ENTERPRISE RIEŠENIA

Disig TSA Signer

Aplikácia na vydávanie časových pečiatok

Aplikácia Disig TSA Signer tvorí srdce autority časovej pečiatky a je zodpovedná za **generovanie a vydávanie časových pečiatok**. Je certifikovaná NBÚ SR, a teda môže byť použitá aj na poskytovanie kvalifikovanej dôveryhodnej služby vydávania elektronických časových pečiatok.

TSA Signer je ideálnym **riešením** nielen **pre poskytovateľov kvalifikovaných dôveryhodných služieb**, ale aj **pre stredné a väčšie organizácie**, ktoré potrebujú zabezpečiť integritu elektronických dokumentov a vytvoriť dôkaz o ich existencii v konkrétnom čase.

Aplikácia kontroluje **správnosť systémového času voči ľubovoľnému referenčnému zdroju** presného času, ktorý je schopný komunikovať prostredníctvom NTP protokolu.

Na uchovávanie informácií o žiadostiach o vydanie časovej pečiatky a vydaných časových pečiatkach je využívaný relačný databázový systém.

CHARAKTERISTIKA

Serverová aplikácia na generovanie časových pečiatok

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

Využíva NTP **protokol na overovanie zhody systémového času s ľubovoľným referenčným zdrojom** presného času

Možnosť **rozloženia záťaže a zabezpečenia vysokej dostupnosti** spustením viacerých inštancií na jedinom systéme

Vytváranie elektronicky podpísaných auditných záznamov na ochranu pred neoprávnenou manipuláciou alebo pozmeňovaním

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

Aplikácia **certifikovaná NBÚ SR** ako „Software for Trustworthy System“

ENTERPRISE RIEŠENIA / DISIG TSA SIGNER

Podporované úložiská kľúčového páru

HSM moduly s podporou OpenSSL engine

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

Podporované komunikačné protokoly

TSP / TCP

TSP / HTTP

Podporované databázové systémy

MySQL

PostgreSQL

SQLite

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 3161 - Internet X.509 Public Key Infrastructure - Time-Stamp Protocol

Systémové požiadavky

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

HSM modul dostupný cez rozhranie OpenSSL engine

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)

Voliteľné rozšírenie „TSA Billing“

Počíta vydané časové pečiatky systémom pre-paid (kredit) alebo post-paid (paušál)

Autentizuje používateľa pomocou zdrojovej IP adresy, HTTP Basic autentizácie alebo klientskeho SSL certifikátu

Disig TSA Appliance

Kompletné riešenie vo forme hardvérového zariadenia s osvedčenými HW komponentmi

Viacjadrový Intel kompatibilný procesor

Operačný systém GNU/Linux

HSM modul THALES nShield Solo certifikovaný v zmysle FIPS 140-2 Level 3

Prevedenie ako 1U sieťové zariadenie montovateľné do štandardného stojanu

Veľkosť diskového priestoru prispôsobiteľná predpokladanej maximálnej záťaži

Samostatné sieťové rozhrania určené pre spracúvanie požiadaviek, auditné správy a manažment zariadenia

V závislosti od konfigurácie až do 300 časových pečiatok za sekundu pri veľkosti RSA kľúča 2048-bit

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

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

Verzia: 01 - 2017