ENTERPRISE RIEŠENIA

Disig OCSP Responder

Aplikácia na okamžité overenie platnosti certifikátu

Aplikácia **Disig OCSP Responder** poskytuje výkonnú a ľahko dostupnú službu potvrdenia platnosti certifikátu (OCSP - Online Certificate Status Protocol), či už kvalifikovaného, serverového alebo iného.

Je určená najmä pre prevádzkovateľov elektronických podateľní a iných informačných systémov, ktorí potrebujú overovať elektronický podpis v reálnom čase.

Služba **OCSP prináša výrazné zrýchlenie procesov** spoliehajúcich sa na elektronický podpis, pretože môže eliminovať nutnosť čakať na vydanie nasledujúceho zoznamu zrušených certifikátov (CRL). Vďaka tomu je možné vykonať úplné overenie elektronického podpisu prakticky okamžite.

Disig OCSP Responder disponuje robustným integračným rozhraním, ktoré umožňuje jeho prevádzku s ľubovoľnou certifikačnou autoritou a môže byť použitý aj ako centrálny prvok validačnej autority.

CHARAKTERISTIKA

Aplikácia implementujúca službu on-line overovania platnosti certifikátov

Základný komponent validačnej autority alebo prídavný modul existujúcej certifikačnej autority

Daemon určený pre operačný systém Ubuntu a Red Hat Linux

Spĺňa vysoké nároky na výkon a spoľahlivosť zapojením viacerých inštancií

Podpora všetkých kľúčových transportných mechanizmov

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 OCSP RESPONDER

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

OCSP / TCP

OCSP / HTTP POST

OCSP / HTTP GET

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

Využívané/implementované štandardy

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

RFC 6960 - X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol – OCSP

RFC 5019 - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments

Podporované databázové systémy

MySQL

PostgreSQL

SQLite

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)

Disig OCSP Responder Appliance

Kompletné riešenie vo forme hardvérového zariadenia s osvedčenými HW komponentmi

Operačný systém GNU/Linux

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

Viacjadrový Intel kompatibilný procesor

Prevedenie ako 1U sieťové zariadenie montovateľné do štandardného stojanu

Veľkosť diskového priestoru prispôsobiteľná počtu obsluhovaných CA

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

[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