DITEC
Data Information Technology & Expert Consulting

Používateľská príručka
D.Signer/XAdES .NET, v3.0

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Podnázov	D.Signer/XAdES .NET, v3.0		
Ref. číslo	GOV_ZEP.160	Verzia	3

Vypracoval	Vittek Róbert	Podpis	Dátum 15.2.2016
Preveril		Podpis	Dátum
Schválil		Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 13.10.2005

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.160	Verzia	3

Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia

Pripomienkovanie a kontrola

Autor	Stanovisko	Dátum	Verzia

Rozdeľovník

	Priezvisko Meno	Firma, Funkcia
Originál		
Kópia		
Kópia		
Kópia		

Obsah

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.

2. 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.

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.

Aplikácia D.Signer/XADES .NET vytvára ZEP v súlade so schválenými formátmi pre zaručený elektronický podpis XAdES_ZEP, 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) a XAdES_ZEP, v2.0 (http://www.ditec.sk/ep/signature_formats/xades_zep/v2.0). Aplikácia D.Signer/XAdES .NET vytvára typ podpisu XAdES_ZEP-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.

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.

3. Systémové požiadavky

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

- OS – MS Windows 2003 Server, 2008 Server, 2012 Server, Vista, Windows 7, Windows 8,
- Platforma – .Net framework, verzia 2.0-3.5,
- certifikované SSCD zariadenie pre generovanie kľúčových párov a vytváranie elektronického podpisu,
- web prehliadač – MS Internet Explorer, v6.0 a vyššia[1] alebo prehliadač s podporou NP API: Firefox v3.x, Google Chrome v12.x – v44, Opera v10.x, Safari 5.1 alebo viac.

Pri vytváraní zaručeného elektronického podpisu pomocou aplikácie D.Signer/XAdES .NET sa vyžaduje použitie certifikovaného zariadenia 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. 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 2.0-3.5. Požiadavky aplikácie na voľný priestor na disku sú nasledujúce:

Komponent	Veľkosť
D.Signer/XAdES .NET	1,73 MB
D.Signer/XAdES .NET – XML Plugin	413 KB
D.Signer/XAdES .NET – PDF Plugin	16,7 MB
D.Signer/XAdES .NET – TXT Plugin	168 KB
D.Signer/XAdES .NET – PNG Plugin	190 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.

[1] D.Signer/XAdES .NET 64bit nespolupracuje s MS Internet Explorer 64bit v10.x a vyššia.

Komponent	Veľkosť
D.Signer/XAdES .NET x86	18,8 MB
D.Signer/XAdES .NET x64	22,1 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.

4. 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,
2) 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.

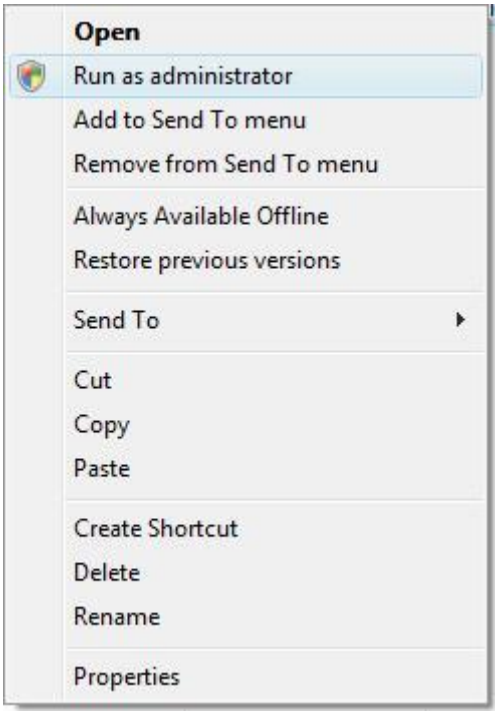
Integritu inštalačných súborov aplikácie je možné overiť náhľadom na vlastnosti inštalačného programu (setup.exe alebo príslušného msi balíčka). Všetky inštalačné súbory musia byť podpísané certifikátom spoločnosti Ditec, a.s. a je na ne vyžiadaná časová pečiatka. To isté platí aj pre všetky knižnice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

Okrem elektronického podpisu certifikátom spoločnosti Ditec, a.s. sú .Net assembly zabezpečené aj pomocou tzv. strong name. 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.[2]

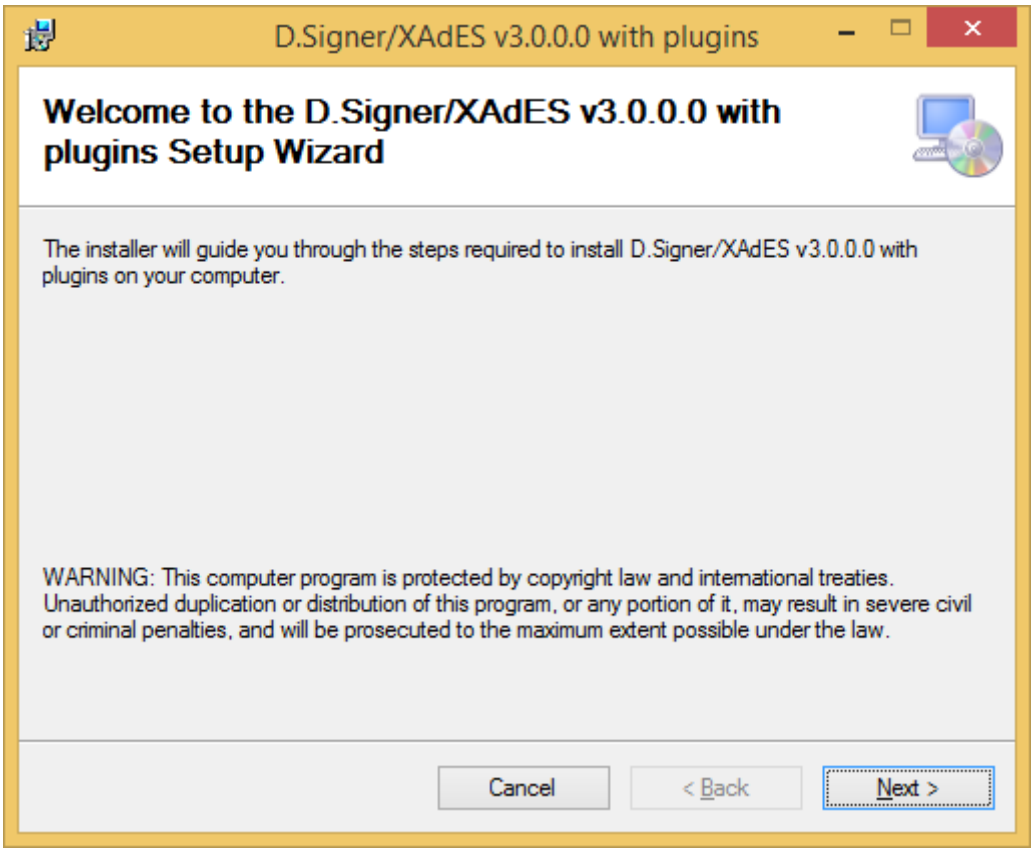
4.1. Inštalácia z distribučného CD

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

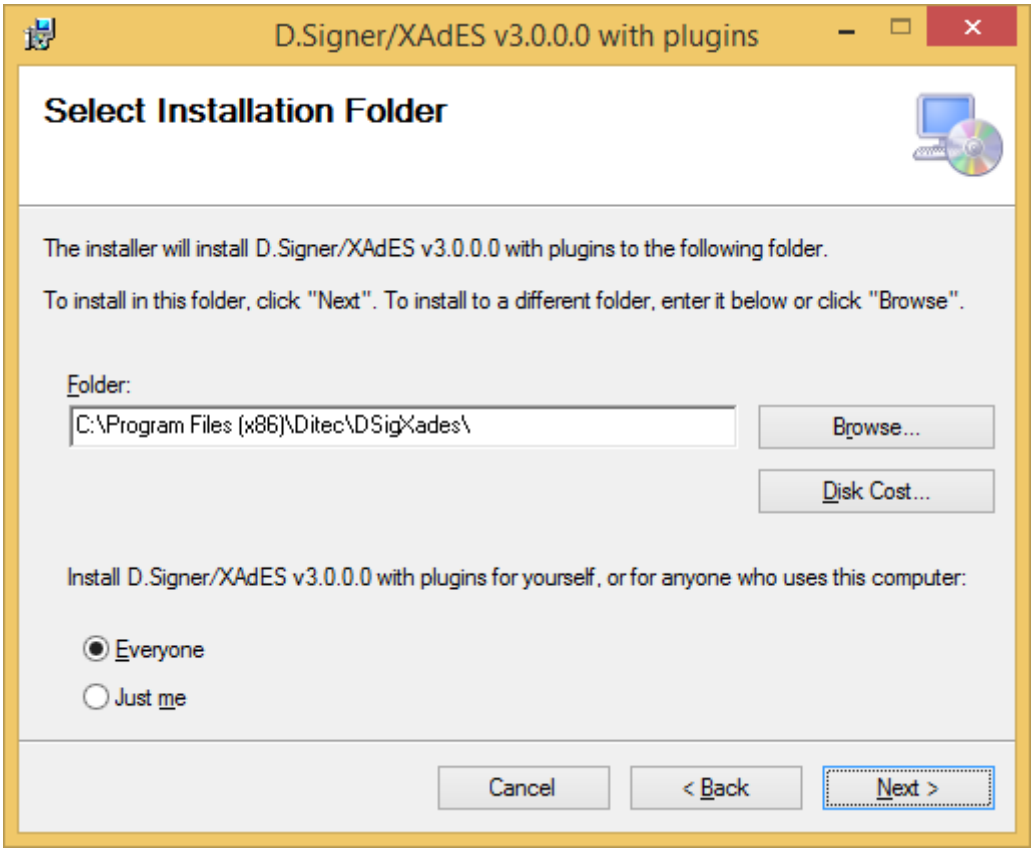
[2] Toto neplatí pre knižnice tretích strán, ktoré môže aplikácia D.Signer/XAdES .NET využívať. Tieto by mali byť chránené príslušným certifikátom ich výrobcu.



Po spustení inštalačného programu sa zobrazí úvodná obrazovka.

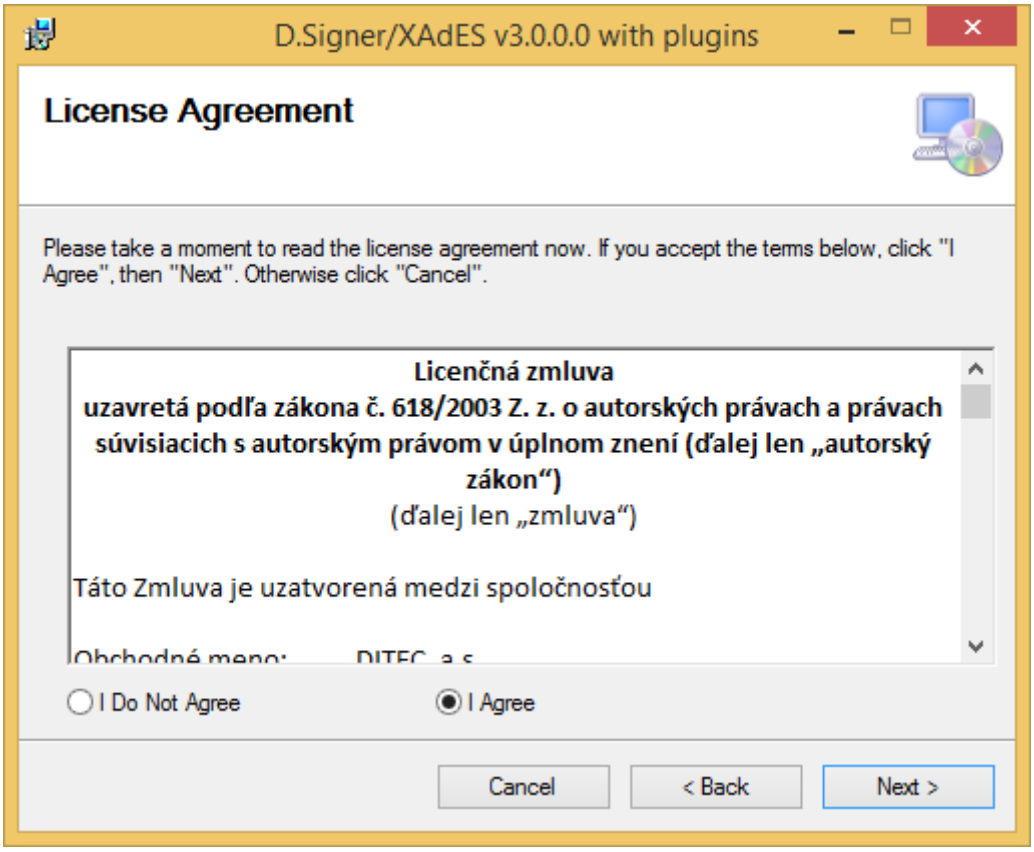


V nasledujúcom kroku potvrďte tlačidlom Next, prípadne zvoľte adresár, do ktorého bude aplikácia D.Signer/XAdES .NET nainštalovaná a špecifikujte, kto bude mať právo aplikáciu na počítači používať.

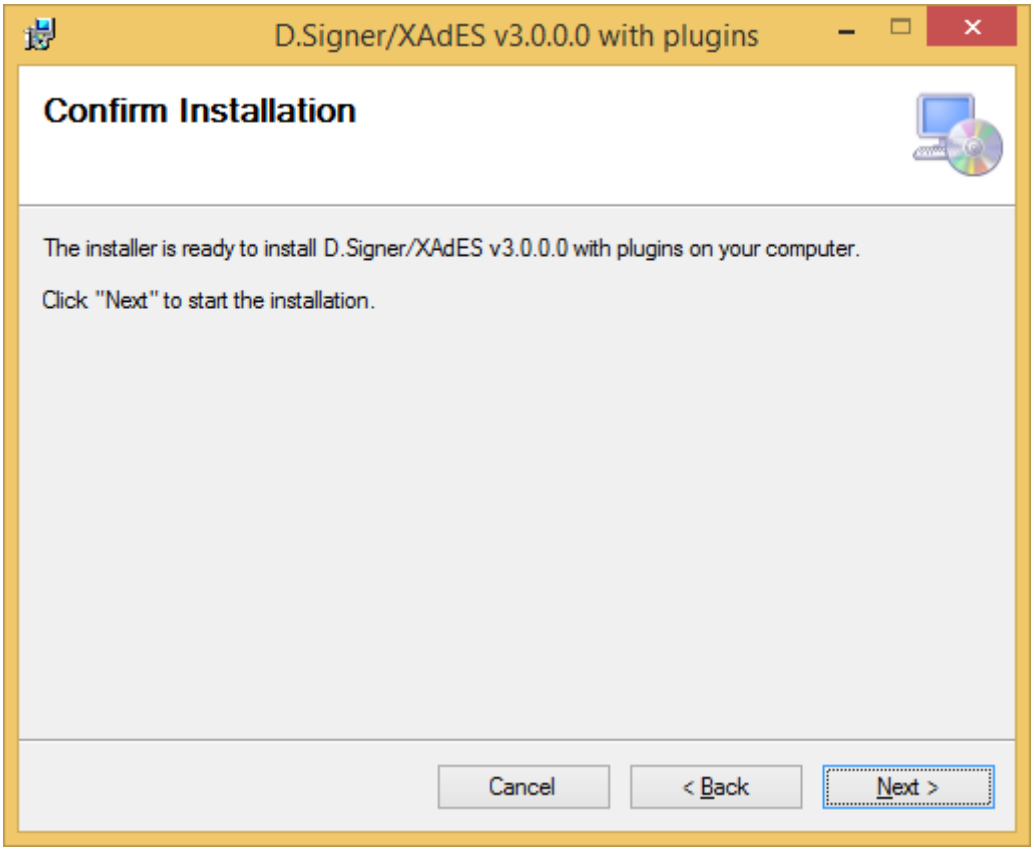


V nasledujúcom kroku je potrebné potvrdiť licenčnú zmluvu pre knižnicu PDFNet SDK[3], ktorá tvorí súčasť PDF Pluginu aplikácie D.Signer/XAdES .NET.

[3] PDF technology in D.Signer/XAdES .NET - PDF Plugin is powered by PDFNet SDK copyright © PDFTron™ Systems Inc., 2001-2014, and distributed by DITEC a.s. under license. All rights reserved.

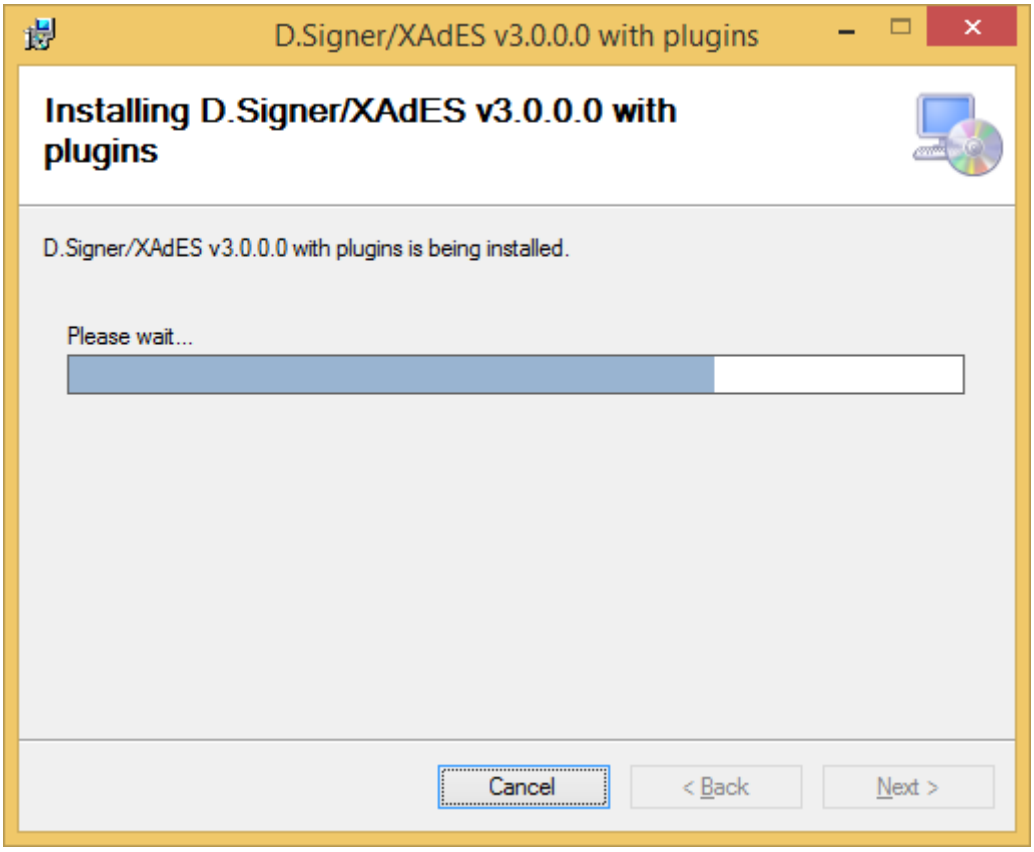


V ďalšom kroku potvrďte inštaláciu aplikácie D.Signer/XAdES .NET s pluginmi pre podpisovanie dátových objektov XML, PDF, TXT a PNG na váš počítač.

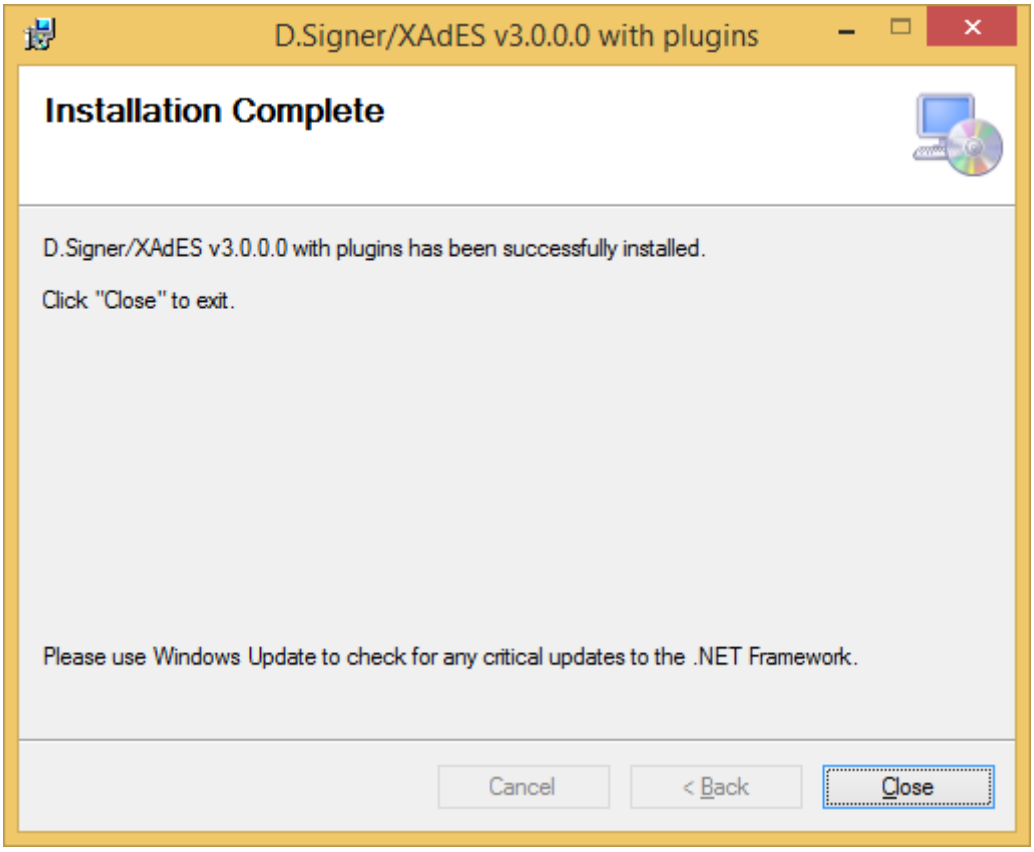


Kliknutím na tlačidlo Next sa spustí samotná inštalácia. Inštalačný program skopíruje požadované aplikačné súbory do špecifikovaného adresára a zabezpečí zaregistrovanie komponentov aplikácie D.Signer/XAdES .NET v rámci operačného systému Windows.

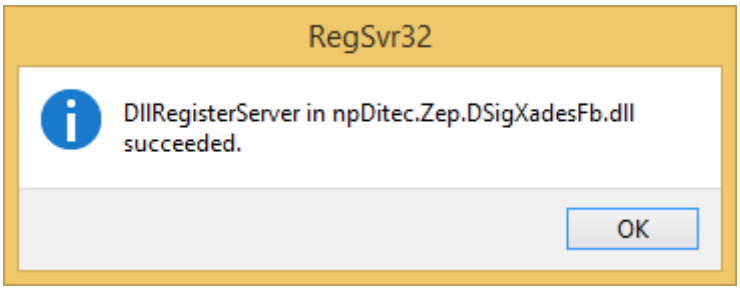
Používateľ je o priebehu inštalácie informovaný v okne inštalačného programu. V každom okamihu je možné inštaláciu aplikácie D.Signer/XAdES .NET prerušiť kliknutím na tlačidlo Cancel (Zrušiť).



Po ukončení inštalácie kliknite na tlačidlo Close (Zavrieť).



V prípade, že ste inštalovali D.Signer/XAdES .NET x64 (teda D.Signer/XAdES .NET určený pre integráciu so 64-bitovými aplikáciami a webovými prehliadačmi), je potrebné ešte manuálne zaregistrovať 64-bitový NP API wrapper pre aplikáciu spustením súboru `C:\Program Files\Ditec\DsigXades\register.vbs`. Systém vypíše nasledujúcu správu o úspešnom zaregistrovaní knižnice NP API wrappera.



4.2. 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.

4.3. Inštalácia z Internetu

V prípade použitia aplikácie D.Signer/XAdES .NET v rámci Internetovej aplikácie doporučujeme, aby tvorca klientskej 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 klientskej Internetovej aplikácie.

5. Vytvorenie ZEP používateľom

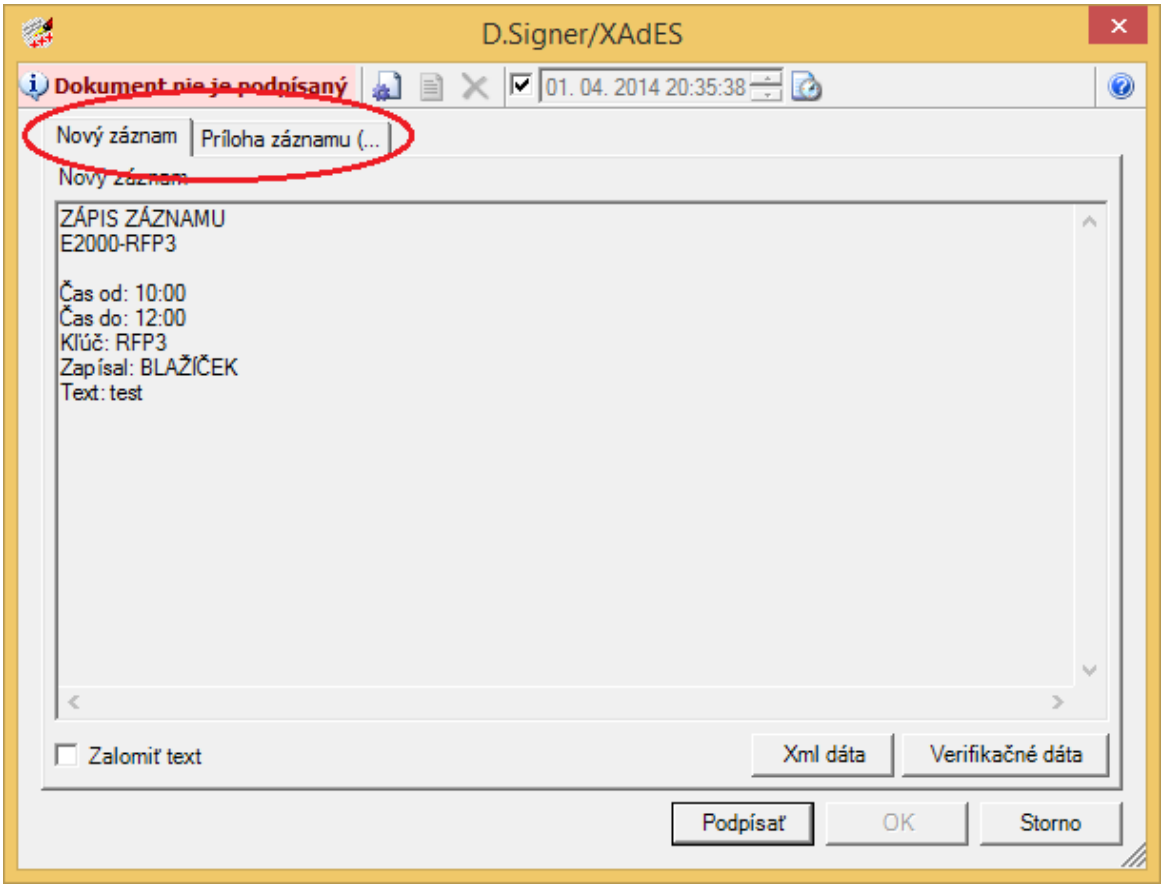
5.1. Načítanie vstupných parametrov

Po zavolaní metódy Sign 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*.

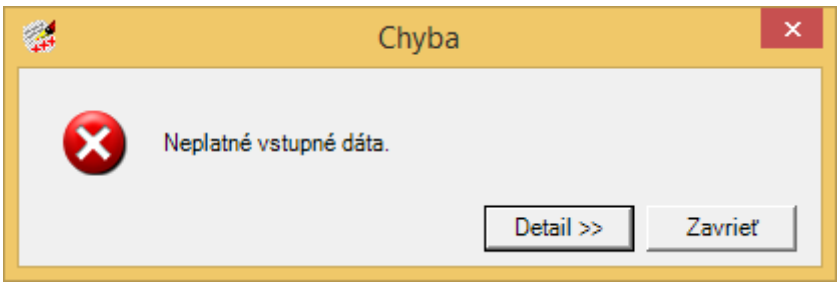
5.2. Zobrazenie podpisovaných dát

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.

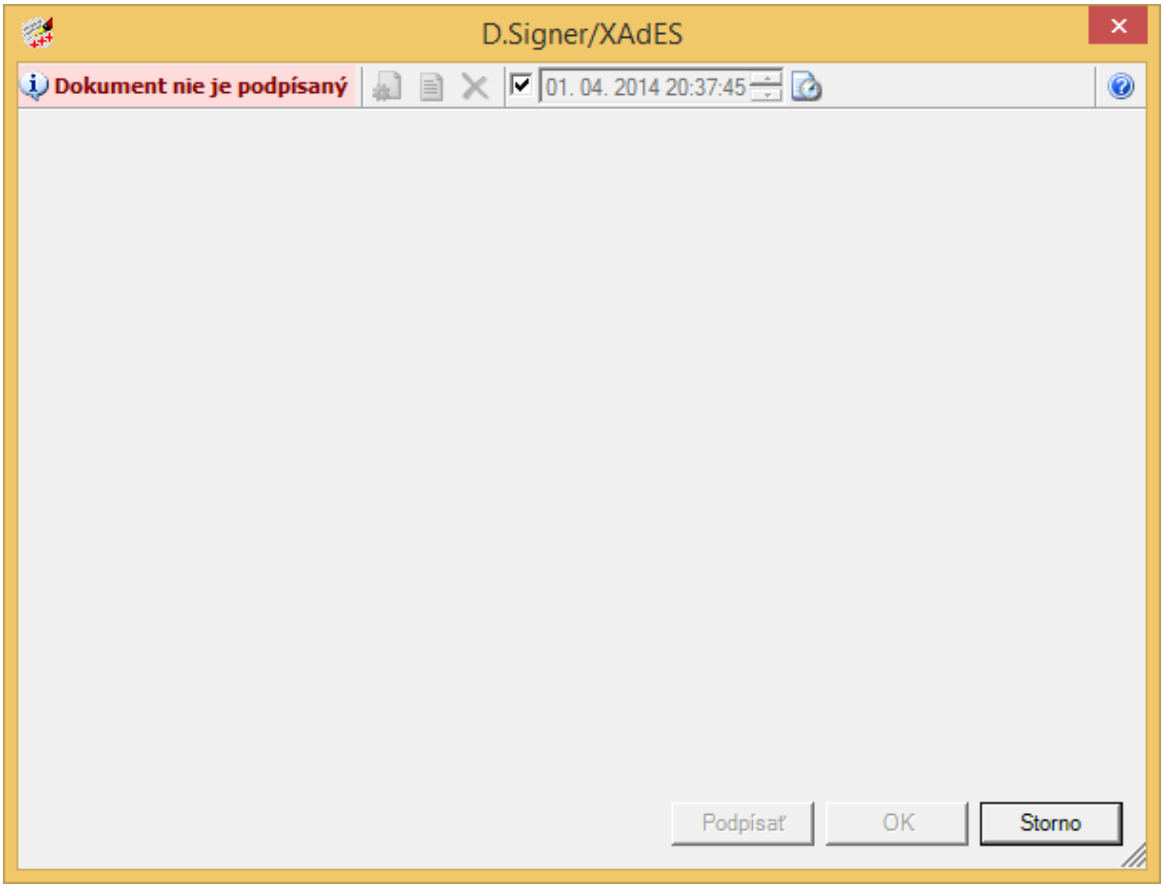
Pozor! Do ZEP sú zahrnuté všetky zobrazované dátové objekty (dokumenty) a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením ZEP používateľ vyjadruje svoj súhlas s obsahom jednotlivých dokumentov, je v jeho záujme, aby sa dôkladne oboznámil s obsahom všetkých zobrazených dátových objektov.



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



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



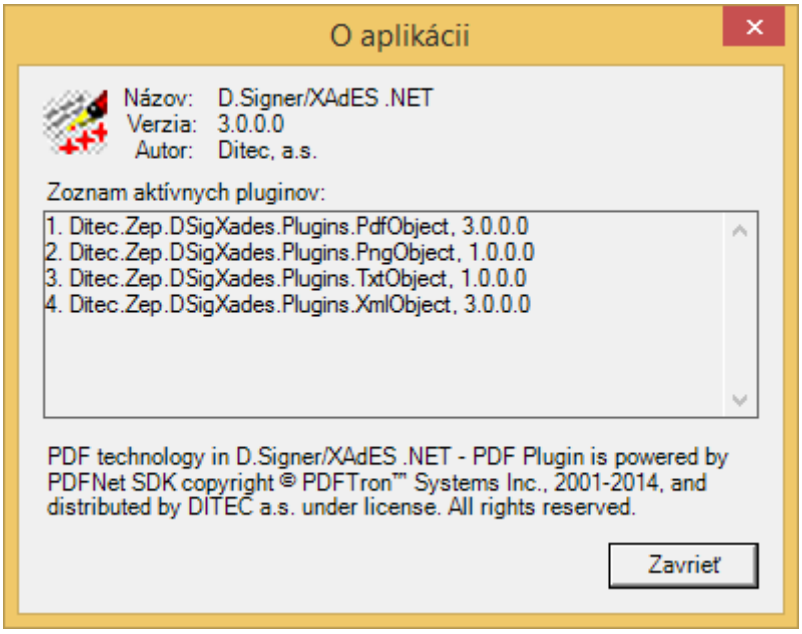
V rámci hlavného okna aplikácie D.Signer/XAdES .NET je tiež zobrazený stav podpisovaného dokumentu, ktorý môže nadobúdať nasledujúce hodnoty:

- 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.

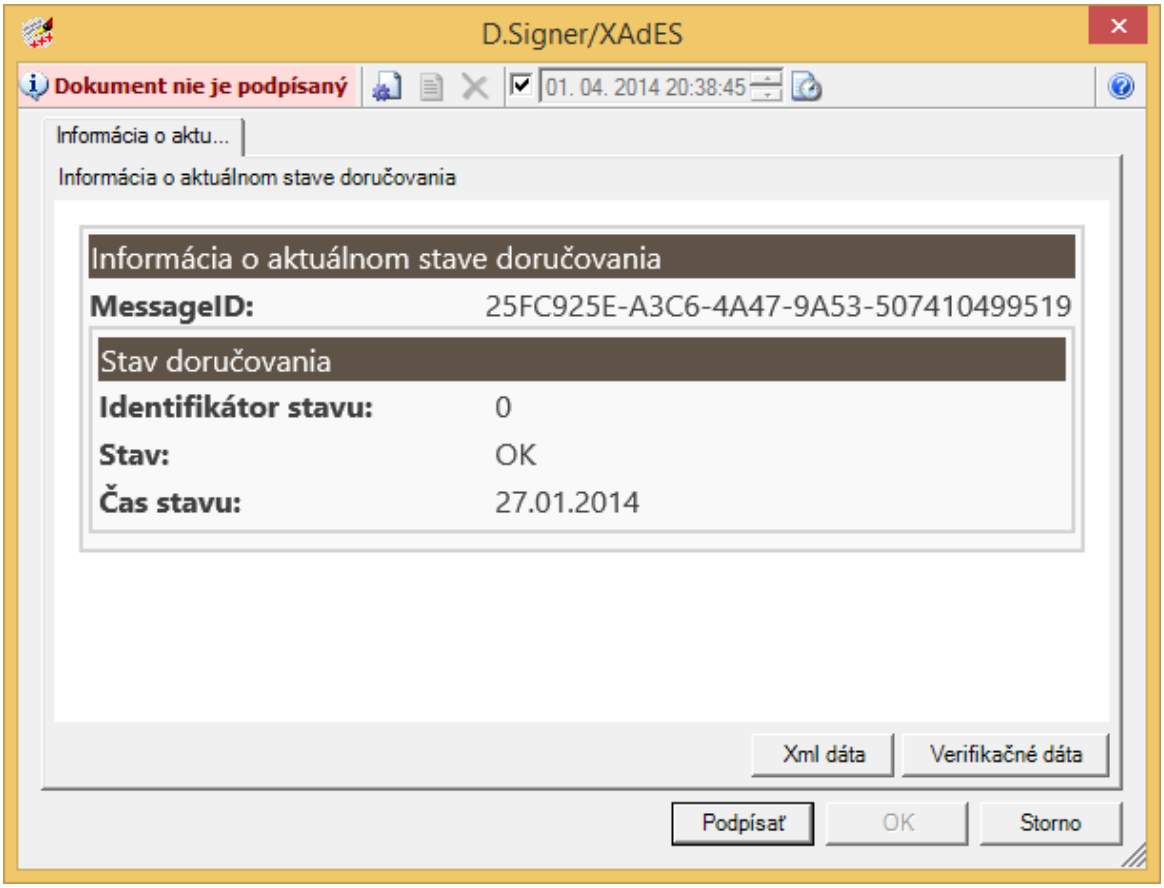
Pre jednotlivé požadované formáty dokumentov musí mať používateľ nainštalované príslušné plugin moduly aplikácie D.Signer/XAdES .NET. Informácia o nainštalovaných plugin moduloch je používateľovi prístupná prostredníctvom tlačidla "O aplikácii" (pravý horný roh okna aplikácie D.Signer/XAdES .NET).



5.2.1. 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.



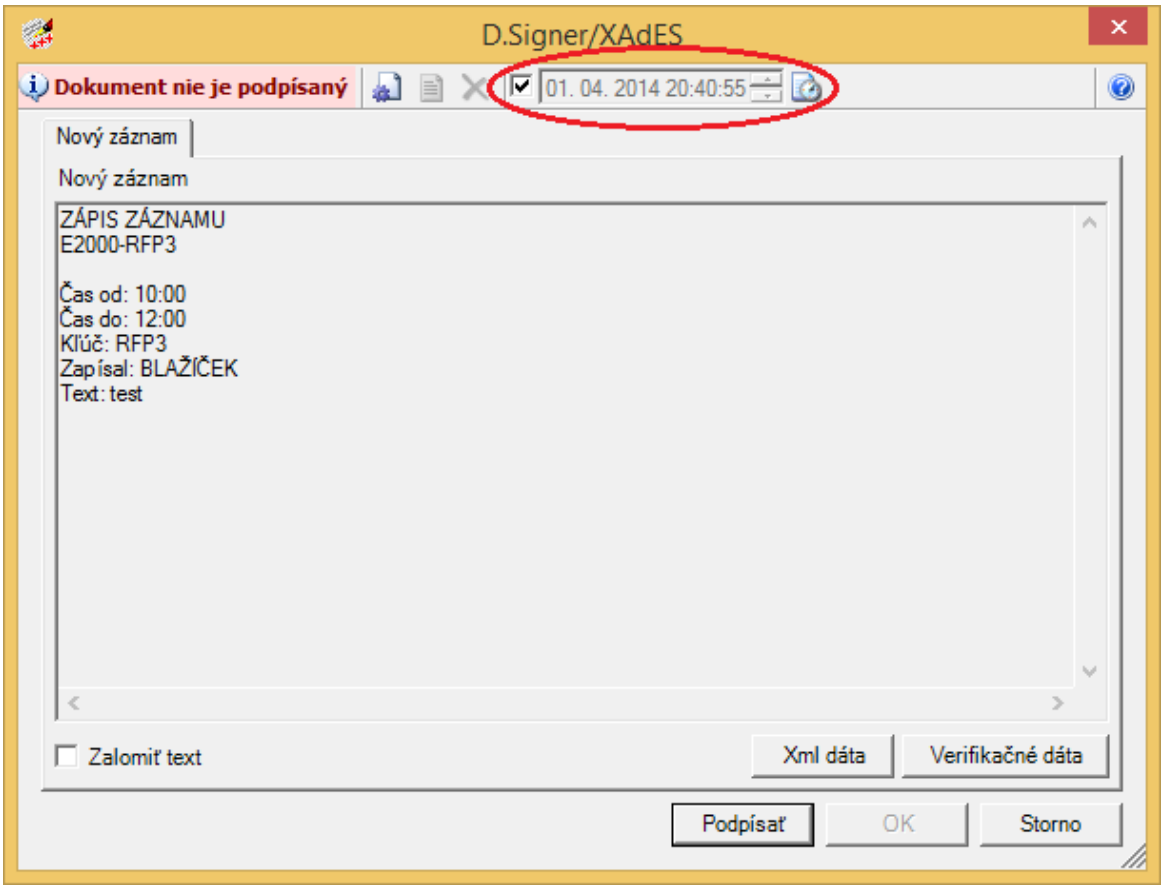
5.3. Nastavenie dátumu a času vytvorenia podpisu

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.

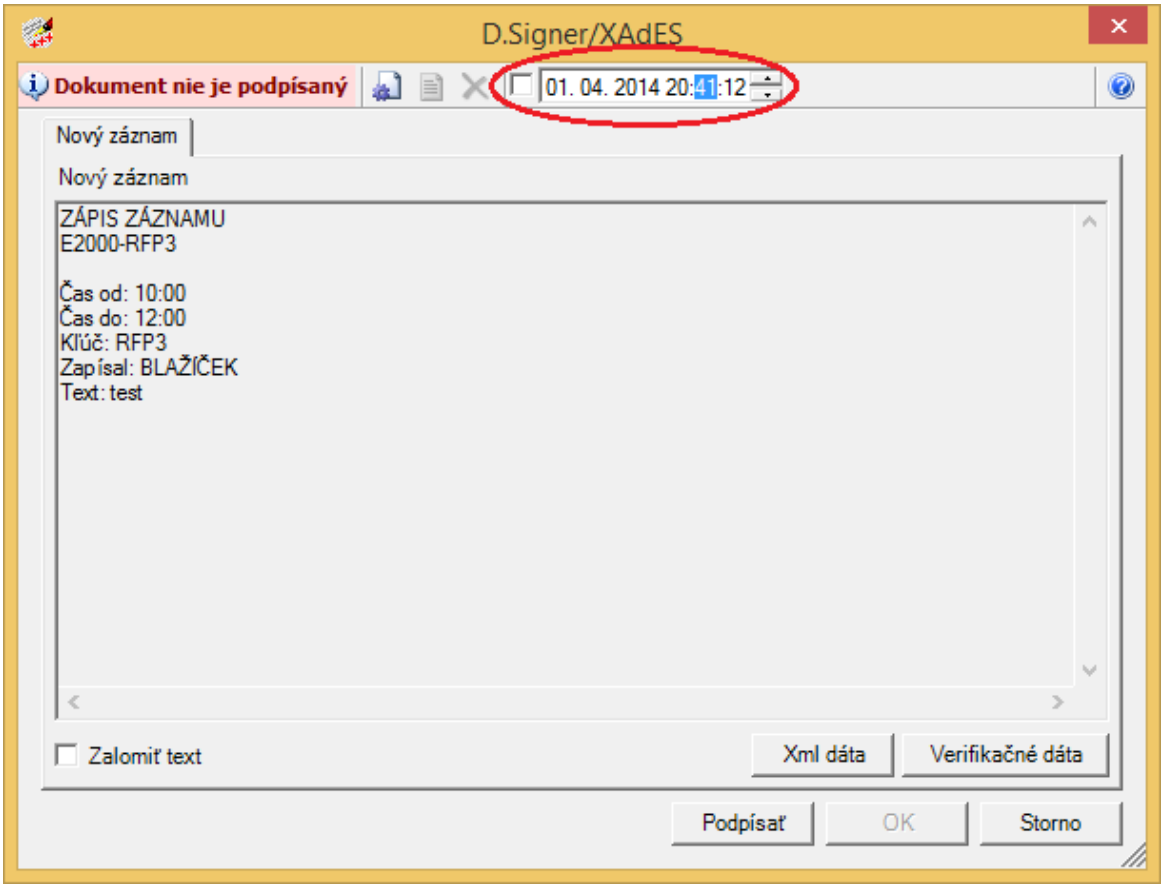
Aplikácia umožňuje používateľovi deklarovať ako čas vytvorenia podpisu:

- 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.

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).

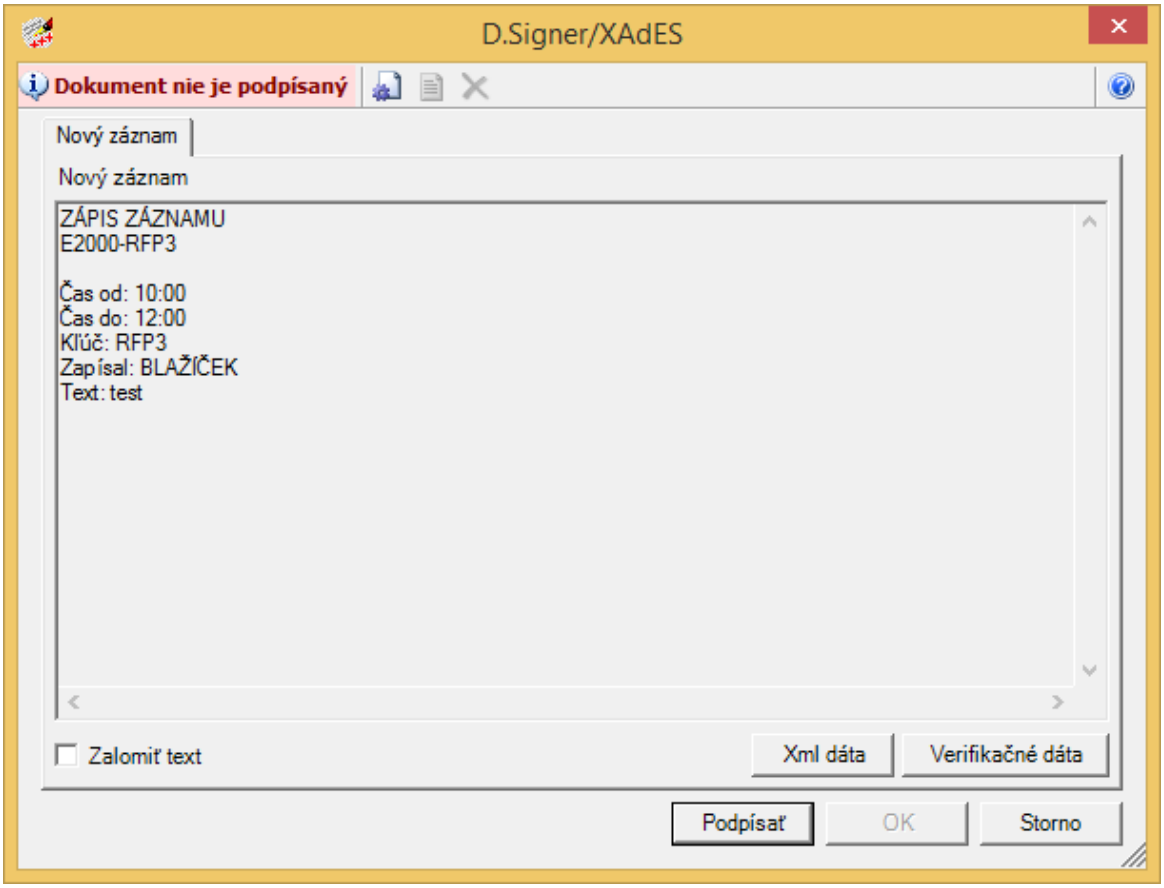


V druhom prípade sa používateľovi sprístupní deklarovaný dátum a čas vytvorenia podpisu na editovanie.



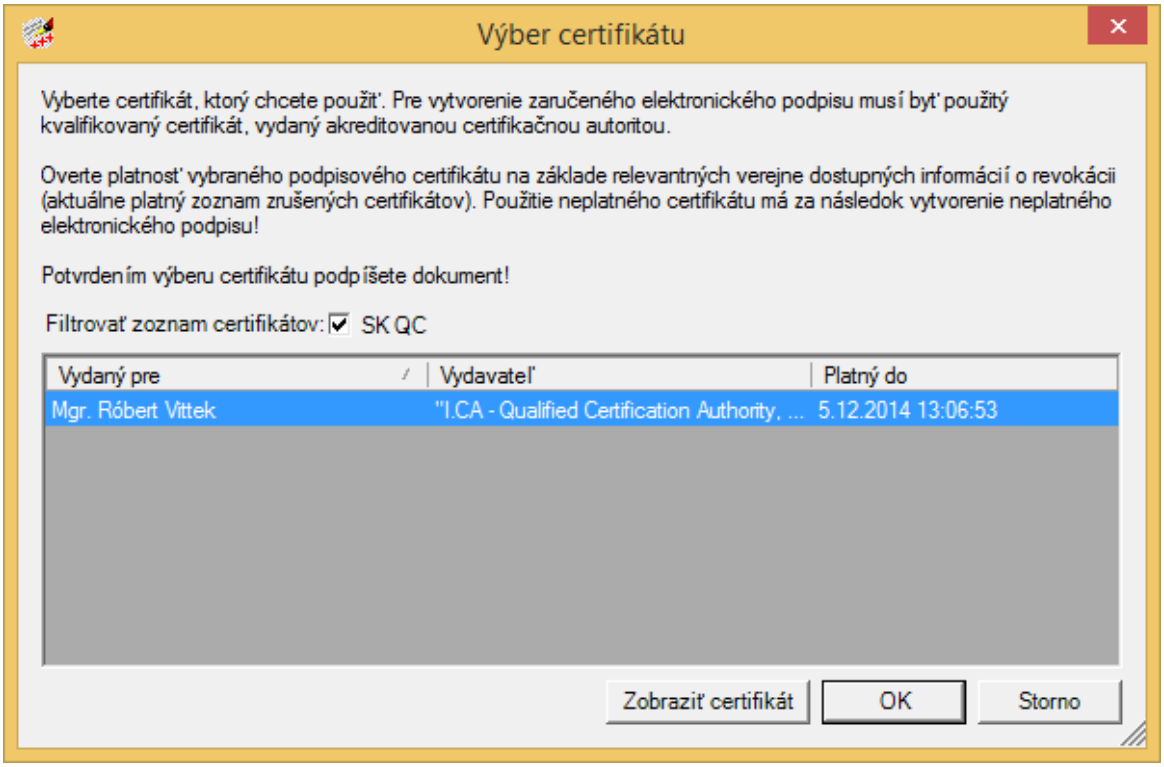
Pozor! Pri vytváraní elektronického podpisu odporúčame použiť správne nastavený aktuálny systémový dátum a čas.

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.



5.4. 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.



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.

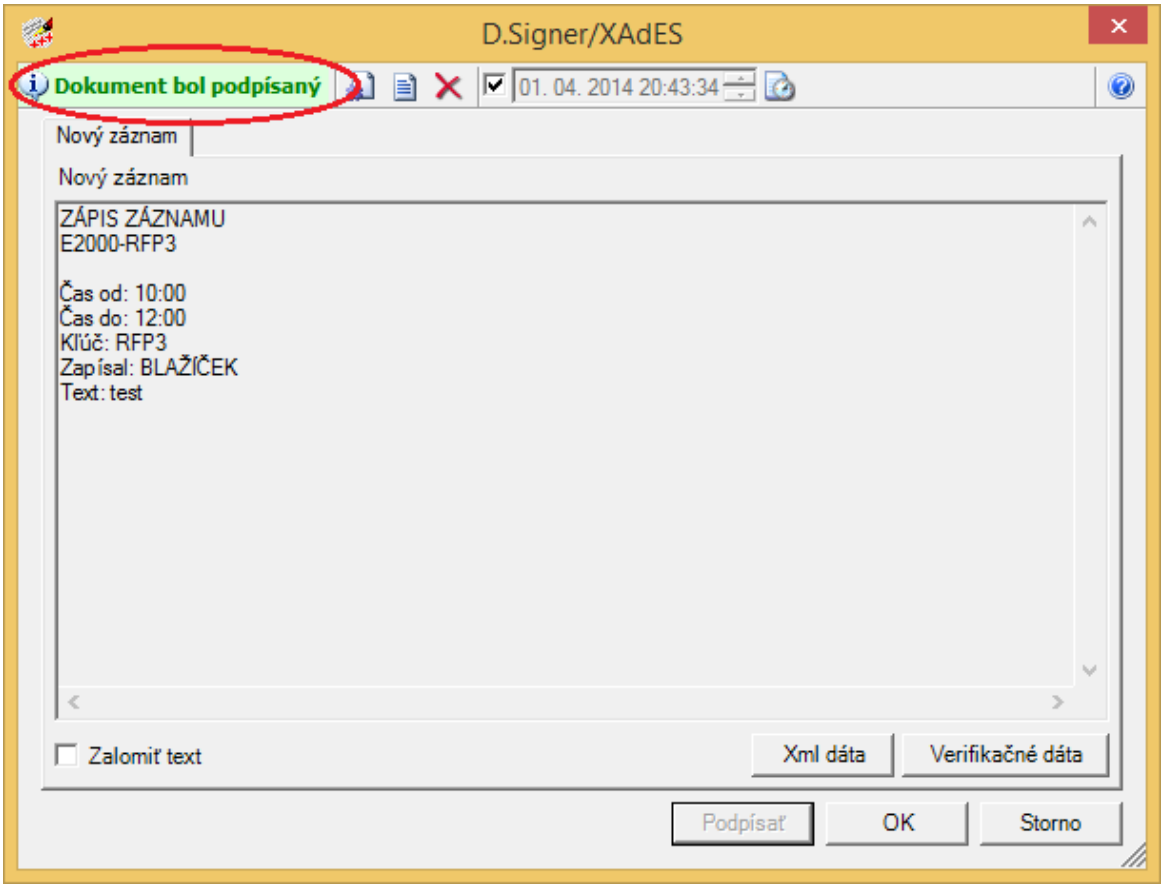
Detaily zvoleného certifikátu je možné prezrieť stlačením tlačidla Zobraziť certifikát.

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.

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.[4]

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

Aplikácia D.Signer/XAdES .NET následne vytvorí a sformátuje výstupný podpísaný dokument v súlade s profilom XAdES_ZEP. 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).



Po úspešnom vytvorení elektronického podpisu je podpísaný dokument odovzdaný klientskej aplikácii až po stlačení tlačidla OK.

5.5. 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 po podpísaní dokumentu. K dispozícii sú všetky tlačidlá, ako aj informácie o formáte vytvoreného podpisu, použitých kryptografických algoritmoch a vypočítaných hodnôt odtlačkov, podpisovej politike, podpisovom certifikáte, ako aj samotná hodnota vytvoreného podpisu.

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.

6. Trademarks

PDF technology in D.Signer/XAdES .NET - PDF Plugin is powered by PDFNet SDK copyright © PDFTron™ Systems Inc., 2001-2014, and distributed by DITEC a.s. under license. All rights reserved.

Microsoft® .NET is software for connecting people, information, systems, and devices.