Technická specifikace elektronického podpisu pro eSOP

Elektronický podpis eSoP za dodavatele (obchodníka) je možný prostředkem vytvářejícím důvěru pro elektronické transakce (kvalifikovanou elektronickou pečetí, resp. kvalifikovaným elektronickým podpisem). Pro podpis nelze použít veřejnou (public) část certifikátu.

Akceptované jsou kvalifikované certifikáty, které vydaly tyto akreditované certifikační autority:

- První certifikační autorita a.s. (ICA) - www.ica.cz/
- Česká pošta s.p. - www.postsignum.cz
- eIdentity a.s. - www.eidentity.cz/

Podporujeme elektronické podpisy podle standardu PAdES (PDF Advanced Electronic Signatures).

Všechny varianty PAdES vycházejí z normy ISO 32000-1.

Samotné podpisy musí být ve vlastním PDF dokumentu ve formátu PKCS#7 (neboli CMS – Cryptographic Message Syntax), který je popsán ve standardu RFC5652.

Podporovány jsou tyto profily PDF podpisů:

- PAdES CMS Profiles based on ISO 32000-1 (E-BES, E-EPES, E-LTV)
  - identifikován subfiltrem adbe.pkcs7.detached
  - standard ETSI EN 319 142-2 V1.1.1 (2016-04)
- PAdES Baseline Profiles (B-B, B-T, B-LT, B-LTA)
  - identifikován subfiltrem ETSI.CAdES.detached
  - standard ETSI EN 319 142-1 V1.1.1 (2016-04)

Podpis typu PKCS#1 není podporován. Subfiltr adbe.pkcs7.sha1 není podporován.

Algoritmy kryptografického otisku MD2, MD4, MD5 a SHA-1 nejsou podporovány.
Doporučený algoritmus kryptografického otisku je SHA-256.