

Rešenje mora da ima sledeće funkcionalnosti: x.509 sertifikati uz korišćenje RSA i ECC ključeva (RFC5280), podršku za XKMS standard, podršku za SCEP, razmenu sertifikata između CA i VA u realnom vremenu.

ŠTAMPAČ ZA PAMETNE KARTICE

Štampač za pametne kartice mora da ima sledeće funkcionalnosti:

- Metod štampanja: Thermalni transfer
- Minimalna rezolucija štampe: 300 dpi
- Štampanje u boji
- Dvostrana štampa
- Kodiranje čipa: kontaktno i bezkontaktno
- Prostor za skladištenje novi i odštampanih kartica koji prijmaju minimum 30 kartica
- Brzina štampe kartica: 75 kartica na sat

SISTEM ZA UPRAVLJANJE SERTIFIKATIMA I KARTICAMA

Rešenje mora da ima sledeće funkcionalnosti:

- Upravljanje PKI kredencijalima
- Upravljanje FIDO kredencijalima
- Podršku za biometrijsku autentifikaciju
- Upravljanje RFID kredencijalima
- Podršku za sledeće sigurnosne uređaje:
 - o ACS ACOS5-64
 - o Aventura MyEID 4.5
 - o Avtor CryptoCard 337
 - o Atos CardOS v4.4
 - o Atos CardOS v5.3
 - o Cryptovision SCinterface
 - o Giesecke+Devrient StarSign® Key Fob

- Giesecke+Devrient StarSign® Crypto USB Token M
- Giesecke+Devrient StarSign® PKI Card
- Giesecke+Devrient StarSign® wristband
- Key-ID PKI
- Feitian ePass FIDO-NFC K9/PlusK9/K40
- Feitian BioPass FIDO2 Plus K27/K26/K45
- Feitian eJava Token
- Feitian Smart Card
- Feitian ePass2003
- Feitian ePass2003 PKI eJava Token
- Feitian ePass2003 PKI Smart Card
- Feitian Fingerprint Smart Card F2000
- Feitian iePass FIDO PIV K44
- Thales IDPrime.NET 510
- Thales IDPrime.NET 5500
- Thales IDPrime MD830/MD840
- Thales IDPrime MD930/ 940
- Thales IDPrime MD3810/ 3840
- Thales IDPrime 3930/3940
- Thales IDPrime 3940 FIDO
- Thales IDPrime 3930 FIDO
- Thales SafeNet IDPrime 940c CC
- Thales IDPrime PIV 2.1
- Thales IDPrime PIV 3.0
- Thales IDPrime Virtual
- Thales MultiApp ID
- Thales Safenet eToken 5100/5110 FIPS
- Thales Safenet eToken 5300
- Thales SafeNet eToken FIDO
- Thales SafeNet eToken Fusion CC
- HID C200/C1150
- HID Crescendo 144K
- Identiv uTrust MD
- Longmai mToken Cryptoid
- Microsoft minidriver enabled devices
- Microsoft Windows Hello for Business
- Idemia ypsID S2
- Idemia ypsID S3
- Idemia ID-One Cosmo 8.1 IAS ECC
- Idemia ID-One Cosmo 8.2 2.4.2 (SPE)
- Idemia ID-One PIV 8.1
- Open FIPS 201 Applet
- SafeTrust -PIV on Placard
- Swissbit iShield Key
- Taglio C2
- Taglio PIVKey
- TCOS TeleSec IDKey
- Virtual Smart Cards

- Yubico YubiKey 5 NFC/5C/5 Nano/5CNano
- Yubico YubiKey 4/ 4 Nano/4C/4C Nano
- Yubico YubiKey NEO/NEO-n
- RFID Physical Access Credentia
- Podršku za sledeće PKI sisteme:
 - Microsoft Certificate Authority from 2008 R2 and above
 - Primekey EJBCA Community and Enterprise
 - Entrust MS10
 - Entrust Gateway PKI CA
 - EverTrust Horizon CADigicert PKI Platform
 - Digicert Certcentral
 - DigiCert ONE
 - Nexus Certificate Manager
 - Verizon UniCERT
 - GlobalSign EPKI
 - IDnomic (formerly known as OpenTrust) PKI
 - Sectigo Certificate Manager
 - certSIGN certSAFE CA
 - MTG Certificate Lifecycle Manager
- Rešenje mora da ima podršku za sledeće sisteme za baze podataka:
 - SQLite
 - MS SQL Support (Native Client: 9.0, 10.0 and 11.0)
 - MySQL/MariaDB
 - Backup / Restore
 - Multi-forest & Multi-domain
- Rešenje mora da ima podršku za sledeće HSM-ove:
 - Thales Safenet Luna / ProtectServer/ DPoD
 - Utimaco SafeGuard CryptoServer
 - Entrust nCipner nShield
 - Entrust nShield as s Service
 - Ultra Electronics (AEP) Keyper Plus
 - Securosys Primus
 - Futurex VirtuCrypt
- Rešenje mora da podržava sledeće štampače pametnih kartica sa sledećim funkcionalnostima:
 - Evolis Primacy
 - HID Fargo HDP5000/5600/6600
 - Entrust DataCard SR300
 - Entrust Datacard CR805
 - Magicard Prima 4
 - Matica 8300
 - Matica EDI Secure
 - Printer support for graphical personalization
 - PIN mailers (both email and regular mail)
 - Contactless RFID interface
 - Batch processing
 - Card stock management

Rešenje mora da ima sledeće sigurnosne funkcionalnosti:

- Sigurno skladište za ključeve
- Sigurni backup i sinhronizaciju baza podataka
- Mogućnost oporavka izgubljenih, ili ukradenih ključeva
- Drugi faktor autentifikacije uz korišćenje OIDC
- Enkriptovani audit log
- Granularnu kontrolu pritupa
- Odobravanje akcija i aktivnosti
- Arhiviranje i vraćanje ključeva
- Mogućnost klasteriovanja zarad postizanja visoke dostupnosti

Rešenje mora da ima mogućnost da beleži sve transakcije u sopstveni repozitorijum

Rešenje mora da ima mogućnost upisivanja svih sistemskih aktivnosti u Windows Event Log

Rešenje mora da ima mogućnost registracije 300.000 korisnika

Rešenje mora da ima mogućnost da podnese i do 100 paralelnih operacija

REMOTE PED I KLJUČEVI ZA POSTOJEĆI HSM

Za potrebe konfiguracije postojećih Luna Netowrk HSM-ova S700, potrebno je nabaviti Remote PED i 10 ključeva.