

ELEKTRONICKÝ PODPIS

# Disig Desktop Signer



## Desktopové riešenie pre kvalifikovaný elektronický podpis a pečať

Aplikácia Disig Desktop Signer umožňuje koncovým používateľom jednoduchým a zároveň rýchlym spôsobom vyhotovovať a overovať **kvalifikovaný elektronický podpis a pečať** v zmysle **európskeho nariadenia eIDAS** a platnej **slovenskej legislatívy**.

Základnú funkcionality aplikácie rozširujú **prídavné moduly Hromadné podpisovanie, Archív a Zaručená konverzia**.

S modulom **Hromadné podpisovanie** je možné podpísať viac dokumentov jedným zadanim PIN kódu. Pomocou modulu **Archív** môžu používatelia udržiavať dlhodobú overiteľnosť elektronických dokumentov podpísaných elektronickým podpisom alebo pečaťou. Modul **Zaručená konverzia** zase umožňuje prevádzať dokumenty z ich listinnej podoby do elektronickej a naopak.

**Prehľadné grafické používateľské rozhranie** aplikácie nekladie zbytočne prehnane nároky na technické schopnosti bežných používateľov, pokročilým používateľom však poskytuje **dostatok ovládacích prvkov a nastavení** pre komfortnú a plnohodnotnú prácu s elektronickým podpisom.

### CHARAKTERISTIKA

Aplikácia na vyhotovovanie a overovanie **kvalifikovaného elektronického podpisu a pečate** určená pre koncových používateľov

Desktopové riešenie pre operačný systém **Microsoft Windows**

Používateľsky **prívetivé a intuitívne rozhranie** na overovanie a podpisovanie dokumentov

Možnosť rozšírenia základnej funkcionality o samostatné moduly **hromadného podpisovania, archivácie a zaručenej konverzie**

Podpora **eID** a všetkých **QSCD zariadení** s dostupným **CSP** alebo **PKCS#11** rozhraním

Podpora **podpisovania a overovania širokého spektra formátov** dokumentov a podpisov

Aplikácia je certifikovaná **NBÚ SR** na vyhotovovanie a overovanie kvalifikovaného **elektronického podpisu a pečate**

## ELEKTRONICKÝ PODPIS / DISIG DESKTOP SIGNER

### Podporované formáty elektronického podpisu

CAdES-BES, CAdES-EPES, CAdES-T, CAdES-X, CAdES-A  
CAAdES-B-B, CAAdES-B-T, CAAdES-B-LT, CAAdES-B-LTA  
XAdES-BES, XAdES-EPES, XAdES-T, XAdES-X, XAdES-A  
XAdES-B-B, XAdES-B-T, XAdES-B-LT, XAdES-B-LTA  
PAdES-BES, PAdES-EPES, PAdES-T, PAdES-LTV  
PAdES-B-B, PAdES-B-T, PAdES-B-LT, PAdES-B-LTA  
XAdES\_ZEP s dátovými objektmi typu XML, PDF a zložený elektronický podpis

### Podporované kryptografické štandardy

X.509 Public Key Certificates  
CMS Advanced Electronic Signatures  
XML Advanced Electronic Signatures  
PDF Advanced Electronic Signatures  
Electronic Signature Policies  
Associated Signature Containers (ASiC)  
ZIP formát súboru pre ZEP (ZEPf)  
Trust-service Status List  
Dôveryhodný zoznam  
Time-Stamp Protocol  
Online Certificate Status Protocol

### Podporované kryptografické algoritmy<sup>1</sup>

RSA, DSA, ECDSA  
MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512  
RIPEMD128, RIPEMD160, RIPEMD256

### Podporované rozhrania pre prácu s QSCD

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

### Podporované formáty dokumentov akceptované orgánmi verejnej moci<sup>2</sup>

PDF/A-1a, TXT, PNG, XMLDataContainer / XML formuláre

### Podporované formáty dokumentov

TXT, PDF<sup>3</sup>, RTE<sup>3</sup>, DOC<sup>3</sup>, DOCX<sup>3</sup>, ODT<sup>3</sup>  
XML, XMLDataContainer / XML formuláre, HTML, XHTML  
PNG<sup>4</sup>, BMP<sup>4</sup>, GIF<sup>4</sup>, JPG<sup>4</sup>, TIFF<sup>4</sup>  
MS Office formáty (XLS, XLSX, PPT, PPTX a ďalšie)<sup>5</sup>  
Ľubovoľný formát spracovateľný externou aplikáciou

### Podporované podpisové kontajnery

CMS, XML, PDF, ASiC-S, ASiC-E, ZEPf, xZEP / ZEPx

### Súlad so štandardami

ETSI TS 101 733, ETSI TS 103 173, ETSI TS 101 903,  
ETSI TS 103 171, ETSI TS 102 778, ETSI TS 103 172,  
ETSI TS 102 918, ETSI TS 103 174, ETSI TS 119 612,  
ETSI TR 102 272, RFC 5280, RFC 3161, RFC 2560

### Zhoda s legislatívou

Nariadenie (EÚ) č. 910/2014 - eIDAS

### Systémové požiadavky

Microsoft Windows XP SP3 a vyššie (32 alebo 64 bit)  
Microsoft .NET Framework 2.0  
Minimálne 1-jadrové CPU a 512 MB RAM, 100 MB miesta na HDD

<sup>1</sup> Uvedená množina algoritmov sa môže meniť v závislosti od použitého QSCD zariadenia

<sup>2</sup> Stanovuje § 57a Výnosu Ministerstva financií Slovenskej republiky 55/2014 Z. z. zo 4. marca 2014

<sup>3</sup> Formát je voliteľne konvertovateľný do formátu PDF/A-1a

<sup>4</sup> Formát je voliteľne konvertovateľný do formátu PNG

<sup>5</sup> Formát je voliteľne konvertovateľný do formátu PDF pokiaľ je dostupná lokálna inštalácia kancelárskeho balíka Microsoft Office



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

