

ENTERPRISE RIEŠENIA

Disig KeyPoint



Cloudové riešenie pre kvalifikovaný elektronický podpis a pečať

Pri vytváraní elektronického podpisu sa zvyčajne používajú lokálne úložiská kľúčového materiálu, ktoré vyžadujú prítomnosť privátneho kľúča na strane klienta. Privátny kľúč je uchovávaný v softvérovej podobe (v súbore) alebo na QSCD zariadení (na čipovej karte).

Vzdialené úložisko kľúčového materiálu poskytované systémom Disig KeyPoint umožňuje koncovým používateľom využívať kľúčový materiál uložený v **centrálnom spravovanom bezpečnom zariadení**. Tento koncept poskytuje obdobnú mieru bezpečnosti ako bežné QSCD zariadenia, no zároveň odbreňuje používateľa od nutnosti takéto zariadenie vlastniť a mať ho fyzicky pripojené k systému, na ktorom podpisuje.

Kľúčový materiál uložený v systéme Disig KeyPoint je klientskym systémom **dostupný bez ohľadu na platformu** a bez väzby na konkrétne zariadenie. Používateľ teda môže s rovnakým privátnym kľúčom podpisovať dokumenty nielen na osobnom počítači, ale aj na mobilnom zariadení.

CHARAKTERISTIKA

Vyhotovovanie kvalifikovaného elektronického podpisu a pečate na ľubovoľnom zariadení

Viacpoužívateľský systém pracujúci s konceptom virtuálnych čipových kariet

Bezpečné uloženie a centralizovaný manažment kryptografických kľúčov

Integrácia s takmer ľubovoľným viacfaktorovým autentizačným systémom

Integrácia so systémom certifikačnej authority pre automatické vydávanie certifikátov

Prakticky neobmedzený počet používateľov a kľúčov

Bezpečný produkt certifikovaný NBÚ SR na generovanie a uchovávanie súkromných kľúčov kvalifikovaných certifikátov a vyhotovovanie kvalifikovaného elektronického podpisu

ENTERPRISE RIEŠENIA/DISIG KEYPOINT

Zhoda s legislatívou

Nariadenie (EÚ) č. 910/2014 - eIDAS

Podporované štandardy

CEN/TS 419241:2014 - Security Requirements
for Trustworthy Systems Supporting Server Signing

Charakteristika systému

Sole Control Level 2 v zmysle CEN/TS 419241:2014

Integrácia s autentizačným systémom

OpenId Connect

WS-Trust

WS-Federation

SAML 1.1/2.0

Integrácia so systémom certifikačnej authority

SOAP Web Services

Integrácia s klientským systémom

SOAP Web Services

PKCS#11: Cryptographic Token Interface Standard

Microsoft Crypto API / Cryptographic Service Provider

Podporované HSM

THALES nShield F3 Solo
s aktivovanou SEE funkcionalitou

THALES nShield F3 Connect
s aktivovanou SEE funkcionalitou

Podporované kryptografické algoritmy

RSA s veľkosťou kľúča do 4096 bit

SHA-1

SHA-256, SHA-384, SHA-512

Podporované klientske platformy

Microsoft Windows

Linux

Mac OS X

Android

iOS

Windows Phone



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

