

# **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	Víttek 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

<b>1.</b>	<b>Úvod .....</b>	<b>5</b>
<b>2.</b>	<b>Zoznam použitých skratiek .....</b>	<b>6</b>
<b>3.</b>	<b>Popis aplikácie .....</b>	<b>7</b>
<b>4.</b>	<b>Systémové požiadavky .....</b>	<b>9</b>
<b>5.</b>	<b>Inštalácia .....</b>	<b>11</b>
5.1.	Inštalácia z distribučného CD.....	12
5.2.	Inštalácia v rámci klientskej aplikácie .....	19
5.3.	Inštalácia z Internetu .....	19
<b>6.</b>	<b>Užívateľské nastavenia .....</b>	<b>20</b>
6.1.	Nastavenie jazyka aplikácie .....	20
<b>7.</b>	<b>Vytvorenie ZEP používateľom.....</b>	<b>21</b>
7.1.	Načítanie vstupných parametrov .....	21
7.2.	Zobrazenie podpisovaných dát .....	21
7.2.1.	Zobrazenie dokumentov .....	24
7.3.	Nastavenie dátumu a času vytvorenia podpisu.....	25
7.4.	Podpísanie dokumentu .....	28
7.5.	Zobrazenie parametrov podpisu .....	32
<b>8.</b>	<b>Trademarks .....</b>	<b>33</b>

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 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 značkový 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 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>), XAdES\_ZEP, v2.0 (<http://www.ditec.sk/ep/signature-formats/xades-zep/v2.0>) a XAdES\_ZEPbp, v1.0 (<http://www.ditec.sk/ep/signature-formats/xades-zepbp/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 typ 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 funkcionality vytvorenia ZEP aj pre osoby so zdravotným postihnutím – pre slabozrakých a nevidiacich pomocou technológie NVDA (<http://www.nvaccess.org/>).

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)<sup>2</sup>.

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 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. 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
-----------	---------

<sup>2</sup> 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 <sup>3</sup>	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.

---

<sup>3</sup> 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

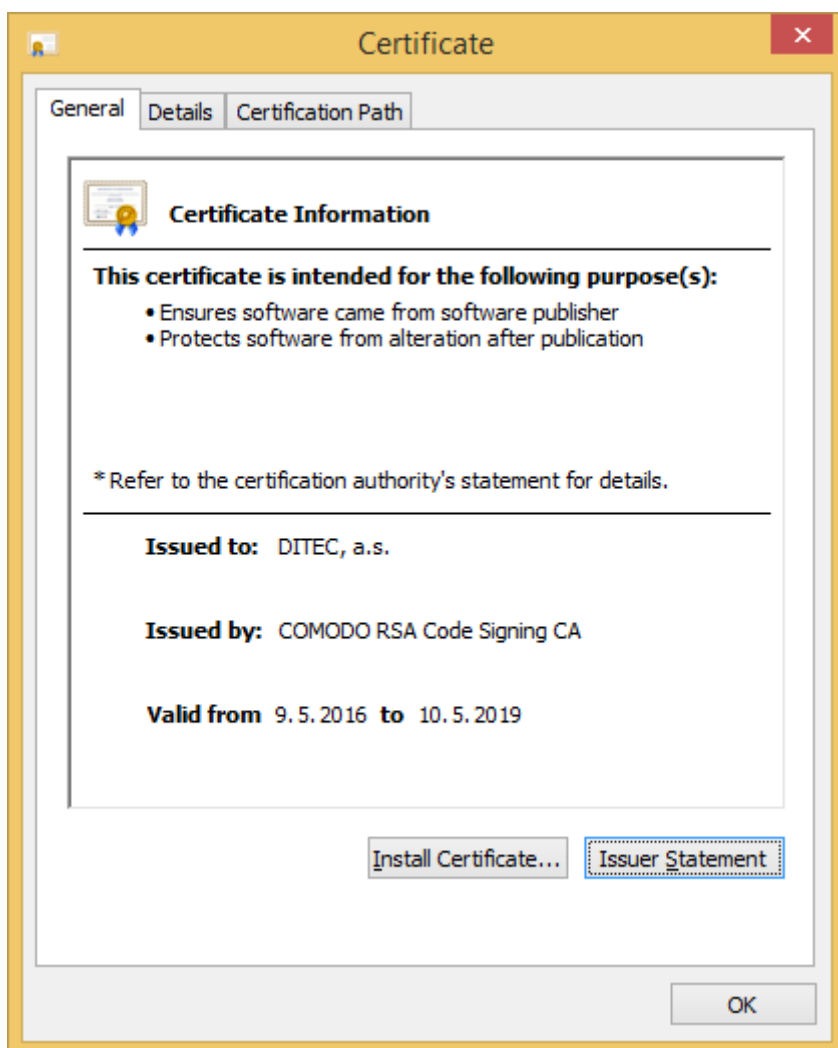
Inštalácia aplikácie D.Signer/XAdES .NET závisí primárne od spôsobu distribúcie komponentov aplikácie:

- 1) inštalácia z distribučného CD – spustením inštalačného programu z distribučného CD,
- 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., 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



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.<sup>4</sup>

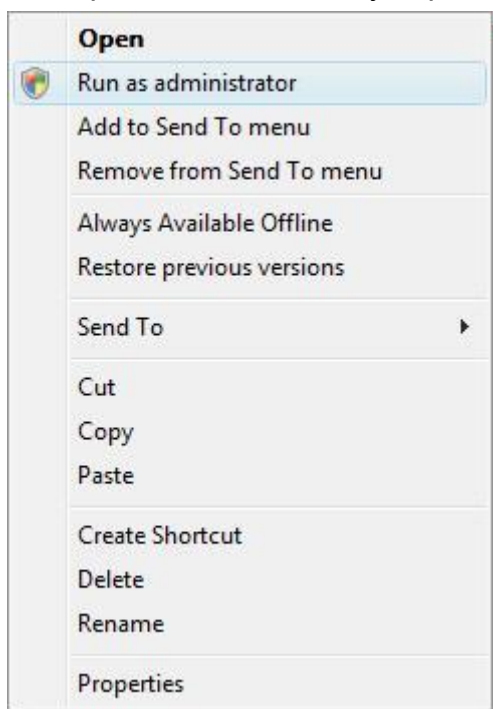
## 5.1. Inštalácia z distribučného CD

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

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

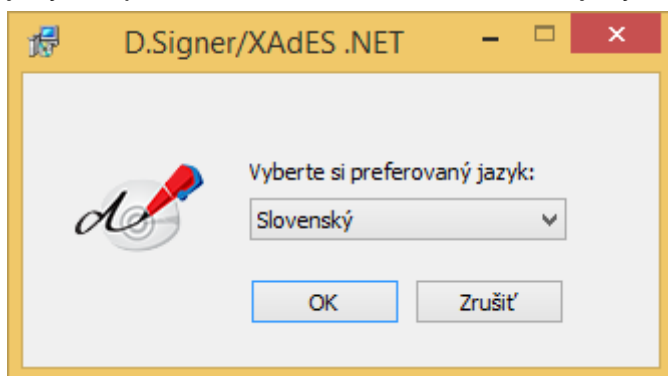
Projekt	GOV_ZEP	A3019_002
Dokument	Používateľská príručka	
Referencia	GOV_ZEP.200	Verzia 1

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



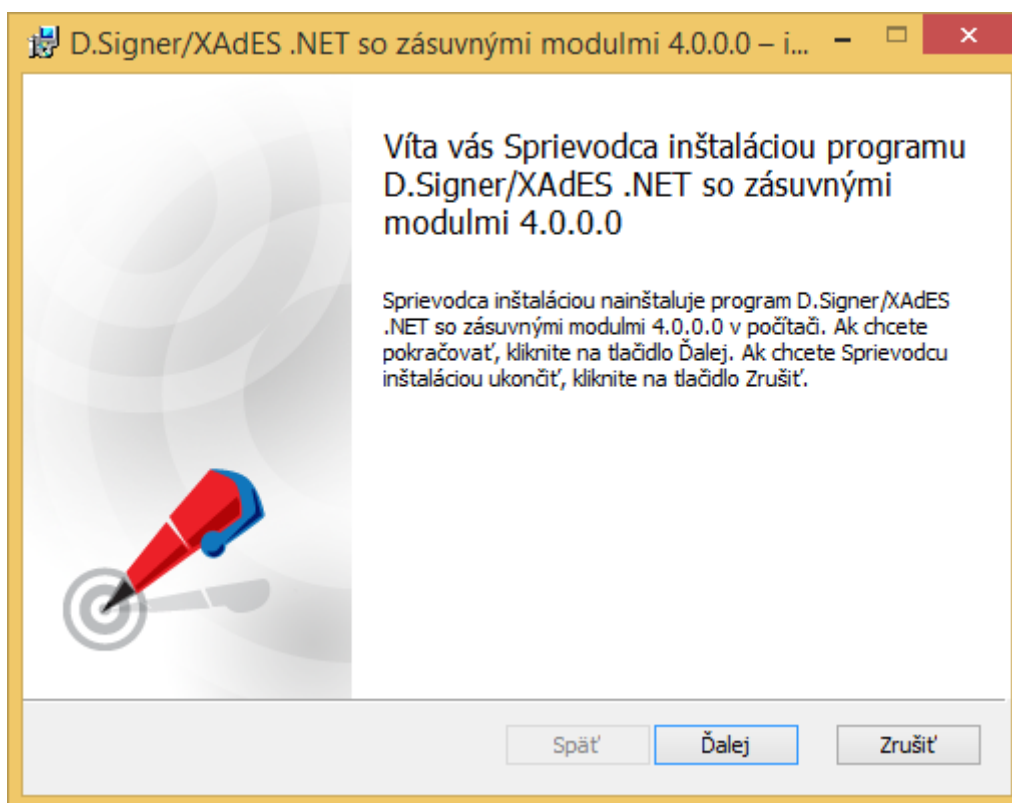
**Pozor! Keďže pri inštalácii aplikácie D.Signer/XAdES .NET je potrebné zaregistrovať v rámci operačného systému Windows aj komponenty pre integráciu aplikácie D.Signer/XAdES .NET do web stránok internetových aplikácií, odporúčame pred spustením inštalačného programu zavrieť otvorené internetové prehliadače.**

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



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

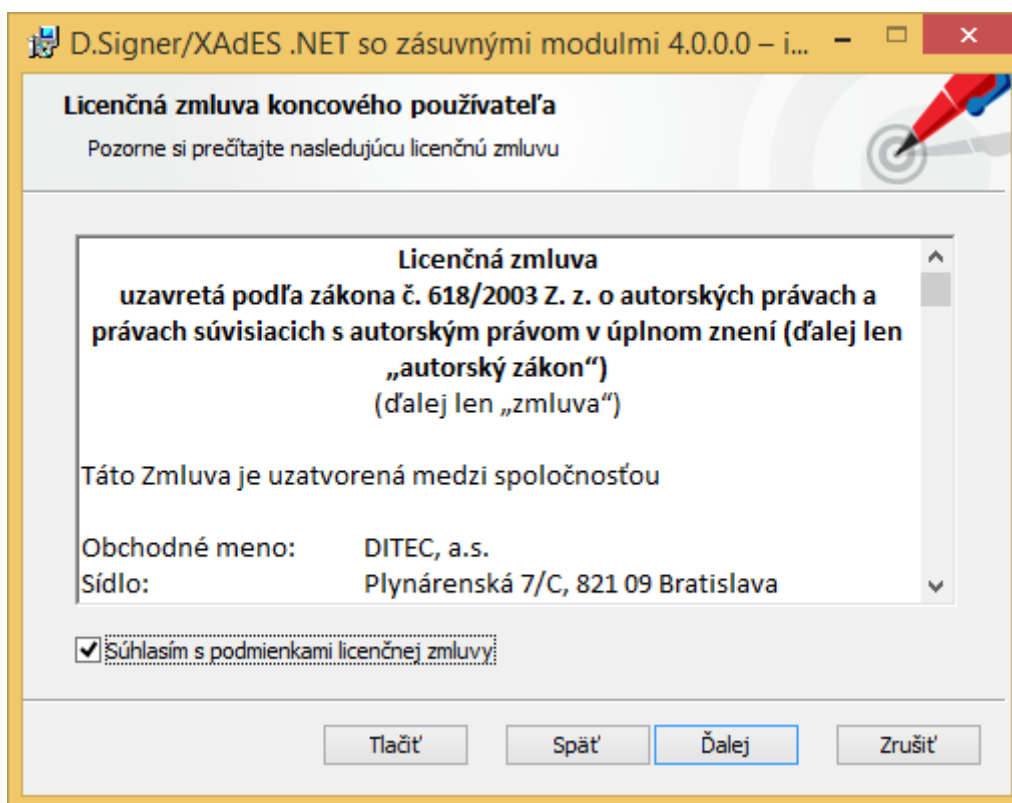
Projekt	GOV_ZEP	A3019_002
Dokument	Používateľská príručka	
Referencia	GOV_ZEP.200	Verzia 1



V nasledujúcom kroku je potrebné potvrdiť licenčnú zmluvu pre knižnicu PDFNet SDK<sup>5</sup>, ktorá tvorí súčasť zásuvného modulu PDF Plugin aplikácie D.Signer/XAdES .NET.

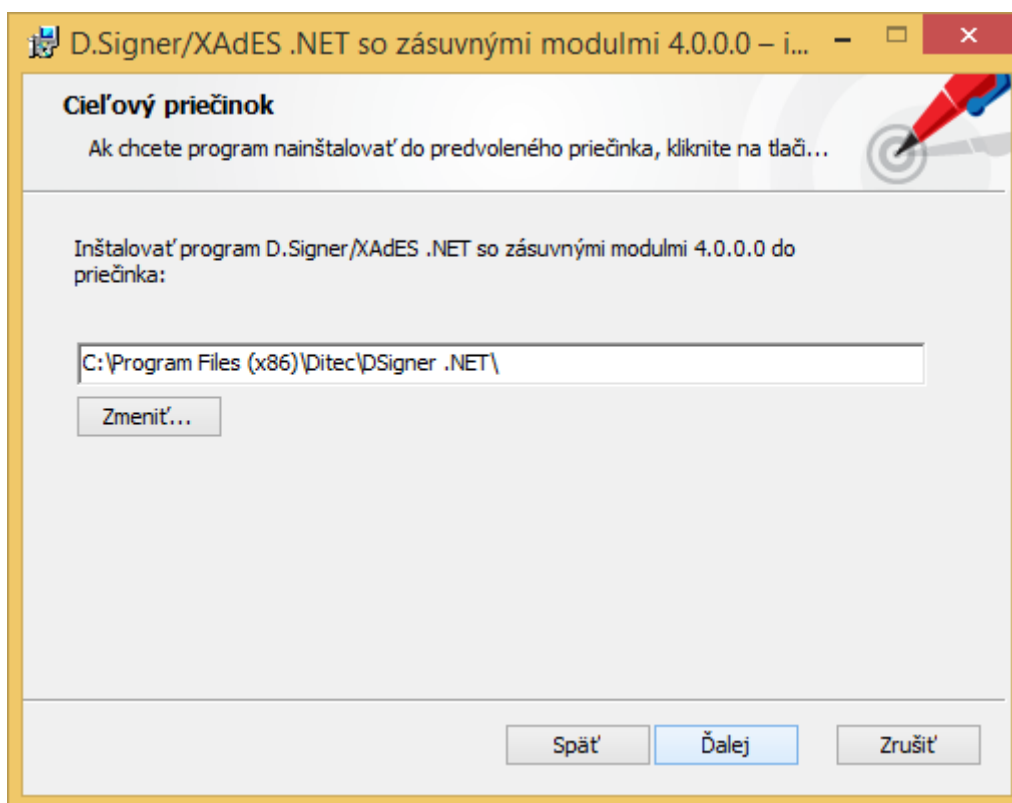
<sup>5</sup> PDF technology in D.Signer/XAdES .NET - PDF Plugin is powered by PDFNet SDK copyright © PDFTron™ Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All rights reserved.

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



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

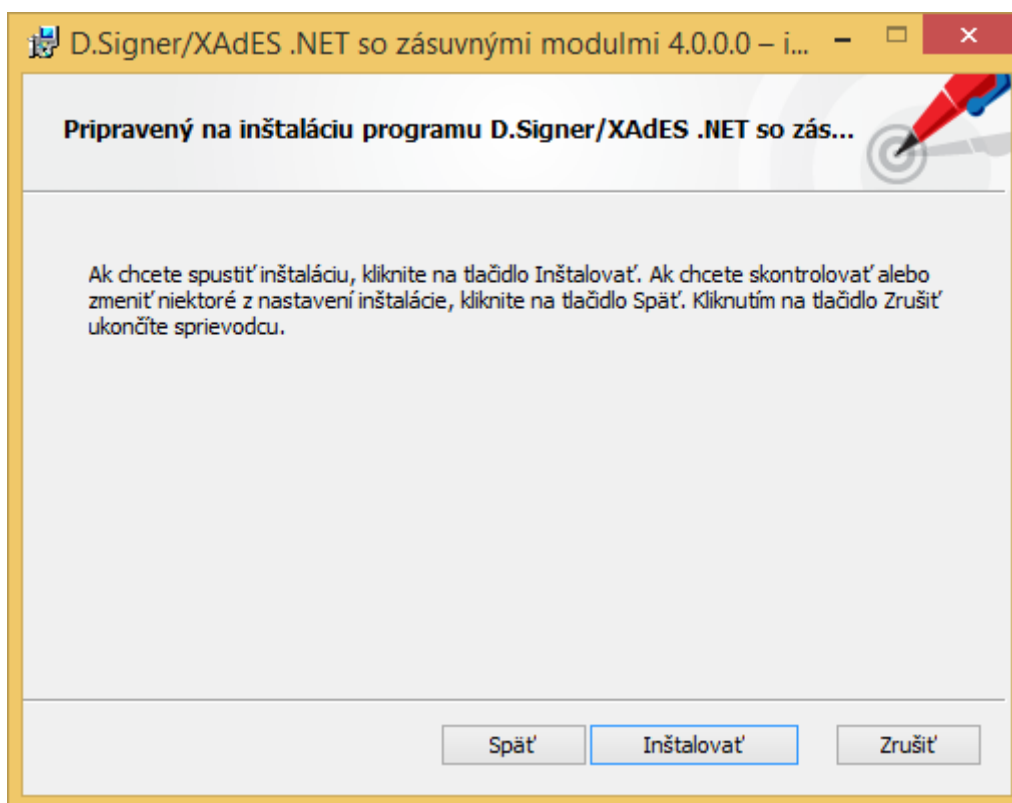
Projekt	GOV_ZEP	A3019_002
Dokument	Používateľská príručka	
Referencia	GOV_ZEP.200	Verzia 1



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



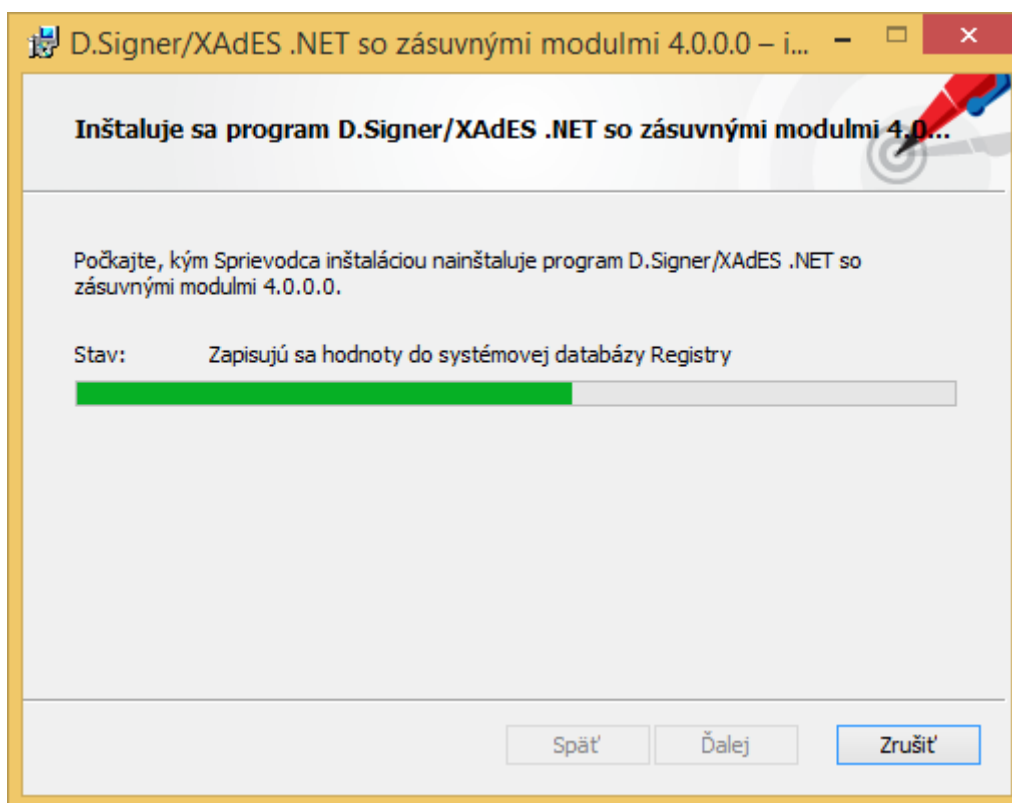
Projekt	GOV_ZEP	A3019_002
Dokument	Používateľská príručka	
Referencia	GOV_ZEP.200	Verzia 1



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

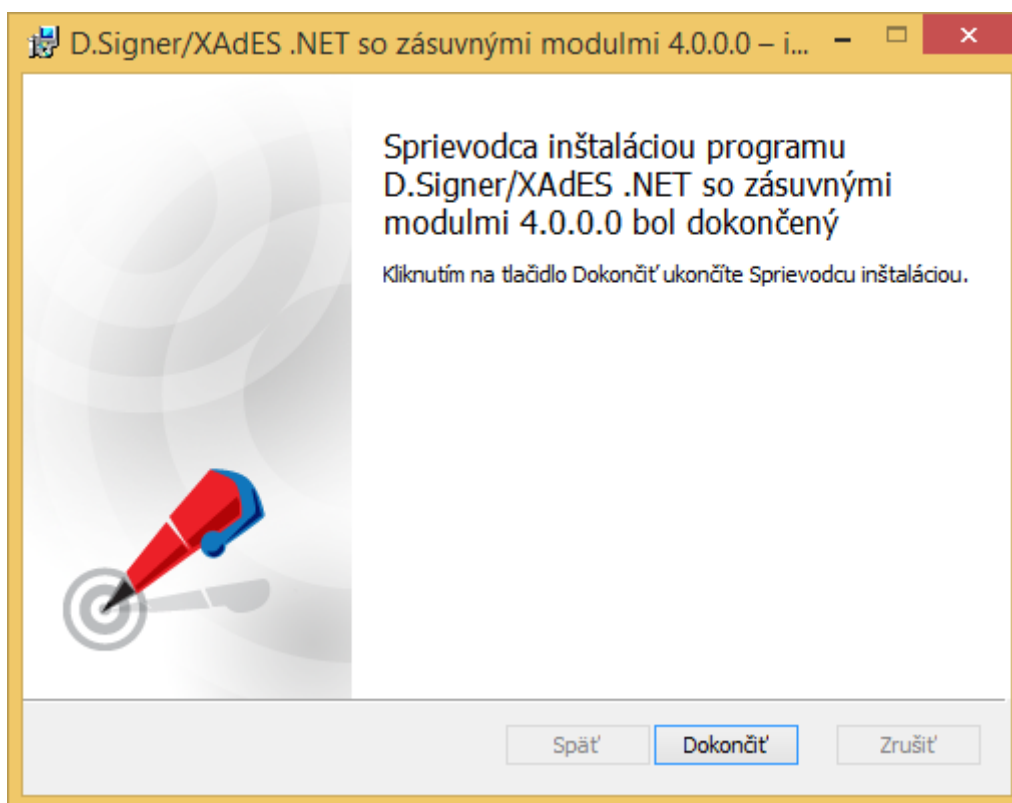
Používateľ je o priebehu inštalácie informovaný v okne inštaláčného programu. V každom okamihu je možné inštaláciu aplikácie D.Signer/XAdES .NET prerušiť kliknutím na tlačidlo Zrušiť.

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



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 inštaláčnej príručky danej klientskej aplikácie.

## 5.3. Inštalácia z Internetu

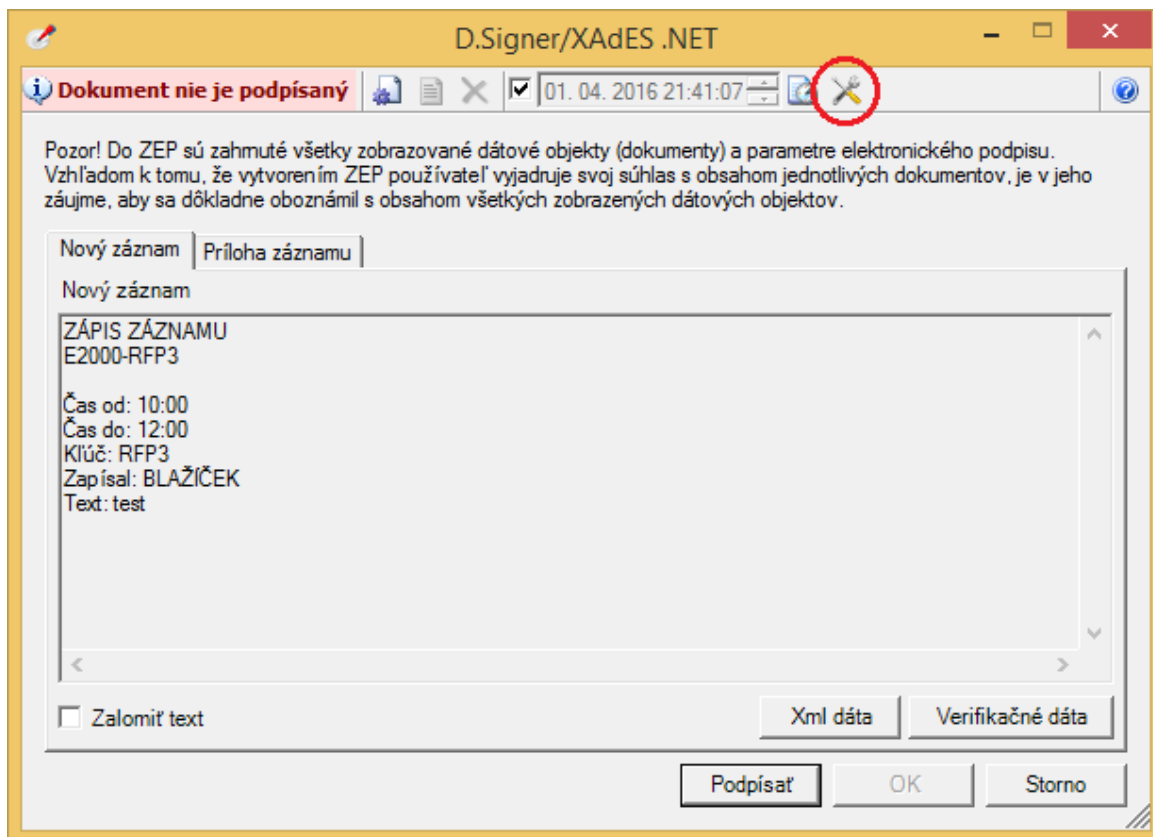
V prípade použitia aplikácie D.Signer/XAdES .NET v rámci Internetovej aplikácie (webového portálu) doporučujeme, aby tvorca Internetovej aplikácie sprístupnil na stránkach svojej aplikácie aj inštalčné súbory jednotlivých komponentov D.Signer/XAdES .NET, najlepšie zabezpečené protokolom HTTPS. Používateľ si bude môcť takto inštalčné 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 inštaláčnej príručky príslušnej Internetovej aplikácie.

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

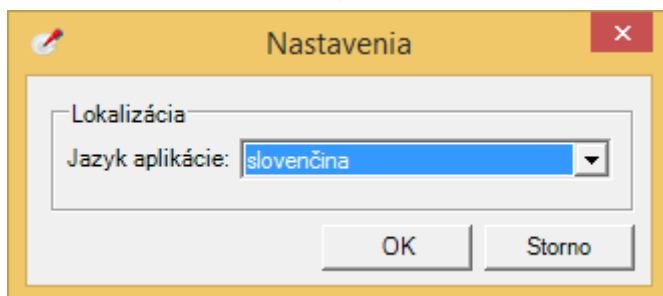
## 6. Užívateľské nastavenia

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



### 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.



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*.

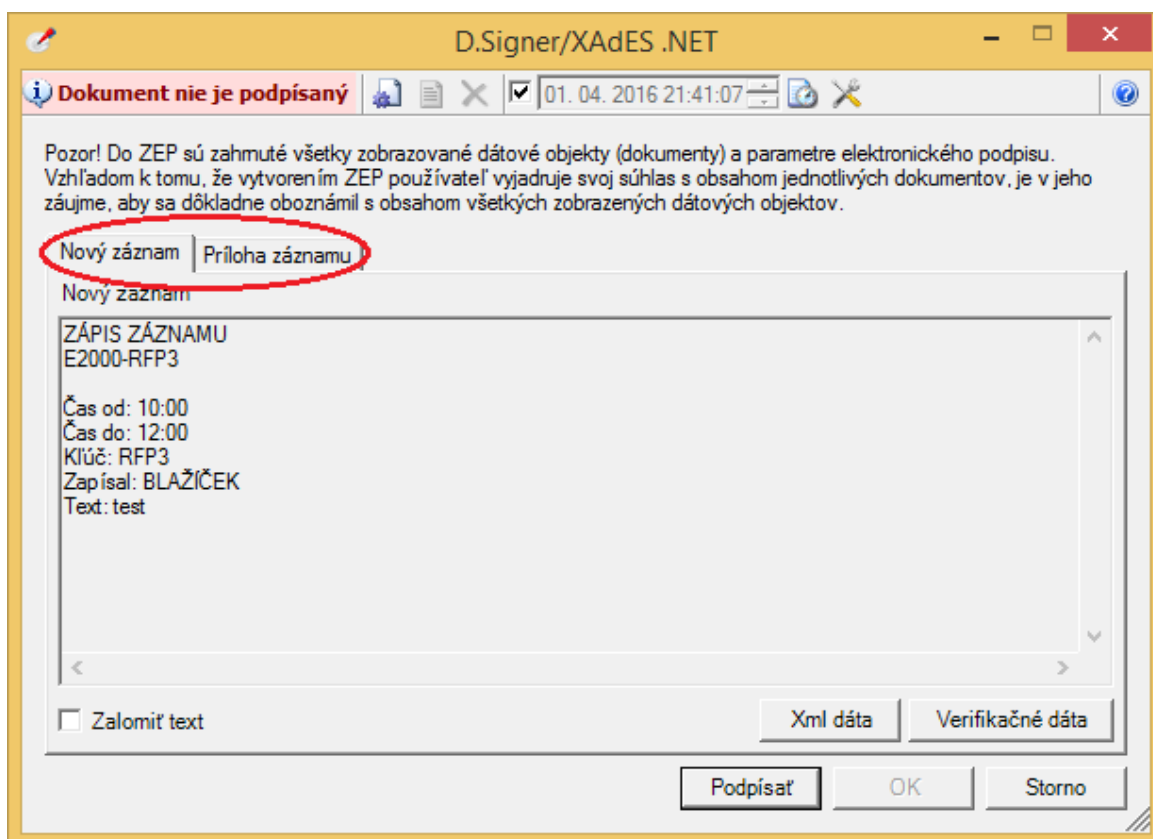


### 7.2. Zobrazenie podpisovaných dát

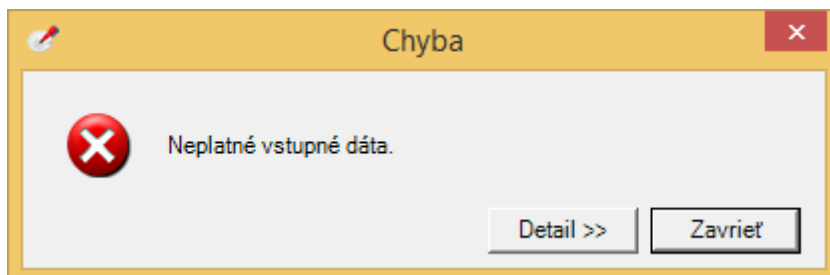
Pokiaľ všetky kontroly vstupných parametrov prebehli úspešne, na jednotlivých záložkách hlavného okna sú zobrazené časti podpisovaného *multipart* dokumentu. Používateľ má možnosť prezrieť všetky podpisované dátové objekty a ďalšie parametre podpisu.

**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

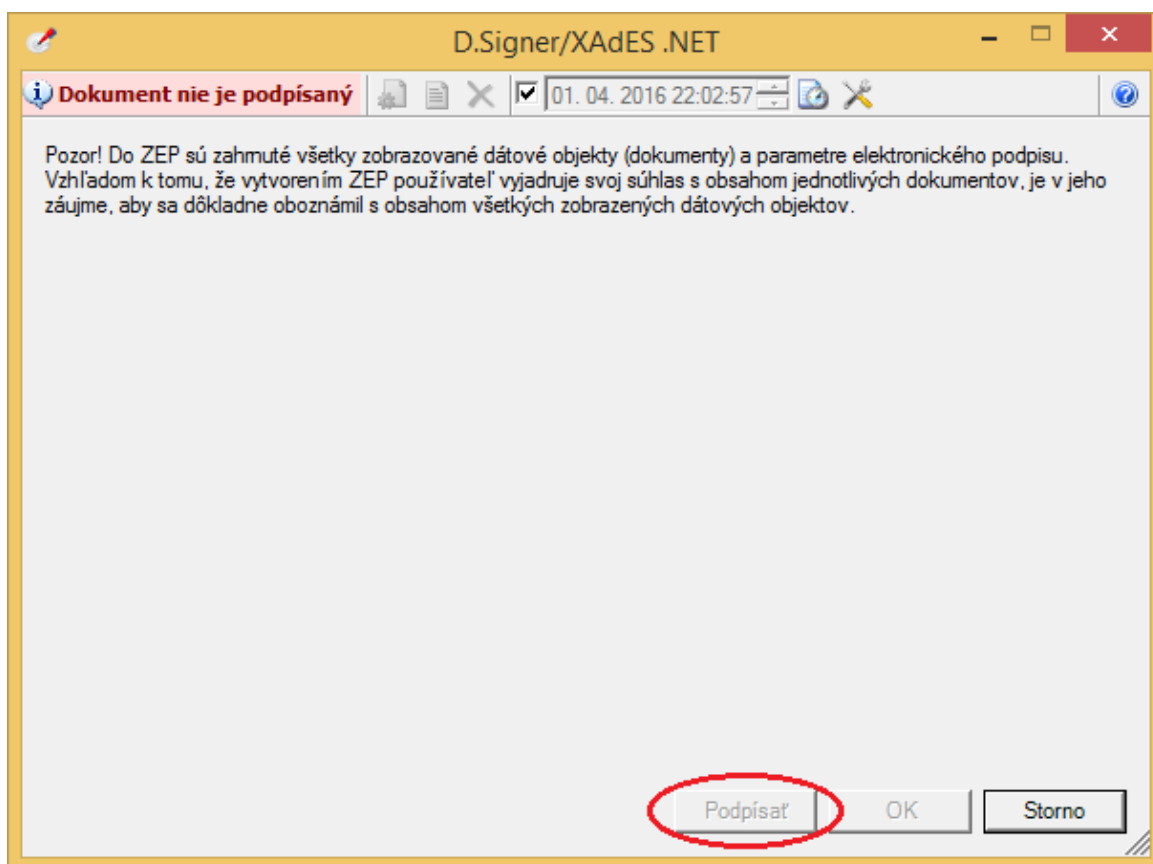


Pokiaľ sa vyskytli pri kontrole vstupných parametrov chyby, aplikácia D.Signer/XAdES .NET zobrazí chybovú správu.



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

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



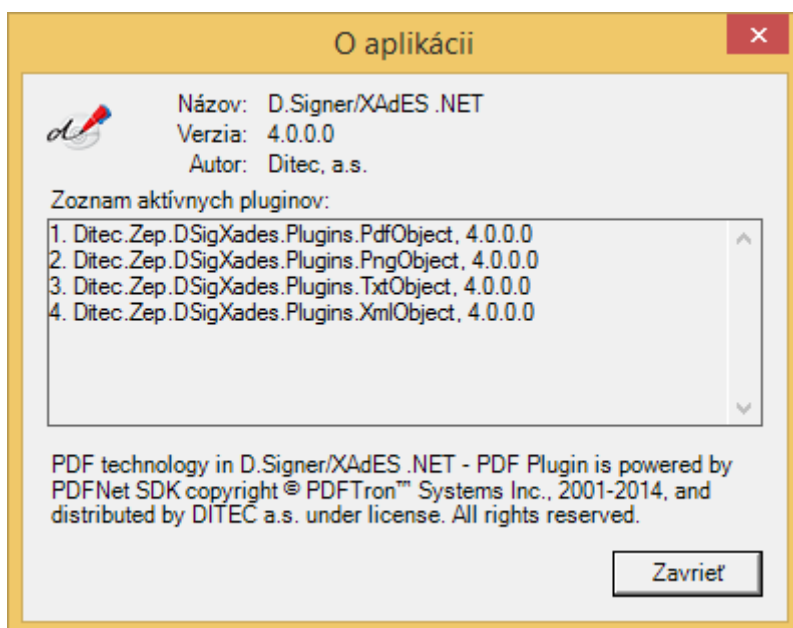
V rámci hlavného okna aplikácie D.Signer/XAdES .NET je tiež zobrazený stav podpisovaného dokumentu, ktorý môže nadobúdať nasledujúce hodnoty:

- 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).

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



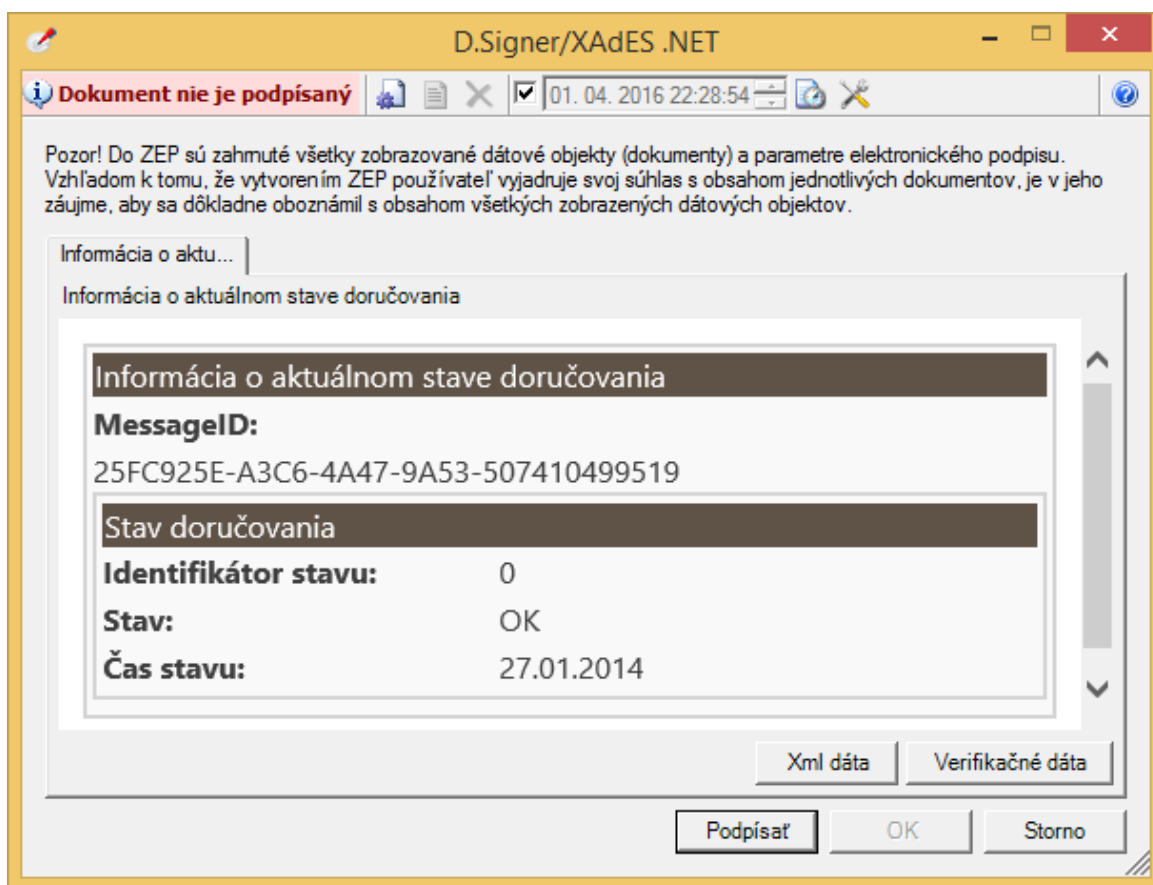
### 7.2.1. Zobrazenie dokumentov

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 podpísované 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 podpísovaných 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



### 7.3. Nastavenie dátumu a času vytvorenia podpisu

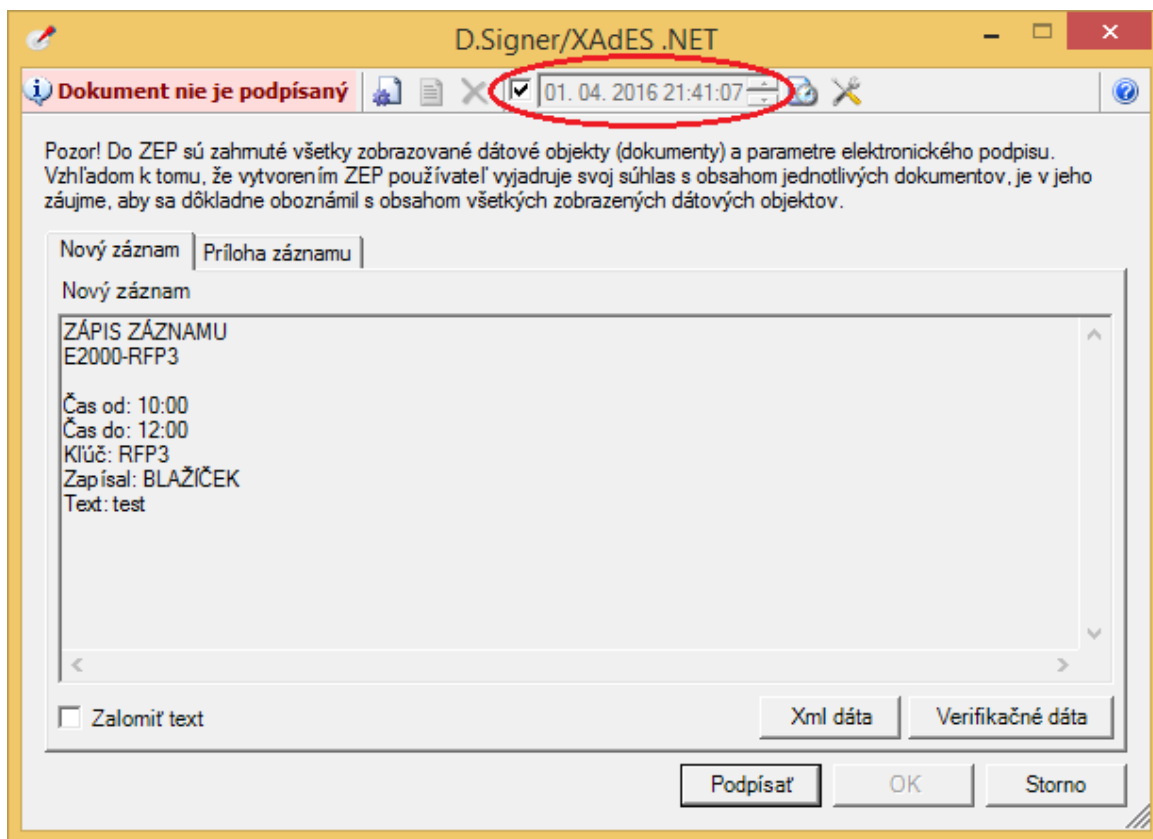
Aplikácia D.Signer/XAdES .NET umožňuje používateľovi v prípade potreby nastaviť pomocou ovládacích prvkov, ktoré sú umiestnené v hornej lište okna aplikácie, dátum a čas vytvorenia podpisu. Používateľ môže takto deklarovať vytvorenie elektronického podpisu v špecifikovanom dátume a čase, pričom tento 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 zaškrávanom políčku použitie systémového dátumu a času,
- alebo manuálne nastaviť deklarovaný dátum a čas vytvorenia podpisu, ak je v zaškrávanom políčku použitie systémového dátumu a času odznačené.

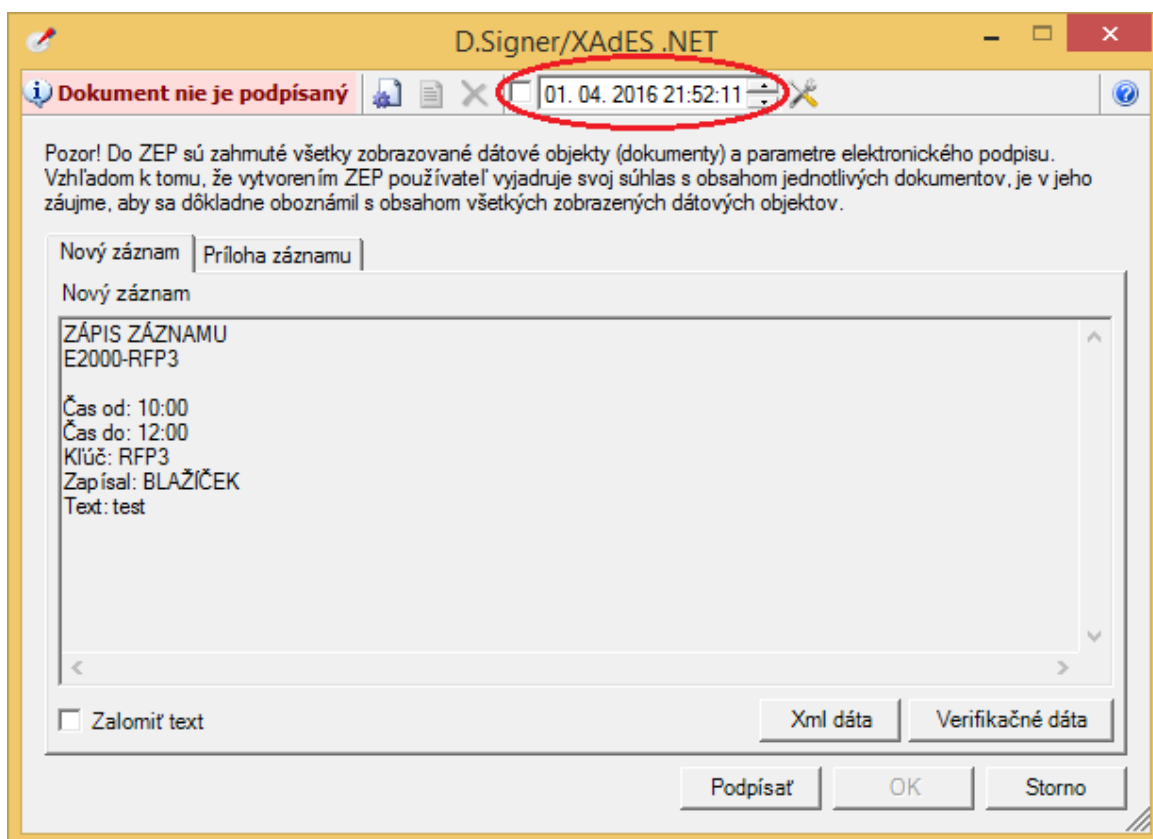
Projekt	GOV_ZEP	A3019_002
Dokument	Používateľská príručka	
Referencia	GOV_ZEP.200	Verzia 1

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).



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

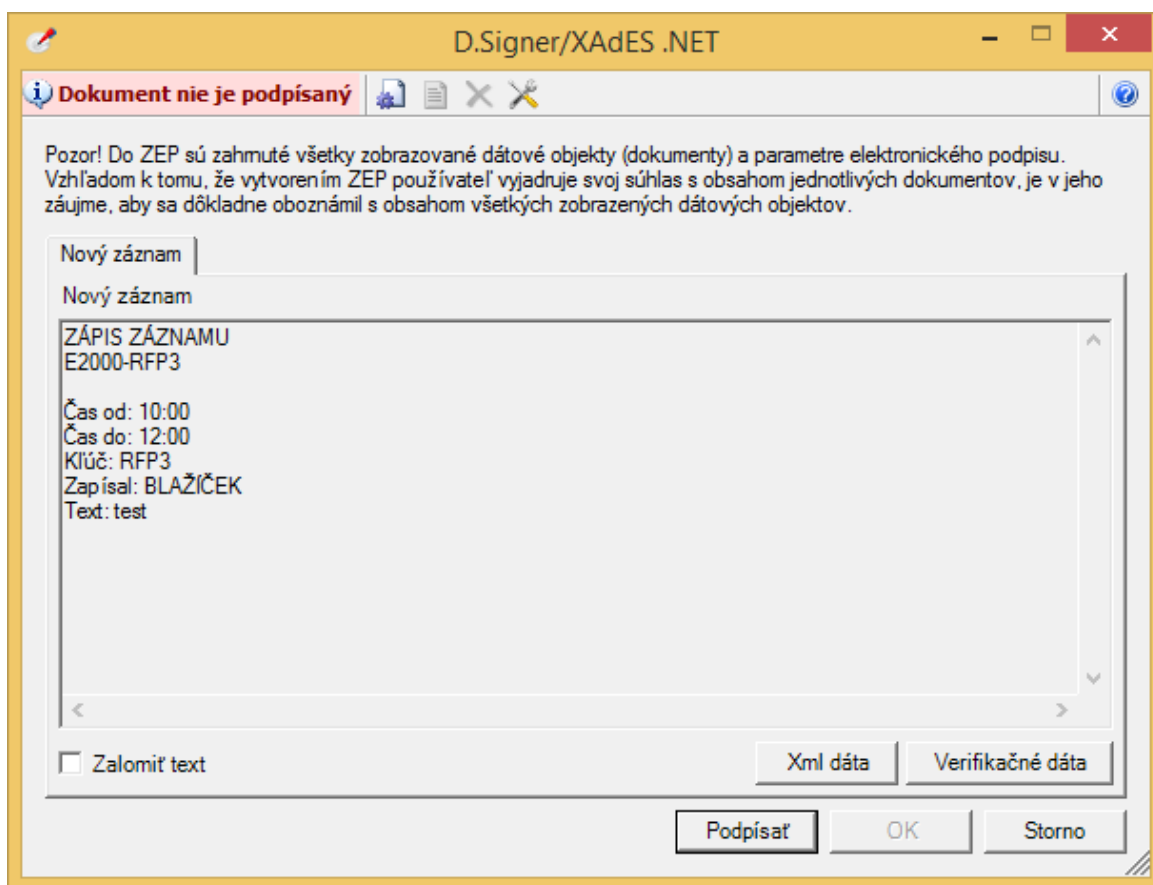
Projekt	GOV_ZEP	A3019_002
Dokument	Používateľská príručka	
Referencia	GOV_ZEP.200	Verzia 1



**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.

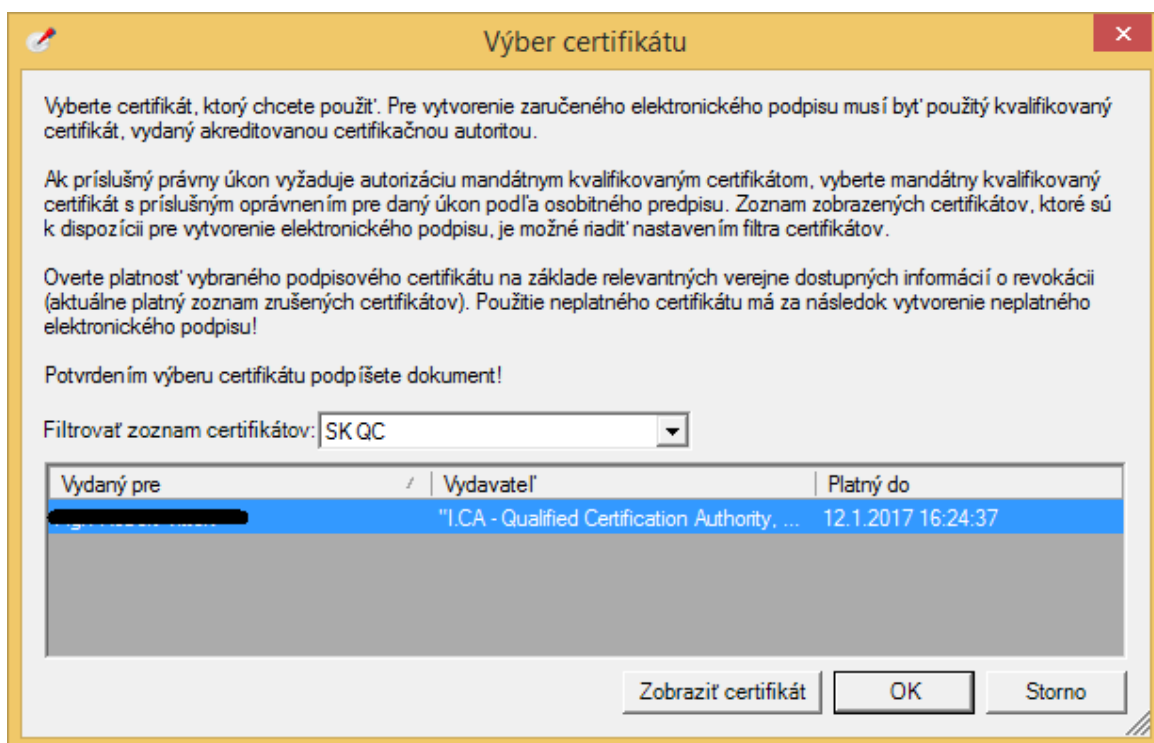
Projekt	GOV_ZEP	A3019_002
Dokument	Používateľská príručka	
Referencia	GOV_ZEP.200	Verzia 1



## 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



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.

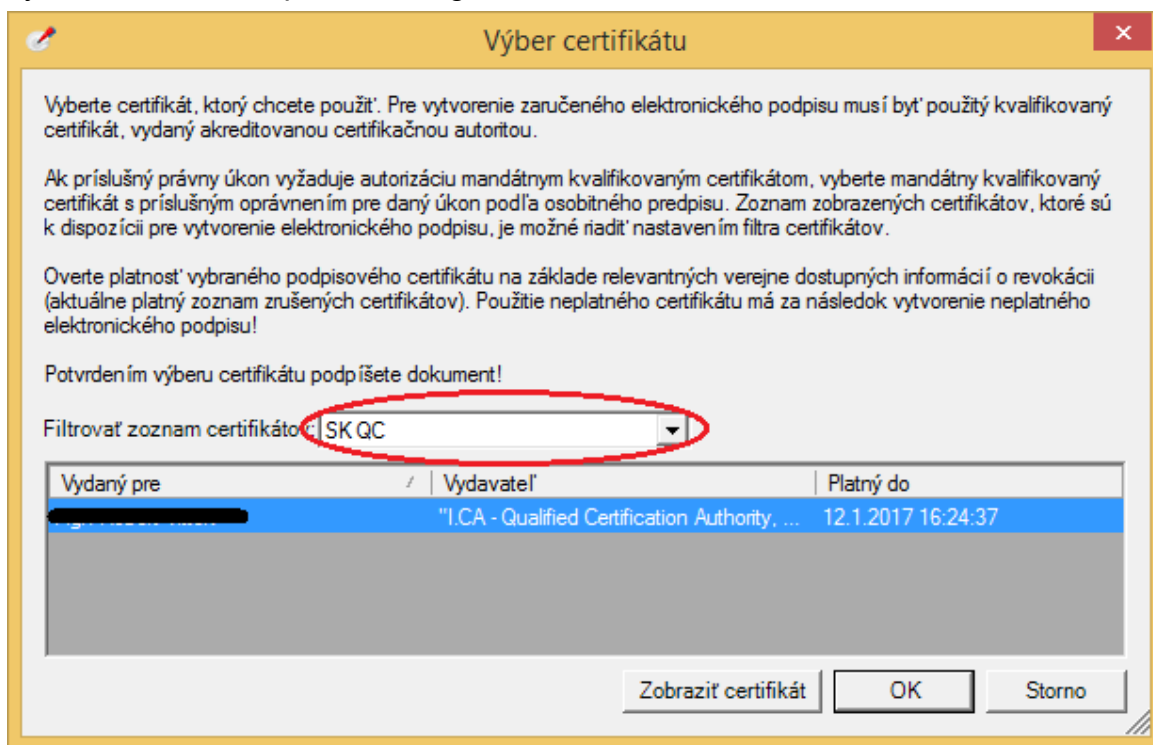
Detaily zvoleného certifikátu je možné prezrieť kliknutím na tlačidlo Zobraziť certifikát.

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.



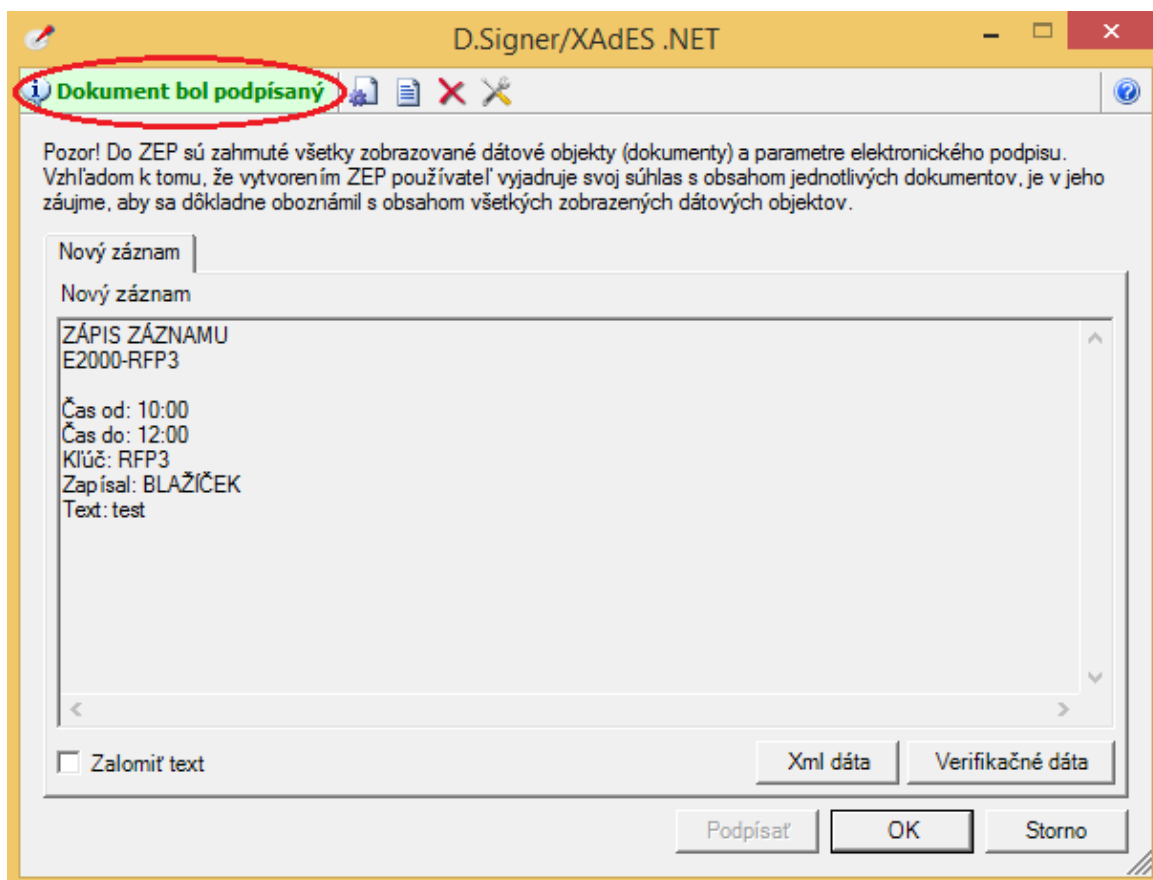
Po zvolení certifikátu a potvrdení výberu tlačidlom OK sa vykoná proces vytvorenia elektronického podpisu. Aplikácia D.Signer/XAdES .NET vytvorí reprezentáciu podpisovaných dát a parametrov podpisu – digitálny odtlačok. Pomocou rozhrania MS CryptoAPI a príslušného SSCD zariadenia, na ktorom je uložený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

<sup>7</sup> 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



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).



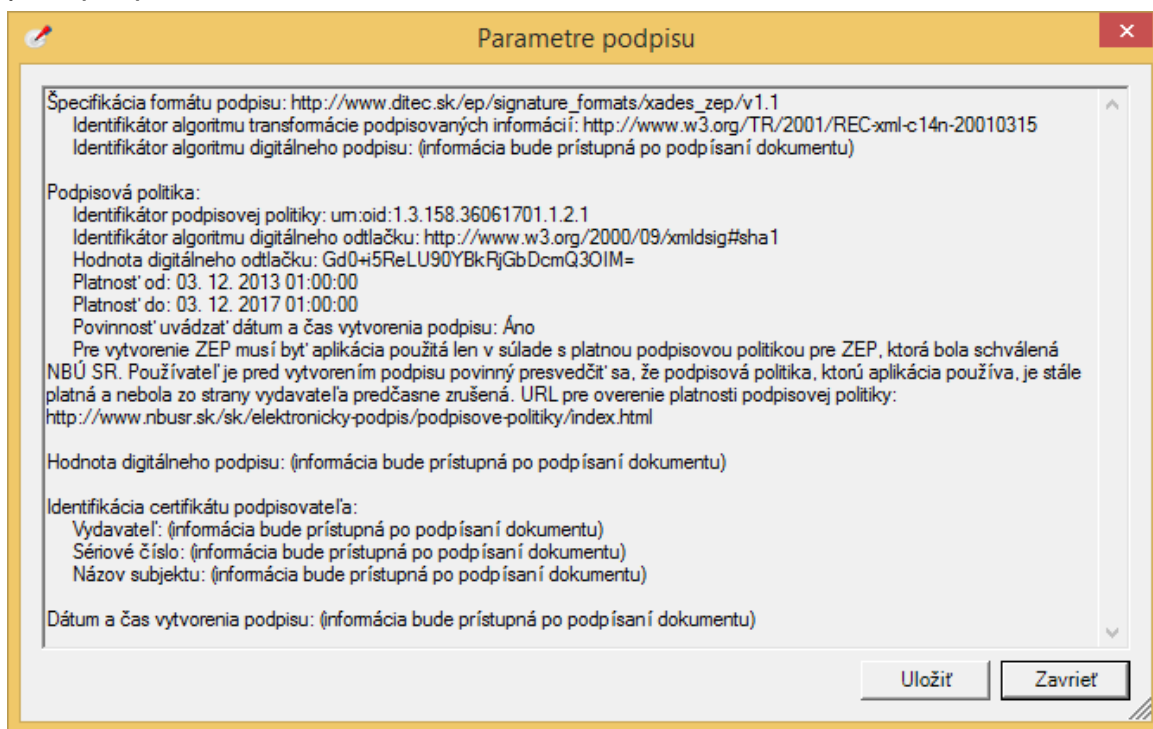
Projekt	GOV_ZEP	A3019_002
Dokument	Používateľská príručka	
Referencia	GOV_ZEP.200	Verzia 1

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.



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 viesť 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.

The logo for PDFTRON, featuring the word "PDFTRON" in a bold, blue, sans-serif font. The letters are closely spaced and have a slight shadow effect.

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