

ENTERPRISE RIEŠENIA

Disig PKI Client

Integrácia PKI služieb na klientsku stanicu

Aplikácia Disig PKI Client integruje operačný systém počítača spolu s vybranými aplikáciami do centralizovanej PKI infraštruktúry.

Z pohľadu používateľa prináša jednoduché nástroje na prácu s pokročilými bezpečnostnými službami ako šifrovanie, podpisovanie, overovanie a bezpečné mazanie súborov.

Pre administrátorov prináša **pohodlné nastavenie bezpečnosti z centrálného bodu** – doménového servera, cez ktorý je možné spravovať úroveň používaných kryptografických algoritmov na definovaných skupinách používateľov alebo pracovných staníc.

Prehľadné grafické používateľské rozhranie aplikácie nekladie zvýšené nároky na technické schopnosti bežných používateľov, **pokročilým používateľom však poskytuje dostatok ovládacích prvkov a nastavení pre komfortnú a plnohodnotnú prácu s kryptografickými nástrojmi a službami.**

CHARAKTERISTIKA

Používateľsky prívetivé PKI riešenie pre operačný systém Microsoft Windows

Nástroje na podpisovanie, šifrovanie, dešifrovanie a bezpečné mazanie súborov bez obmedzenia ich veľkosti

Integrácia s certifikovanými produktmi pre kvalifikovaný elektronický podpis

Integrácia s Microsoft Active Directory a vynucovanie bezpečnostných politík pomocou Group Policy

Manažment čipovej karty a objektov na nej uložených

Notifikácie pred vypršaním platnosti používateľských certifikátov a podporné procesy pre ich včasné prevydanie

Zálohovanie a obnova kľúčového materiálu na centrálnom serveri

Prispôsobivosť aplikácie podľa veľkosti a komplexnosti nasadenia v organizácii

ENTERPRISE RIEŠENIA/DISIG PKI CLIENT

Integrácia s technológiami systému

Microsoft Windows

Windows Logon
Active Directory
Group Policy

Integrácia s externými systémami

Disig PKI Server
Disig Key Recovery
Disig SWACA

Podporované aplikácie pre integráciu

Microsoft Outlook
Podpisovanie a šifrovanie e-mailov
Disig pdfSigner
Podpisovanie PDF dokumentov
Disig Dektop Signer
Vytváranie a overovanie QES

Podporované rozhrania pre prácu s QSCD

PKCS #11: Cryptographic Token Interface Standard
Microsoft Crypto API / Cryptographic Service Provider

Podporované kryptografické štandardy

RFC 5280 - X.509 Public Key Certificates
RFC 5652 - Cryptographic Message Syntax
RFC 3161 - Time-Stamp Protocol

Podporované asymetrické algoritmy¹

RSA so schémou RSAES-PKCS1-v1_5
RSA so schémou RSASSA-PKCS1-v1_5

Podporované symetrické algoritmy¹

3DES CBC
AES 128 CBC, AES 192 CBC, AES 256 CBC

Podporované hash algoritmy¹

SHA-1
SHA-256, SHA-384, SHA-512

Podporované algoritmy mazania dát

Germain FOIS
DOD 5220.22-M
NAVSO P-5239-26

Systemové požiadavky

Microsoft Windows 7 a vyššie (32 alebo 64 bit)
Microsoft .NET Framework 3.5 a vyššie
Minimálne 1-jadrové CPU a 512 MB RAM,
100 MB miesta na HDD

¹Uvedená množina algoritmov môže byť zúžená alebo rozšírená v závislosti od použitého QSCD zariadenia.



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

