

Opis predmetu zákazky

Funkcia:

Hromadné podpisovanie elektronických dokumentov kvalifikovaným elektronickým podpisom.

Aplikácia je nainštalovaná a prevádzkovaná na pracovnej stanici, na ktorej je umiestnené aj bezpečné zariadenie pre vytváranie elektronického podpisu (USB Token alebo čipová karta). Podporované prevádzkové prostredie je min. MS Windows 10.

Spôsob použitia:

- po spustení je zadaný vstupný adresár (obsahujúci elektronické dokumenty určené na podpísanie) a výstupný adresár (do ktorého budú ukladané podpísané dokumenty)
- po aktivácii procesu podpisovania vloží bezpečné zariadenie na pracovnú stanicu (USB token alebo čipovú kartu) je používateľ prostredníctvom ovládača karty požiadaný o zadanie aktivačného PINu (podmienka aktivácie procesu podpisovania na čipe)
- aplikácia postupne vykoná podpísanie všetkých dokumentov vo vstupnom adresári a podpísané dokumenty umiestni do výstupného adresára, prípadne oznámi ak vznikla v procese podpisovania chyba.

Popis funkčnosti - aplikácia zabezpečuje nasledujúcu funkcionality:

- vytváranie kvalifikovaného elektronického podpisu a / alebo kvalifikovanej elektronickej pečate hromadným spôsobom.

Elektronickým podpisom sú podpísané všetky dokumenty uložené vo vstupnom adresári (ktorý môže byť aj „vzdialený“, t.j. adresár ku ktorému má používateľ z pracovnej stanice prístup, a uloženie podpísaných dokumentov do výstupného adresára. Aplikácia podľa nastavenia a výberu umožní prípadné pripojenie časovej pečiatky k podpisu (integrácia na službu I.CA).

Podpora pre :

- vytváranie elektronického podpisu v súlade s eIDAS vo formáte PAdES a podpisových kontajnerov ASiC-E,
- možnosť pripojiť pečiatku pri vytváraní elektronického podpisu a používať vlastný zdroj časových pečiatok,
- hromadného podpisovania dokumentov,
- overovanie elektronického podpisu vo formáte PAdES a podpisových kontajnerov vytvorených v súlade s eIDAS,
- zaručenú konverziu z listinnej do elektronickej formy,
- zaručenú konverziu z elektronickej do listinnej formy,
- rozhrania PKCS#11,
- čipové karty Starcos 3.0 a 3.5,

- mandátne certifikáty,
- operačné systémy Windows, Linux a MacOS,
- API pre vytváranie elektronického podpisu a pre integráciu do aplikácii tretích strán,
- formát vytváraného podpisu je XAdES_ZEP alebo ASiC,
- podpora podpisovania nasledujúcich formátov elektronických dokumentov:
 - textové dokumenty vo formátoch PDF/A (aplikácia zabezpečuje konverziu z PDF do tohto formátu), TXT,
 - obrázky vo formátoch PNG,
 - XML dokumenty vo forme elektronických formulárov, ktoré budú podpisované v súlade s nasledujúcimi štandardami:
 - o XMLDataContainer pre formát ASiC,
 - o XAdES_ZEP 2.0,
- možnosť konfigurácie aplikácie / modulu:
 - formát vytváraného podpisu,
 - parametre pre použitie služby časovej pečiatky, integrácia na možnosť použitia certifikátu aj na čipovej karte,
 - určenie vstupného a výstupného adresára,
- evidencia údajov potrebných pre podpisovanie elektronických formulárov:
 - XSD, XSLT a ďalšie údaje potrebné pri vytváraní podpisových štruktúr,
 - určenie či sa jedná o formulár v MEF, t.j. či sa do podpisových štruktúr vkladajú referencie alebo plné hodnoty objektov,
 - túto evidenciu je možné spravovať:
 - o prezerateľ evidované formuláre a k nim viazané údaje;
 - o odoberateľ uchovávané formuláre a k nim viazané údaje;
 - o pridávať formuláre do evidencie – toto sa realizuje prostredníctvom ZIP súborov, ktoré možné získať z MEF;
 - o realizovať export a import tejto evidencie,
- reportovanie prípadných chýb vznikajúcich pri podpisovaní, t.j. ktoré dokumenty neboli podpísané a prečo. V prípade absencie chyby informácia o úspešnom ukončení procesu podpisovania,
- možnosť uchovania chybového reportu do súboru,

Rozhranie aplikácie / modulu: aktivácia z príkazového riadku (command line pri zadaní vstupného a výstupného adresára ako parametra, v prípade nezadania default nastavenie), alebo GUI. PIN nie je možné zadať z externého prostredia (napr. do príkazového riadku). Na základe typu volania bude podpísaný vždy každý dokument samostatne, alebo viac dokumentov spolu.

Ďalšie požiadavky:

- Platná certifikácia komponentu / aplikácie Národným bezpečnostným úradom SR **do 26.6.2021;**
- Výkon - počet podpísaných PDF v jednej dávke: **min. 18000 ks;**
- Výkon za hod. (počet podpísaných PDF dokumentov za 1 hodinu): **min. 2500 ks;**
- Počet súčasne bežiacich licencií : **1 až 5 ks;**

- Spôsobilosť bezpečného produktu na vyhotovovanie kvalifikovaného elektronického podpisu typu XAdES v schválených formátoch pre prostredie **.NET**;
- Podpora prevádzkových platforiem **.NET**;
- Podpora nasadenia v rámci operačných systémov: **min. Microsoft Windows 10**
- Podpora kryptografických funkcií:
 - Hashovacie funkcie – **SHA1, SHA256, SHA384, SHA512**;
 - Asymetrické šifrovanie – **DSA, RSA**;
- Podpora využívania QSCD pre uchovávanie súkromných kľúčov prostredníctvom rozhraní **MS CryptoAPI**, resp. **PKCS#11**;
- Podpora vytvárania elektronických podpisov vo formáte **XAdES v profile eIDAS** - baseline profile **v 2.1.1 - ETSI TS 103 171** – Electronic Signatures and Infrastructures (ESI) XAdES Baseline Profile;
- Podpora vytvárania elektronických podpisov vo formáte **XAdES** v profiloch publikovaných NBÚ ako štandardy pre SR („Formáty zaručených elektronických podpisov, v3.0“) - **XAdES_ZEP, v1.0, v1.1, v2.0**;
- Informácie ukladané v elektronickom podpise, ktoré sú súčasťou elektronického podpisu: informácia o čase vytvorenia elektronického podpisu; certifikát podpisovateľa; referencia podpisovej politiky použitej pri vytváraní elektronického podpisu; informácie o typoch a formátoch podpísaných dátových objektov;
- Podpora formátov podpisových kontajnerov ASiC v súlade so štandardami **eIDAS v1.3.1 - ETSI TS 102 918** – Electronic Signatures and Infrastructures (ESI) Associated Signature Containers (ASiC);
- Podpora formátov podpisových kontajnerov ASiC v súlade so štandardami **eIDAS v2.2.1 - ETSI TS 103 174** – Electronic Signatures and Infrastructures (ESI) ASiC Baseline Profile;
- Podpora formátov podpisového kontajneru pre jednoduchý elektronický podpis v súlade s profilmi **XAdES_ZEP – DataEnvelope, v1.0, v1.1, v2.0**;
- Podpora podpisovania elektronických dokumentov v súlade s **§ 57a Výnosu MF SR č. 55/2014** o štandardoch pre IS VS, vrátane údajov vo formáte XML podpisovaných vo forme XMLDataCointainera;
- Podpora podpisovania elektronických formulárov vytvorených v súlade s **Výnosom MF SR č. 55/2014** o štandardoch pre IS VS;
- Časovo obmedzená licencia v trvaní **366 dní**.