DITEC
Data Information Technology & Expert Consulting

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

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	9

Vypracoval	Vittek Róbert	Podpis	Dátum 29. 7. 2024
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.200	Verzia	9

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 5

2. Zoznam použitých skratiek 6

3. Popis aplikácie 7

4. Systémové požiadavky 9

5. Inštalácia 11

5.1. Inštalácia z distribučného CD 12

5.2. Inštalácia v rámci klientskej aplikácie 18

5.3. Inštalácia z Internetu 18

6. Užívateľské nastavenia 19

6.1. Všeobecné nastavenia aplikácie 19

6.2. Sieťové nastavenia 21

7. Vytvorenie ZEP/KEP používateľom 22

7.1. Načítanie vstupných parametrov 22

7.2. Zobrazenie podpisovaných dát 22

7.2.1. Zobrazenie dokumentov 25

7.3. Nastavenie dátumu a času vytvorenia podpisu 26

7.4. Podpísanie dokumentu 29

7.5. Zobrazenie parametrov podpisu 35

8. Trademarks 37

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/kvalifikovaný elektronický podpis (ZEP/KEP) 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. Zoznam použitých skratiek

CRL – Certificate Revocation List; zoznam zneplatnených certifikátov

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

HTTPS – HyperText Transfer Protocol Secure; zabezpečený hypertextový prenosový protokol

KEP – kvalifikovaný elektronický podpis

NBÚ – Národný bezpečnostný úrad

OCSP – Online Certificate Status Protocol

PDF – formát dokumentov Portable Document Format

PNG – grafický formát Portable Network Graphics

QSCD – Qualified Signature Creating Device; zariadenie na vytváranie kvalifikovaného podpisu

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 kvalifikovaného elektronického podpisu na báze XAdES baseline profile

ZEP – Zaručený elektronický podpis

3. Popis aplikácie

Aplikácia D.Signer/XAdES .NET predstavuje riešenie pre vytváranie zaručeného/kvalifikovaného elektronického podpisu (ZEP/KEP) 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/kvalifikovaný 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/KEP 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/KEP musí byť aplikácia použitá len v súlade s platnou podpisovou politikou pre ZEP/KEP, 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/KEP, definovaného v rámci podpisovej politiky, je zodpovedný podpisovateľ. Za správne vyhodnotenie platnosti vytvoreného ZEP/KEP a za špecifikovanie parametrov procesu verifikácie ZEP/KEP v súlade s podpisovou politikou je zodpovedný prijímateľ alebo prevádzkovateľ systému, ktorý tieto dáta spracováva.

Požiadavky NBÚ SR na vytváraný formát ZEP/KEP 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

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 KEP v súlade s profilom pre kvalifikovaný elektronický podpis 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 .NET implementovaná takým spôsobom, aby poskytovala funkcionalitu vytvorenia ZEP/KEP aj pre osoby so zdravotným postihnutím – pre slabozrakých a nevidiacich pomocou technológie NVDA (http://www.nvaccess.org/).

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

4. Systémové požiadavky

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

- OS – MS aWindows 7, Windows 8.x, Windows 10, Windows 11,
- Platforma – .Net framework, verzia 4.6.2 alebo vyššia,
- občiansky preukaz s čipom alebo iné certifikované SSCD/QSCD zariadenie pre generovanie kľúčových párov a vytváranie elektronického podpisu + čítačka a ovládače podľa odporúčaní akreditovanej certifikačnej autority (ACA),
- web prehliadač – MS Internet Explorer, v7.0 alebo vyššia (len 32 bit), Mozilla Firefox, v45 – v51, resp. v59 ESR (len 32 bit, s podporou NP API)[1],
- prístup na internet (prípadne správne nastavenia pre proxy),
- správne nastavený aktuálny systémový dátum a čas.

Ak je aplikácia D.Signer/XAdES .NET spúšťaná z web portálu pomocou aplikácie D.Launcher v1.x, tak požiadavky na web prehliadač zahŕňajú aj prehliadače:

- MS Internet Explorer verzia 10/11 (aj 64 bit), Mozilla Firefox, v45 a vyššia aj 64-bit, 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/kvalifikovaného elektronického podpisu pomocou aplikácie D.Signer/XAdES .NET sa vyžaduje použitie certifikovaného zariadenia pre generovanie a uloženie privátneho kľúča a pre vytvorenie zaručeného/kvalifikovaného elektronického podpisu (SSCD/QSCD – 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/QSCD zariadeniu prostredníctvom príslušného CSP providera (implementácia MS Crypto API pre dané SSCD/QSCD zariadenie) alebo implementácie KSP providera CNG.

Pre aplikáciu D.Signer/XAdES .NET nie sú potrebné vyššie hardwarové požiadavky, ako vyžaduje samotný operačný systém, prípadne platforma .Net

[1] Pokiaľ je aplikácia D.Signer/XAdES .NET integrovaná v rámci web stránok web portálu.

framework 4.0 alebo vyššia. Požiadavky aplikácie na voľný priestor na disku sú nasledujúce:

Komponent	Veľkosť
D.Signer/XAdES .NET	4,45 MB
D.Signer/XAdES .NET – XML Plugin	1,67 MB
D.Signer/XAdES .NET – PDF Plugin[2]	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/kvalifikovaný 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	15,5 MB

Podrobný popis požiadaviek na prevádzku aplikácie D.Signer/XAdES .NET, teda požiadaviek na SSCD/QSCD 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.

[2] 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.

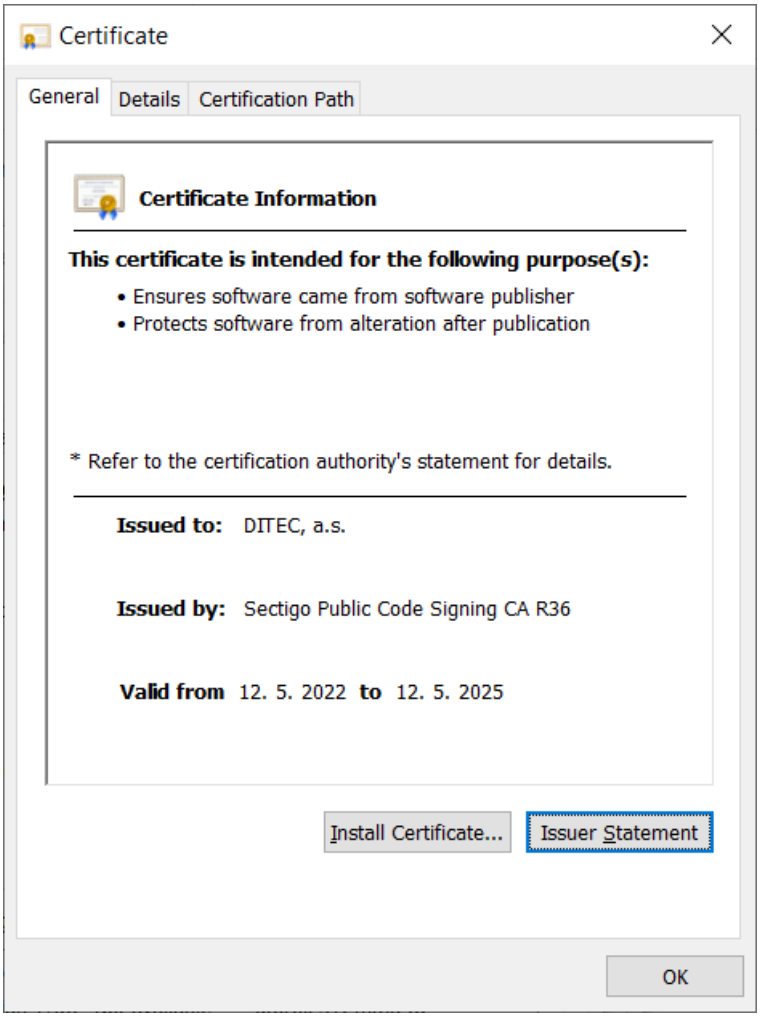
5. Inštalácia

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/KEP využíva a v rámci ktorej sa distribuuje),
3) inštalácia z Internetu – spustením inštalácie z web stránky Internetovej klientskej aplikácie, ktorá komponent pre ZEP/KEP 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 Sectigo, 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.



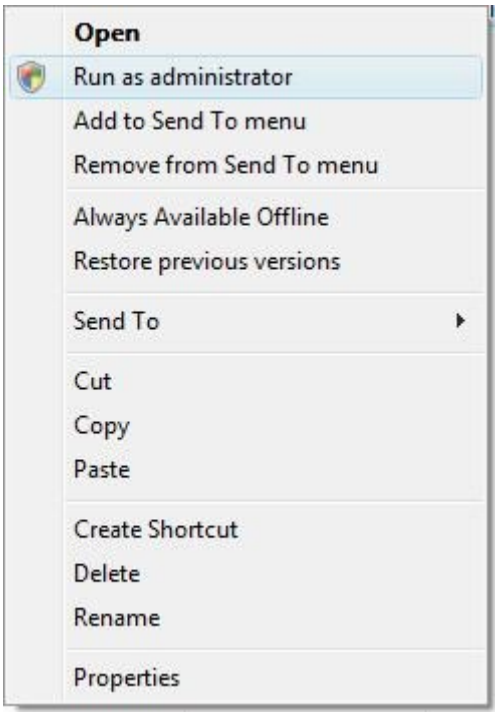
Okrem elektronického podpisu certifikátom spoločnosti DITEC, a.s. sú .Net assembly zabezpečené aj pomocou tzv. strong name. Pre príslušný počítač, na ktorom je aplikácia D.Signer/XAdES .NET nainštalovaná, resp. pre príslušnú klientsku aplikáciu musí byť vypnutý tzv. strong name bypass. Daná kontrola 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.[3]

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

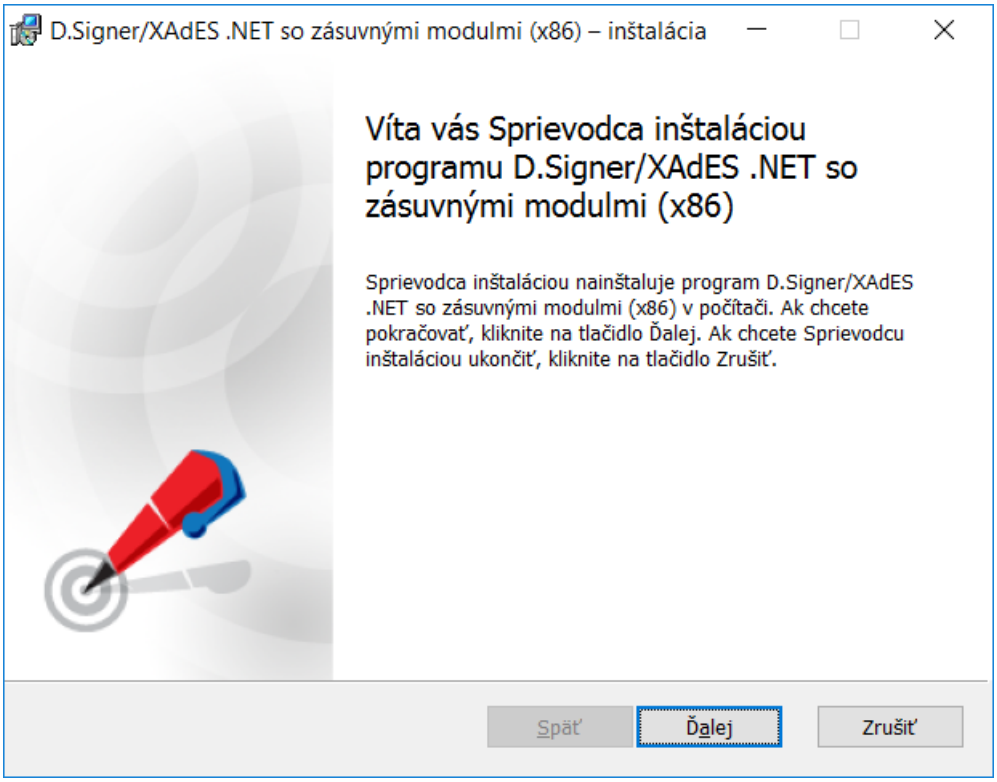
[3] Toto neplatí pre knižnice tretích strán, ktoré môže aplikácia D.Signer/XAdES .NET využívať. Tieto by mali byť chránené príslušným certifikátom ich výrobcu.

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

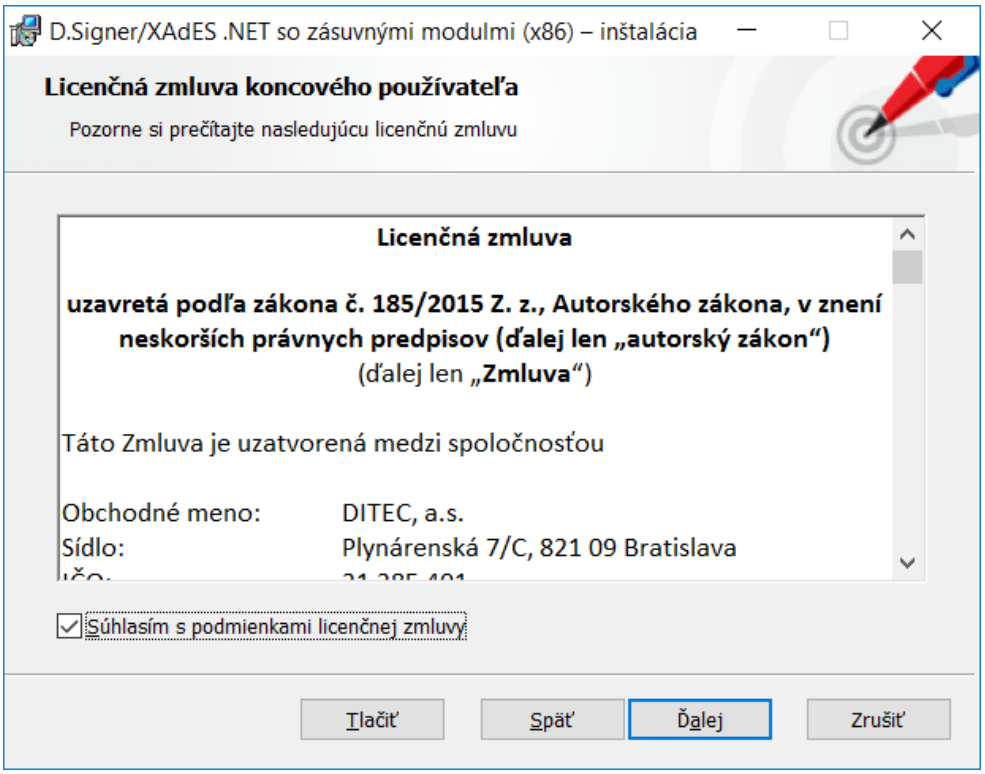


Pozor! Keďže pri inštalácii aplikácie D.Signer/XAdES .NET je potrebné zaregistrovať v rámci operačného systému Windows aj komponenty pre integráciu aplikácie D.Signer/XAdES .NET do web stránok internetových aplikácií, odporúčame pred spustením inštalačného programu zavrieť otvorené internetové prehliadače.

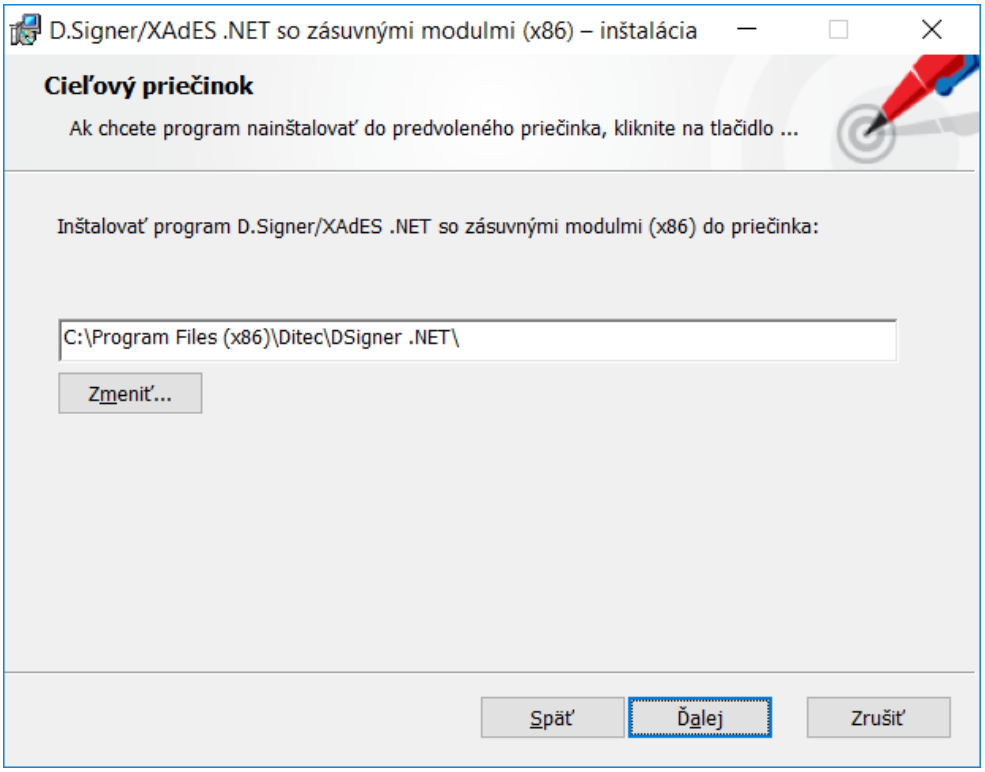
Po spustení inštalačného programu sa zobrazí úvodná obrazovka sprievodcu inštaláciou aplikácie D.Signer/XAdES .NET.



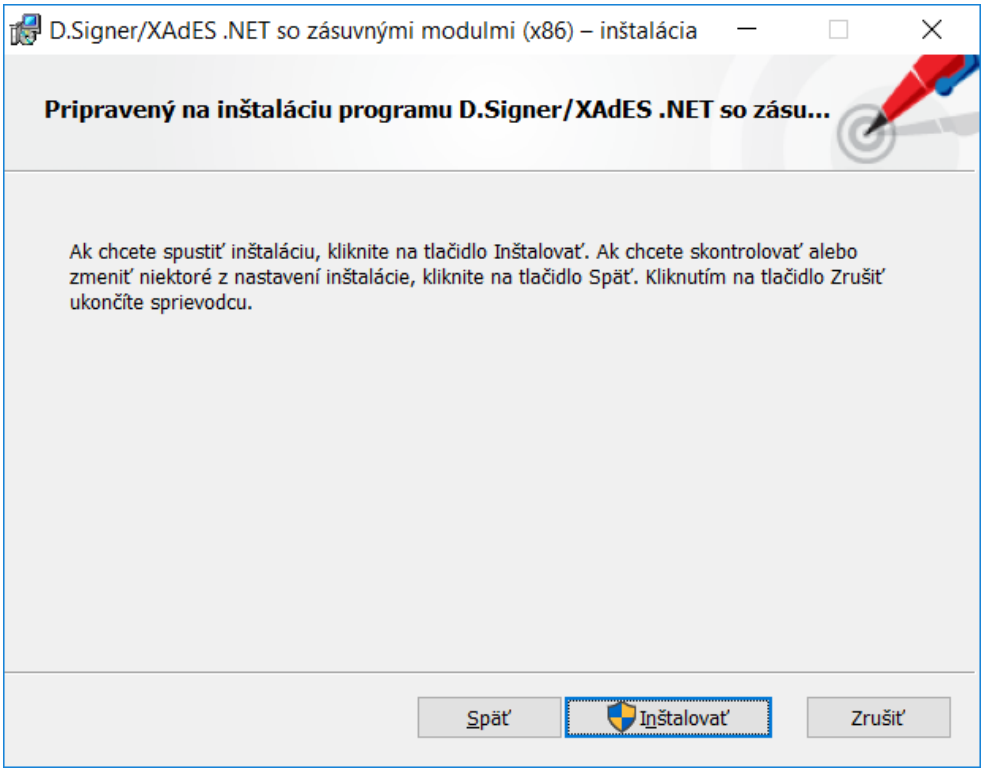
V nasledujúcom kroku je potrebné prečítať si a potvrdiť súhlas s licenčnou zmluvou pre aplikáciu D.Signer/XAdES .NET.



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

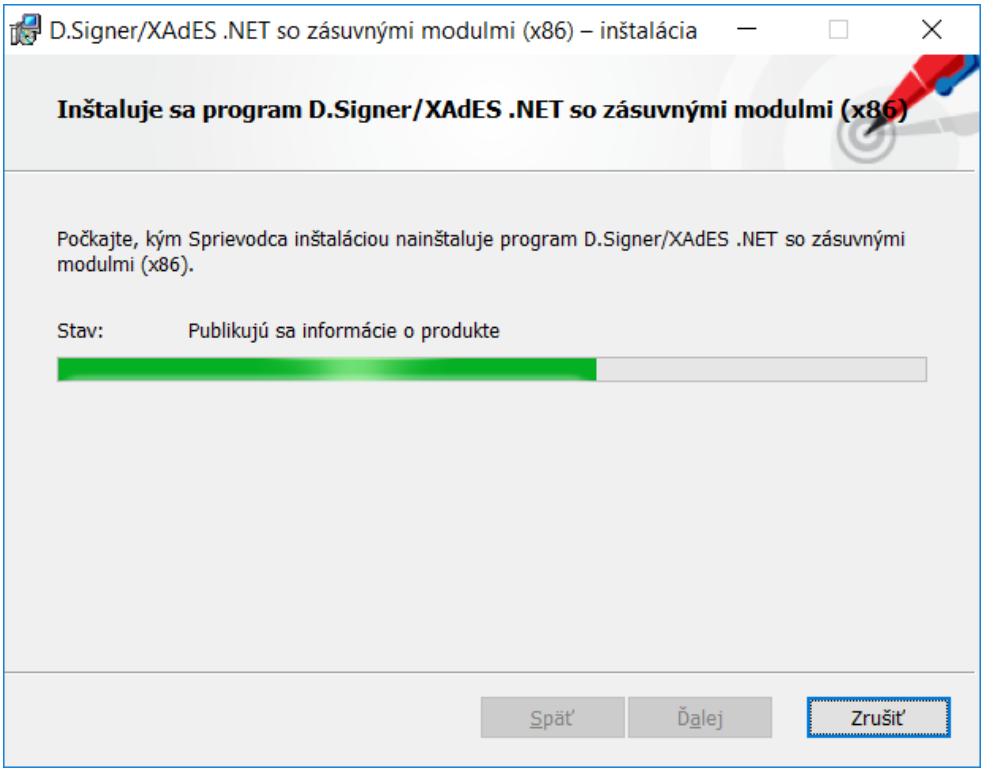


V ďalšom kroku potvrďte tlačidlom "Inštalovať" inštaláciu aplikácie D.Signer/XAdES .NET so zásuvnými modulmi (pluginmi) pre podpisovanie dátových objektov XML, PDF, TXT a PNG na váš počítač.

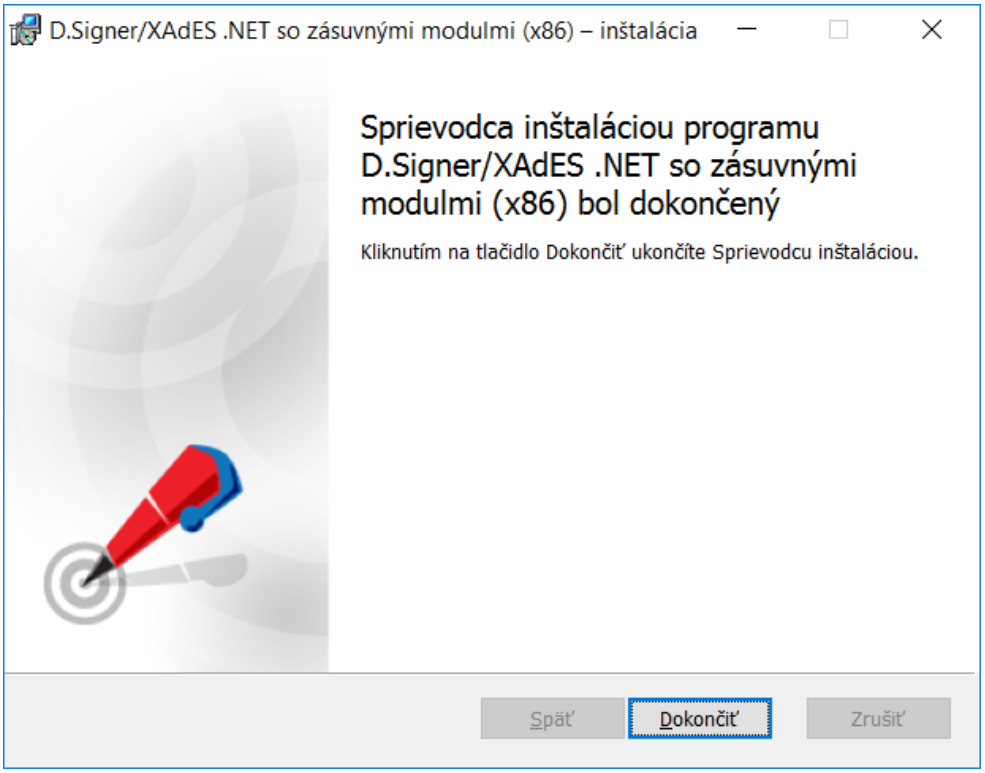


Kliknutím na tlačidlo "Inštalovať" sa spustí samotná inštalácia. Inštalačný program skopíruje požadované aplikačné súbory do špecifikovaného adresára a zabezpečí zaregistrovanie komponentov aplikácie D.Signer/XAdES .NET v rámci operačného systému Windows.

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".



Po ukončení inštalácie kliknite na tlačidlo "Dokončiť".



5.2. Inštalácia v rámci klientskej aplikácie

V prípade inštalácie aplikácie D.Signer/XAdES .NET v rámci inštalácie klientskej aplikácie (ktorá komponent pre zaručený/kvalifikovaný 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.

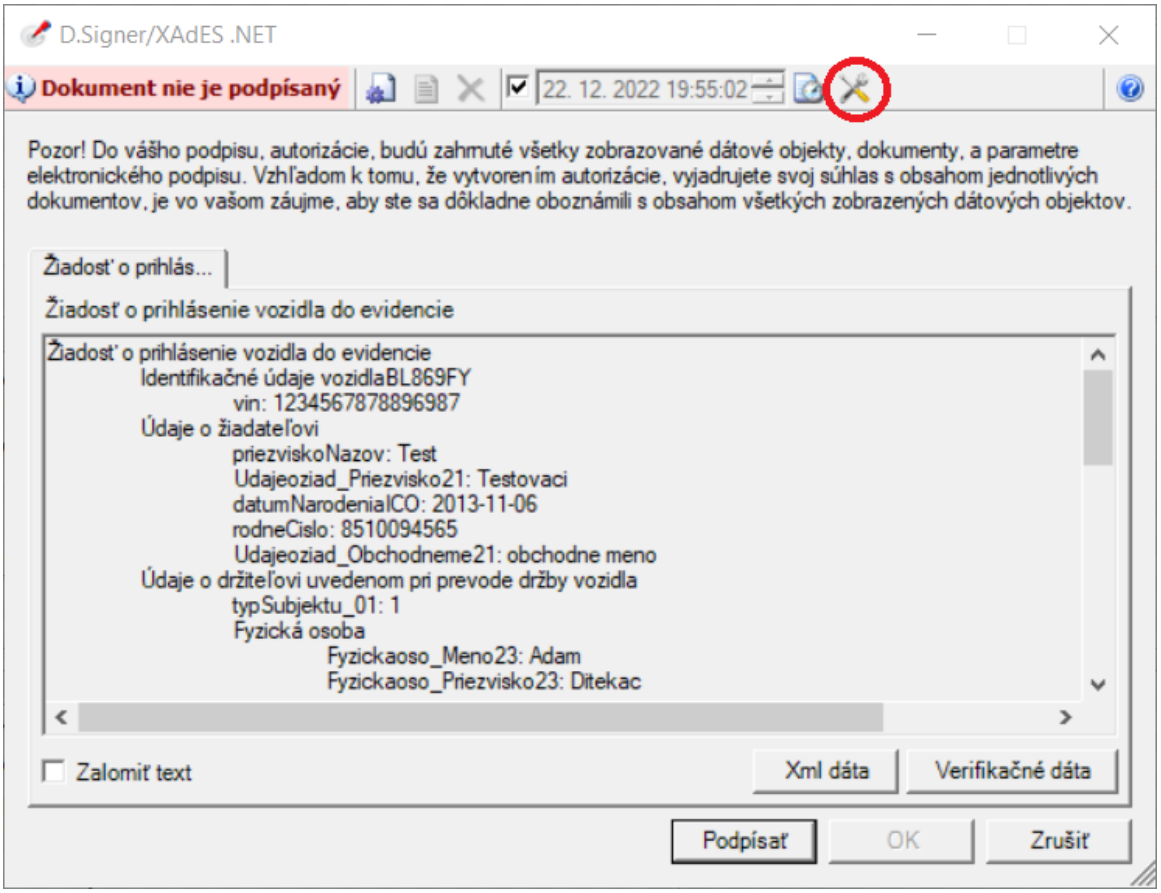
5.3. Inštalácia z Internetu

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.

6. Užívateľské nastavenia

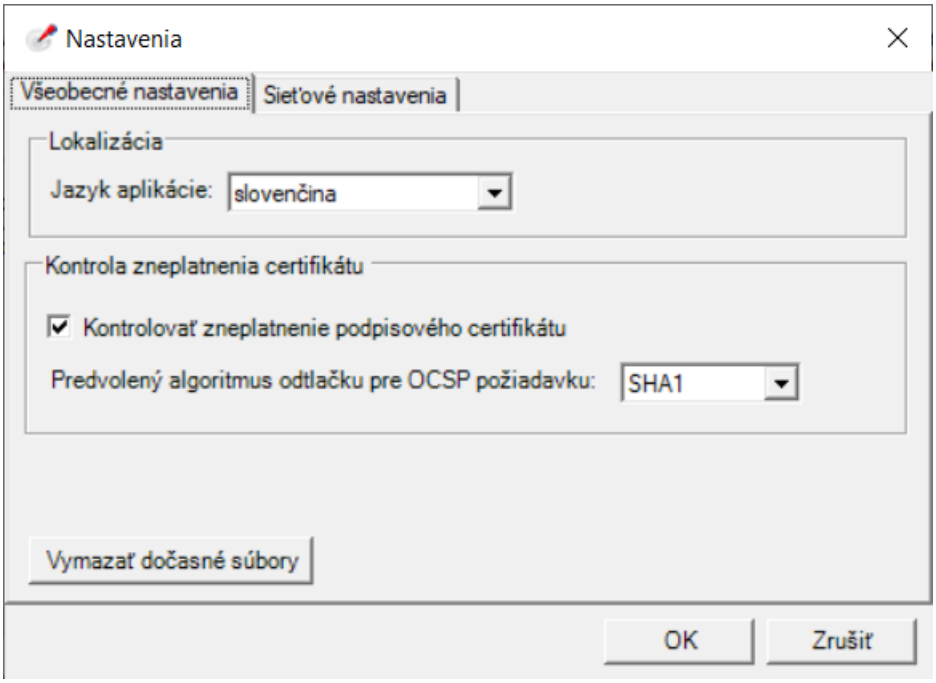
Obrazovka s užívateľskými nastaveniami aplikácie D.Signer/XAdES .NET je prístupná z hlavného okna aplikácie D.Signer/XAdES .NET prostredníctvom tlačidla "Nastavenia".



6.1. Všeobecné nastavenia aplikácie

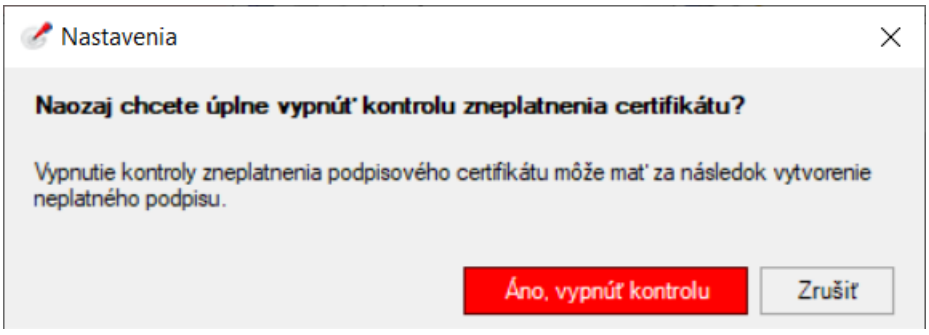
V rámci všeobecných nastavení aplikácie D.Signer/XAdES .NET môže používateľ zmeniť:

- nastavenie jazyka aplikácie,
- nastavenia kontroly zneplatnenia podpisového certifikátu pred podpisom.



Jazyk aplikácie D.Signer/XAdES .NET vyberá používateľ v rámci procesu inštalácie aplikácie. Nastavenie nového jazyka sa aplikuje pri ďalšom spustení aplikácie D.Signer/XAdES .NET. V prípade vynútenia jazyka aplikácie D.Signer/XAdES .NET z prostredia klientskej aplikácie nebude konfiguračné nastavenie jazyka aplikácie pre používateľa prístupné.

Aplikácia D.Signer/XAdES .NET pred vytvorením elektronického podpisu kontroluje, či zvolený podpisový certifikát nebol zneplatnený, resp. revokovaný. V prípade, že napríklad aplikácia nemá prístup na internet, je možné túto kontrolu v GUI Nastavenia aplikácie D.Signer/XAdES .NET vypnúť. Aplikácia v tom prípade vyžaduje potvrdenie vypnutia kontroly zneplatnenia certifikátu.



Pozor! Odporúčame nevypínať v konfiguračných nastaveniach kontrolu zneplatnenia podpisového certifikátu. Vypnutie kontroly zneplatnenia

podpisového certifikátu môže mať za následok vytvorenie neplatného podpisu.

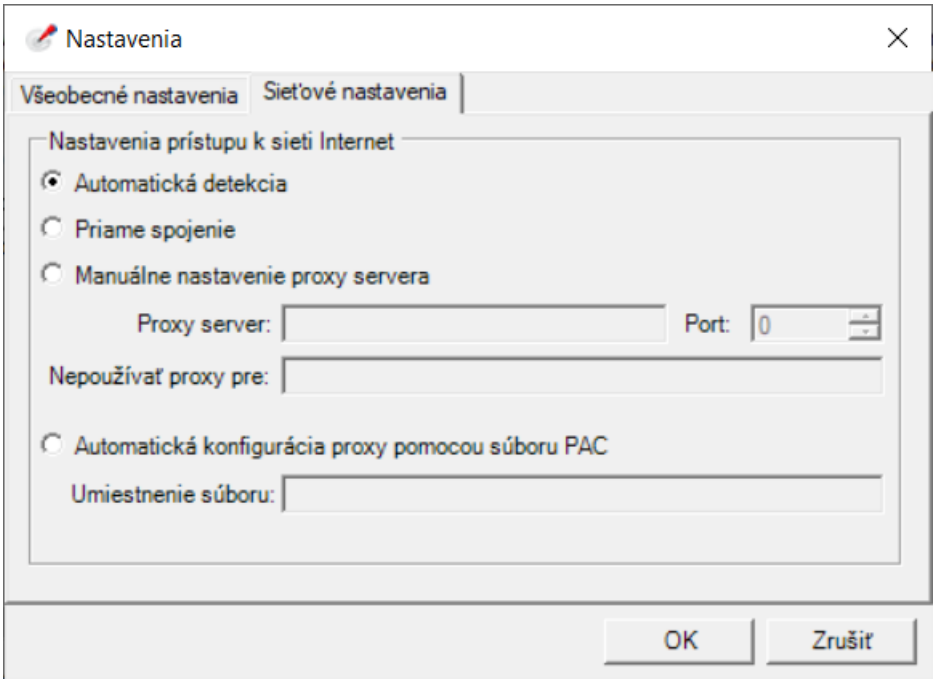
V nastaveniach kontroly zneplatnenia certifikátu je takisto možné zmeniť predvolený algoritmus odtlačku pre OCSP požiadavku v prípade, že certifikačná autorita, ktorá vydala podpisový certifikát podporuje pre OCSP službu iný algoritmus odtlačku pre OCSP požiadavku.

Tlačidlo "Vymazať dočasné súbory" slúži na vymazanie uložených informácií o stave zneplatnenia podpisových certifikátov.

6.2. Sieťové nastavenia

Konfigurácia sieťových nastavení umožňuje správne nastaviť prístup k sieti internet. Možnosti nastavenia prístupu sú nasledujúce:

- automatická detekcia,
- priame spojenie,
- manuálne nastavenie proxy servera,
- automatická konfigurácia proxy pomocou súboru PAC.



Odporúčame ponechať štandardné nastavenie – Automatická detekcia a len v prípade potreby neštandardnej konfigurácie prístupu k sieti internet sa obrátiť na administrátora vašej lokálnej siete, ktorý vám detaily nastavenia prístupu na internet cez proxy server poskytne.

7. Vytvorenie ZEP/KEP používateľom

7.1. Načítanie vstupných parametrov

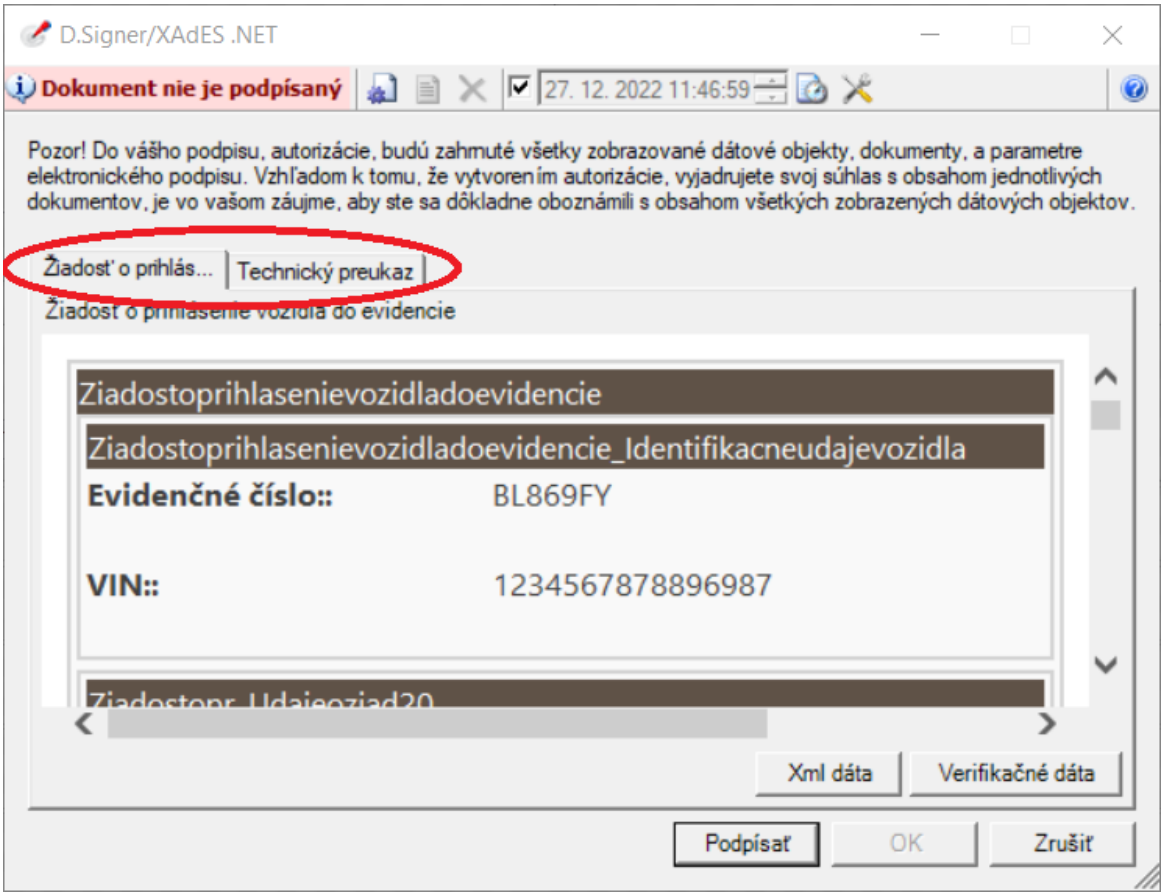
Po zavolaní funkcie pre vytvorenie elektronického podpisu, aplikácia D.Signer/XAdES .NET vykoná validáciu vstupných parametrov (teda jednotlivých podpisovaných častí *multipart* dokumentu) a zobrazí hlavné dialógové okno aplikácie. Spracovanie vstupných parametrov, najmä rozsiahlych dokumentov, môže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



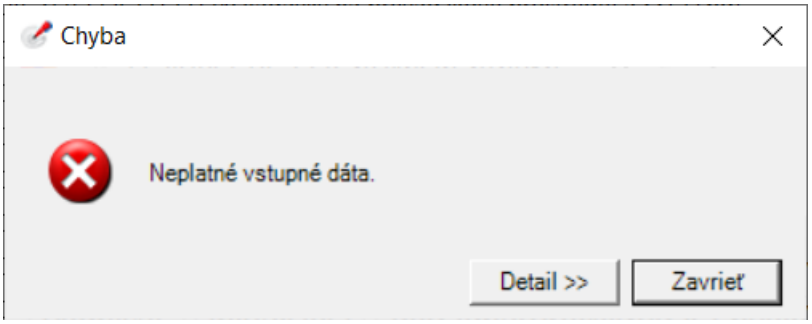
7.2. Zobrazenie podpisovaných dát

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.

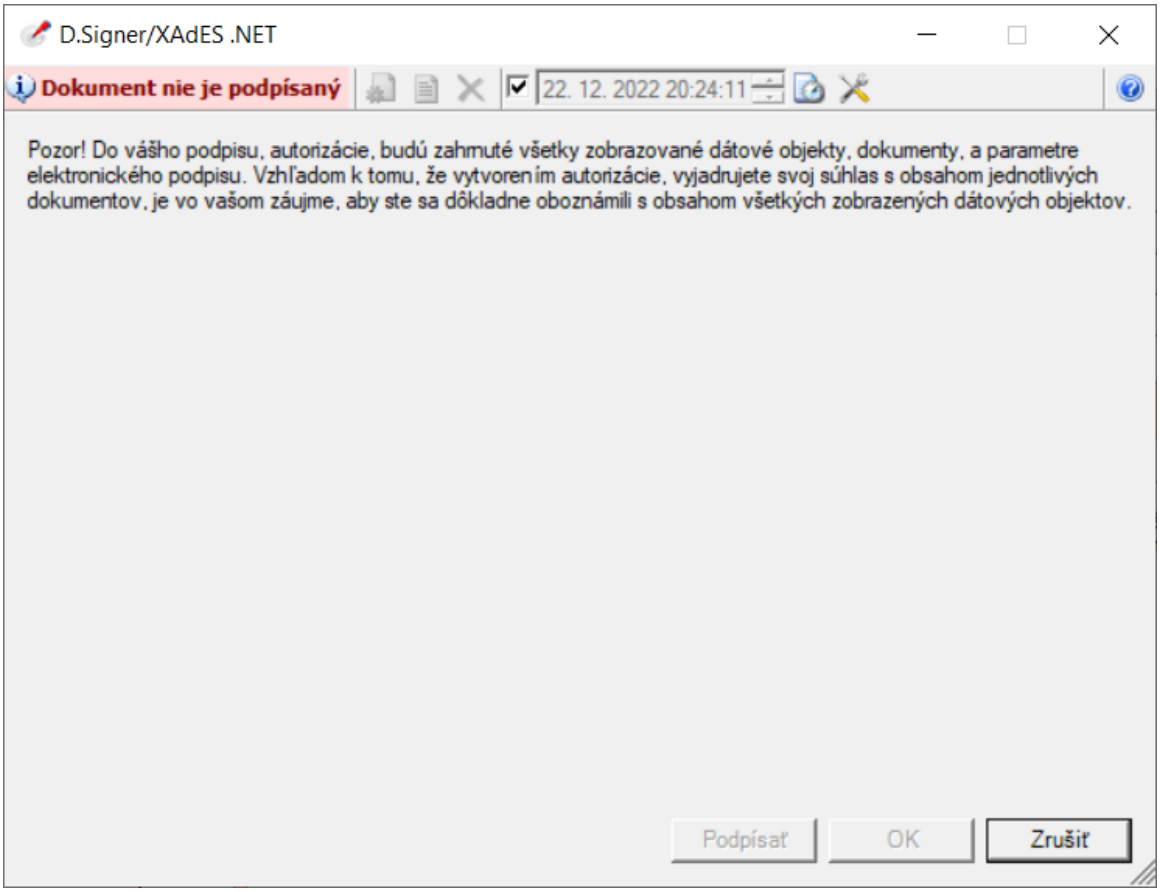
Pozor! Do vášho podpisu, autorizácie, budú zahrnuté všetky zobrazované dátové objekty, dokumenty, a parametre elektronického podpisu. Vzhľadom k tomu, že vytvorením autorizácie, vyjadrujete svoj súhlas s obsahom jednotlivých dokumentov, je vo vašom záujme, aby ste sa dôkladne oboznámili s obsahom všetkých 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).

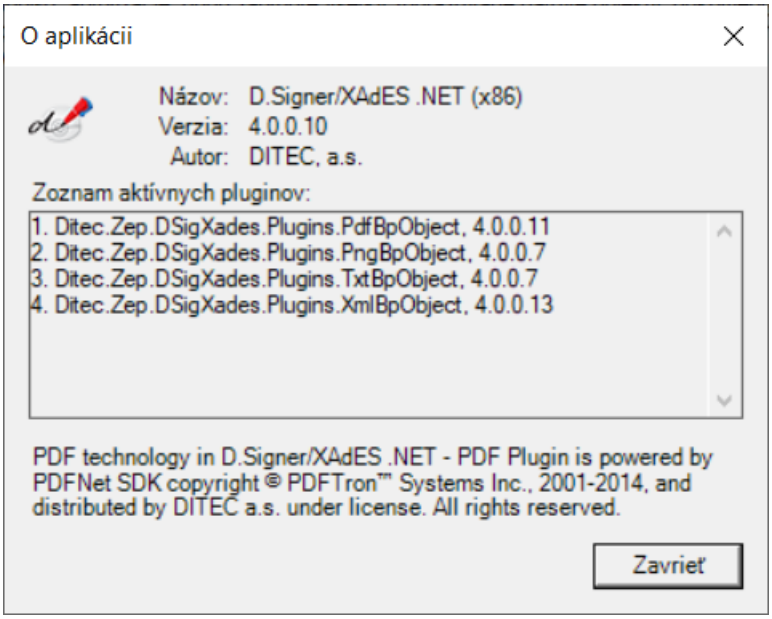


V rámci hlavného okna aplikcácie D.Signer/XAdES .NET je tiež zobrazený stav podpisovaného dokumentu, ktorý môže nadobúdať nasledujúce hodnoty:

- 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.

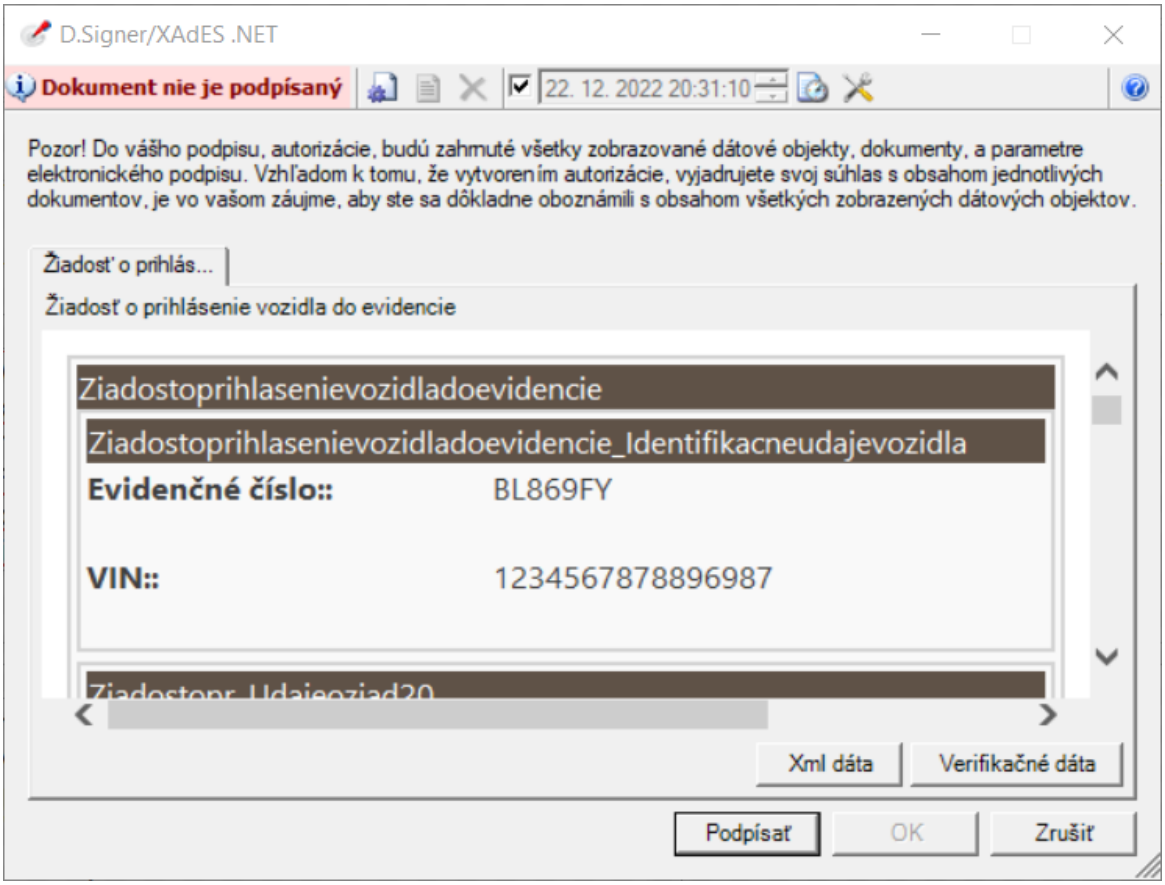
Aplikácia D.Signer/XAdES .NET slúži na vytváranie elektronického podpisu nad množinou rôznych formátov dokumentov, resp. typov dát (XML dokumenty, PDF dokumenty atď.), prípadne nad ľubovoľnou kombináciou podporovaných formátov dát, ktoré spolu vytvárajú tzv. *multipart* dokument. Pre jednotlivé požadované 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).



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.



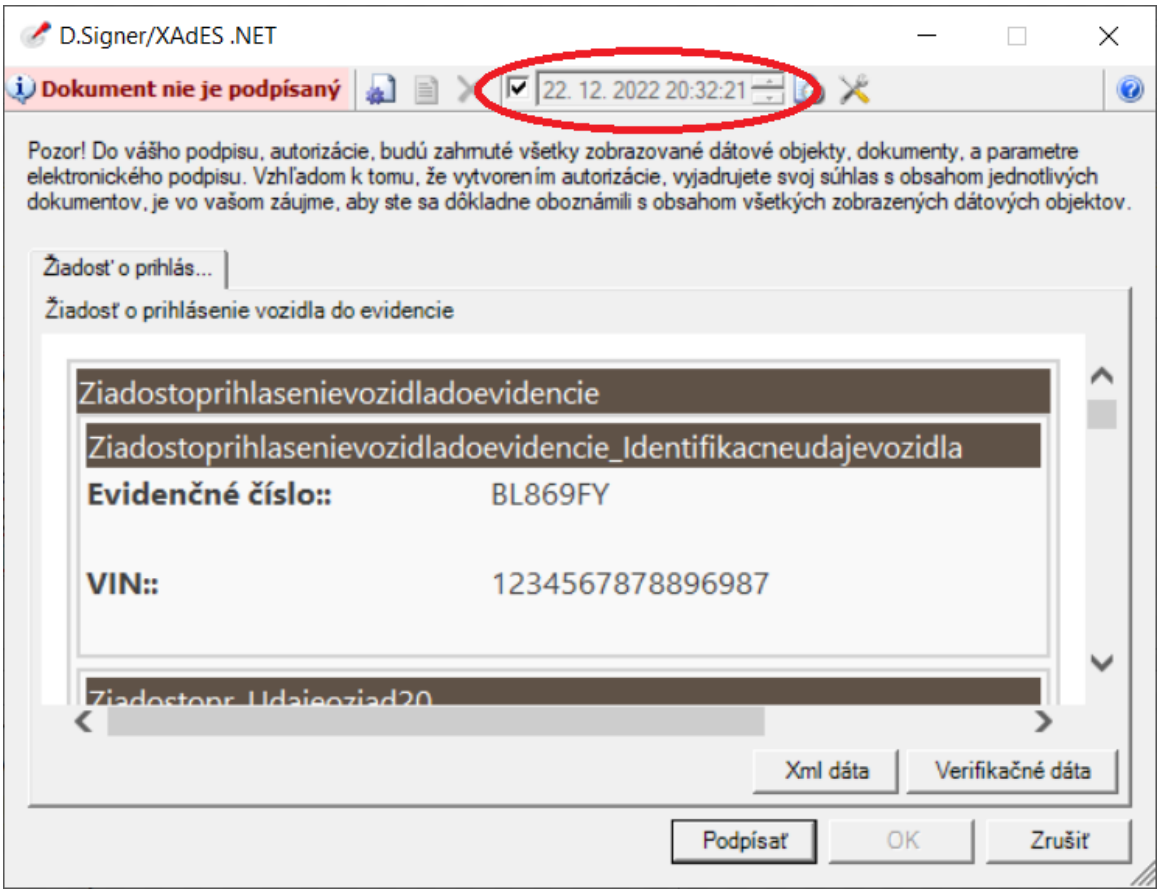
7.3. Nastavenie dátumu a času vytvorenia podpisu

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.

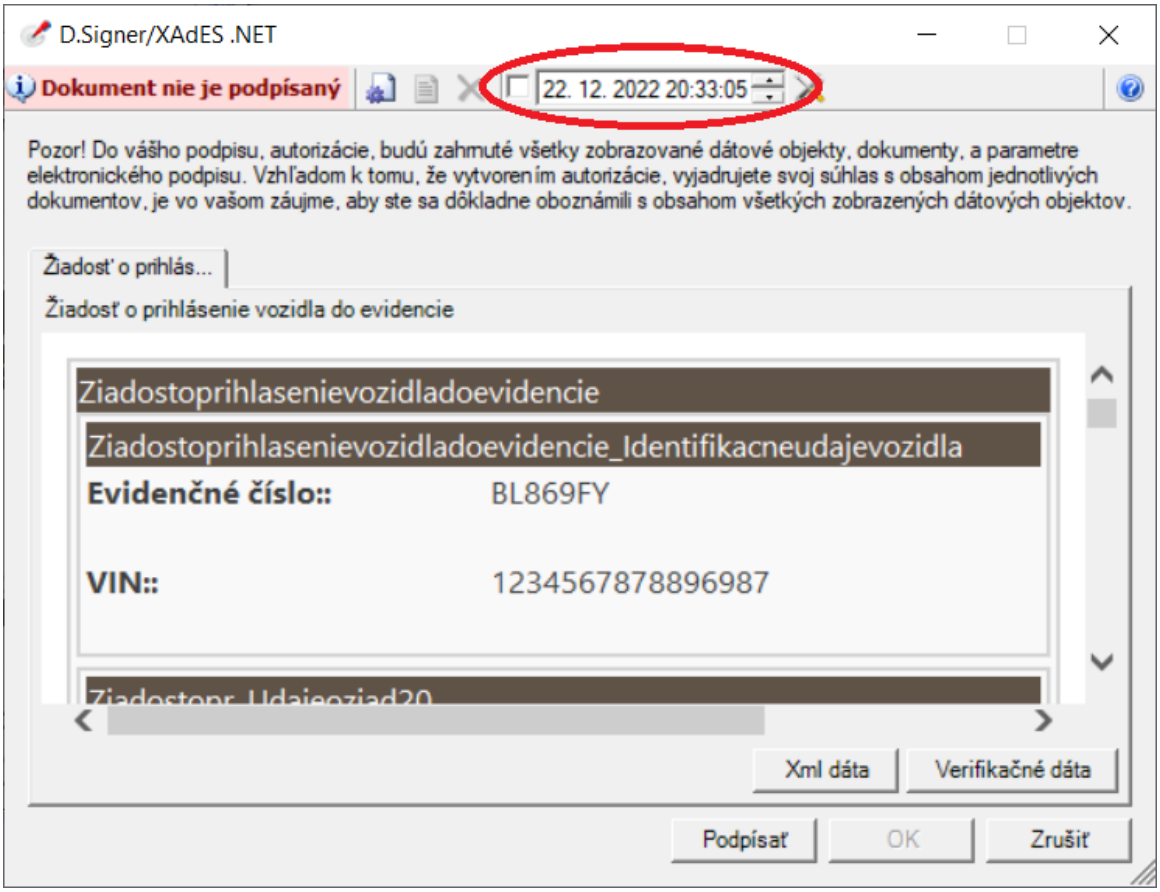
Aplikácia umožňuje používateľovi deklarovať ako čas vytvorenia podpisu:

- 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.

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).

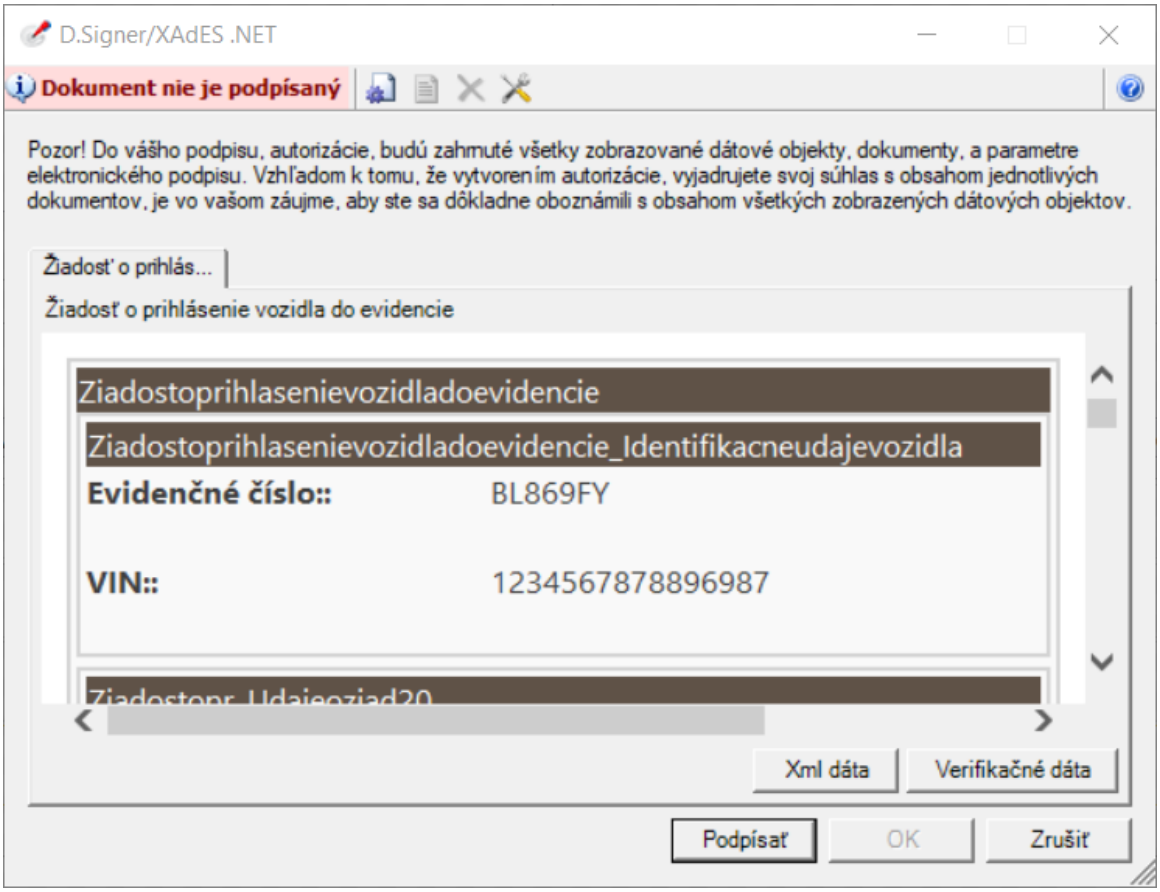


V druhom prípade sa používateľovi sprístupní deklarovaný dátum a čas vytvorenia podpisu na editovanie.



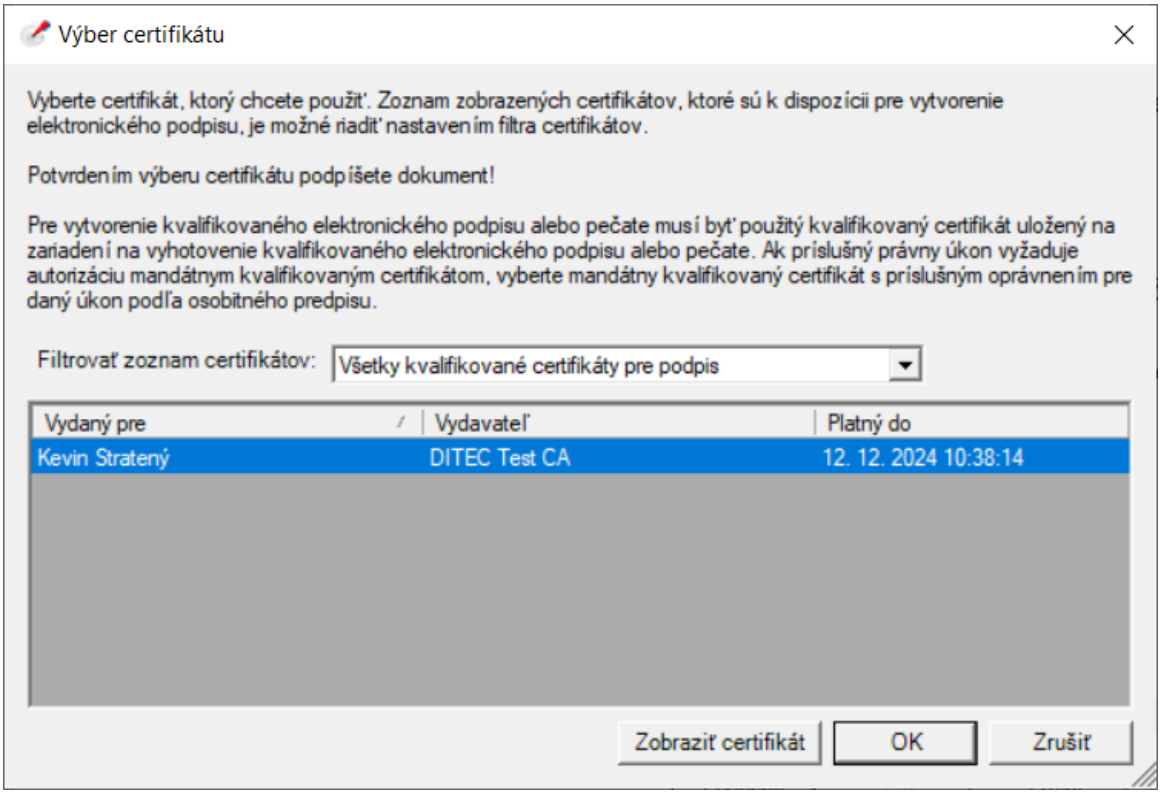
Pozor! Pri vytváraní elektronického podpisu odporúčame použiť správne nastavený aktuálny systémový dátum a čas.

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.



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.



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.

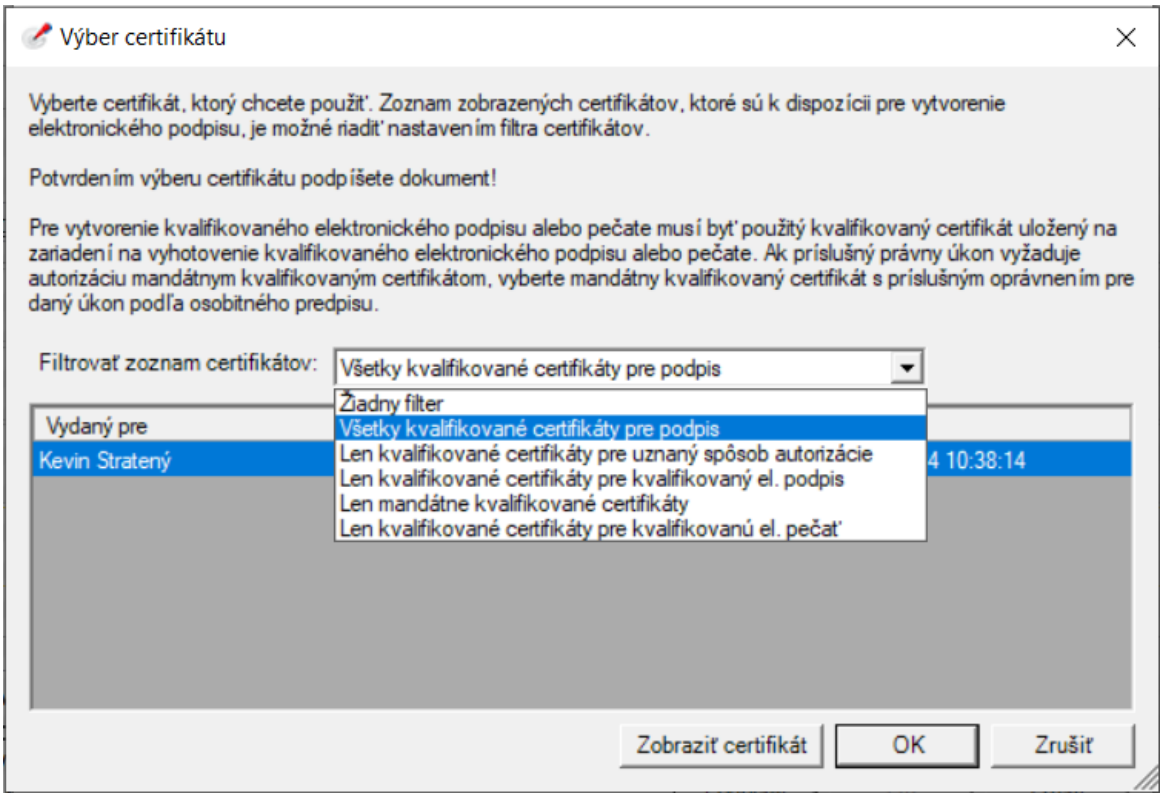
Aplikácia D.Signer/XAdES .NET ponúkne na výber len certifikáty, ktorým ešte neuplynul dátum exspirácie. Detaily zvoleného certifikátu je možné prezrieť kliknutím na tlačidlo "Zobraziť certifikát".

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/kvalifikovaného elektronického podpisu musí podpisovateľ zvoliť zo svojho personálneho úložiska certifikátov kvalifikovaný certifikát, ktorý bol vydaný poskytovateľom dôveryhodnej služby vydávania kvalifikovaných certifikátov. Ak príslušný právny úkon vyžaduje autorizáciu mandátnym kvalifikovaným certifikátom, používateľ musí zvoliť mandátny kvalifikovaný certifikát s príslušným oprávnením pre daný úkon podľa osobitného predpisu. Ak príslušný právny úkon umožňuje použiť kvalifikovaný certifikát pre uznaný spôsob autorizácie, používateľ si ich môže zobraziť nastavením filtra certifikátov na položku "Len kvalifikované certifikáty pre uznaný spôsob

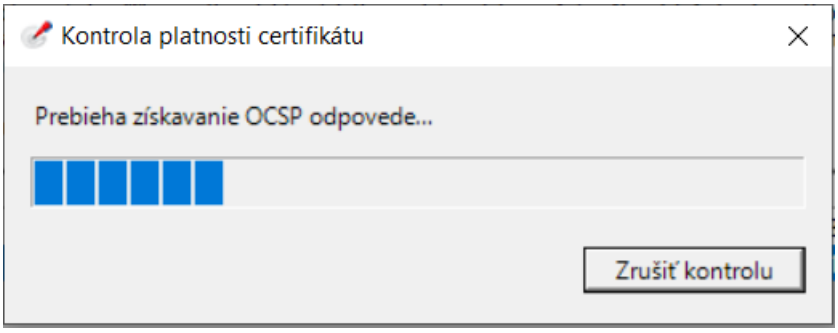
autorizácie". Pre vytvorenie obyčajného elektronického podpisu nie je potrebné použiť kvalifikovaný certifikát.

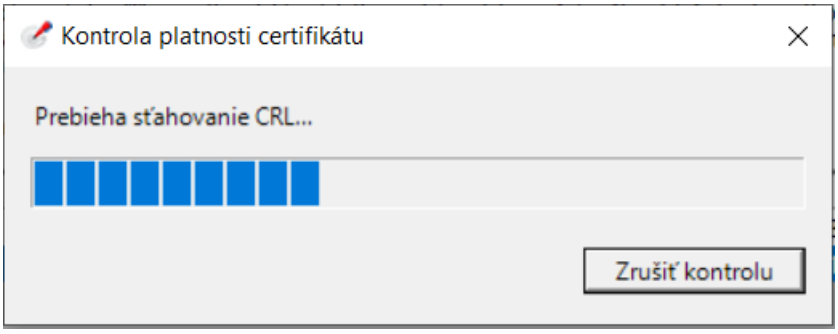
Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov v okne pre výber certifikátu v aplikácii D.Signer/XADES .NET.



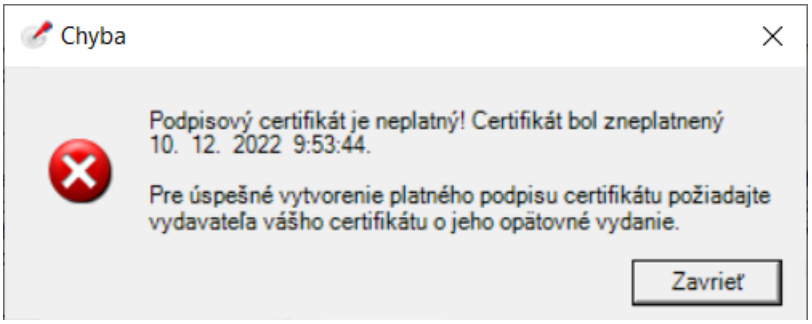
Po zvolení podpisového certifikátu a potvrdení výberu tlačidlom "OK" aplikácia D.Signer/XAdES .NET vykoná kontrolu stavu zneplatnenia podpisového certifikátu.[4] Primárne aplikácia vykoná kontrolu zneplatnenia zvoleného podpisového certifikátu pomocou služby OCSP. Ak je kontrola neúspešná, napr. z dôvodu nedostupnej služby OCSP, tak aplikácia vykoná kontrolu zneplatnenia zvoleného podpisového certifikátu aj pomocou CRL.

[4] V prípade, že kontrola zneplatnenia podpisového certifikátu je v konfiguračných nastaveniach aplikácie D.Signer/XAdES .NET zapnutá.



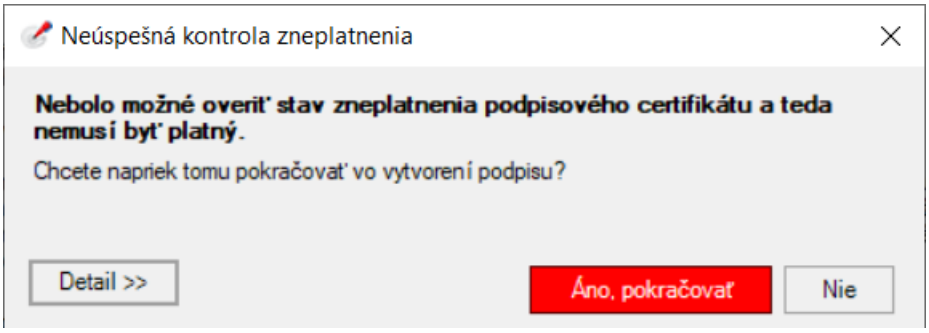


Ak aplikácia zistí, že certifikát bol zneplatnený, tak o tom informuje používateľa s odporúčaním, aby požiadal vydavateľa svojho certifikátu o jeho opätovné vydanie, a nepokračuje vo vytvorení elektronického podpisu.



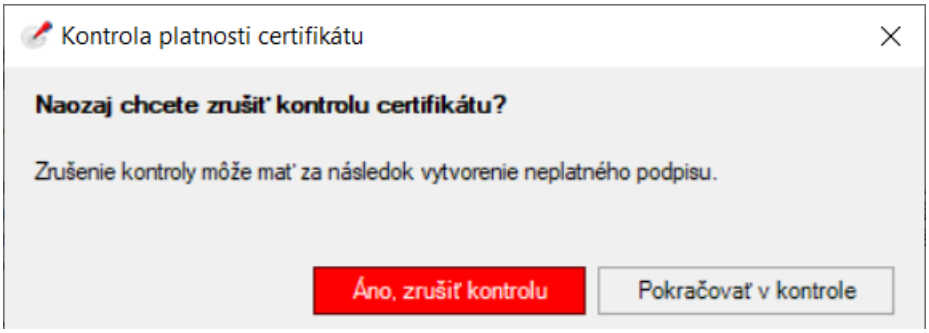
Ak je kontrola zneplatnenia zvoleného podpisového certifikátu neúspešná, tak aplikácia zobrazí upozornenie, že nebolo možné overiť stav zneplatnenia podpisového certifikátu a teda certifikát nemusí byť platný. Zároveň ponúkne používateľovi možnosti:

- Áno, pokračovať – vo vytvorení podpisu,
- Nie – nepokračovať vo vytvorení podpisu.



Ak kontrola zneplatnenia podpisového certifikátu trvá príliš dlho napr. z dôvodu slabého internetového pripojenia, používateľ má možnosť kontrolu zneplatnenia zrušiť kliknutím na tlačidlo "Zrušiť kontrolu". Vtedy aplikácia D.Signer/XAdES .NET upozorní používateľa, že zrušenie kontroly môže mať za následok vytvorenie neplatného podpisu a vyžaduje potvrdenie zrušenia kontroly zneplatnenia, teda zobrazí okno s možnosťami:

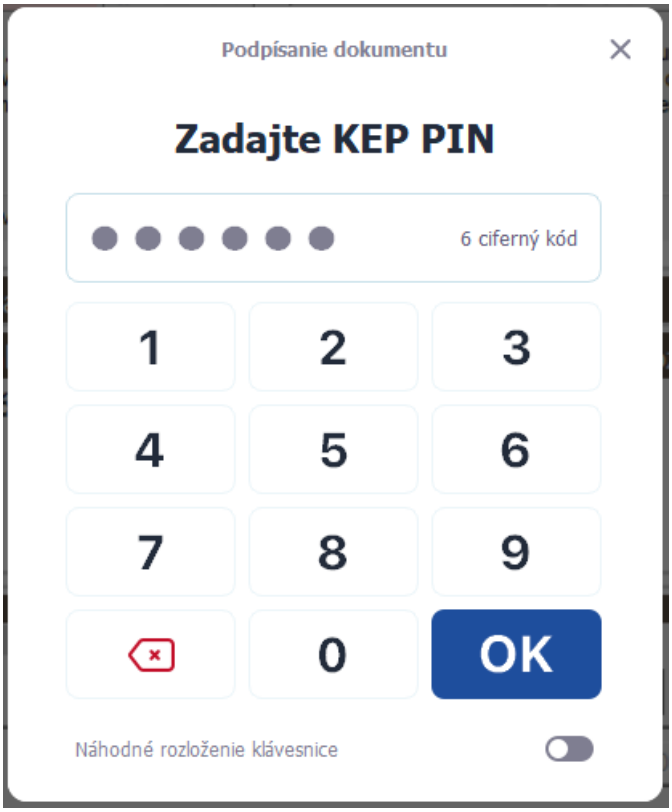
- Áno, zrušiť kontrolu,
- Pokračovať v kontrole.



Pozor! Odporúčame nerušiť kontrolu zneplatnenia podpisového certifikátu. Zrušenie kontroly zneplatnenia podpisového certifikátu môže mať za následok vytvorenie neplatného podpisu.

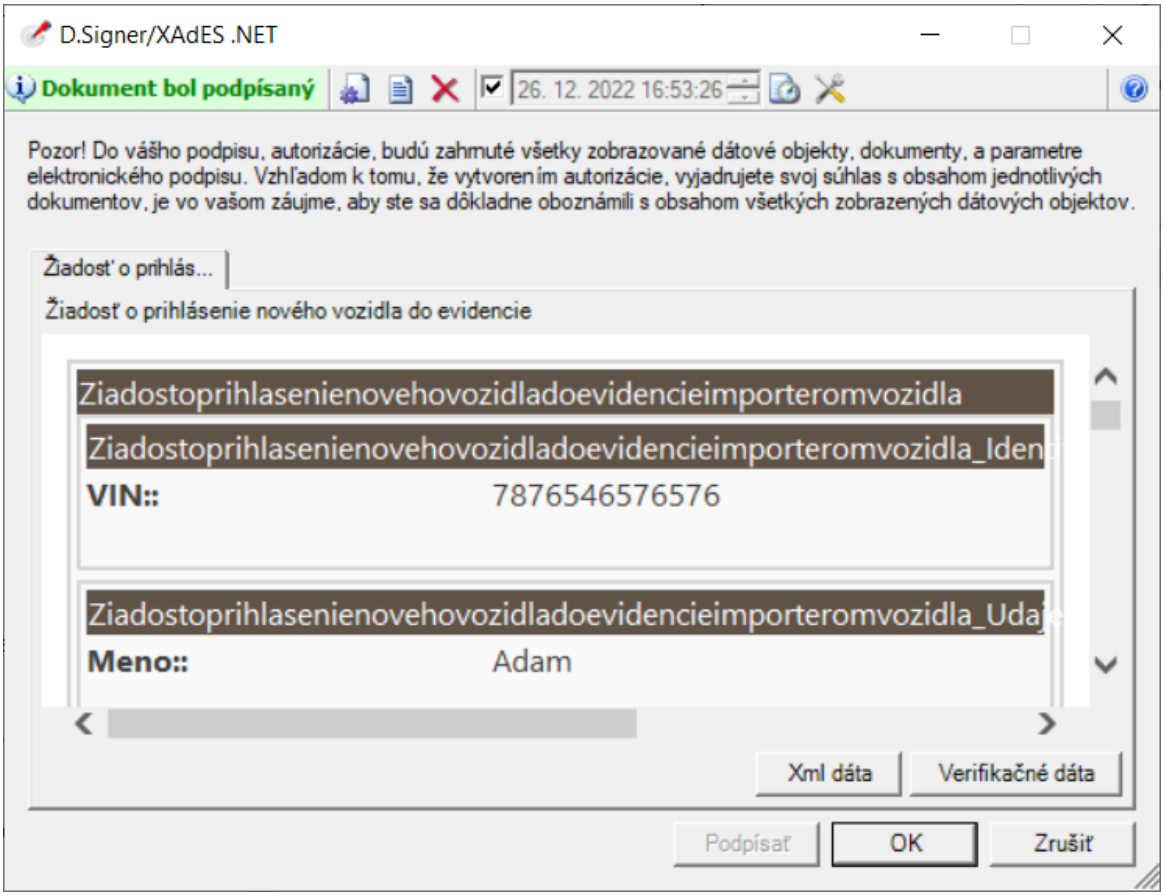
Ak aplikácia pomocou kontroly zneplatnenia zistí, že certifikát je platný, vykoná proces vytvorenia elektronického podpisu. Aplikácia D.Signer/XAdES .NET vytvorí reprezentáciu podpisovaných dát a parametrov podpisu – digitálny odtlačok. Pomocou rozhrania MS CryptoAPI alebo CNG a príslušného SSCD/QSCD zariadenia, na ktorom je uložený privátny kľúč patriaci k zvolenému podpisovému certifikátu, vytvorí hodnotu elektronického podpisu. Sprístupnenie privátneho kľúča na SSCD/QSCD zariadení môže vyžadovať autentifikáciu používateľa – zadanie BOKu[5] a/alebo PINu.[6]

[5] Bezpečnostný osobný kód.



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).

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

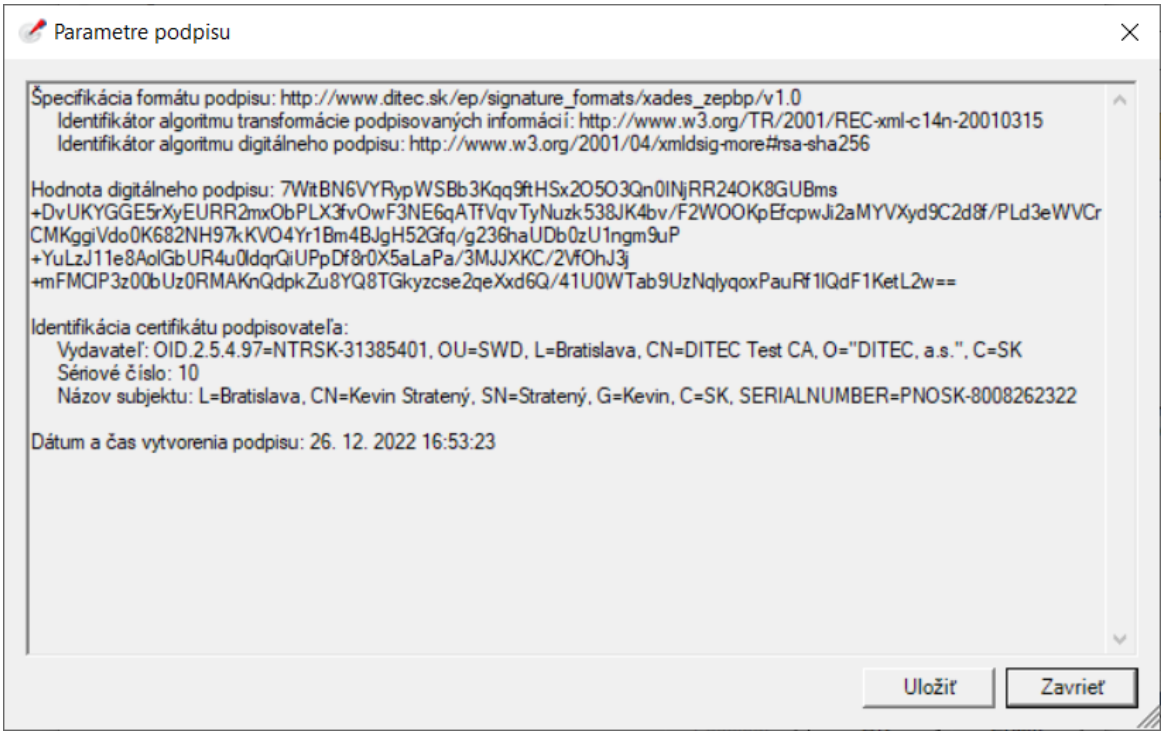


Po úspešnom vytvorení elektronického podpisu je podpísaný dokument odovzdaný klientskej aplikácii až po kliknutí na tlačidlo "OK".

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 uviesť tak aplikáciu do východzieho stavu.

8. Trademarks

PDF technology in D.Signer/XAdES .NET - PDF Plugin is powered by PDFNet SDK copyright © PDFTron™ Systems Inc., 2001-2020, and distributed by DITEC a.s. under license. All rights reserved.



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