ENTERPRISE RIEŠENIA

Disig CA Signer

Aplikácia na poskytovanie certifikačných služieb

Aplikácia **Disig CA Signer** je kľúčový softvérový modul certifikačnej autority slúžiaci na **vydávanie certifikátov**, **rušenie certifikátov** a na **generovanie zoznamov zrušených certifikátov** (CRL) v PKI – infraštruktúre verejného kľúča.

Disig CA Signer implementuje **progresívne kryptografické algoritmy** a poskytuje prevádzkovateľovi viacero unikátnych vlastností, ako je napríklad **možnosť definovať rozšírenia certifikátov** až na úrovni vlastných ASN.1 štruktúr. S aplikáciou Disig CA Signer je teda možné **vydávať certifikáty a CRL s rozšíreniami**, ktoré sú v maximálnej možnej miere prispôsobené potrebám prevádzkovateľa.

Informácie o vydaných certifikátoch a zoznamoch zrušených certifikátov **sú uchovávané v relačnom databázovom systéme**, ktorý predstavuje hlavné integračné rozhranie aplikácie.

CHARAKTERISTIKA

Aplikácia na vydávanie certifikátov, rušenie certifikátov a vytváranie zoznamu zrušených certifikátov

Daemon určený pre operačný systém **Ubuntu** a **Red Hat Linux**

Možnosť **súčasnej prevádzky viacerých certifikačných autorít**

Podpora substitúcií v rozšíreniach certifikátov umožňujúca vkladať do certifikátov jedinečné informácie o držiteľovi

Vytváranie elektronicky podpísaných auditných záznamov na ochranu pred neoprávnenou manipuláciou resp. pozmeňovaním

Podpisový komponent vyvíjaný v zmysle požiadaviek Common Criteria (ISO/IEC 15408)

Aplikácia certifikovaná NBÚ SR ako „Software for Trustworthy System“

ENTERPRISE RIEŠENIA / DISIG CA SIGNER

Podporované úložiská kľúčového páru

HSM moduly s podporou OpenSSL engine

PEM súbor s kľúčovým párom vo formáte PKCS#8 chránený symetrickou šifrou

Podporované formáty žiadostí o vydanie certifikátu

PKCS#10

SPKAC

Podporované formáty sériových čísel certifikátov

Sekvenčné

Randomizované (obsahuje fixnú, náhodnú a inkrementálnu zložku)

Podporované kryptografické algoritmy[1]

RSA s veľkosťou kľúča do 4096 bit

MD2, MD4, MD5

RIPEMD128, RIPEMD160, RIPEMD256, RIPEMD320

SHA-1

SHA-224, SHA-256, SHA-384, SHA-512

Podporované kryptografické štandardy

RFC 5280 – Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile

RFC 2986 – PKCS #10: Certification Request Syntax Specification

XMLDSig – XML Signature Syntax and Processing

Systémové požiadavky

Operačný systém GNU/Linux (Ubuntu 8.04 a vyšší alebo RedHat 5)

HSM modul dostupný cez rozhranie OpenSSL engine

Databázový systém PostgreSQL 8.1 a vyšší

Minimálne 1-jadrové CPU, 512MB RAM a 50 MB miesta na HDD (bez databázy)

Odporúčané aspoň 2-jadrové CPU, 2GB RAM a 50 MB miesta na HDD (bez databázy)

[1] Uvedená množina algoritmov môže byť zúžená alebo rozšírená v závislosti od použitého HSM modulu.

ISO QSCert 9001 · ISO/IEC QSCert 27001 · ISO QSCert 14001 · AQAP QSCert 2110

Disig a.s.,
Záhradnícka 151,
821 08 Bratislava 2
Tel: +421 (0)2 208 50 140
www.disig.sk

Verzia: 01 - 2016