

Používateľská príručka D.Signer/XAdES .NET, v4.0

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

Copyright

Všetky práva vyhradené

Tento dokument je vlastníctvom spoločnosti DITEC, a. s. Žiadna jeho časť sa nesmie akýmkoľvek spôsobom (elektronickým, mechanickým) poskytnúť tretej strane, rozmnožovať, kopírovať, vrátane spätného prevodu do elektronickej podoby, bez písomného povolenia spracovávateľa.

Popisné charakteristiky dokumentu

| Projekt | GOV_ZEP | | A3019_002 |
|------------|---------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Podnázov | D.Signer/XAdES .NET, v4.0 | | |
| Ref. číslo | GOV_ZEP.200 | Verzia | 1 |

| Vypracoval | Vittek Róbert | Podpis | Dátum 29.3.2016 |
|------------|---------------|--------|-----------------|
| Preveril | | Podpis | Dátum |
| Schválil | | Podpis | Dátum |

| Formulár | Dokument | | |
|------------|----------|------------------------------|------------------|
| Ref. číslo | Fo 11 | Dátum poslednej aktualizácie | Dátum 14.10.2005 |

Akceptované dňa : <Dátum akceptácie>

Za < Objednávateľa>:

Za <Dodávateľa>.:

<Meno zodpovednej osoby>

< Meno zodpovednej osoby >

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

Záznamy o zmenách

| Autor | Popis zmien | Dátum | Verzia |
|-------|-------------|-------|--------|
| | | | |
| | | | |
| | | | |

Pripomienkovanie a kontrola

| Autor | Stanovisko | Dátum | Verzia |
|-------|------------|-------|--------|
| | | | |
| | | | |
| | | | |

Rozdeľovník

| | Priezvisko Meno | Firma, Funkcia |
|----------|-----------------|----------------|
| Originál | | |
| Kópia | | |
| Kópia | | |
| Kópia | | |

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

Obsah

| 1. | Úvod | 5 |
|----|---|----|
| 2. | Zoznam použitých skratiek | 6 |
| 3. | Popis aplikácie | 7 |
| 4. | Systémové požiadavky | 9 |
| 5. | Inštalácia | 11 |
| 5. | Inštalácia z distribučného CD | 12 |
| 5. | Inštalácia v rámci klientskej aplikácie | 19 |
| 5. | Inštalácia z Internetu | 19 |
| 6. | Užívateľské nastavenia | 20 |
| 6. | Nastavenie jazyka aplikácie | 20 |
| 7. | Vytvorenie ZEP používateľom | 21 |
| 7. | Načítanie vstupných parametrov | 21 |
| 7. | Zobrazenie podpisovaných dát | 21 |
| | 2.1. Zobrazenie dokumentov | 24 |
| 7. | Nastavenie dátumu a času vytvorenia podpisu | 25 |
| 7. | Podpísanie dokumentu | |
| 7. | Zobrazenie parametrov podpisu | |
| 8. | Trademarks | 33 |

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

1. Úvod

Tento dokument je určený pre používateľov aplikácie D.Signer/XAdES .NET, resp. pre používateľov informačných systémov a aplikácií, v rámci ktorých bude aplikácia D.Signer/XAdES .NET pre zaručený elektronický podpis (ZEP) integrovaná.

Jednotlivé časti dokumentácie aplikácie D.Signer/XAdES .NET je možné použiť pri tvorbe používateľských príručiek týchto klientských informačných systémov systémov a aplikácií po dohode s vlastníkmi autorských práv aplikácie D.Signer/XAdES .NET.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

2. Zoznam použitých skratiek

HTML – HyperText Markup Language; hypertextový značkový jazyk na vytváranie webových stránok

HTTPS – HyperText Transfer Protocol Secure; zabezpečený hypertextový prenosový protokol

NBÚ – Národný bezpečnostný úrad

PDF – formát dokumentov Portable Document Format

PNG – grafický formát Portable Network Graphics

SSCD – Secure Signature Creating Device; bezpečné zariadenie na vytváranie elektronického podpisu

TXT – formát textových súborov

XML – eXtensible Markup Language; rozšíriteľný značkovací jazyk pre štruktúrované dáta

XAdES – XML Advanced Electronic Signatures; formát pokročilého elektronického podpisu na báze XML

XAdES_ZEP – profil formátu elektronického podpisu XAdES pre ZEP

XAdES_ZEPbp – profil formátu zaručeného elektronického podpisu na báze XAdES baseline profile

ZEP – Zaručený elektronický podpis

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

3. Popis aplikácie

Aplikácia D.Signer/XAdES .NET predstavuje riešenie pre vytváranie zaručeného elektronického podpisu (ZEP) nad množinou rôznych formátov dokumentov, resp. typov dát (XML dokumenty, PDF dokumenty atď.), prípadne nad ľubovoľnou kombináciou podporovaných formátov dát, ktoré spolu vytvárajú tzv. *multipart* dokument. Povolené formáty podpisovaných elektronických dokumentov v administratívnom styku špecifikuje Výnos MF SR č. 55/2014 o štandardoch pre IS VS. Požiadavky na formát a obsah podpisovaných dát stanovuje dokument NBÚ SR – Upresnenia obsahu a formálne špecifikácie formátov dokumentov pre ZEP, v1.0.

Zaručený elektronický podpis na druhej strane zabezpečuje integritu podpísaných dát a nepopierateľnosť podpisu. Aplikácia D.Signer/XAdES .NET môže byť teda nasadená v rámci akéhokoľvek systému, kde je potrebné zabezpečiť jednak integritu prenášaných a spracovávaných dokumentov, ako aj nepopierateľnosť identity ich podpisovateľa.

Aplikácia D.Signer/XAdES .NET pred samotnou procedúrou vytvorenia ZEP v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov:

- zabezpečí podpisovateľovi zobrazenie všetkých podpisovaných dát jednoznačným a adekvátnym spôsobom,
- zaručí, že dáta sa pri podpise nezmenia.

Pre vytvorenie ZEP musí byť aplikácia použitá len v súlade s platnou podpisovou politikou pre ZEP, ktorá bola schválená NBÚ SR. Používateľ je pred vytvorením podpisu povinný presvedčiť sa, že podpisová politika, ktorú aplikácia používa, je stále platná a nebola zo strany vydavateľa predčasne zrušená. Výrobca, resp. integrátor aplikácie D.Signer/XAdES .NET je povinný zabezpečiť také nastavenie konfigurácie aplikácie a parametrov volania metód rozhrania aplikácie, aby aplikácia vytvárala podpis v súlade so špecifikovanou podpisovou politikou.

Za obsah a sformátovanie vstupných dát (dokumentov), ako aj za dodržanie správneho postupu vytvorenia ZEP, definovaného v rámci podpisovej politiky, je zodpovedný podpisovateľ. Za správne vyhodnotenie platnosti vytvoreného ZEP a za špecifikovanie parametrov procesu verifikácie ZEP v súlade s podpisovou politikou je zodpovedný prijímateľ alebo prevádzkovateľ systému, ktorý tieto dáta spracováva.

Požiadavky NBÚ SR na vytváraný formát ZEP upravuje dokument – Formáty zaručených elektronických podpisov, v3.0. Minimálne požiadavky EÚ na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu stanovuje rozhodnutie komisie 2014/148/EU, ktoré nahrádza rozhodnutie komisie 2011/130/EU. Špecifikácie týkajúce sa formátov

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať ustanovuje Rozhodnutie komisie 2015/1506/EU.

Aplikácia D.Signer/XADES .NET vytvára ZEP v súlade so schválenými formátmi elektronický podpis XAdES ZEP, pre zaručený v1.0 (http://www.ditec.sk/ep/signature_formats/xades_zep/v1.0), XAdES_ZEP. v1.1 (http://www.ditec.sk/ep/signature formats/xades zep/v1.1), XAdES ZEP, v2.0 (http://www.ditec.sk/ep/signature_formats/xades_zep/v2.0) a XAdES_ZEPbp, (http://www.ditec.sk/ep/signature_formats/xades_zepbp/v1.0). v1.0 Aplikácia D.Signer/XAdES .NET vytvára typ podpisu XAdES ZEP-EPES, resp. XAdES_ZEPbp-EPES, teda elektronický podpis rozšírený o informáciu o čase vzniku ZEP, o explicitnú podpísanú referenciu podpisovej politiky a podpísané informácie o typoch a formátoch podpísaných dátových objektov, a tiež XAdES_ZEP-T, resp. XAdES_ZEPbp-T, teda elektronický podpis rozšírený o časovú pečiatku podpisu. Aplikácia D.Signer/XAdES .NET umožňuje vytvárať aj tvp podpisu XAdES_ZEPbp-BES, to znamená typ elektronického podpisu bez explicitne uvedenej referencie podpisovej politiky, v súlade s príslušnými nariadeniami komisie 2011/130/EU, 2014/148/EU, 2015/1506/EU a príslušným baseline profilom pre XAdES ETSI TS 103 171.

Aplikácia D.Signer/XAdES .NET môže byť použitá taktiež pre vytváranie tzv. obyčajného elektronického podpisu zmysle zákona č. 215/2002 Z.z. o elektronickom podpise.

V súlade s §4, odsek (5) zákona č. 305/2013 Z.z. o e-Governmente v znení neskorších predpisov je aplikácia D.Signer/XAdES Java implementovaná takým spôsobom, aby poskytovala funkcionalitu vytvorenia ZEP aj pre osoby so zdravotným postihnutím – pre slabozrakých a nevidiacich pomocou technológie NVDA (<u>http://www.nvaccess.org/</u>).

Aplikácia D.Signer/XAdES Java je lokalizovaná v slovenskom a v anglickom jazyku.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

4. Systémové požiadavky

Systémové požiadavky aplikácie D.Signer/XADES .NET sú nasledujúce:

- OS MS Windows 2008 Server, 2012 Server, Vista, Windows 7, Windows 8.x, Windows 10,
- Platforma .Net framework, verzia 4.0 alebo vyššia,
- certifikované SSCD zariadenie pre generovanie kľúčových párov a vytváranie elektronického podpisu,
- web prehliadač MS Internet Explorer, v7.0 alebo vyššia (len 32 bit), Mozilla Firefox, v45 alebo vyššia (len 32 bit, s podporou NP API)².

Ak je aplikácia D.Signer/XAdES .NET spúšťaná z web portálu pomocou aplikácie D.Launcher, tak požiadavky na web prehliadač zahŕňajú aj prehliadače:

Google Chrome v51 alebo vyššia (prípadne Chromium), Opera v38 alebo vyššia, MS Edge v25 alebo vyššia.

D.Signer/XAdES .NET x64 je možné spúšťať výlučne pomocou aplikácie D.Launcher. Systémové požiadavky pre aplikáciu D.Launcher sú špecifikované v rámci používateľskej príručky pre aplikáciu D.Launcher.

Pri vytváraní zaručeného elektronického podpisu pomocou aplikácie D.Signer/XAdES .NET vyžaduje použitie certifikovaného zariadenia sa pre generovanie a uloženie privátneho kľúča a pre vytvorenie zaručeného elektronického podpisu (SSCD – napr. čipová karta, USB token apod.) a použitie kvalifikovaného certifikátu, vydaného akreditovanou certifikačnou autoritou. Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, používateľ musí zvoliť mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov v okne pre výber certifikátu v aplikácii D.Signer/XADES .NET. Aplikácia D.Signer/XAdES .NET pristupuje k danému SSCD zariadeniu prostredníctvom príslušného CSP providera (implementácia MS Crypto API pre dané SSCD zariadenie).

Pre aplikáciu D.Signer/XAdES .NET nie sú potrebné vyššie hardwarové požiadavky, ako vyžaduje samotný operačný systém, prípadne platforma .Net framework 4.0 alebo vyššia. Požiadavky aplikácie na voľný priestor na disku sú nasledujúce:

Komponent

Veľkosť

Systémové požiadavky

² Pokiaľ je aplikácia D.Signer/XAdES .NET integrovaná v rámci web stránok web portálu.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| D.Signer/XAdES .NET | 4,45 MB |
|---|---------|
| D.Signer/XAdES .NET – XML Plugin | 1,67 MB |
| D.Signer/XAdES .NET – PDF Plugin ³ | 19,4 MB |
| D.Signer/XAdES .NET – TXT Plugin | 170 KB |
| D.Signer/XAdES .NET – PNG Plugin | 197 KB |

Aplikácia D.Signer/XAdES .NET môže byť distribuovaná na inštalačnom CD alebo v rámci klientskej aplikácie, ktorá komponent pre zaručený elektronický podpis používa, či už v rámci jej inštalačných súborov alebo priamo cez Internet na HTTPS stránkach danej web aplikácie. Veľkosť distribučných, resp. inštalačných súborov jednotlivých komponentov aplikácie D.Signer/XAdES .NET je uvedená v nasledujúcej tabuľke.

| Komponent | Veľkosť |
|-------------------------|---------|
| D.Signer/XAdES .NET x86 | 15,5 MB |
| D.Signer/XAdES .NET x64 | 17,0 MB |

Podrobný popis požiadaviek na prevádzku aplikácie D.Signer/XAdES .NET, teda požiadaviek na SSCD zariadenie, požiadaviek na prevádzkové prostredie aplikácie, bezpečnostných požiadaviek apod. je špecifikovaný v rámci dokumentu Požiadavky na prevádzkové prostredie a SSCD.

Špecifické systémové požiadavky pre jednotlivé pluginy aplikácie D.Signer/XAdES .NET sú uvedené v rámci príslušnej integračnej príručky pre daný plugin.

³ PDF technology in D.Signer/XAdES .NET - PDF Plugin is powered by PDFNet SDK copyright © PDFTron[™] Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All rights reserved.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

5. Inštalácia

Inštalácia aplikácie D.Signer/XAdES .NET závisí primárne od spôsobu distribúcie komponentov aplikácie:

- 1) inštalácia z distribučného CD spustením inštalačného programu z distribučného CD,
- inštalácia v rámci klientskej aplikácie spustením inštalačného programu klientskej aplikácie (ktorá komponent pre ZEP využíva a v rámci ktorej sa distribuuje),
- 3) inštalácia z Internetu spustením inštalácie z web stránky Internetovej klientskej aplikácie, ktorá komponent pre ZEP využíva.

Integritu inštalačných súborov aplikácie je možné overiť náhľadom na vlastnosti inštalačného programu (setup.exe alebo príslušného msi balíčka). Všetky inštalačné súbory musia byť podpísané certifikátom spoločnosti DITEC, a.s., ktorého vydavateľom je certifikačná autorita Comodo, a je na ne vyžiadaná časová pečiatka. To isté platí aj pre všetky knižnice (dll súbory), ktoré tvoria aplikáciu.

Na nasledujúcom obrázku je zobrazený náhľad na aktuálny podpisový certifikát spoločnosti DITEC, a.s.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| Certificate × | | | | |
|--|--|--|--|--|
| General Details Certification Path | | | | |
| Certificate Information | | | | |
| This certificate is intended for the following purpose(s): • Ensures software came from software publisher • Protects software from alteration after publication | | | | |
| * Refer to the certification authority's statement for details. | | | | |
| Issued to: DITEC, a.s. | | | | |
| Issued by: COMODO RSA Code Signing CA | | | | |
| Valid from 9.5.2016 to 10.5.2019 | | | | |
| Install Certificate Issuer Statement | | | | |
| ОК | | | | |

Okrem elektronického podpisu certifikátom spoločnosti DITEC, a.s. sú .Net assembly zabezpečené aj pomocou tzv. strong name. Pre príslušný počítač, na ktorom je aplikácia D.Signer/XAdES .NET nainštalovaná, resp. pre príslušnú klientsku aplikáciu musí byť vypnutý tzv. strong name bypass. Daná kontrola sa uplatňuje napr. pri spustení aplikácie D.Signer/XAdES .NET – aplikácia načíta len také plugin moduly, ktoré boli podpísané tým istým kľúčom ako hlavná aplikácia.⁴

5.1. Inštalácia z distribučného CD

Inštalácia samotnej aplikácie D.Signer/XAdES .NET sa vykoná spustením programu SETUP.EXE. Pre úspešnú inštaláciu musí mať používateľ v rámci operačného systému administrátorské privilégia. V novších verziách operačného

⁴ Toto neplatí pre knižnice tretích strán, ktoré môže aplikácia D.Signer/XAdES .NET využívať. Tieto by mali byť chránené príslušným certifikátom ich výrobcu.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

systému MS Windows je možné spustiť inštaláciu aplikácie D.Signer/XAdES .NET pod administrátorskými privilégiami z kontextového menu.

| | Open | |
|---|---------------------------|---|
| ۲ | Run as administrator | |
| | Add to Send To menu | |
| | Remove from Send To menu | |
| | Always Available Offline | |
| | Restore previous versions | |
| | Send To | × |
| | Cut | |
| | Сору | |
| | Paste | |
| | Create Shortcut | |
| | Delete | |
| | Rename | |
| | Properties | |

Pozor! Keďže pri inštalácii aplikácie D.Signer/XAdES .NET je potrebné zaregistrovať v rámci operačného systému Windows aj komponenty pre integráciu aplikácie D.Signer/XAdES .NET do web stránok internetových aplikácií, odporúčame pred spustením inštalačného programu zavrieť otvorené internetové prehliadače.

Po spustení inštalačného programu sa zobrazí úvodná obrazovka s výberom jazyka sprievodcu inštaláciou a zároveň jazyka aplikácie D.Signer/XAdES .NET.

| 🛃 🛛 D.Signe | r/XAdES .NET | | × |
|-------------|--|----------------------------|---|
| d | Vyberte si preferov Slovenský OK | ′aný jazyk: ✓ Zrušiť | |

Po zvolení jazyka sa zobrazí úvodná obrazovka sprievodcu inštaláciou aplikácie D.Signer/XAdES .NET.

Inštalácia

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |



V nasledujúcom kroku je potrebné potvrdiť licenčnú zmluvu pre knižnicu PDFNet SDK⁵, ktorá tvorí súčasť zásuvného modulu PDF Plugin aplikácie D.Signer/XAdES .NET.

⁵ PDF technology in D.Signer/XAdES .NET - PDF Plugin is powered by PDFNet SDK copyright © PDFTron[™] Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All rights reserved.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| 👸 D.Signer/XAdES .NE | T so zásuvnými modulmi 4.0.0.0 – i… 🗧 | × |
|---|---|--------|
| Licenčná zmluva konce Pozorne si prečítajte nask | ového používateľa edujúcu licenčnú zmluvu | |
| uzavretá podľa zá právach súvisiacich | Licenčná zmluva íkona č. 618/2003 Z. z. o autorských právach a s autorským právom v úplnom znení (ďalej le "autorský zákon") (ďalej len "zmluva") | n |
| Táto Zmluva je uzatv | vorená medzi spoločnosťou | |
| Obchodné meno: Sídlo: | DITEC, a.s. Plynárenská 7/C, 821 09 Bratislava | ~ |
| ✓ Súhlasím s podmienkami | i licenčnej zmluvy | |
| [| Tlačiť Späť Ďalej Z | 'rušiť |

V ďalšom kroku potvrďte tlačidlom Ďalej predvolený adresár, prípadne zvoľte iný adresár, do ktorého bude aplikácia D.Signer/XAdES .NET nainštalovaná.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| 😸 D.Signer/XAdES .NET so zásuvnými modulmi 4.0.0.0 – i 😑 🔍 🗙 |
|--|
| Cieľový priečinok Ak chcete program nainštalovať do predvoleného priečinka, kliknite na tlači |
| Inštalovať program D.Signer/XAdES .NET so zásuvnými modulmi 4.0.0.0 do priečinka: |
| C:\Program Files (x86)\Ditec\DSigner .NET\ Zmenit' |
| Späť Ďalej Zrušiť |

V ďalšom kroku potvrďte tlačidlom Inštalovať inštaláciu aplikácie D.Signer/XAdES .NET so zásuvnými modulmi (pluginmi) pre podpisovanie dátových objektov XML, PDF, TXT a PNG na váš počítač.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| 😼 D.Signer/XAdES .NET so zásuvnými modulmi 4.0.0.0 – i 🗕 🗆 🗙 |
|--|
| Pripravený na inštaláciu programu D.Signer/XAdES .NET so zás |
| Ak chcete spustiť inštaláciu, kliknite na tlačidlo Inštalovať. Ak chcete skontrolovať alebo zmeniť niektoré z nastavení inštalácie, kliknite na tlačidlo Späť. Kliknutím na tlačidlo Zrušiť ukončíte sprievodcu. |
| |
| Späť Inštalovať Zrušiť |

Kliknutím na tlačidlo Inštalovať sa spustí samotná inštalácia. Inštalačný program skopíruje požadované aplikačné súbory do špecifikovaného adresára a zabezpečí zaregistrovanie komponentov aplikácie D.Signer/XAdES .NET v rámci operačného systému Windows.

Používateľ je o priebehu inštalácie informovaný v okne inštalačného programu. V každom okamihu je možné inštaláciu aplikácie D.Signer/XAdES .NET prerušiť kliknutím na tlačidlo Zrušiť.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| 😸 D.Signer/XAdES .NET so zásuvnými modulmi 4.0.0.0 – i 😑 🔍 🗙 |
|---|
| Inštaluje sa program D.Signer/XAdES .NET so zásuvnými modulmi 4.0 |
| Počkajte, kým Sprievodca inštaláciou nainštaluje program D.Signer/XAdES .NET so zásuvnými modulmi 4.0.0.0. |
| Stav: Zapisujú sa hodnoty do systémovej databázy Registry |
| |
| |
| |
| |
| |
| Späť Ďalej Zrušiť |
| Späť Ďalej Zrušiť |

Po ukončení inštalácie kliknite na tlačidlo Dokončiť.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |



5.2. Inštalácia v rámci klientskej aplikácie

V prípade inštalácie aplikácie D.Signer/XAdES .NET v rámci inštalácie klientskej aplikácie (ktorá komponent pre zaručený elektronický podpis využíva a v rámci ktorej sa distribuuje), musí správne nainštalovanie a zaregistrovanie jednotlivých komponentov aplikácie D.Signer/XAdES .NET zabezpečiť výrobca klientskej aplikácie. Odporúčame, aby používateľ postupoval podľa inštalačnej príručky danej klientskej aplikácie.

5.3. Inštalácia z Internetu

V prípade použitia aplikácie D.Signer/XAdES .NET v rámci Internetovej aplikácie (webového portálu) doporučujeme, aby tvorca Internetovej aplikácie sprístupnil na stránkach svojej aplikácie aj inštalačné súbory jednotlivých komponentov D.Signer/XAdES .NET, najlepšie zabezpečené protokolom HTTPS. Používateľ si bude môcť takto inštalačné súbory bezpečne stiahnuť a spustiť na svojom PC.

Opäť je potrebné zabezpečiť, aby používateľ, ktorý inštaluje komponenty aplikácie D.Signer/XAdES .NET z Internetu mal počas inštalácie administrátorské práva. Odporúčame, aby používateľ postupoval podľa inštalačnej príručky príslušnej Internetovej aplikácie.

Inštalácia

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

6. Užívateľské nastavenia

Obrazovka s užívateľskými nastaveniami aplikácie D.Signer/XAdES .NET je prístupná z hlavného okna aplikácie D.Signer/XAdES .NET prostredníctvom tlačidla Nastavenia.

| 🧭 D.Signer/XAdES .NET 💦 – 🗆 🗙 |
|---|
| 😺 Dokument nie je podpísaný 📓 🖹 🔀 🔽 01. 04. 2016 21:41:07 🕂 🕅 🗶 🔘 |
| Pozor! Do ZEP sú zahmuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov. |
| Nový záznam Príloha záznamu |
| Nový záznam |
| ZÁPIS ZÁZNAMU A E2000-RFP3 |
| Čas od: 10:00 Čas do: 12:00 Klúč: RFP3 Zapísal: BLAŽIČEK Text: test |
| < |
| Zalomiť text Xml dáta Verifikačné dáta |
| Podpísať OK Storno |

6.1. Nastavenie jazyka aplikácie

V rámci nastavení aplikácie D.Signer/XAdES .NET môže používateľ zmeniť nastavenie jazyka aplikácie. Nastavenie nového jazyka sa aplikuje pri ďalšom spustení aplikácie D.Signer/XAdES .NET.

| 🧭 Nastavenia 🗙 | | |
|---|-----|--------|
| Lokalizácia Jazyk aplikácie: slovenč | ina | • |
| | ОК | Storno |

Užívateľské nastavenia

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

7. Vytvorenie ZEP používateľom

7.1. Načítanie vstupných parametrov

Po zavolaní funkcie pre vytvorenie elektronického podpisu, aplikácia D.Signer/XAdES .NET vykoná validáciu vstupných parametrov (teda jednotlivých podpisovaných častí *multipart* dokumentu) a zobrazí hlavné dialógové okno aplikácie. Spracovanie vstupných parametrov, najmä rozsiahlych dokumentov, môže vyžadovať istý čas, počas ktorého je zobrazený tzv. *splash screen*.



7.2. Zobrazenie podpisovaných dát

Pokiaľ všetky kontroly vstupných parametrov prebehli úspešne, na jednotlivých záložkách hlavného okna sú zobrazené časti podpisovaného *multipart* dokumentu. Používateľ má možnosť prezrieť všetky podpisované dátové objekty a ďalšie parametre podpisu.

Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| đ | D.Signer/XAdES .NET – 🗆 | × |
|---|---|----|
| 🗼 Dokument nie je podpísaný | 🔊 🖹 🔀 🔽 01. 04. 2016 21:41:07 🚔 🙆 🔀 | 0 |
| Pozor! Do ZEP sú zahmuté všetky z Vzhľadom k tomu, že vytvorením Z záujme, aby sa dôkladne oboznámil Nový záznam Príloha záznamu | zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. EP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho s obsahom všetkých zobrazených dátových objektov. | -1 |
| Nový zaznam ZÁPIS ZÁZNAMU E2000-RFP3 Čas od: 10:00 Čas do: 12:00 Klúč: RFP3 Zapísal: BLAŽIČEK Text: test | ^ | - |
| < | > | |
| Zalomiť text | Xml dáta Verifikačné dáta | |
| | Podpísať OK Storno | |

Pokiaľ sa vyskytli pri kontrole vstupných parametrov chyby, aplikácia D.Signer/XAdES .NET zobrazí chybovú správu.

| e | Chyba |
|---|------------------------|
| 8 | Neplatné vstupné dáta. |
| | |

V takomto prípade sa tiež zobrazí hlavné okno aplikácie D.Signer/XAdES .NET, ale nebude možné uskutočniť vytvorenie podpisu (tlačidlo Podpísať bude neprístupné).

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| D.Signer/XAdES .NET – □ × | | |
|---|--|--|
| 😲 Dokument nie je podpísaný 🝶 📄 💥 🗹 01. 04. 2016 22:02:57 芸 🙆 🗶 🛛 🧕 | | |
| Pozor! Do ZEP sú zahmuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov. | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Podpísať OK Storno | | |

V rámci hlavného okna aplikcácie D.Signer/XAdES .NET je tiež zobrazený stav podpisovaného dokumentu, ktorý môže nadobúdať nasledujúce hodnoty:

- Dokument nie je podpísaný
- Dokument bol podpísaný

V závislosti od stavu dokumentu sú jednotlivé tlačidlá hlavného okna aplikácie D.Signer/XAdES .NET prístupné alebo neprístupné.

Aplikácia D.Signer/XAdES .NET slúži na vytváranie (zaručeného) elektronického podpisu nad množinou rôznych formátov dokumentov, resp. typov dát (XML dokumenty, PDF dokumenty atď.), prípadne nad ľubovoľnou kombináciou podporovaných formátov dát, ktoré spolu vytvárajú tzv. *multipart* dokument. Pre jednotlivé požadované formáty dokumentov musí mať používateľ nainštalované príslušné plugin moduly aplikácie D.Signer/XAdES .NET. Informácia o nainštalovaných plugin moduloch je používateľovi prístupná prostredníctvom tlačidla "O aplikácii" (pravý horný roh okna aplikácie D.Signer/XAdES .NET).

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| | O aplikácii | × |
|---|---|-------------|
| Názov: D.: Verzia: 4.0 Autor: Dit | Signer/XAdES .NET).0.0 tec, a.s. | |
| Zoznam aktívnych plugir | iov: | |
| Ditec.Zep.DSigXades.F Ditec.Zep.DSigXades.F Ditec.Zep.DSigXades.F Ditec.Zep.DSigXades.F Ditec.Zep.DSigXades.F | Plugins.PdfObject, 4.0.0.0 Plugins.PngObject, 4.0.0.0 Plugins.TxtObject, 4.0.0.0 Plugins.XmlObject, 4.0.0.0 | |
| PDF technology in D.Sig PDFNet SDK copyright [@] distributed by DITEC a.s | ner/XAdES .NET - PDF Plugin is powere PDFTron™ Systems Inc., 2001-2014, a . under license. All rights reserved. | ed by nd |
| | Zav | rrieť |

7.2.1. Zobrazenie dokumentov

Zobrazenie dokumentov je realizované v rámci aplikácie D.Signer/XAdES .NET pomocou príslušného pluginu pre daný typ dát, ktorý poskytuje aplikácii D.Signer/XAdES .NET funkcie pre vizualizáciu dát daného typu. Jednotlivé podpisované dátové objekty (resp. dokumenty) sú zobrazené na samostatných záložkách, ktorých názov bližšie určuje obsah príslušného dokumentu. Používateľ má takto možnosť pred vytvorením elektronického podpisu prezrieť obsah všetkých podpisovaných dokumentov.

Na nasledujúcom obrázku je príklad zobrazenia XML dokumentu v HTML vizualizácii v rámci aplikácie D.Signer/XAdES .NET.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| e e | D.Signer/XAdES .N | iet – | □ × |
|---|--|--|-----------------------|
| 🔃 Dokument nie je podpísaný 🛛 🔒 | 1. 04. 2016 2 | 2:28:54 🕂 🙆 🔀 | 0 |
| Pozor! Do ZEP sú zahmuté všetky zobrazo Vzhľadom k tomu, že vytvorením ZEP použ záujme, aby sa dôkladne oboznámil s obsah | vané dátové objekty (dokun ívateľ vyjadruje svoj súhlas nom všetkých zobrazených (| nenty) a parametre elektronického pod s obsahom jednotlivých dokumentov dátových objektov. | dpisu. , je v jeho |
| Informácia o aktu | | | |
| Informácia o aktuálnom stave doručova | nia | | |
| Informácia o aktuálnom s | tave doručovania | | ^ |
| MessageID: | | | |
| 25FC925E-A3C6-4A47-9A | 53-507410499519 | | |
| Stav doručovania | | | |
| Identifikátor stavu: | 0 | | |
| Stav: | OK | | |
| Čas stavu: | 27.01.2014 | | |
| | | | |
| | | Xml dáta Verifikač | né dáta |
| | [| Podpísať OK | Storno |

7.3. Nastavenie dátumu a času vytvorenia podpisu

Aplikácia D.Signer/XAdES .NET umožňuje používateľovi v prípade potreby nastaviť pomocou ovládacích prvkov, ktoré sú umiestnené v hornej lište okna aplikácie, dátum a čas vytvorenia podpisu. Používateľ môže takto deklarovať vytvorenie elektronického podpisu v špecifikovanom dátume a čase, pričom tento deklarovaný dátum a čas vytvorenia podpisu je zahrnutý do podpisovaných atribútov vytváraného elektronického podpisu a následne vyhodnocovaný na strane overovateľa. Je teda potrebné, aby používateľ pri vytváraní elektronického podpisu nastavil taký dátum a čas vytvorenia podpisu, ktorý neznemožní spracovanie vytvoreného elektronického podpisu na strane overovateľa.

Aplikácia umožňuje používateľovi deklarovať ako čas vytvorenia podpisu:

- buď aktuálny systémový dátum a čas, ak je zvolené v zaškrtávacom políčku použitie systémového dátumu a času,
- alebo manuálne nastaviť deklarovaný dátum a čas vytvorenia podpisu, ak je v zaškrtávacom políčku použitie systémového dátumu a času odznačené.

Vytvorenie ZEP používateľom

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

V prvom prípade nie je možné manuálne nastaviť deklarovaný dátum a čas vytvorenia podpisu. Používateľ môže iba prostredníctvom príslušného tlačidla nastaviť systémový dátum a čas (ak má na to príslušné oprávnenia v rámci systému Windows).

| e e | D.Signer/XAdES .NET | - 🗆 🗙 |
|--|--|-------------------------------------|
| 🤃 Dokument nie je podpísaný 🔓 |) 📄 🗙 ए 01. 04. 2016 21:41:07 🕂 🙆 🌿 | 0 |
| Pozor! Do ZEP sú zahmuté všetky zob Vzhľadom k tomu, že vytvorením ZEP záujme, aby sa dôkladne oboznámil s o | azované dátové objekty (dokumenty) a parametre elektronick používateľ vyjadruje svoj súhlas s obsahom jednotlivých doku bsahom všetkých zobrazených dátových objektov. | tého podpisu. imentov, je v jeho |
| Nový záznam Príloha záznamu | | |
| Nový záznam | | |
| ZÁPIS ZÁZNAMU E2000-RFP3 | | ^ |
| Čas od: 10:00 Čas do: 12:00 Klúč: RFP3 Zapísal: BLAŽÍČEK Text: test | | |
| | | ~ |
| < | | > |
| 🔲 Zalomiť text | Xml dáta | Verifikačné dáta |
| | Podpísať OK | Storno |

V druhom prípade sa používateľovi sprístupní deklarovaný dátum a čas vytvorenia podpisu na editovanie.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| D.Signer/XAdES .NET – □ × | |
|---|---|
| 🗼 Dokument nie je podpísaný 📓 🖹 🔪 🚺 01. 04. 2016 21:52:11 🔿 🗶 🎯 | ٥ |
| Pozor! Do ZEP sú zahmuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov. | |
| Nový záznam Príloha záznamu | |
| Nový záznam | |
| ZÁPIS ZÁZNAMU E2000-RFP3 Čas od: 10:00 Čas do: 12:00 Klúč: RFP3 Zapísal: BLAŽIČEK Text: test | |
| < | |
| Zalomiť text Xml dáta Verifikačné dáta | |
| Podpísať OK Storno | |

Pozor! Pri vytváraní elektronického podpisu odporúčame použiť správne nastavený aktuálny systémový dátum a čas.

V prípade, že v rámci danej klientskej aplikácie nie je potrebné do parametrov podpisu zahrnúť aj používateľom deklarovaný dátum a čas vytvorenia podpisu, nemusia byť príslušné ovládacie prvky pre jeho nastavenie k dispozícii. Ich zobrazenie závisí na zavolaní príslušných funkcií aplikačného rozhrania aplikácie D.Signer/XAdES .NET z klientskej aplikácie.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| D.Signer/XAdES .NET – □ × | |
|---|---|
| 🗼 Dokument nie je podpísaný 📓 🖹 🗙 🔀 | 0 |
| Pozor! Do ZEP sú zahmuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov. | |
| Nový záznam | |
| Nový záznam | |
| ZAPIS ZAZNAMU E2000-RFP3 Čas od: 10:00 Čas do: 12:00 Kľúč: RFP3 Zapísal: BLAŽIČEK Text: test | |
| | |
| →]< | |
| Zalomiť text Xml dáta Verifikačné dáta | |
| Podpísať OK Storno | |

7.4. Podpísanie dokumentu

V prípade úspešného načítania všetkých častí podpisovaného dokumentu je prístupné tlačidlo Podpísať, ktoré aktivuje proces vytvorenia elektronického podpisu dokumentu. Prvým krokom procesu vytvorenia podpisu je výber certifikátu, ktorým bude daný dokument podpísaný. Na nasledujúcom obrázku je znázornený dialóg pre výber certifikátu podpisovateľa.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| đ | Výber certifikátu | × | | |
|---|---|--|--|--|
| Vyberte certifikát, ktorý chcete použiť. Pr certifikát, vydaný akreditovanou certifikad | Vyberte certifikát, ktorý chcete použiť. Pre vytvorenie zaručeného elektronického podpisu musí byť použitý kvalifikovaný certifikát, vydaný akreditovanou certifikačnou autoritou. | | | |
| Ak príslušný právny úkon vyžaduje autori certifikát s príslušným oprávnením pre da k dispozícii pre vytvorenie elektronického | Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, vyberte mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov. | | | |
| Overte platnosť vybraného podpisového (aktuálne platný zoznam zrušených certiři elektronického podpisu! | certifikátu na základe relevantných verejne d kátov). Použitie neplatného certifikátu má za | ostupných informácií o revokácii následok vytvorenie neplatného | | |
| Potvrden ím výberu certifikátu podpíšete | dokument! | | | |
| Filtrovať zoznam certifikátov: SK QC 🔹 | | | | |
| Vydaný pre | Vydavateľ | Platný do | | |
| | "I.CA - Qualified Certification Authority, | 12.1.2017 16:24:37 | | |
| | | | | |
| | Zobraziť certifikát | OK Storno | | |

V rámci zoznamu osobných certifikátov na danom PC sú zobrazené položky:

- meno subjektu, pre ktorý bol certifikát vydaný,
- meno vydavateľa certifikátu,
- dátum konca platnosti certifikátu.

Detaily zvoleného certifikátu je možné prezrieť kliknutím na tlačidlo Zobraziť certifikát.

Integrátor aplikácie D.Signer/XAdES .NET môže spolu s aplikáciou distribuovať tiež nastavenia filtra pre zobrazenie len určitých certifikátov, ktoré spĺňajú definované pravidlá. V uvedenom dialógu pre výber certifikátu podpisovateľa sú napríklad zobrazené len kvalifikované certifikáty vydané v súlade so slovenskou legislatívou.

Pre vytvorenie zaručeného elektronického podpisu musí podpisovateľ zvoliť zo svojho personálneho úložiska certifikátov kvalifikovaný certifikát, ktorý bol vydaný akreditovanou certifikačnou autoritou. Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, používateľ musí zvoliť mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Pre vytvorenie obyčajného elektronického podpisu nie je potrebné použiť kvalifikovaný certifikát vydaný akreditovanou certifikačnou autoritou.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov v okne pre výber certifikátu v aplikácii D.Signer/XADES .NET.

| e 🖉 | Výber certifikátu | × | | |
|--|---|--|--|--|
| Vyberte certifikát, ktorý chcete certifikát, vydaný akreditovano | Vyberte certifikát, ktorý chcete použiť. Pre vytvorenie zaručeného elektronického podpisu musí byť použitý kvalifikovaný certifikát, vydaný akreditovanou certifikačnou autoritou. | | | |
| Ak príslušný právny úkon vyža certifikát s príslušným oprávne k dispozícii pre vytvorenie eleł | Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, vyberte mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov. | | | |
| Overte platnosť vybraného pod (aktuálne platný zoznam zrušen elektronického podpisu! | lpisového certifikátu na základe relevantný rých certifikátov). Použitie neplatného certi | ich verejne dostupných informácií o revokácii fikátu má za následok vytvorenie neplatného | | |
| Potvrden ím výberu certifikátu | oodp íšete dokument! | | | |
| Filtrovať zoznam certifikáto | SK QC 💽 | > | | |
| Vydaný pre | ∕ Vydavateľ | Platný do | | |
| | "I.CA - Qualified Certification | Authority, 12.1.2017 16:24:37 | | |
| | | | | |
| | | | | |
| | | | | |
| | Zobra | ziť certifikát OK Storno | | |

Po zvolení certifikátu a potvrdení výberu tlačidlom OK sa vykoná proces vytvorenia elektronického podpisu. Aplikácia D.Signer/XAdES .NET vytvorí reprezentáciu podpisovaných dát a parametrov podpisu – digitálny odtlačok. Pomocou rozhrania MS CryptoAPI a príslušného SSCD zariadenia, na ktorom je uložený privátny kľúč patriaci k zvolenému podpisovému certifikátu, vytvorí hodnotu elektronického podpisu. Sprístupnenie privátneho kľúča na SSCD zariadení môže vyžadovať autentifikáciu používateľa – zadanie PINu.⁷

⁷ Nastavenia SSCD (napr. timeout pre PIN, dĺžka PIN apod.) sú v správe používateľa SSCD zariadenia. Aplikácia D.Signer/XAdES .NET neumožňuje meniť tieto nastavenia.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

| SecureStoreCSP - zadať PIN | × |
|--|---|
| K uskutočneniu operácie je potrebné zadať PIN. Operácia : Podpis dát kľúčom umiestneným na karte | |
| PIN: **** | |
| C Zapamätať PIN | |
| OK Storno | |

Aplikácia D.Signer/XAdES .NET následne vytvorí a sformátuje výstupný podpísaný dokument v súlade s profilom XAdES_ZEP, resp. XAdES_ZEPbp. V prípade chyby v rámci procesu vytvorenia podpisu sa zobrazí príslušné chybové hlásenie. Ak sa dokument podarilo podpísať, v hlavnom okne sa zmení stav dokumentu a niektorých tlačidiel (sprístupnia sa tlačidlá tých funkcií, ktoré je možné vykonať len nad podpísaným dokumentom).

| 1 | D.Signer/XAdES .NET | - 🗆 🗙 |
|---|---|-----------------------------------|
| 🔃 Dokument bol podpísaný 🔬 🚦 | ×× | 0 |
| Pozor! Do ZEP sú zahmuté všetky zobra Vzhľadom k tomu, že vytvorením ZEP p záujme, aby sa dôkladne oboznámil s ob | ované dátové objekty (dokumenty) a parametre elektronicky užívateľ vyjadruje svoj súhlas s obsahom jednotlivých doku ahom všetkých zobrazených dátových objektov. | ého podpisu. mentov, je v jeho |
| Nový záznam | | |
| Nový záznam | | |
| ZÁPIS ZÁZNAMU E2000-RFP3 Čas od: 10:00 Čas do: 12:00 Kľúč: RFP3 Zapísal: BLAŽÍČEK Text: test | | |
| < | | > |
| 🗖 Zalomiť text | Xml dáta Ve | erifikačné dáta |
| | Podpísať OK | Storno |

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

Po úspešnom vytvorení elektronického podpisu je podpísaný dokument odovzdaný klientskej aplikácii až po kliknutí na tlačidlo OK.

7.5. Zobrazenie parametrov podpisu

Používateľ, resp. podpisovateľ si môže pred alebo po podpísaní dokumentu zobraziť parametre podpisu (ikona s ozubeným kolieskom v hornej časti). V prípade ich zobrazenia pred vytvorením podpisu, resp. po vymazaní podpisu (tlačidlo Zmazať podpis – s ikonou s červeným krížikom v hornej časti okna), zobrazené informácie nebudú úplné, pretože niektoré z nich sú závislé na výbere podpisového certifikátu.

Na nasledujúcom obrázku je zobrazené dialógové okno s parametrami podpisu pred podpísaním dokumentu.

| e 🖉 | Parametre podpisu | × | | | |
|---|---|---|--|--|--|
| Špec Id Id | ifikácia formátu podpisu: http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1 lentifikátor algoritmu transformácie podpisovaných informácií: http://www.w3.org/TR/2001/REC-xml-c14n-20010315 lentifikátor algoritmu digitálneho podpisu: (informácia bude prístupná po podpísaní dokumentu) | ^ | | | |
| Podp Id Id PI PI Pr NBÚ platn: http:/ | Podpisová politika: Identifikátor podpisovej politiky: um:oid:1.3.158.36061701.1.2.1 Identifikátor algoritmu digitálneho odtlačku: http://www.w3.org/2000/09/xmldsig#sha1 Hodnota digitálneho odtlačku: Gd0+i5ReLU90YBkRjGbDcmQ30IM= Platnosť od: 03. 12. 2013 01:00:00 Platnosť do: 03. 12. 2017 01:00:00 Povinnosť uvádzať dátum a čas vytvorenia podpisu: Áno Pre vytvorenie ZEP musí byť aplikácia použitá len v súlade s platnou podpisovou politikou pre ZEP, ktorá bola schválená NBÚ SR. Používateľ je pred vytvorením podpisu povinný presvedčiť sa, že podpisová politika, ktorú aplikácia používa, je stále platná a nebola zo strany vydavateľa predčasne zrušená. URL pre overenie platnosti podpisovej politiky: http://www.nbusr.sk/sk/elektronicky-podpis/podpisove-politiky/index.html | | | | |
| Hodn Ident Vj Se Ni | nota digitálneho podpisu: (informácia bude prístupná po podpísaní dokumentu) ifikácia certifikátu podpisovateľa: ydavateľ: (informácia bude prístupná po podpísaní dokumentu) ériové číslo: (informácia bude prístupná po podpísaní dokumentu) ázov subjektu: (informácia bude prístupná po podpísaní dokumentu) | | | | |
| Dátu | m a čas vytvorenia podpisu: (informácia bude prístupná po podpísaní dokumentu) Uložiť Zavrieť | ř | | | |
| | | | | | |

V prípade, že podpis je z nejakého dôvodu potrebné zrušiť, tak je toto umožnené kliknutím na ikonu s červeným krížikom v hornej časti – Zrušiť vytvorený podpis a uviesť tak aplikáciu do východzieho stavu.

| Projekt | GOV_ZEP | | A3019_002 |
|------------|------------------------|--------|-----------|
| Dokument | Používateľská príručka | | |
| Referencia | GOV_ZEP.200 | Verzia | 1 |

8. Trademarks

PDF technology in D.Signer/XAdES .NET - PDF Plugin is powered by PDFNet SDK copyright © PDFTron[™] Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All rights reserved.



 $\mathsf{Microsoft} \circledast$.NET is software for connecting people, information, systems, and devices.