DITEC
Data Information Technology & Expert Consulting

Používateľská príručka
D.Signer/XAdES Java, v2.0

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 Java, v2.0		
Ref. číslo	GOV_ZEP.212	Verzia	10

Vypracoval	Vittek Róbert	Podpis	Dátum 31. 7. 2024
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.212	Verzia	10

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. Distribúcia a inštalácia 12

6. Užívateľské nastavenia 15

6.1. Nastavenie spôsobu prístupu k SSCD/QSCD a podpisovým certifikátom 15

6.2. Všeobecné nastavenie aplikácie 20

6.3. Sieťové nastavenia 21

7. Vytvorenie ZEP/KEP používateľom 23

7.1. Načítanie vstupných parametrov 23

7.2. Súhlas s licenčnou zmluvou 23

7.3. Zobrazenie podpisovaných dát 24

7.3.1. Zobrazenie dokumentov 26

7.4. Nastavenie dátumu a času vytvorenia podpisu 27

7.5. Podpísanie dokumentu 30

7.6. Zobrazenie parametrov podpisu 37

8. Trademarks 39

1. Úvod

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

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

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 Java 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 Java 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 Java 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 Java 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 Java 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 Java 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 Java 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 Java môže byť použitá taktiež pre vytváranie tzv. obyčajného elektronického podpisu zmysle zákona č. 215/2002 Z.z. o elektronickom podpise.

V súlade s §4, odsek (5) zákona č. 305/2013 Z.z. o e-Governmente v znení neskorších predpisov je aplikácia D.Signer/XAdES Java implementovaná takým spôsobom, aby poskytovala funkcionalitu vytvorenia ZEP/KEP 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.

4. Systémové požiadavky

Systémové požiadavky aplikácie D.Signer/XAdES Java sú nasledujúce:

- operačný systém MS Windows 7 / 8 / 10 / 11, Mac OS X: verzia 10.12 – 10.15, 11, 12, procesor (architektúra CPU): x86_64, arm (M1), prekladač Rosetta 2 – v prípade procesora arm (M1), GNU/Linux: Mint verzia 13, 17.x, 18, 19.x, 20.0, 20.1, 20.2, 20.3; Debian verzia 8, Mint Debian Edition 4, 5; Ubuntu verzia 12.04 LTS, 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS, 21.04, 21.10, 22.04; Fedora: verzia 23, 24, 25, 33, 34, 35, 36; Manjaro 21.0, 21.2.2,
- ak je aplikácia D.Sig XAdES Extender Java spúšťaná z web portálu pomocou aplikácie D.Launcher v1.x:
  - ⇒ Oracle Java 8 (https://www.java.com/en/download/manual.jsp), pozn. kombinácia OpenJDK a IcedTea nie je podporovaná,
  - ⇒ Java plugin do webového prehliadača, Java Web Start a Java FX verzia 2.1 a vyššia (súčasť inštalácie Oracle Java),
- 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); prípadne PKCS#12 súbor ako úložisko podpisového certifikátu,
- príslušná CSP implementácia MS CryptoAPI, alebo implementácia KSP CNG (iba MS Windows), alebo implementácia PKCS #11 rozhrania (32 bit / 64 bit podľa platformy Java); súčasť softvéru dodávaného s SSCD/QSCD zariadením,
- web prehliadač podporujúci spúšťanie Java appletov[1] – MS Internet Explorer v7.0 alebo vyššia (len 32 bit), Mozilla Firefox, v45 – v51, resp. v59 ESR (len 32 bit, s podporou NP API), Safari 14, 15,
- prístup na internet (prípadne správne nastavenia pre proxy),
- správne nastavený aktuálny systémový dátum a čas.

Ak je aplikácia D.Signer/XAdES Java 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.

V tomto prípade je Java plugin vyžadovaný pre MS Internet Explorer 7/8/9, voliteľný pre MS Internet Explorer 10/11; môže byť nutné ho v prehliadači MS Internet Explorer povoliť pomocou voľby Tools/Manage add-ons. Systémové

[1] Ak je aplikácia D.Signer/XAdES Java spúšťaná ako Java applet.

požiadavky pre aplikáciu D.Launcher sú špecifikované v rámci používateľskej príručky pre aplikáciu D.Launcher.

Ak je aplikácia D.Sig XAdES Extender Java spúšťaná z web portálu pomocou aplikácie D.Launcher v2.x a rozšírenia D.Bridge 2:

- webový prehliadač – MS Internet Explorer 11 (len 32bit verzia), Mozilla Firefox 78, 89, 91, 101, Google Chrome 91, 100, 101, Chromium 91, 100, 101, Opera 76, 78, Microsoft Edge 91, 96, 97,
- vo webovom prehliadači nainštalované a povolené rozšírenie D.Bridge 2, pre MS Internet Explorer sa vyžaduje vypnutý chránený režim.

Pri vytváraní zaručeného/kvalifikovaného elektronického podpisu pomocou aplikácie D.Signer/XAdES Java 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 Java. Aplikácia D.Signer/XAdES Java pristupuje k danému SSCD/QSCD zariadeniu prostredníctvom príslušného CSP providera (implementácia MS Crypto API pre dané SSCD/QSCD zariadenie), alebo implementácie KSP providera CNG, alebo prostredníctvom príslušnej implementácie PKCS#11 rozhrania.

Pri vytváraní tzv. obyčajného elektronického podpisu pomocou aplikácie D.Signer/XAdES Java nie je potrebné použiť kvalifikovaný certifikát vydaný akreditovanou certifikačnou autoritou, ani certifikované SSCD/QSCD zariadenie. Použitá podpisová politika by mala jasne deklarovať, o aký elektronický podpis ide.

Veľkosť distribučných súborov jednotlivých komponentov aplikácie D.Signer/XAdES Java je uvedená v nasledujúcej tabuľke.

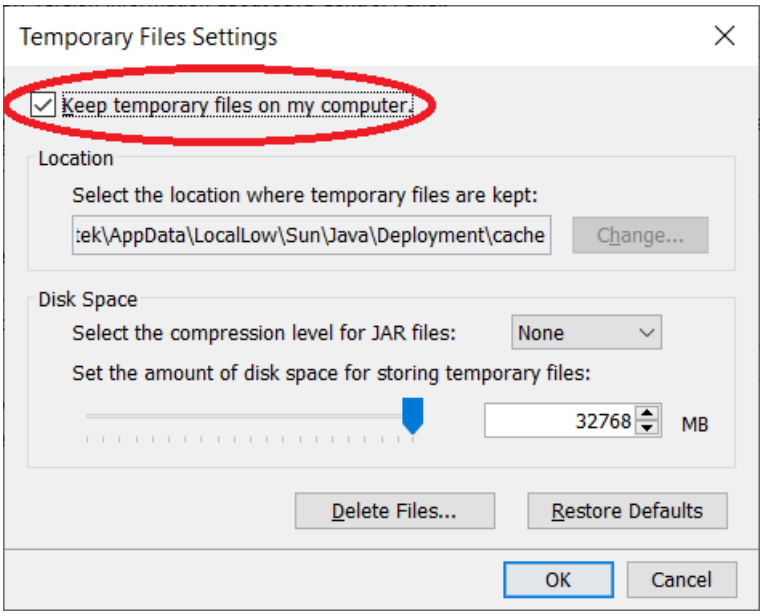
Komponent	**Veľkosť**
D.Signer/XadES Java	10,5 MB
D.Signer/XAdES Java – XML Plugin	450 kB
D.Signer/XAdES Java – PDF Plugin[2]	11,3 MB (MS Windows) 11,6 MB (GNU/Linux)

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

	20,4 MB (Mac OS X)
D.Signer/XAdES Java – TXT Plugin	40 kB
D.Signer/XAdES Java – PNG Plugin	45 kB

Tzn. že pre konkrétnu platformu (OS, 32/64-bit) je veľkosť distribučných súborov cca 22,5 – 32 MB; ak sú skomprimované, tak dokonca len 15 – 25 MB.

Aplikácia D.Signer/XAdES Java vyžaduje, aby bolo v nastaveniach Java povolené ukladanie dočasných súborov. Toto nastavenie je prístupné z Java Control Panel a prednastavená hodnota je povolené ukladanie dočasných súborov.

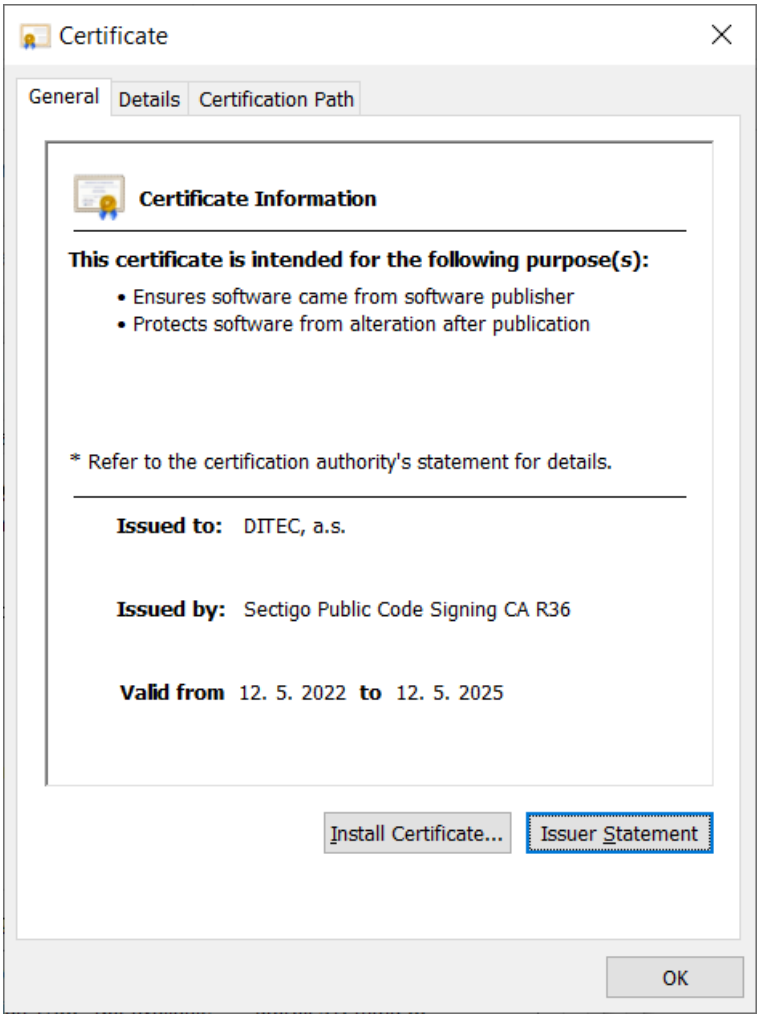


Podrobný popis požiadaviek na prevádzku aplikácie D.Signer/XAdES Java, teda požiadaviek na SSCD/QSCD zariadenie, požiadaviek na prevádzkové prostredie aplikácie, bezpečnostných požiadaviek apod. je špecifikovaný v rámci dokumentu Požiadavky na prevádzkové prostredie a SSCD.

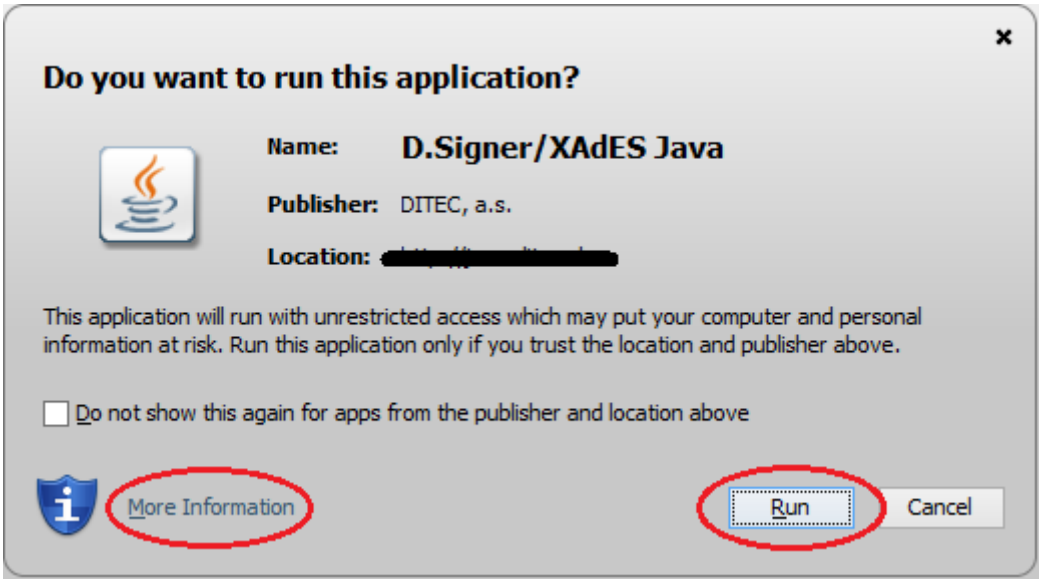
5. Distribúcia a inštalácia

Aplikácia D.Signer/XAdES Java môže byť integrovaná ako applet v rámci web aplikácie alebo ako komponent v rámci klientskej Java aplikácie bežiacej v JRE. Ak je distribúcia a inštalácia aplikácie D.Signer/XAdES Java na PC používateľa zabezpečená pomocou technológie webstart, tak integritu súborov aplikácie overuje technológia webstart pri spustení aplikácie. Jednotlivé JAR knižnice sú podpísané certifikátom výrobcu aplikácie (spoločnosť DITEC, a.s.) a je na ne vyžiadaná časová pečiatka.

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

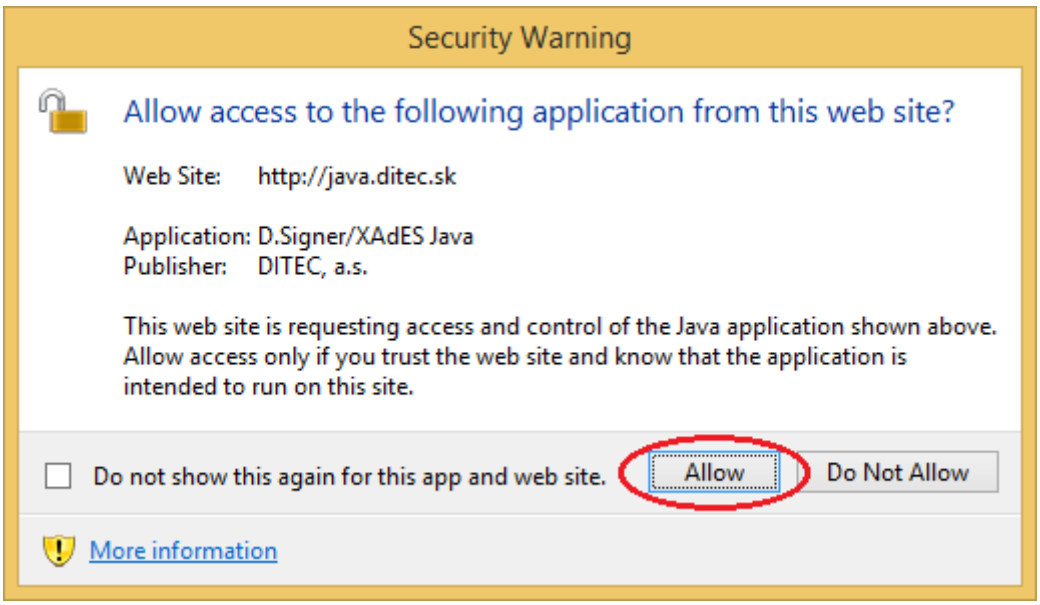


Používateľ si môže skontrolovať podrobnosti a platnosť certifikátu výrobcu kliknutím na link "More information" (prekl. Viac informácií) a potvrdiť spustenie aplikácie kliknutím na tlačidlo "Run" (prekl. Spustiť).



(Pozn. opätovnému zobrazovaniu tohto okna pri každom spustení aplikácie D.Signer/XAdES Java je možné zamedziť zaškrtnutím poľa: Do not show this again for apps from the publisher and location above; prekl. Nezobrazovať opäť pre hore uvedeného vydavateľa a miesto distribúcie aplikácie.)

Pri komunikácii webového prehliadača s Java Runtime môže byť tiež potrebné najprv povoliť prístup webového prehliadača k aplikácii D.Signer/XAdES Java kliknutím na tlačidlo "Allow" (prekl. Povoliť).



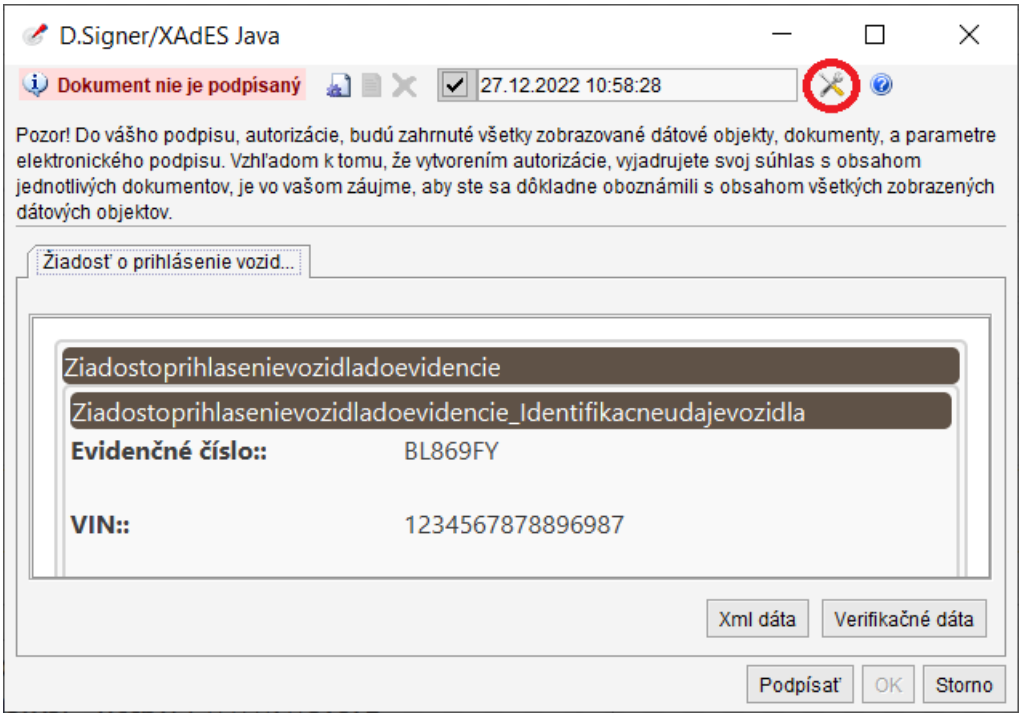
(Pozn. opätovnému zobrazovaniu tohto okna pri každom spustení aplikácie D.Signer/XAdES Java je možné zamedziť zaškrtnutím poľa: Do not show this

again for this app and web site; prekl. Nezobrazovať opäť pre túto aplikáciu a web.)

Alternatívnou možnosťou je distribúcia aplikácie D.Signer/XAdES Java spolu s klientskou aplikáciou, v rámci ktorej je integrovaná, z dôveryhodného zdroja napr. na CD médiu v rámci inštalačných súborov klientskej aplikácie. V tomto prípade je integrita súborov aplikácie D.Signer/XAdES Java zabezpečená samotným spôsobom distribúcie.

6. Užívateľské nastavenia

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



6.1. Nastavenie spôsobu prístupu k SSCD/QSCD a podpisovým certifikátom

Aplikácia D.Signer/XAdES Java využíva pri vytváraní zaručeného/kvalifikovaného elektronického podpisu certifikované SSCD/QSCD zariadenie pre generovanie kľúčových párov a vytváranie elektronického podpisu, ku ktorému pristupuje pomocou CSP implementácie MS Crypto API, alebo implementácie KSP providera CNG, alebo príslušnej PKCS#11 knižnice. Zároveň umožňuje vytvoriť aj obyčajný elektronický podpis napr. pomocou certifikátu uloženom v rámci PKCS#12 súboru. Predvolený spôsob prístupu k SSCD/QSCD, resp. k PKCS#12 súboru (a teda aké podpisové certifikáty bude mať používateľ k dispozícii), je uložený v rámci konfigurácie aplikácie.

Po vytvorení inštancie modulu D.Signer/XAdES Java sa aplikácia v rámci inicializácie pokúsi načítať nastavenia pre prístup k SSCD/QSCD a podpisovým

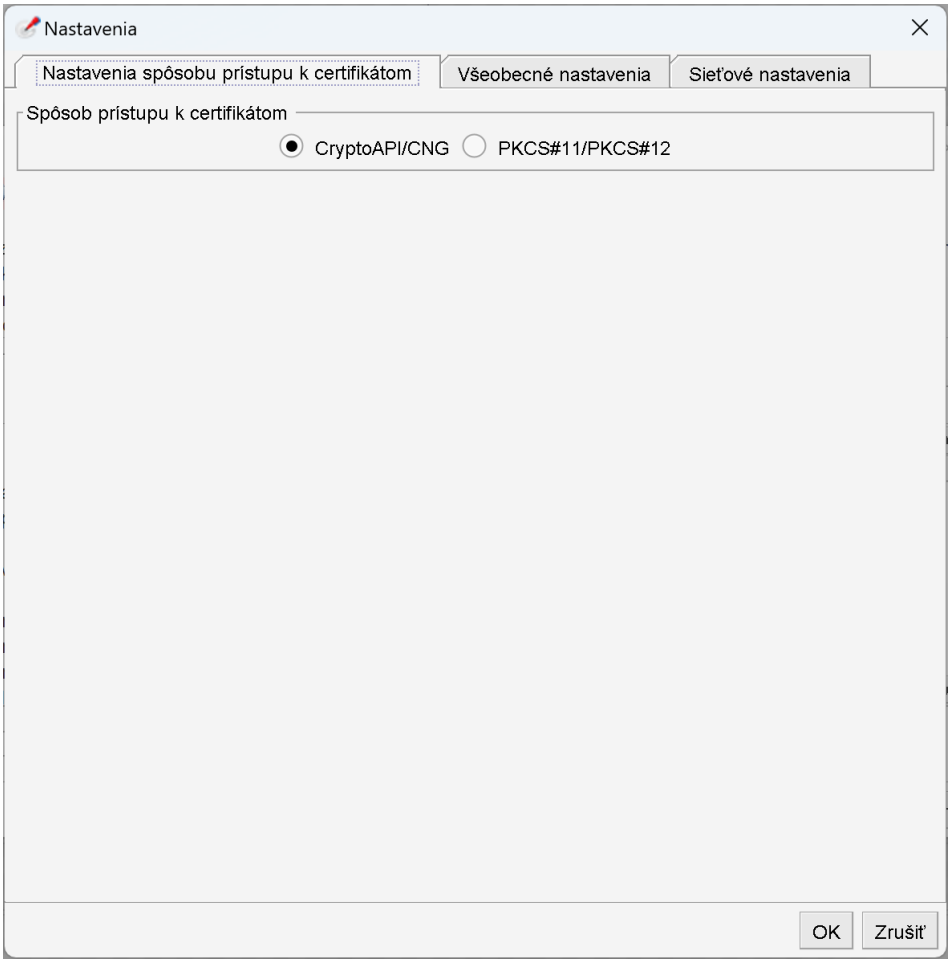
certifikátom, ktoré sú uložené v rámci konfigurácie. Ak takéto nastavenia ešte neexistujú, tak otvorí používateľovi dialóg, v ktorom mu umožní nastaviť:

- buď prístup k SSCD/QSCD pomocou MS Crypto API, alebo implementácie KSP providera CNG – v tomto prípade bude mať používateľ pri výbere certifikátu k dispozícii všetky platné certifikáty uložené v MS Personal Certificate Store, ku ktorým existuje privátny kľúč,
- alebo pomocou PKCS#11 knižnice – používateľ bude môcť špecifikovať cestu k PKCS#11 knižnici, ktorú má nainštalovanú v systéme. V tomto prípade bude mať používateľ pri výbere certifikátu k dispozícii všetky platné certifikáty uložené na príslušnom SSCD/QSCD zariadení, ktoré je prístupné pomocou špecifikovanej PKCS#11 knižnice a ku ktorým existuje privátny kľúč,
- alebo prístup k PKCS#12 (PFX) súboru, ktorý má uložený na disku. V tomto prípade bude mať používateľ pri výbere certifikátu k dispozícii všetky platné certifikáty uložené v špecifikovanom PFX súbore, ku ktorým existuje privátny kľúč.

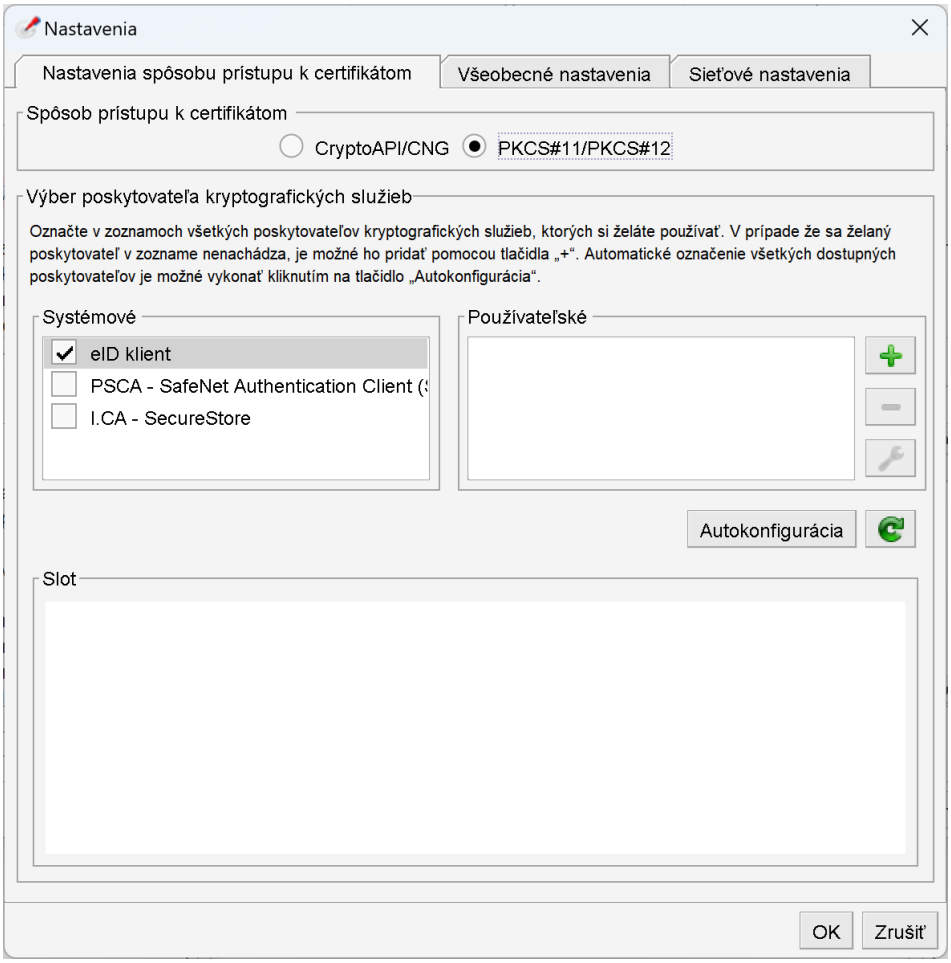
Na platforme Windows sa dialóg pre nastavenie prístupu k SSCD/QSCD neotvorí, ale sa štandardne nastaví prístup k SSCD/QSCD prostredníctvom MS Crypto API, alebo CNG.

Po potvrdení konfigurácie prístupných SSCD/QSCD zariadení a podpisových certifikátov aplikácia D.Signer/XAdES Java uloží tieto nastavenia v rámci konfigurácie aplikácie. Správa prístupných SSCD/QSCD zariadení a podpisových certifikátov je používateľovi k dispozícii takisto z prostredia aplikácie D.Signer/XAdES Java prostredníctvom tlačidla "Nastavenia".

Na nasledujúcom obrázku je zobrazený príklad nastavenia prístupu k SSCD/QSCD pomocou MS Crypto API, resp. CNG.



Na nasledujúcom obrázku je zobrazený príklad nastavenia prístupu k SSCD/QSCD pomocou PKCS#11 knižnice a prístup k certifikátom, ktoré sú uložené v rámci PKCS#12 (PFX) súborov.



Aplikácia D.Signer/XAdES Java obsahuje konfiguráciu preddefinovaných systémových poskytovateľov kryptografických služieb a umožňuje tiež konfiguráciu používateľom definovaných poskytovateľov kryptografických služieb.

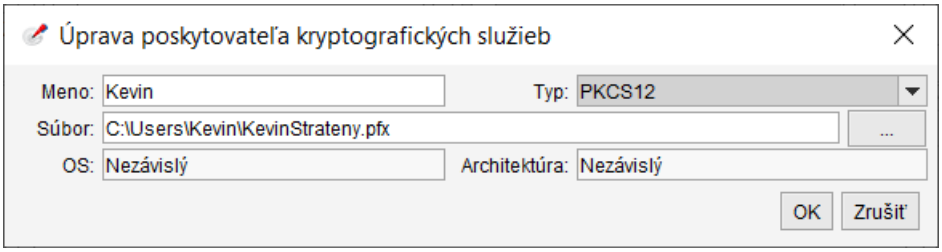
V rámci systémových poskytovateľov sú preddefinované nastavenia pre prístup k najbežnejšie používaným SSCD/QSCD zariadeniam, ktoré sú distribuované používateľom akreditovanými certifikačnými autoritami pri zaobstaraní si kvalifikovaného certifikátu pre vytvorenie ZEP/KEP. Používateľ môže definovať zoznam povolených poskytovateľov kryptografických služieb[3] – stačí označiť tých systémových poskytovateľov kryptografických služieb, ktorých si želá používať (resp. systémových poskytovateľov kryptografických služieb k tým SSCD/QSCD zariadeniam, na ktorých má uložené svoje kvalifikované certifikáty, ktoré si želá používať). Automatické označenie všetkých dostupných poskytovateľov je možné vykonať kliknutím na tlačidlo "Autokonfigurácia".

[3] Teda tých poskytovateľov kryptografických služieb, ktorí budú k dispozícii pri výbere podpisového certifikátu.

Definovanie predvoleného (default) poskytovateľa kryptografických služieb je možné označením jeho mena a výberom slotu (úložiska certifikátov na SSCD/QSCD zariadení). Kliknutím na tlačidlo s ikonou  je možné aktualizovať zoznam slotov predvoleného poskytovateľa kryptografických služieb.

V prípade, že sa želaný poskytovateľ kryptografických služieb v zozname systémových a používateľských poskytovateľov nenachádza, je možné ho pridať do zoznamu používateľských poskytovateľov pomocou tlačidla "+". Nepotrebného poskytovateľa kryptografických služieb je možné odobrať zo zoznamu používateľských poskytovateľov pomocou tlačidla "-". Pomocou tlačidla s ikonou kľúča je možné zmeniť nastavenia pre používateľom definovaného poskytovateľa kryptografických služieb.

Na nasledujúcom obrázku je zobrazená obrazovka pre používateľom definovaného nového poskytovateľa kryptografických služieb.



Pri definovaní nového poskytovateľa kryptografických služieb musí používateľ špecifikovať:

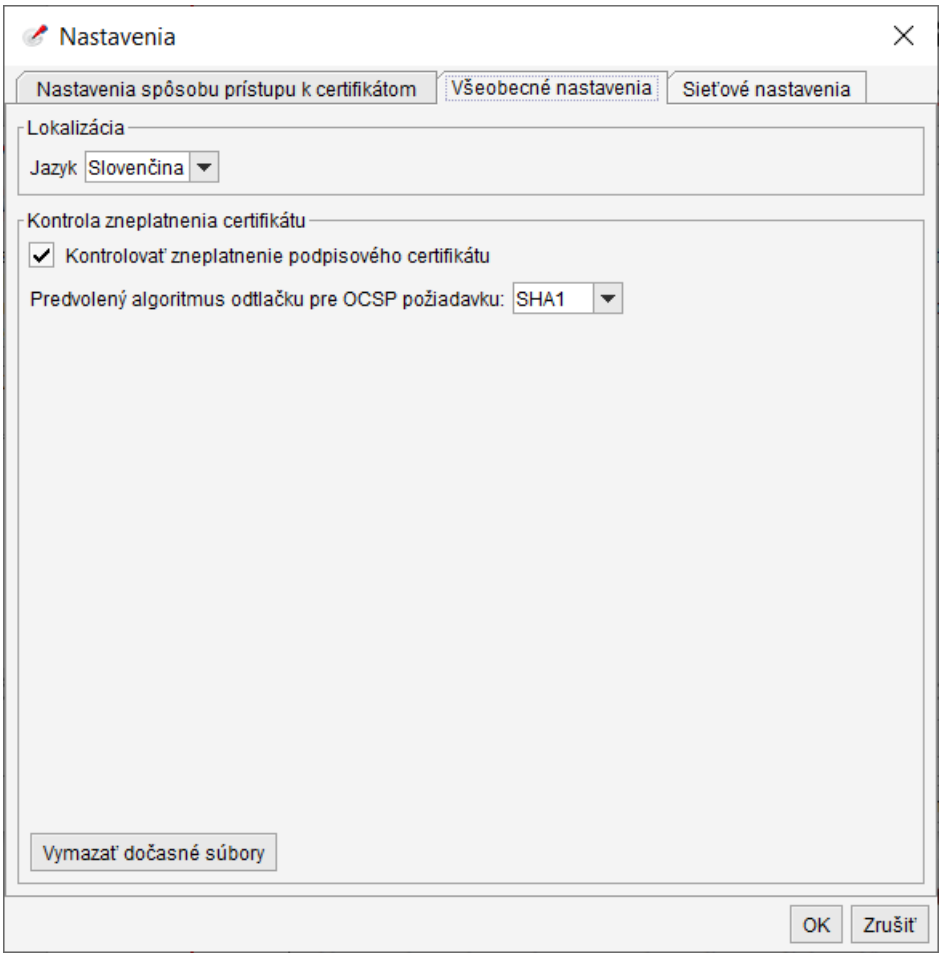
- meno poskytovateľa kryptografických služieb (používateľom špecifikované meno),
- typ poskytovateľa kryptografických služieb:
  - ⇒ PKCS#11, ak chce definovať poskytovaľa kryptografických služieb pre prístup k SSCD/QSCD zariadeniu,
  - ⇒ PKCS#12, ak chce špecifikovať prístup k PKCS#12 (PFX) súboru s podpisovým certifikátom,
- cestu k PKCS#11 knižnici poskytovateľa kryptografických služieb alebo cestu k PKCS#12 (PFX) súboru s podpisovým certifikátom,
- hodnoty polí OS (operačný systém; možné hodnoty: "Windows", "Linux", "Mac OS X") a architektúra (možné hodnoty: "x86", "i386", "x86_64", "amd64") budú nastavené automaticky na základe Java platformy, v rámci ktorej je aplikácia D.Signer/XAdES Java spustená.

Pri výbere PKCS#11 knižnice je potrebné zvoliť knižnicu, ktorá zodpovedá identifikovanému operačnému systému a architektúre Java Runtime.

6.2. Všeobecné nastavenie aplikácie

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

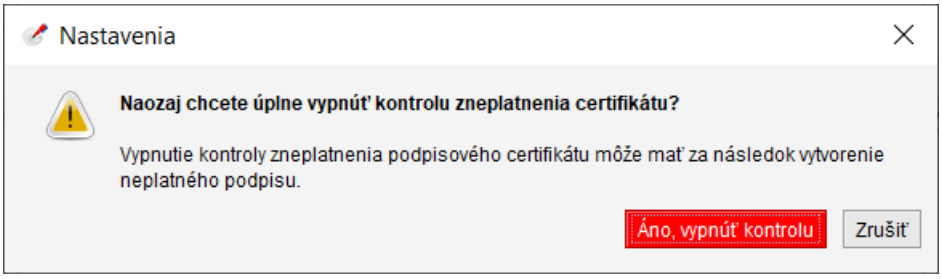
- nastavenie jazyka aplikácie,
- nastavenia kontroly zneplatnenia podpisového certifikátu pred podpisom.



Nastavenie nového jazyka sa aplikuje pri ďalšom spustení aplikácie D.Signer/XAdES Java.

V prípade vynútenia jazyka aplikácie D.Signer/XAdES Java z prostredia klientskej aplikácie nebudú konfiguračné nastavenia jazyka aplikácie pre používateľa prístupné.

Aplikácia D.Signer/XAdES Java 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 Java 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.

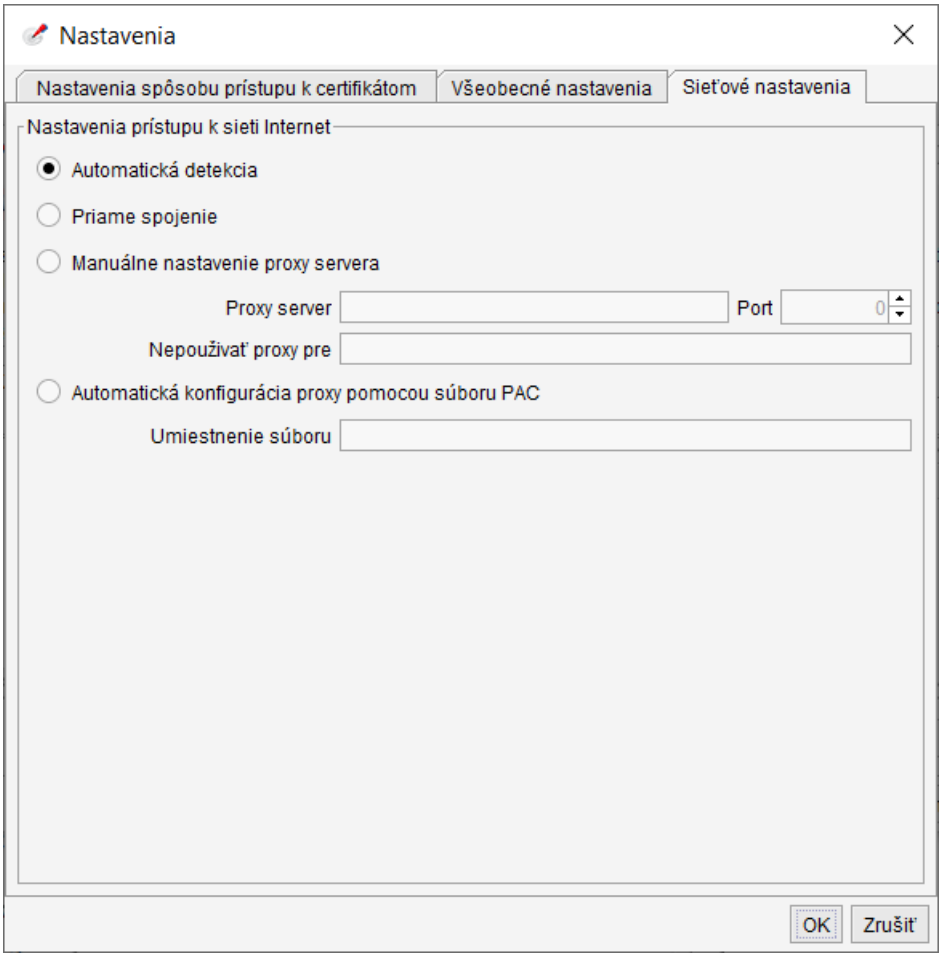
V nastaveniach kontroly zneplatnenia certifikátu je takisto možné zmeniť predvolený algoritmus odtlačku pre OCSP požiadavku v prípade, že certifikačná autorita, ktorá vydala podpisový certifikát podporuje pre OCSP službu iný algoritmus odtlačku pre OCSP požiadavku.

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

6.3. 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

Stiahnutie všetkých komponentov aplikácie D.Signer/XAdES Java pomocou technológie webstart môže vyžadovať istý čas, počas ktorého môže byť proces sťahovania aplikácie indikovaný na danej web stránke napríklad prostredníctvom nasledujúceho indikátora.



7.2. Súhlas s licenčnou zmluvou

V prípade, že súčasťou distribúcie aplikácie D.Signer/XAdES Java je aj PDF Plugin, tak je potrebné potvrdiť licenčnú zmluvu pre použitie knižnice PDFNet SDK[4], ktorá tvorí súčasť PDF Pluginu aplikácie D.Signer/XAdES Java.

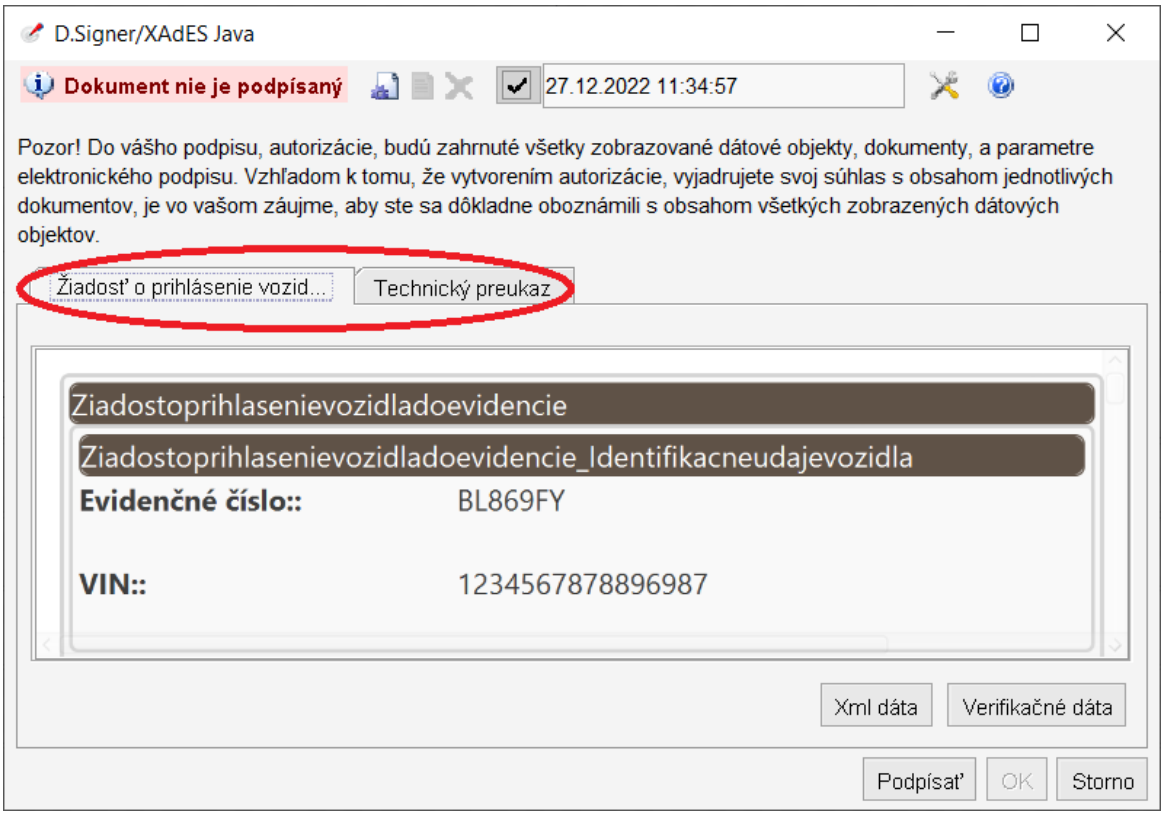


[4] PDF technology in D.Signer/XAdES Java - PDF Plugin is powered by PDFNet SDK copyright © PDFTron™ Systems Inc., 2001-2016, and distributed by DITEC a.s. under license. All rights reserved.

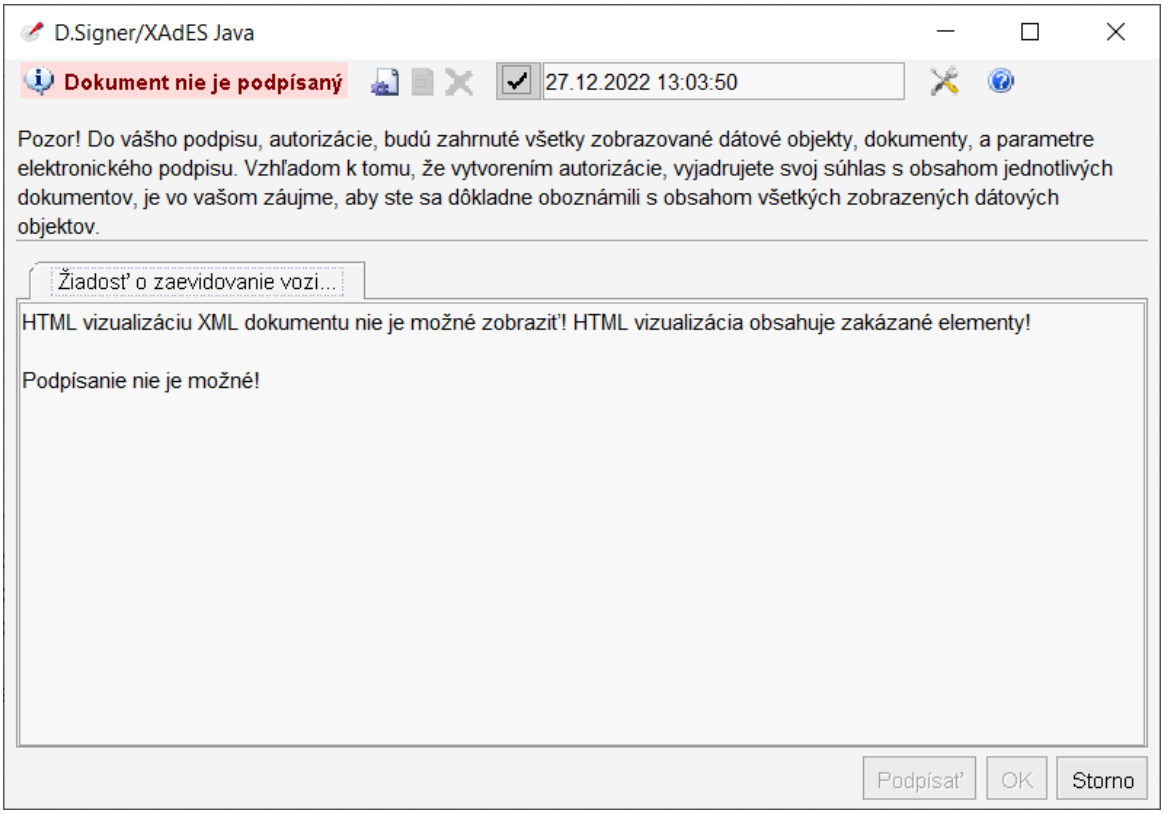
7.3. Zobrazenie podpisovaných dát

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



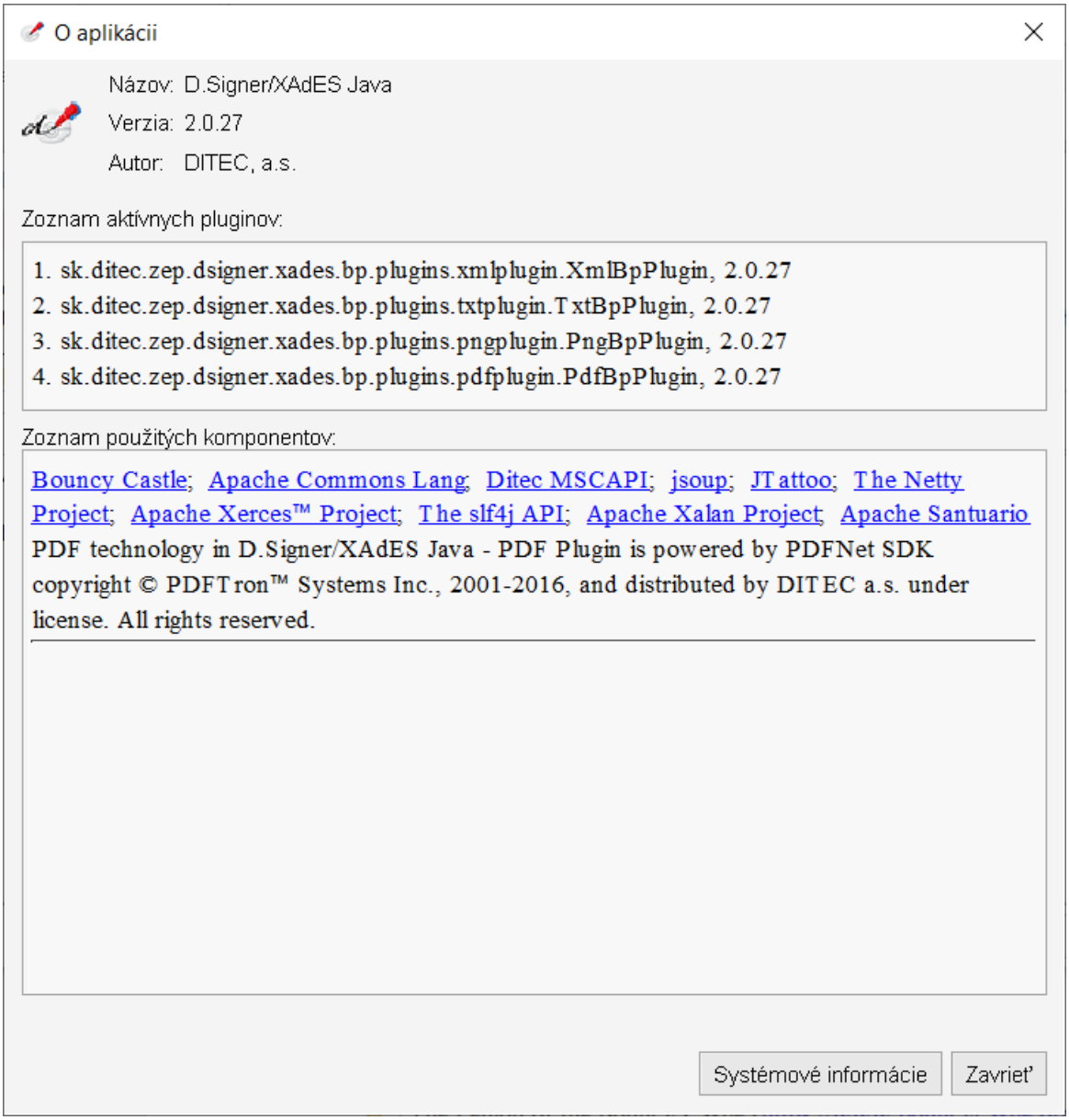
V rámci hlavného okna aplikcácie D.Signer/XAdES Java je tiež zobrazený stav podpisovaného dokumentu, ktorý môže nadobúdať nasledujúce hodnoty:

- Dokument nie je podpísaný
- Dokument bol podpísaný

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

Aplikácia D.Signer/XAdES Java 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 Java. Informácia o nainštalovaných plugin moduloch je používateľovi prístupná prostredníctvom tlačidla "Pomoc".



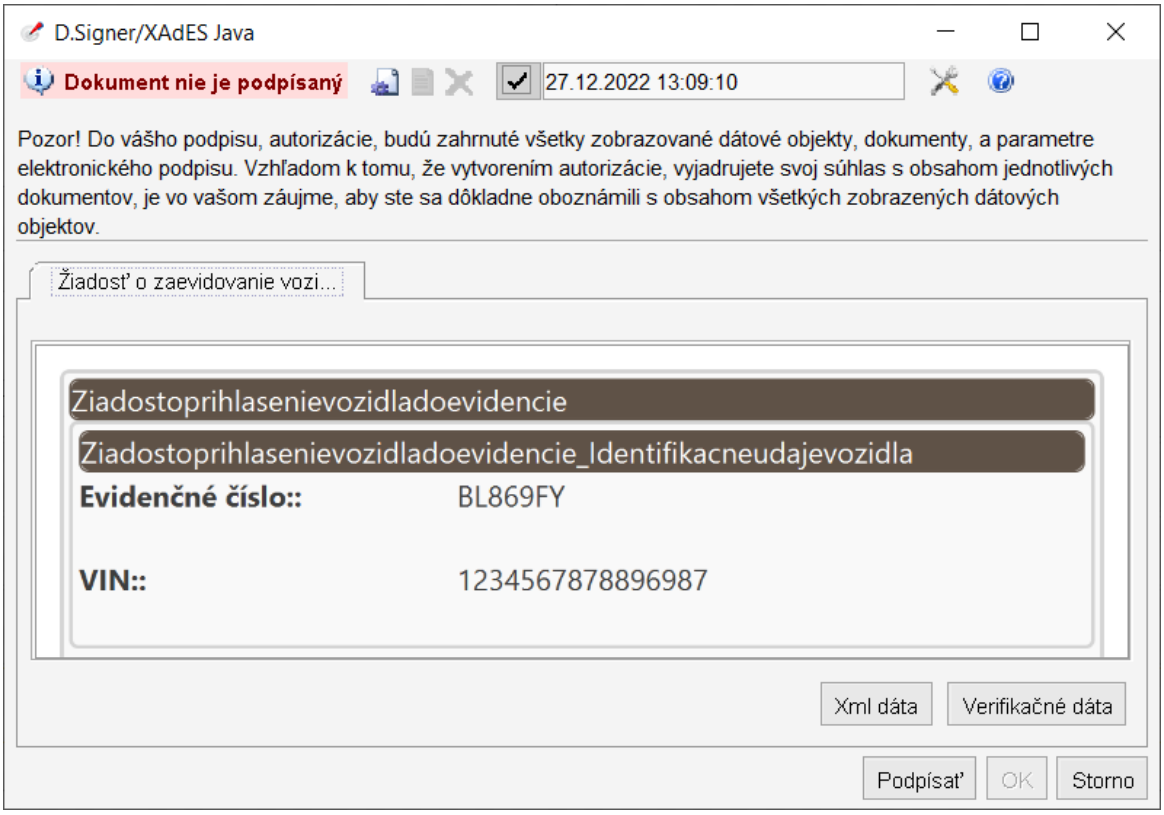
Zároveň sú na obrazovke zobrazené informácie o použitých komponentoch aplikácie D.Signer/XAdES Java a v prípade problémov je možné získať pre pracovníkov podpory ďalšie systémové informácie o prostredí aplikácie kliknutím na tlačidlo "Systémové informácie".

7.3.1. Zobrazenie dokumentov

Zobrazenie dokumentov je realizované v rámci aplikácie D.Signer/XAdES Java pomocou príslušného pluginu pre daný typ dát, ktorý poskytuje aplikácii D.Signer/XAdES Java 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 Java.



7.4. Nastavenie dátumu a času vytvorenia podpisu

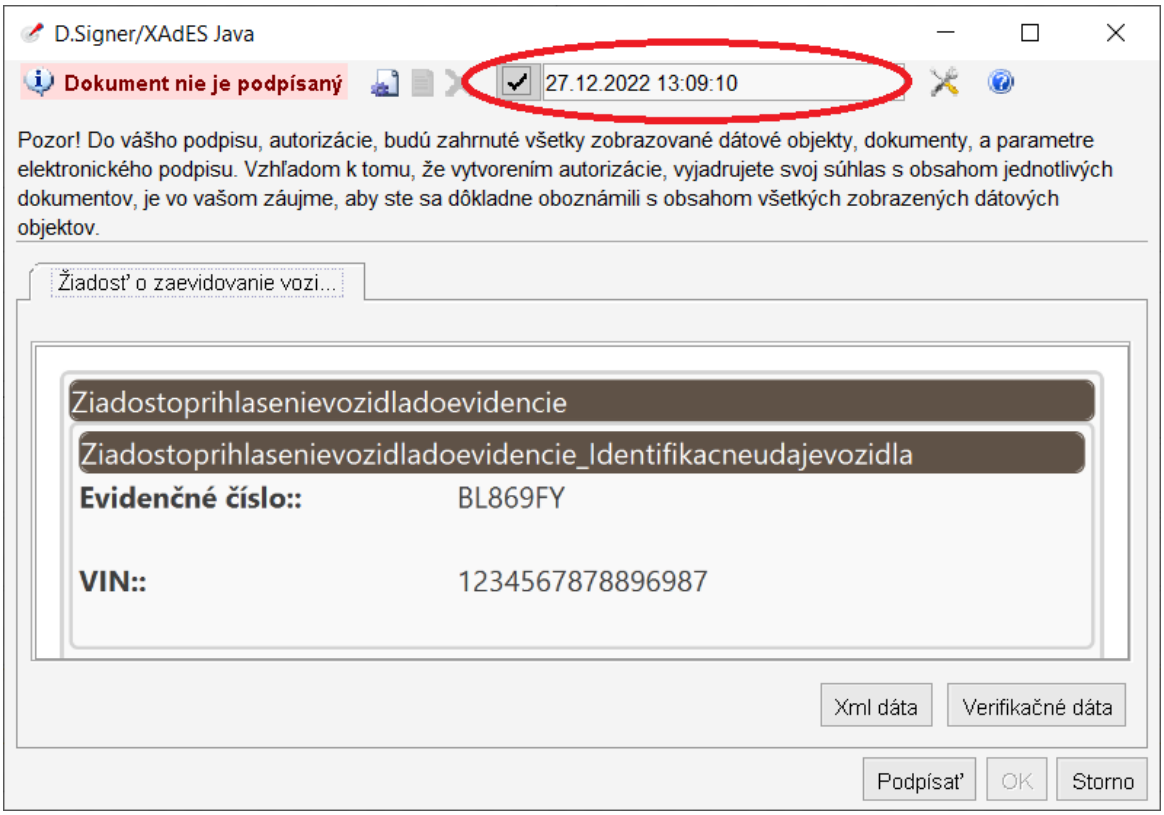
Aplikácia D.Signer/XAdES Java umožňuje používateľovi v prípade potreby nastaviť pomocou ovládacích prvkov, ktoré sú umiestnené v hornej lište okna aplikácie, dátum a čas vytvorenia podpisu. Používateľ môže takto deklarovať vytvorenie elektronického podpisu v špecifikovanom dátume a čase, pričom tento 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:

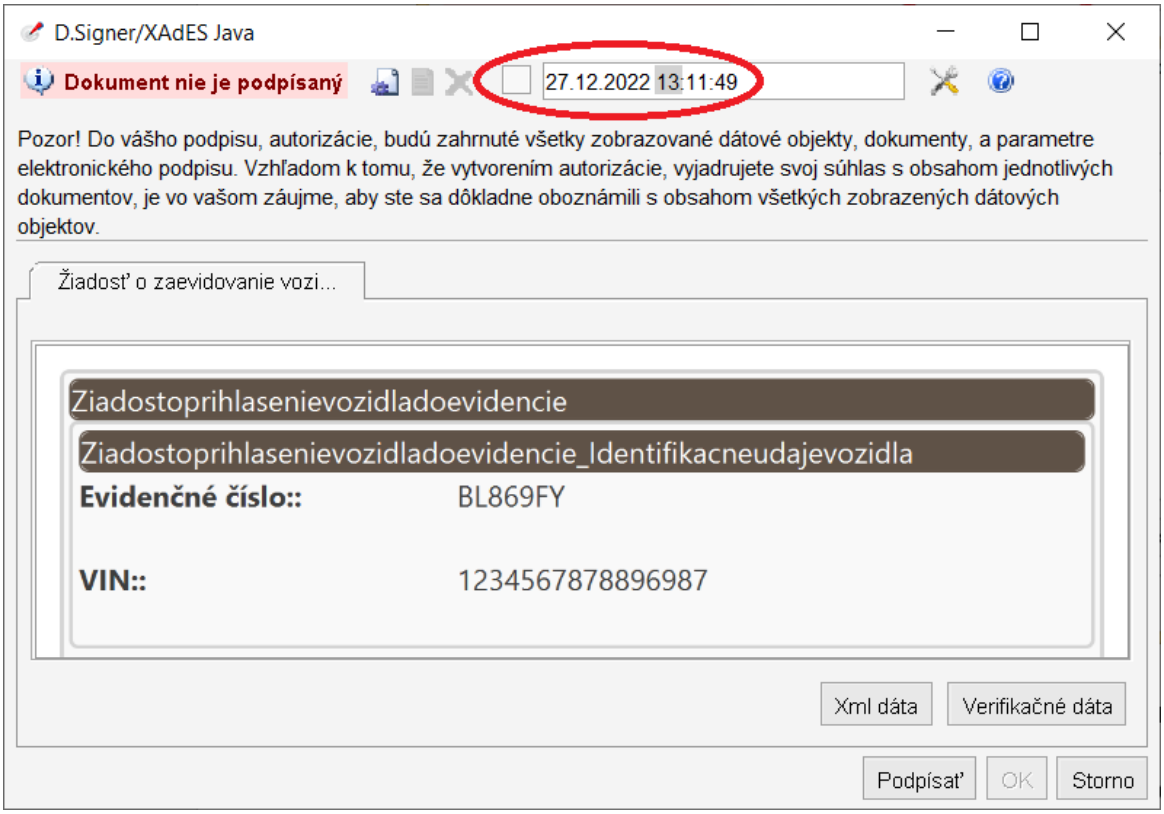
- buď aktuálny systémový dátum a čas, ak je zvolené v zaškrtávacom políčku použitie systémového dátumu a času,

- 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, použije sa aktuálny systémový dátum a čas.

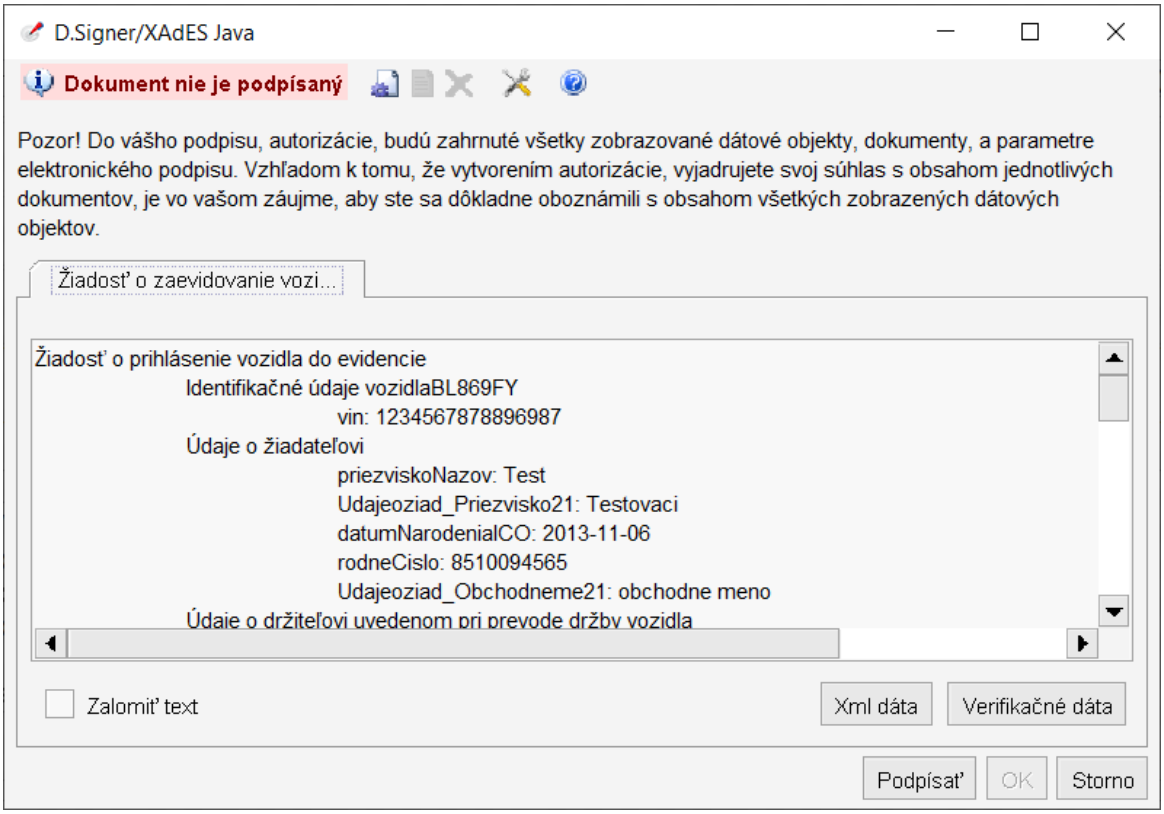


V druhom prípade sa používateľovi sprístupní deklarovaný dátum a čas vytvorenia podpisu na editovanie.



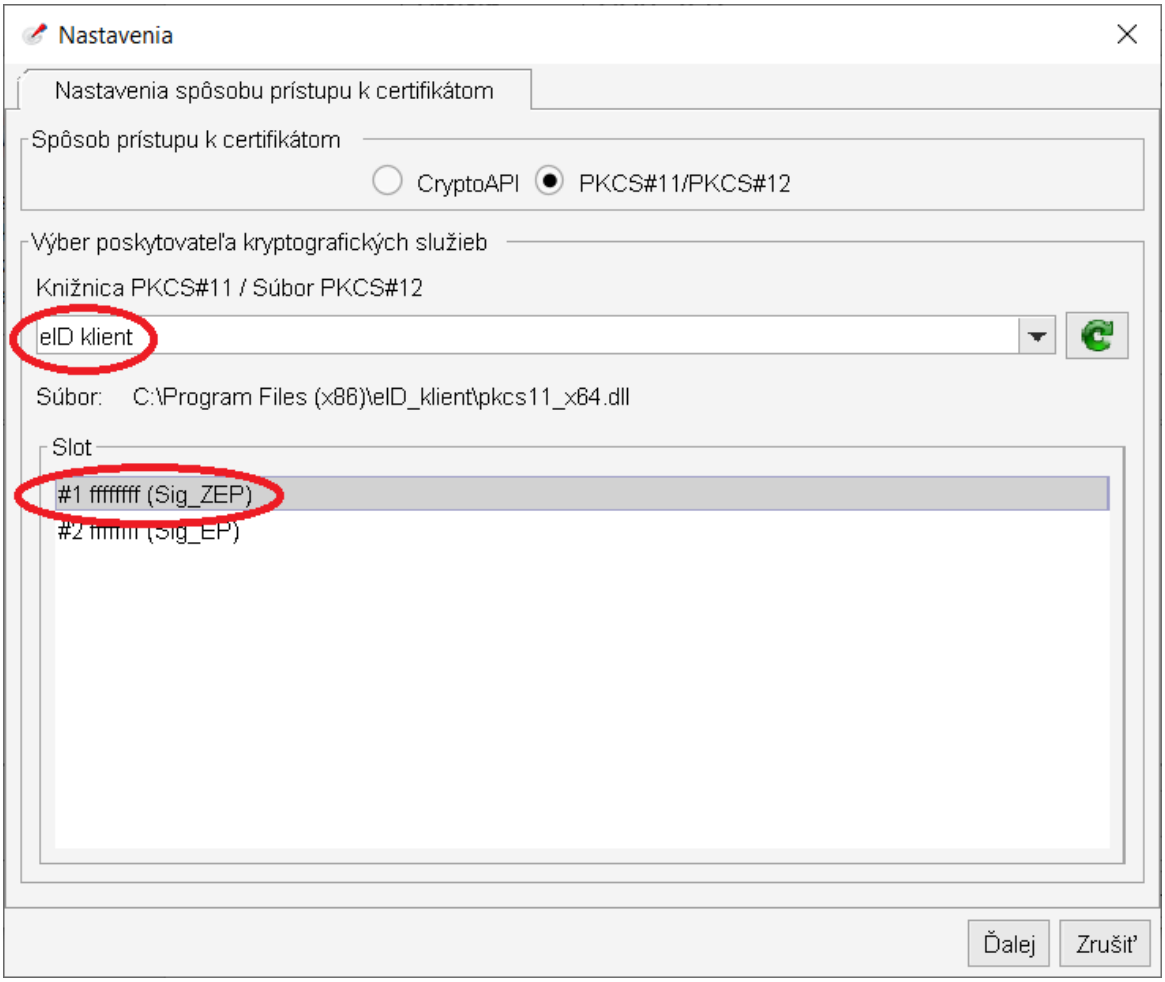
Pozor! Pri vytváraní elektronického podpisu odporúčame použiť správne nastavený aktuálny systémový dátum a čas.

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 Java z klientskej aplikácie.

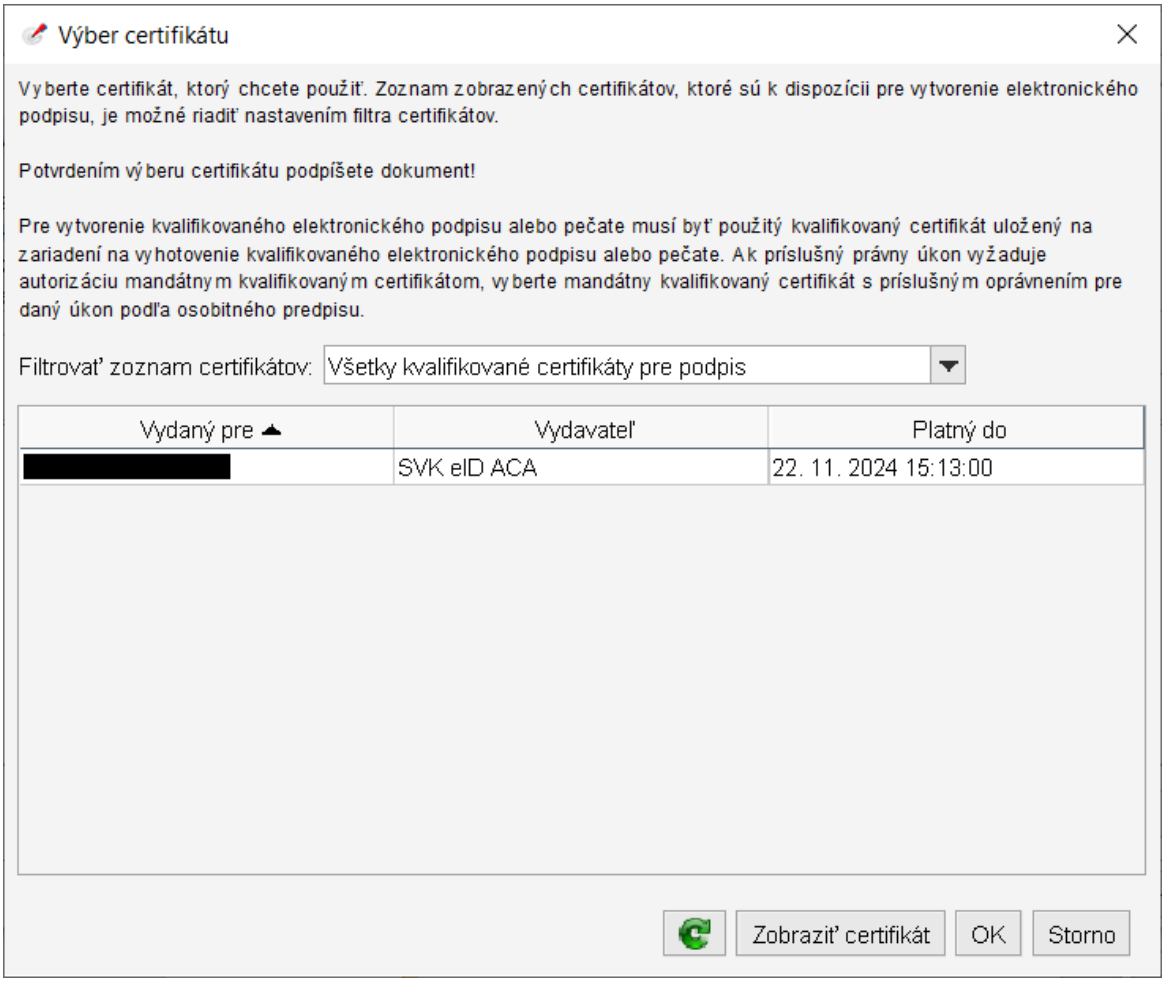


7.5. Podpísanie dokumentu

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. V prípade, že nastavený spôsob prístupu k SSCD/QSCD a podpisovým certifikátom je prostredníctvom PKCS#11 knižnice, tak pred výberom podpisového certifikátu je ešte potrebné zvoliť poskytovateľa kryptografických služieb zo zoznamu povolených poskytovateľov a slot (úložisko certifikátov na SSCD/QSCD zariadení).



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.

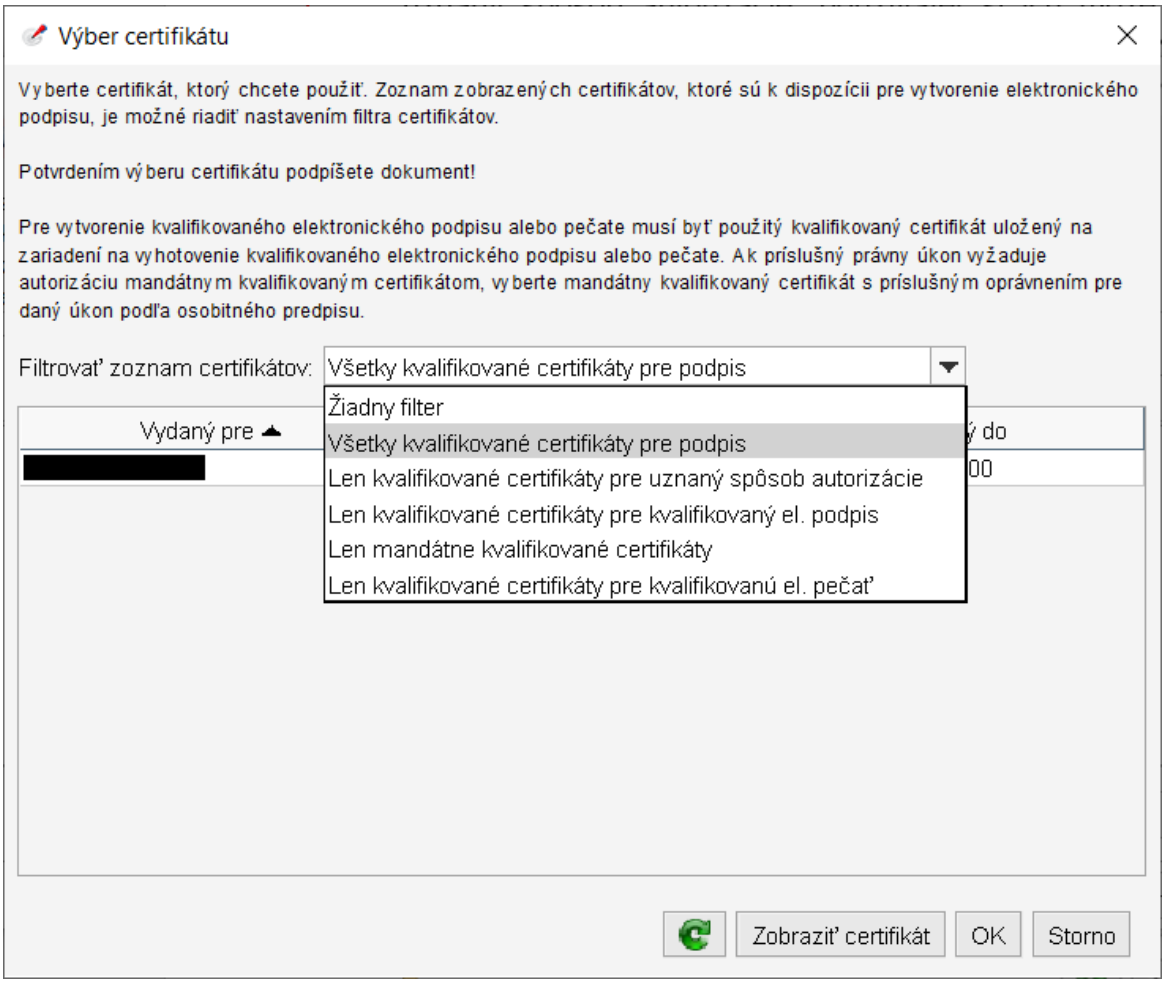
Aplikácia D.Signer/XAdES Java ponúkne na výber len certifikáty, ktorým ešte neuplynul dátum exspirácie. Detaily zvoleného certifikátu je možné prezrieť kliknutím na tlačidlo "Zobraziť certifikát". V prípade potreby je možné kliknutím na tlačidlo s ikonou aktualizovať zoznam zobrazených certifikátov.

Integrátor aplikácie D.Signer/XAdES Java 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.

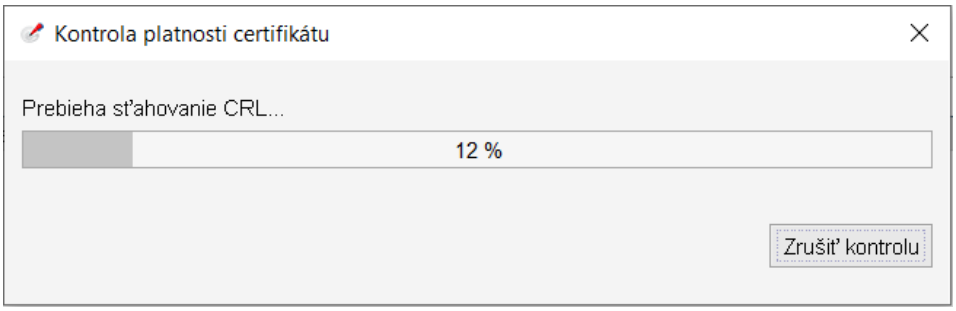
Zoznam zobrazených certifikátov, ktoré sú k dispozícii pre vytvorenie elektronického podpisu, je možné riadiť nastavením filtra certifikátov v okne pre výber certifikátu v aplikácii D.Signer/XADES Java.



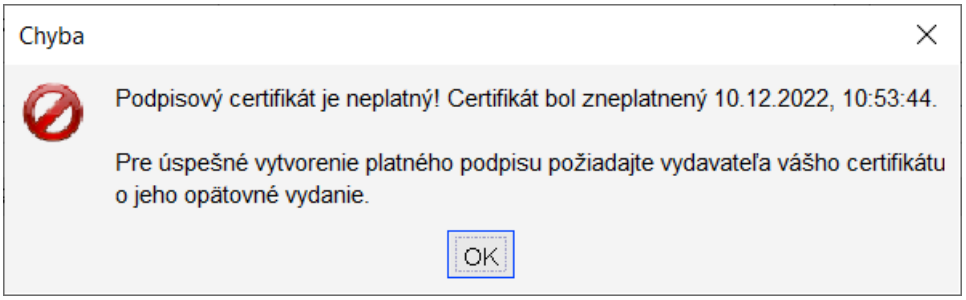
Po zvolení podpisového certifikátu a potvrdení výberu tlačidlom "OK" aplikácia D.Signer/XAdES Java vykoná kontrolu stavu zneplatnenia podpisového

certifikátu.[5] 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.





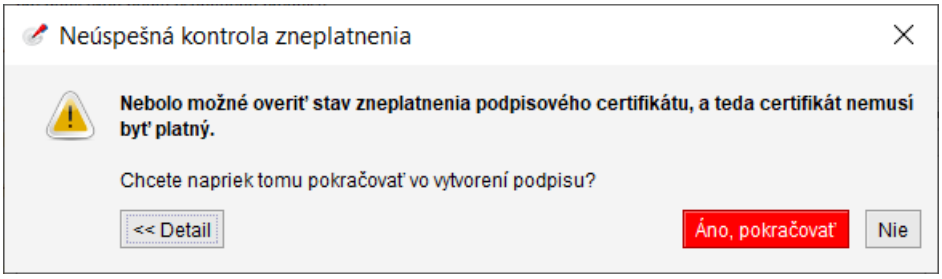
Ak aplikácia zistí, že certifikát bol zneplatnený, tak o tom informuje používateľa s odporúčaním, aby požiadal vydavateľa svojho certifikátu o jeho opätovné vydanie, a nepokračuje vo vytvorení elektronického podpisu.



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:

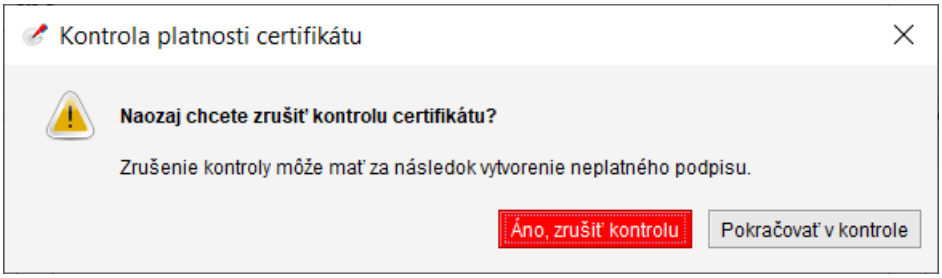
- Áno, pokračovať – vo vytvorení podpisu,
- Nie – nepokračovať vo vytvorení podpisu.

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



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 Java 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.

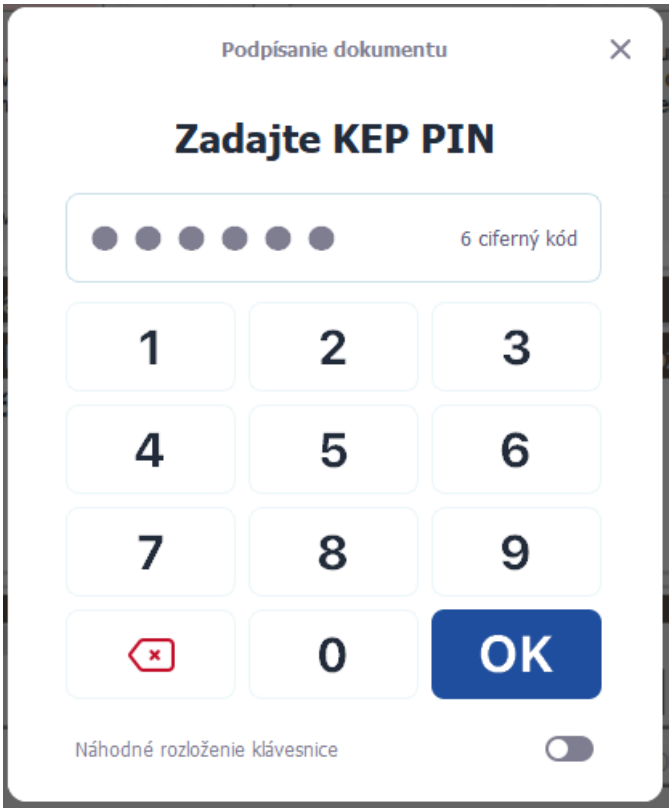


Pozor! Odporúčame nezrušiť kontrolu zneplatnenia podpisového certifikátu. Zrušenie kontroly zneplatnenia podpisového certifikátu môže mať za následok vytvorenie neplatného podpisu.

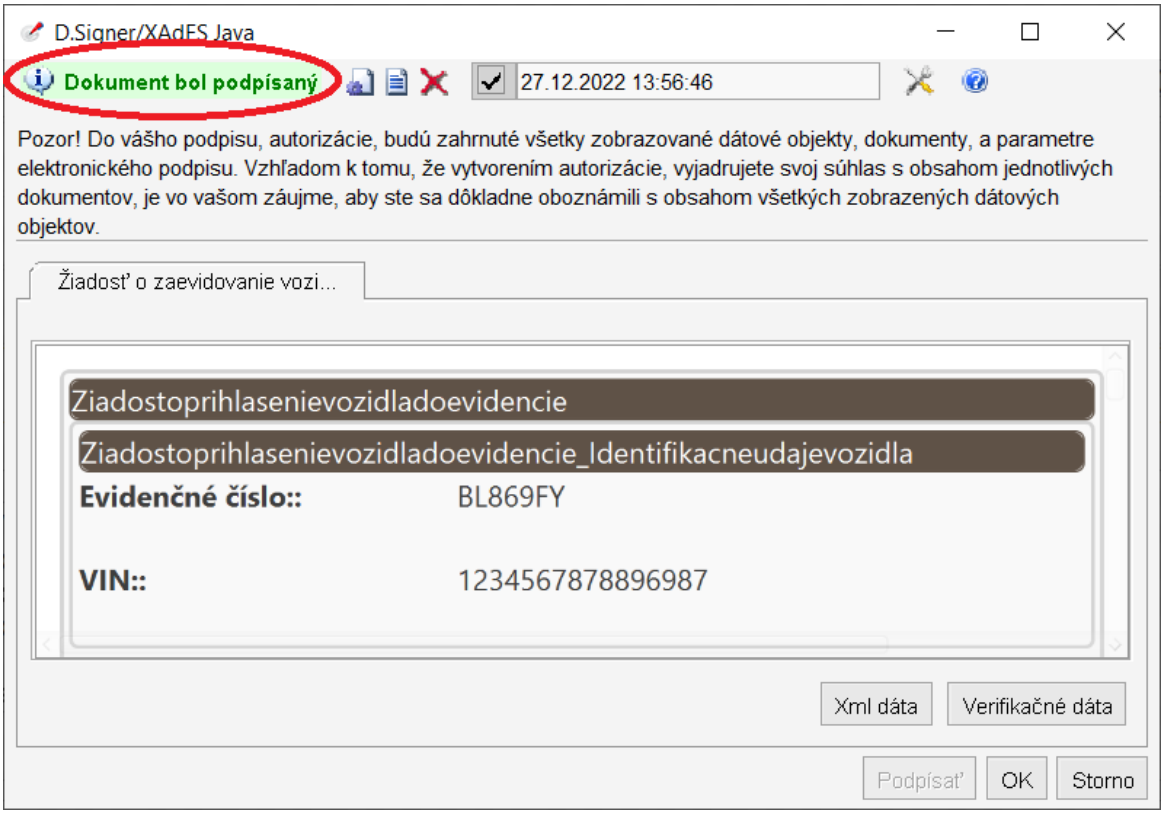
Ak aplikácia pomocou kontroly zneplatnenia zistí, že certifikát je platný, vykoná proces vytvorenia elektronického podpisu. Aplikácia D.Signer/XAdES Java vytvorí reprezentáciu podpisovaných dát a parametrov podpisu – digitálny odtlačok. Pomocou rozhrania MS CryptoAPI, CNG, resp. PKCS#11 knižnice a príslušného 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[6] a/alebo PINu.[7]

[6] Bezpečnostný osobný kód.

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



Aplikácia D.Signer/XAdES Java 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).

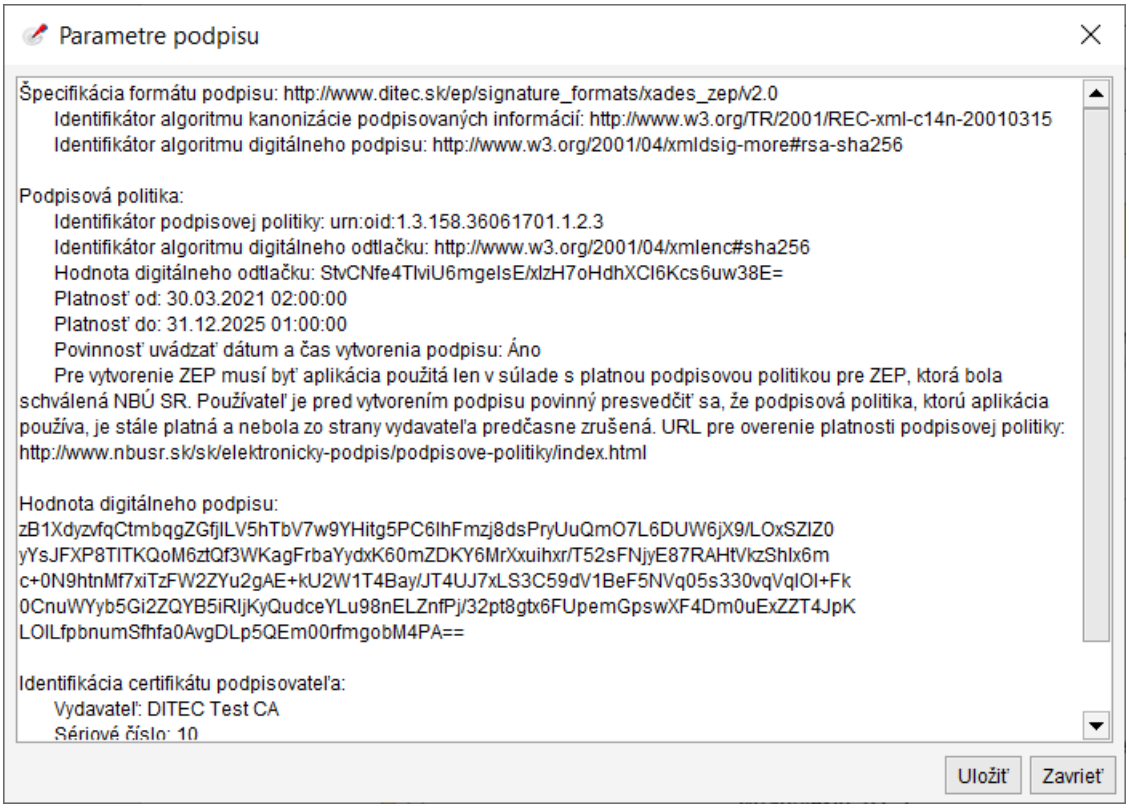


Po úspešnom vytvorení elektronického podpisu je podpísaný dokument odovzdaný klientskej aplikácii až po kliknutí na tlačidlo "OK".

7.6. 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.

8. Trademarks

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

