DITEC
Data Information Technology & Expert Consulting

Používateľská príručka
D.Viewer 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.Viewer Java v2.0		
Ref. číslo	GOV_ZEP.245	Verzia	10

Vypracoval	Tomáš Baran	Podpis	Dátum 13. 3. 2023
Preveril		Podpis	Dátum
Schválil		Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 18. 5. 2005

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.245	Verzia	11

Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia
T. Baran	Doplnená možnosť výberu typu vizualizácie pre XDC, XML alebo FO formulár	12.5.2020	
T. Baran	Pridaná podpora pre zobrazovanie SkTalk správ. Pridaná funcionalita uloženia jednotlivých objektov MessageContajnera.	7.10.2020	

Pripomienkovanie a kontrola

Autor	Stanovisko	Dátum	Verzia

Rozdeľovník

	Priezvisko Meno	Firma, Funkcia
Originál		
Kópia		
Kópia		
Kópia		

Obsah

1. Úvod 6

2. Referencie 7

3. Systémové požiadavky 8

4. Distribúcia a inštalácia 10

5. Práca s aplikáciou 13

5.1. Menu aplikácie 14

6. Vizualizácia dátových štruktúr 18

6.1. SkTalk 19

6.2. MessageContainer 19

6.2.1. Overenie podania voči doručenke 21

6.2.2. Uloženie vybraného objektu elektronickej správy 24

6.3. Registration 24

6.4. XAdES_ZEP 25

6.5. DataSignatures 28

6.6. ASiC Baseline Profile 29

6.7. CAdES_ZEP 30

6.8. ZIP formát súboru (ZEPf) 34

6.9. Vizualizácia súčastí dátových štruktúr 35

6.9.1. Podpis 35

6.9.1.1. XAdES podpis 35

6.9.1.1.1. Parametre podpisu 36

6.9.1.2. CAdES podpis 37

6.9.1.2.1. Parametre podpisu 38

6.9.2. MIME obálka 38

6.9.3. Vnorené podpísané dáta 39

6.9.4. Certifikát 40

6.9.5. Časová pečiatka 42

6.9.6. Zoznam revokovaných certifikátov 43

6.9.7. OCSP odpoveď 45

6.9.8. Referencia certifikátu 47

6.9.9. Referencia zoznamu zrušených certifikátov 48

6.9.10. Podpísané dokumenty 49

6.9.10.1. Podpísaný objekt typu XMLDataContainer 50

6.9.10.2. Vizualizácia obsahu podpísaných dokumentov.....51

7. Podpora pre nevidiacich pomocou NVDA 55

7.1. Systémové požiadavky pre NVDA 55

7.1.1. Aktivácia Java Access Bridge.....55

1. Úvod

D.Viewer Java je nástrojom na prezeranie dátových štruktúr slúžiacich na elektronickú výmenu dát, najmä elektronických podaní a elektronických úradných dokumentov, podpísaných (zaručeným) elektronickým podpisom alebo opatrených (zaručenou) elektronickou pečaťou. Aplikácia extrahuje obsah zvolenej dátovej štruktúry a následne umožňuje zobrazenie obsahu používateľovi prostredníctvom integrovaných vizualizácii. Prednosťou D.Viewer Java je, že nepracuje len rich klient, ale jeho komponenty možno využiť aj pri tvorbe webových stránok.

Tento dokument je určený pre používateľov aplikácie D.Viewer Java, resp. pre používateľov informačných systémov a aplikácií, v rámci ktorých bude aplikácia D.Viewer Java integrovaná. Jednotlivé časti dokumentácie aplikácie D.Viewer Java je možné použiť pri tvorbe používateľských príručiek týchto informačných systémov po dohode s vlastníkmi autorských práv aplikácie D.Viewer Java.

2. Referencie

[1] „Výnos MF SR č. 55/2014 o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov“.

[2] „Výnos MF SR č. 96/2014 o jednotnom formáte elektronických správ vytváraných a odosielaných prostredníctvom prístupových miest v znení neskorších predpisov“.

[3] „Formát elektronického podania, Registration v1.0, http://www.ditec.sk/ekr/registration/v1.0,“ DITEC, a.s..

[4] „Profil XAdES_ZEP – formát ZEP na báze XAdES, v1.0,“ Ditec, a.s., 2008.

[5] „Profil XAdES_ZEP – formát ZEP na báze XAdES, v1.1,“ Ditec, a.s., 2009.

[6] „Profil XAdES_ZEP – formát ZEP na báze XAdES, v2.0,“ Ditec, a.s., 2011.

[7] „Profil XAdES_ZEPbp – formát ZEP na báze XAdES BP, v1.0,“ Ditec, a.s., 2016.

[8] Electronic Signatures and Infrastructures, „ETSI TS 103 174 v2.2.1 ASiC Baseline Profile,“ 2012.

[9] „Profil CAdES_ZEP - formát ZEP na báze CAdES, v1.0,“ DITEC, a.s..

[10] „Profil CAdES_ZEP - formát ZEP na báze CAdES, v2.0,“ 2016.

[11] „Formáty zaručených elektronických podpisov v3.0,“ NBÚ SR, 2009.

3. Systémové požiadavky

Systémové požiadavky aplikácie D.Viewer 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; 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),
- 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).

Ak je aplikácia D.Viewer 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 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.

Veľkosť distribučných súborov aplikácie D.Viewer Java je uvedená v nasledujúcej tabuľke.

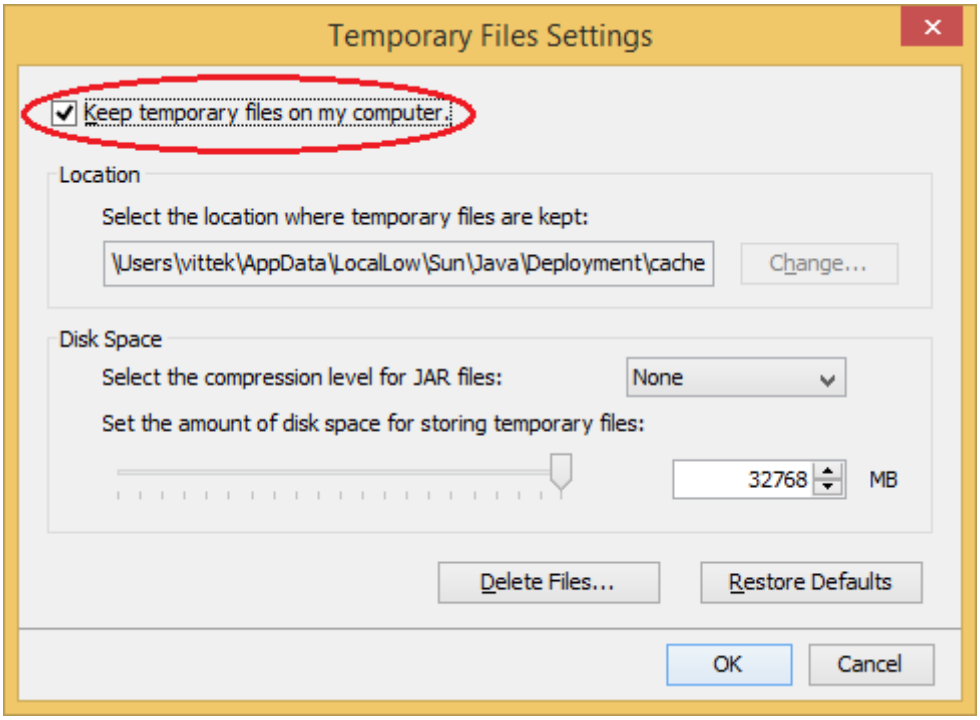
---

[1] Ak je aplikácia D.Viewer Java spúšťaná ako Java applet.

Komponent	Veľkosť
D.Viewer Java	14 MB

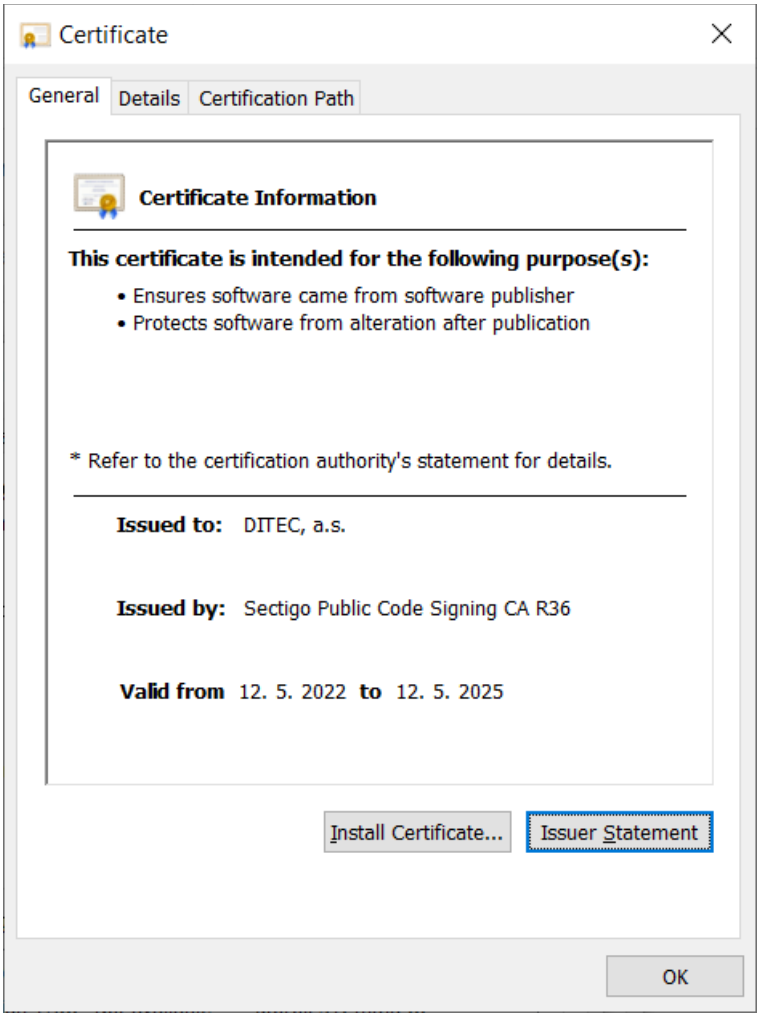
Tzn. že pre konkrétnu platformu (OS, 32/64-bit) je veľkosť distribučných súborov cca 14 MB; ak sú skomprimované, tak dokonca len 4,5 MB.

Aplikácia D.Viewer 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.



4. Distribúcia a inštalácia

Aplikácia D.Viewer 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.Viewer 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.

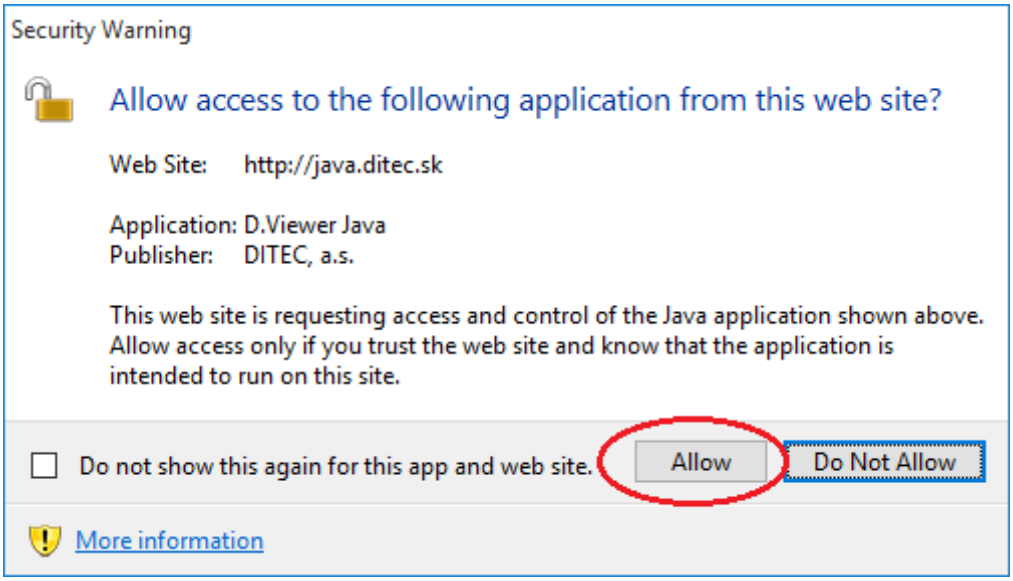


Používateľ si môže skontrolovať podrobnosti a platnosť certifikátu výrobcu kliknutím na link "More information" (prekl. Viac informácií) a potvrdiť spustenie aplikácie kliknutím na tlačidlo "Run" (prekl. Spustiť).



(Pozn. opätovnému zobrazovaniu tohto okna pri každom spustení aplikácie D.Viewer 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.Viewer Java kliknutím na tlačidlo "Allow" (prekl. Povoliť).

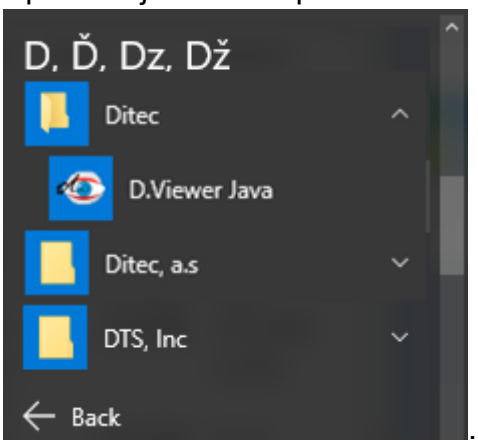


(Pozn. opätovnému zobrazovaniu tohto okna pri každom spustení aplikácie D.Viewer Java je možné zamedziť zaškrtnutím poľa: Do not show this again for this app and web site; prekl. Nezobrazovať opäť pre túto aplikáciu a web.)

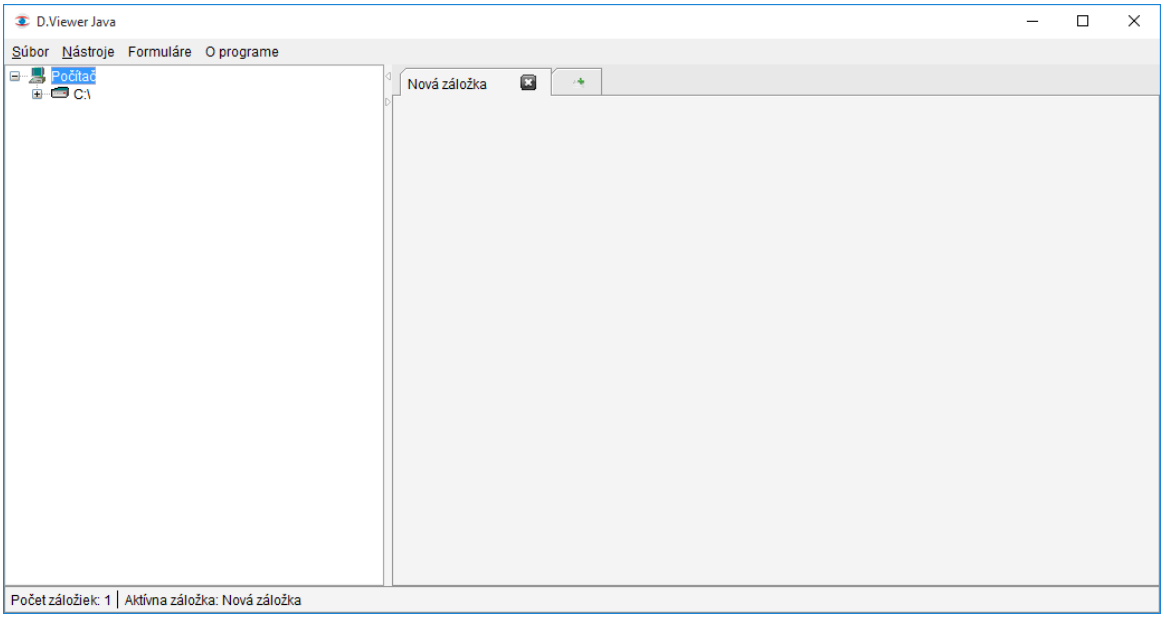
Alternatívnou možnosťou je distribúcia aplikácie D.Viewer Java spolu s klientskou aplikáciou, v rámci ktorej je integrovaná, z dôveryhodného zdroja napr. na CD médiu v rámci inštalačných súborov klientskej aplikácie. V tomto prípade je integrita súborov aplikácie D.Viewer Java zabezpečená samotným spôsobom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

5. Práca s aplikáciou

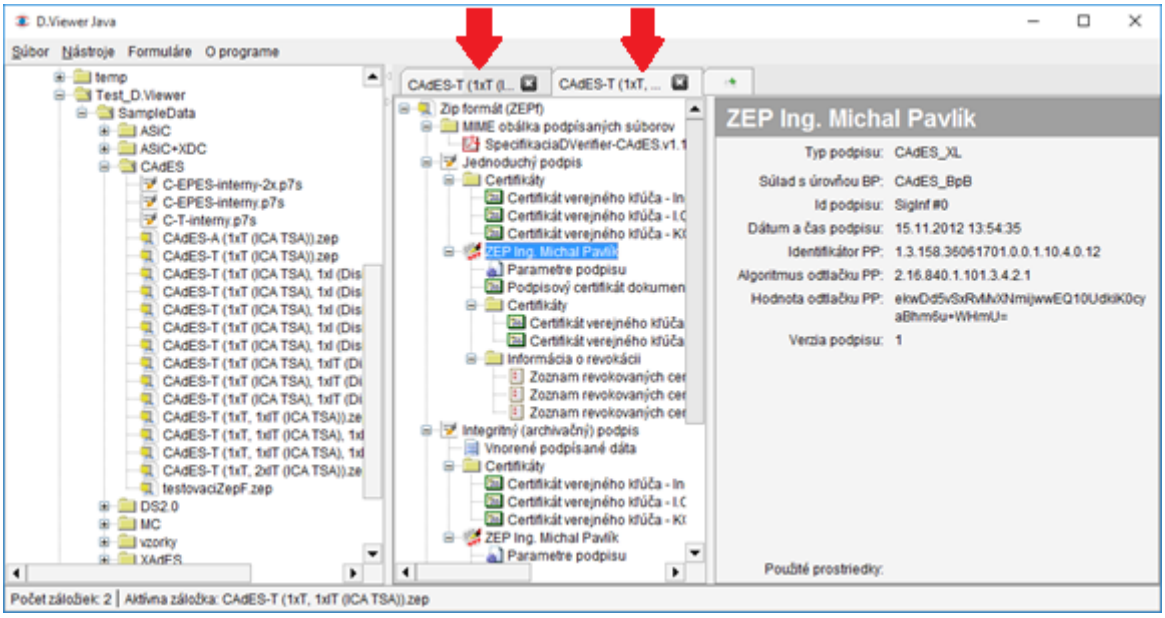
Aplikáciu je možné spustiť z menu Štart → Programy → Ditec → D.Viewer Java.



Po spustení sa zobrazí základná obrazovka aplikácie.

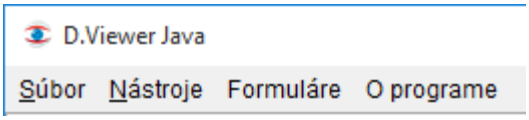


V ľavej časti sa nachádza adresárová štruktúra PC. Kliknutím na vybraný súbor je zobrazovaný obsah dátovej štruktúry na v strednej časti obrazovky. Kliknutím na jednotlivé dátové objekty v zobrazenom strome dátovej štruktúry sa používateľovi zobrazí detail objektu v pravej časti obrazovky. V jednom čase je možné mať otvorené viac ako jeden súbor, umožňujú to záložky.



5.1. Menu aplikácie

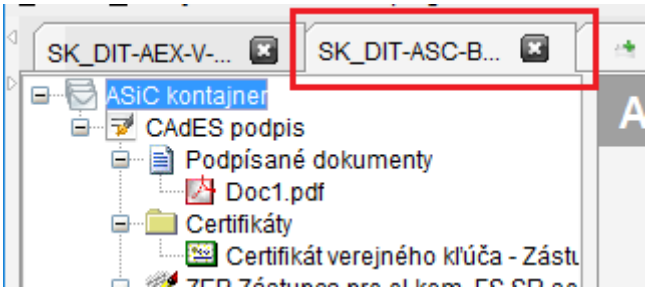
Menu aplikácie D.Viewer Java má nasledovnú štruktúru.



Pozn. Menu aplikácie D.Viewer Java je používateľovi prístupné len v prípade, ak je aplikácia D.Viewer Java spúšťaná ako standalone aplikácia z menu Štart alebo ak je integrovaná v rámci klientskej Java aplikácie bežiacej v JRE.

Ďalej je uvedený popis jednotlivých príkazov menu aplikácie.

Súbor → **Otvoriť** – otvorí dialógové okno pre otvorenie súboru. Po vybraní je tento súbor otvorený v novej záložke. Súbor je tiež možné otvoriť metódou **drag&drop**, teda presunutím označeného súboru do priestoru obrazovky aplikácie D.Viewer Java. Takto otvorený súbor je tiež otvorený v novej záložke.

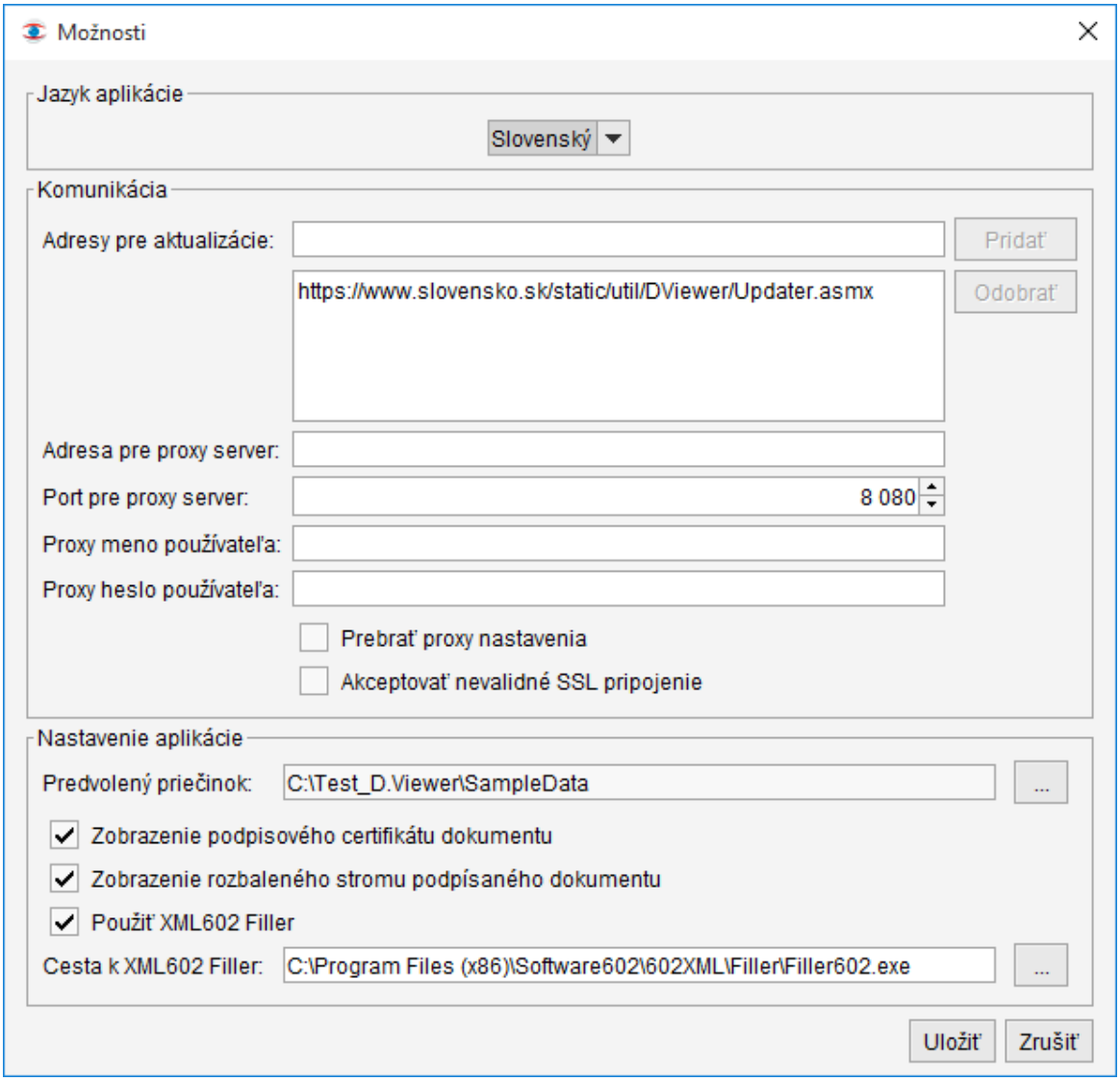


Súbor → **Zavrieť** – zatvorí aktuálnu záložku.

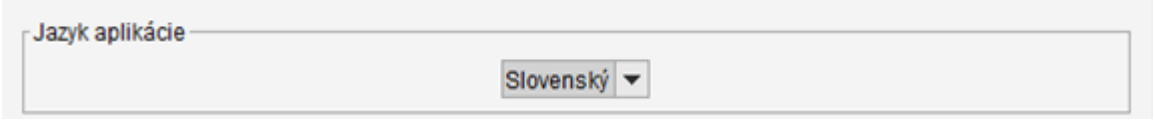
Súbor → **Zavrieť všetky** – zatvorí všetky záložky.

Súbor → **Koniec** – ukončí aplikáciu.

Nástroje → Možnosti – zobrazí okno konfiguračných nastavení. Okno je rozdelené na tri časti. V prvej časti časti je možné nastaviť jazyk aplikácie, v druhej časti obrazovky sú komunikačné nastavenia pre aktualizáciu vizualizácií elektronických dokumentov a prípadné sieťové nastavenia. V spodnej časti sú lokálne nastavenia aplikácie. Všetky uložené zmeny v konfiguračných nastaveniach aplikácie sa prejavia pri ďalšom spustení aplikácie D.Viewer Java.

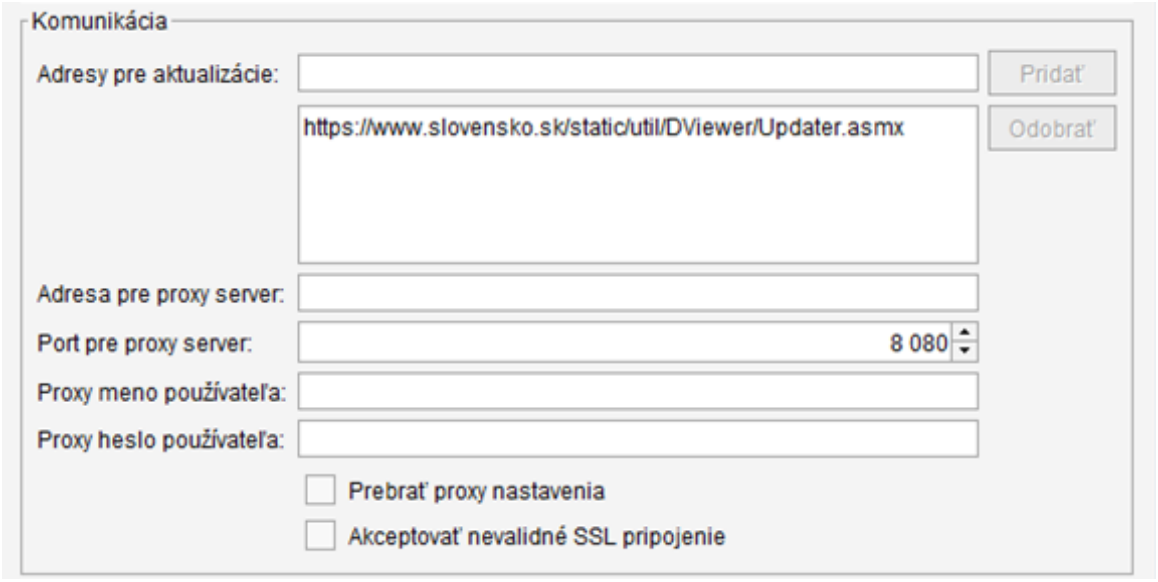


Jazyk aplikácie: nastavenie slovenského alebo anglického jazyka.



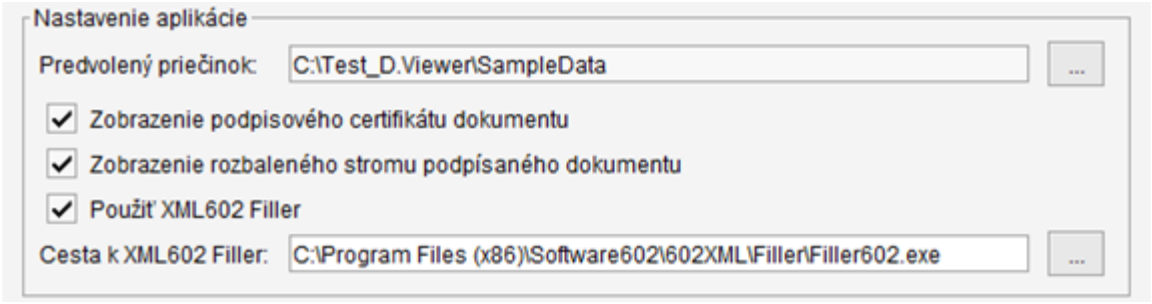
V prípade vynútenia jazyka aplikácie D.Viewer Java z prostredia klientskej aplikácie nebudú konfiguračné nastavenia jazyka aplikácie pre používateľa prístupné.

Komunikačné nastavenia:



- pre aktualizáciu vizualizácií je možné nastaviť viacero serverov, podľa toho, s akými elektronickými formulármi chce používateľ pracovať. V prípade potreby zaevidovania novej URL adresy pre stiahnutie vizualizáciií je potrebné do riadku „Adresy pre aktualizácie“ vypísať URL adresu a následne kliknúť na „Pridať“,
- v prípade prístupu na internet cez proxy server umožňuje aplikácia D.Viewer Java nastaviť adresu proxy servera, port, proxy meno používateľa a proxy heslo používateľa. Taktiež je možné nastaviť či aplikácia bude pri sťahovaní vizualizácií akceptovať nevalidné SSL spojenie.

Lokálne nastavenia aplikácie:

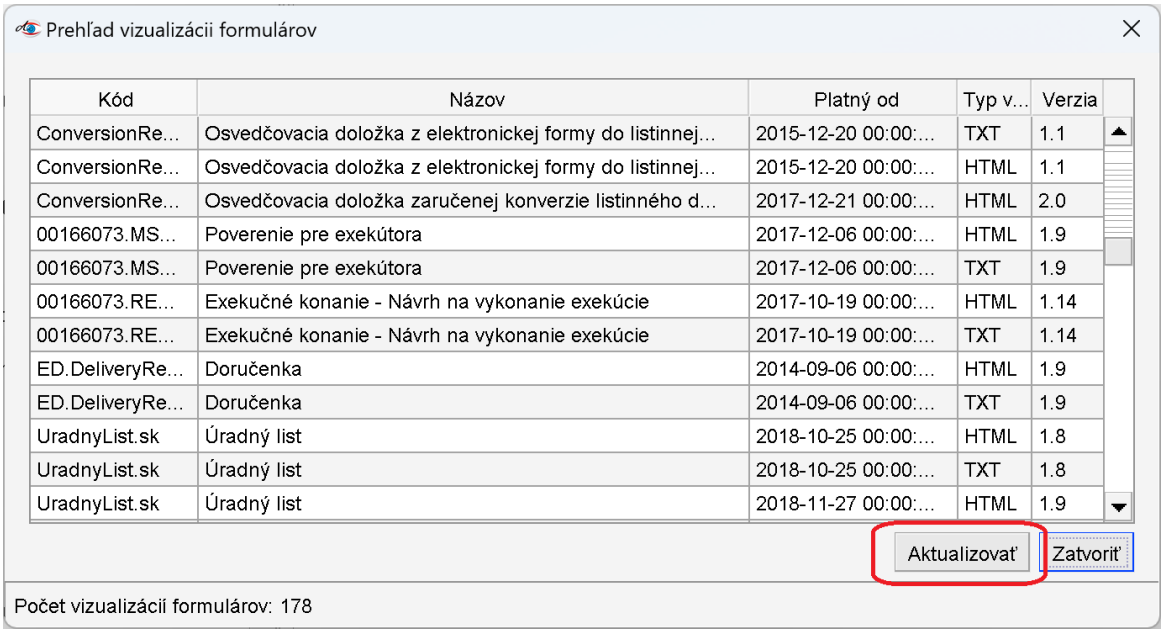


- predvolený priečinok – výber priečinka, ktorý bude otvorený v stromovej štruktúre v ľavej časti obrazovky po štarte aplikácie,
- zobrazenie podpisového certifikátu dokumentu – zobrazuje/skrýva podpisový certifikát dokumentu v strome zobrazenej dátovej štruktúry,

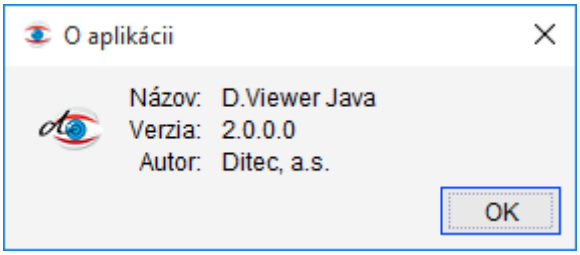
- zobrazovanie rozbaleného stromu podpísaného dokumentu – prepína zobrazovanie rozbaleného/zbaleného stromu dátovej štruktúry po otvorení súboru,
- jazyk aplikácie – nastavenie slovenského alebo anglického jazyka,
- použiť XML602 Filler – prepína použitie aplikácie XML602 Filler pri vizualizácii FO formulárov,
- cesta k aplikácii XML602 Filler – napr. C:\Program Files (x86)\Software602\602XML\Filler\Filler602.exe pre platformu x86 OS MS Windows.

Nástroje → Otvoriť konfiguračný priečinok – otvorí adresár konfiguračných nastavení aplikácie, v ktorom sa nachádzajú konfiguračné konfiguračný súbory ap[likácie a adresár vizualizačných schém elektronických formulárov.

Formuláre – zobrazí okno prehľadu formulárov. V okne sú v tabuľke zobrazené všetky lokálne dostupné vizualizácie (uložené v adresári konfiguračných nastavení aplikácie). Tlačidlom Aktualizovať sa stiahnu najnovšie vizualizácie zo servera, resp. zo serverov, podľa konfiguračných nastavení aplikácie.



O programe – zobrazí informačné okno o verzii aplikácie.



6. Vizualizácia dátových štruktúr

D.Viewer Java v2.0 podporuje vizualizáciu nasledovných dátových štruktúr:

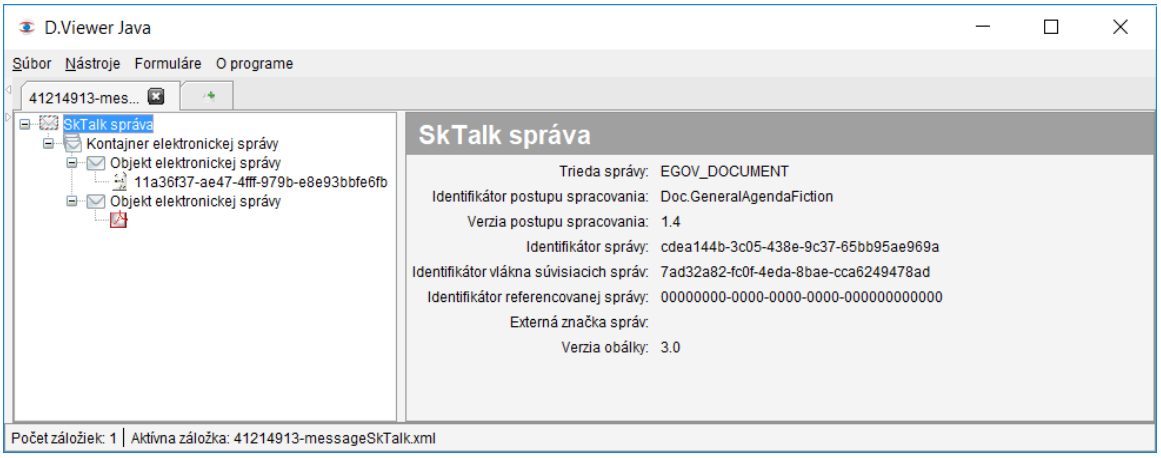
- formát správy pre asynchrónnu komunikáciu v rámci ÚPVS
  - ⇒ SkTalk v2.0 [1],
  - ⇒ SkTalk v3.0 [1],
- formát elektronickej správy
  - ⇒ MessageContainer v1.0 [2],
- formát elektronického podania
  - ⇒ Registration v1.0 [3],
- formát zaručeného elektronického podpisu na báze XAdES
  - ⇒ XAdES_ZEP v1.0 [4],
  - ⇒ XAdES_ZEP v1.1 [5],
  - ⇒ XAdES_ZEP v2.0 [6],
- formát zaručeného elektronického podpisu na báze XAdES Baseline Profile
  - ⇒ XAdES_ZEPbp v1.0 [7],
- formát zloženého elektronického podpisu, pozostávajúceho z viacerých samostatných elektronických podpisov XAdES_ZEP
  - ⇒ DataSignatures v1.0 [4],
  - ⇒ DataSignatures v1.1 [5],
  - ⇒ DataSignatures v2.0 [6],
- formát obálky pre podpis(y) a ďalšie informácie súvisiace s podpisovanými dátovými objektami na báze ASiC Baseline Profile
  - ⇒ ASiC_bp v1.0 [8],
- formát zaručeného elektronického podpisu na báze CAdES
  - ⇒ CAdES_ZEP v1.0 [9],
  - ⇒ CAdES_ZEP v2.0 [10],
- formát ZIP obálky pre CAdES podpis(y) a ďalšie informácie súvisiace s podpisovanými dátovými objektami
  - ⇒ ZIP formát súboru (ZEPf) [11],
- formát kontajnera XML údajov
  - ⇒ XMLDataContainer v1.0 [1],
  - ⇒ XMLDataContainer v1.1 [1].

6.1. SkTalk

SkTalk je definovaný formát správ založený na XML dokumentoch určených pre asynchrónnu komunikáciu jednotlivých modulov v rámci ÚPVS podľa [1]. SkTalk je dátový prvok, ktory môže obsahovať viaceré kontajnery elektronickej správy (6.2) a/alebo viaceré objekty elektronickej správy. Aplikácia D.Viewer Java zobrazuje SkTalk pod názvom SkTalk správa a v rámci detailu sa zobrazujú atribúty:

- trieda správy - primárny identifikátor typu správy, podľa ktorého moduly UPVS a prijímateľ rozpoznávajú obsah dokumentu a na základe ktorého sa riadi spracovanie, overenie a smerovanie danej správy,
- identifikátor postupu spracovania – sekundárny identifikátor typu správy, na základe ktorého sa riadi spracovanie, overenie a smerovanie danej správy,
- verzia postupu spracovania – je rozšírenie identifikátora postupu spracovania. Hodnota elementu udáva verziu postupu spracovania, ktorá má byť použitá pre spracovanie správy v rámci ÚPVS,
- identifikátor správy – jednoznačne identifikuje správu,
- identifikátor vlákna súvisiacich správ – slúži na vzájomné previazanie všetkých správ týkajúcich sa jedného konkrétneho podania,
- identifikátor referencovanej správy – slúži na previazanie správ na inú (referenčnú) správu. Obsahuje hodnotu identifikátora správy správy, ku ktorej sa viaže,
- externá značka správy – identifikátor jednoznačne identifikujúci správu. Môže byť v čitateľnom tvare. Jeho formát určuje poskytovateľ služby,
- verzia obálky - použitá verzia formátu pre komunikáciu. Pre verziu SKTalk 3.0 obsahuje číslo 3.0.

Príklad zobrazenia SkTalk, ktorý obsahuje jeden kontajner elektronickej správy a v ňom dva objekty elektronickej správy.



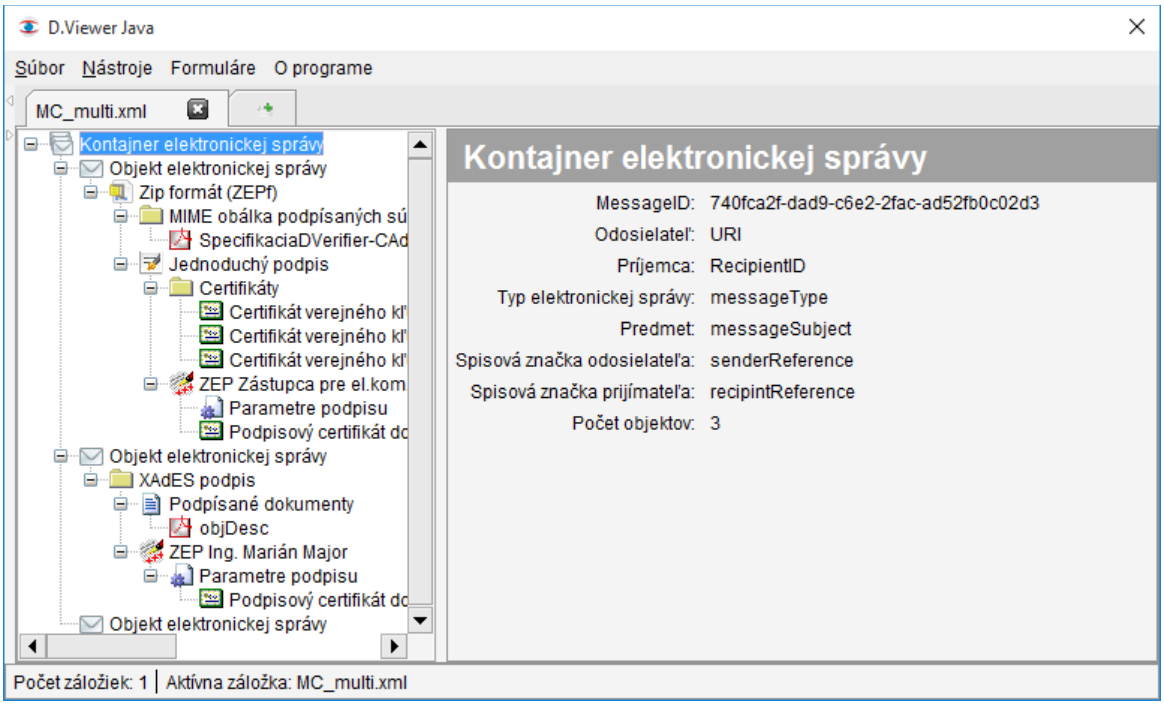
6.2. MessageContainer

Kontajner elektronickej správy, resp. Elektronické podanie (MessageContainer) je dátový prvok, ktory môže obsahovať viaceré objekty elektronickej správy. Aplikácia

D.Viewer Java zobrazuje MessageContainer pod názvom Kontajner elektronickej správy a v rámci detailu sa zobrazujú atribúty:

- messageId - jednoznačný identifikátor elektronickej správy,
- odosielateľ - jednoznačný identifikátor odosielateľa elektronickej správy,
- príjemca - jednoznačný identifikátor prijímateľa elektronickej správy,
- typ elektronickej správy - identifikuje typ podania, rozhodnutia a podobne,
- predmet - stručný popis predmetu elektronickej správy,
- spisová značka odosielateľa - spisová značka odosielateľa elektronickej správy,
- spisová značka prijímateľa - spisová značka prijímateľa elektronickej správy,
- počet objektov – počet objektov kontajnera elektronickej správy.

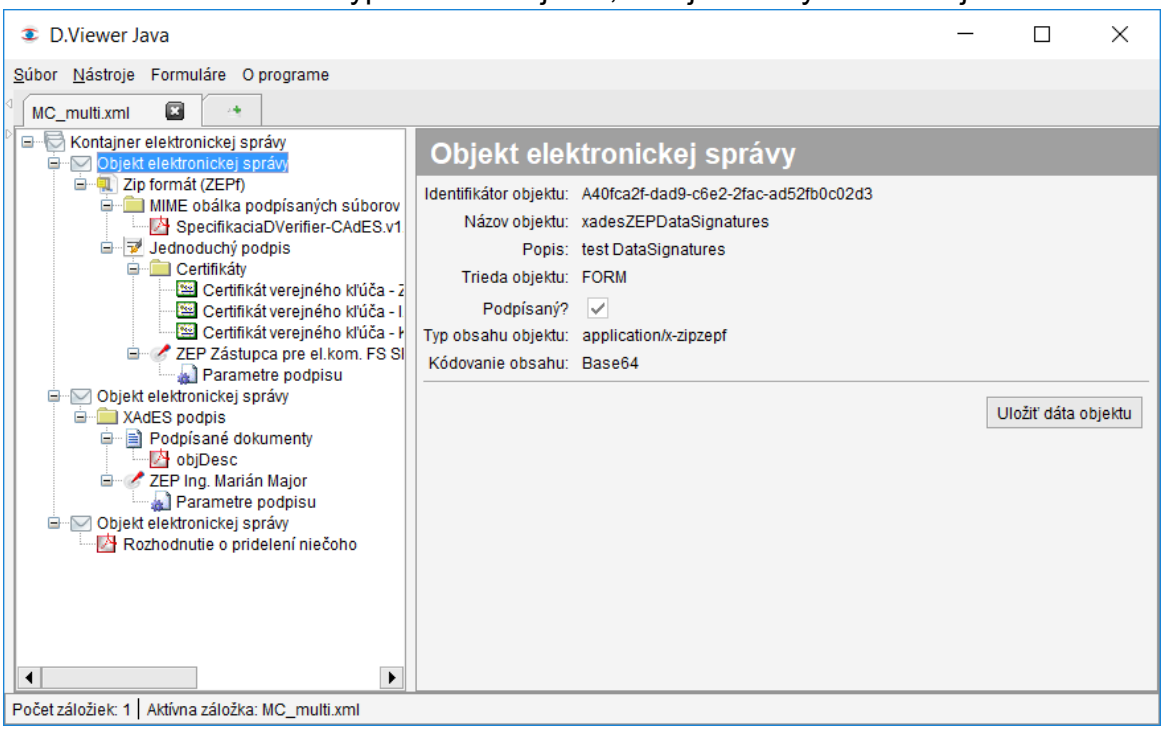
Príklad zobrazenia kontajnera elektronickej správy (MessageContainer), ktorý obsahuje tri objekty elektronickej správy. Dva podpísané elektronickým podpisom vo formáte XAdES_ZEP, z čoho je jeden zabalený do ZEPfZIP obálky a tretí nepodpísaný objekt elektronickej správy.



V rámci detailov vybraného objektu elektronickej správy sa zobrazujú nasledovné atribúty:

- identifikátor objektu - reťazec slúžiaci ako jednoznačný identifikátor objektu elektronickej správy,
- názov objektu - názov objektu, spravidla názov pôvodného súboru,
- popis - popis objektu, určený na zobrazenie,

- trieda objektu - trieda objektu, slúži na identifikovanie typu / účelu použitia objektu,
- podpísaný - príznak, či je objekt elektronicky podpísaný,
- kódovanie obsahu - typ obsahu objektu, určuje dátový formát objektu.



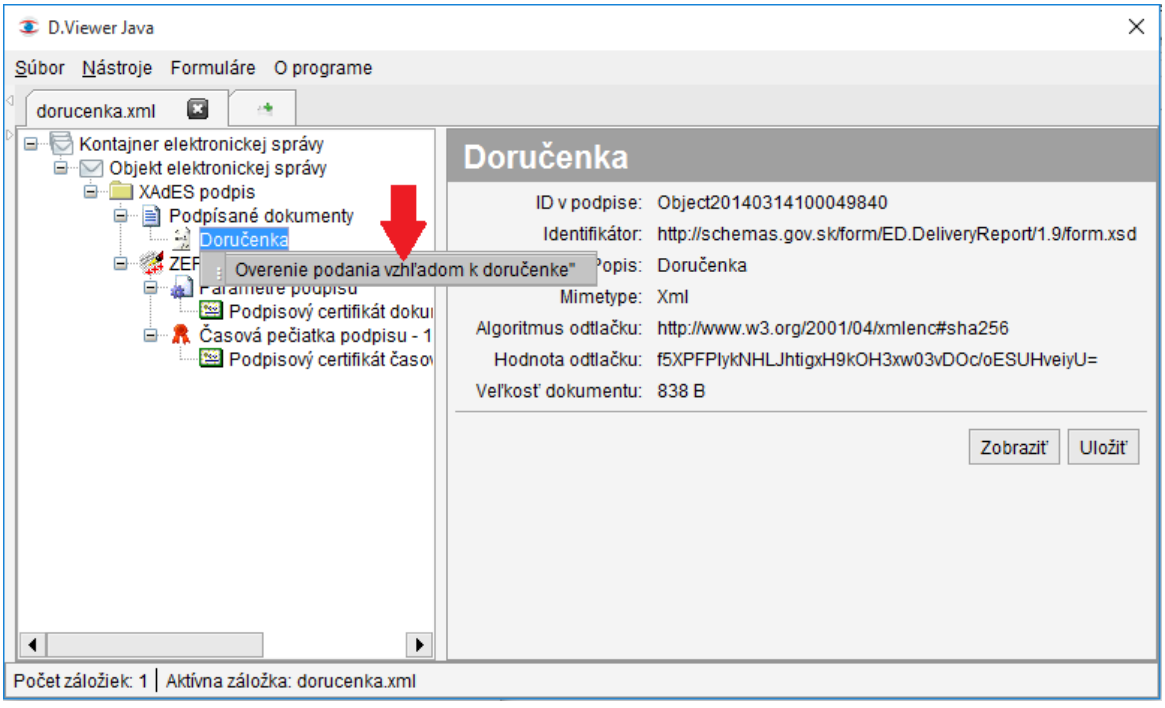
6.2.1. Overenie podania voči doručenke

Doručenka je elektronický dokument, obsahujúci údaj o dni, hodine, minúte a sekunde elektronického doručenia, identifikátor osoby prijímateľa, identifikátor osoby odosielateľa a identifikáciu elektronickej správy a elektronických dokumentov, ktoré sa elektronicky doručujú. Ak je adresátom orgán verejnej moci, doručenku vytvára a potvrdzuje elektronická podateľňa tohto orgánu. Ak adresátom nie je orgán verejnej moci, doručenku vytvára automatizovaným spôsobom modul elektronického doručovania a úrad vlády prostredníctvom modulu elektronických schránok zabezpečuje, aby prijímateľ pri preberaní doručovaného elektronického dokumentu vždy pred sprístupnením dokumentu mal k dispozícii a bol povinný potvrdiť doručenku. Doručenkou prijímateľ potvrdzuje jej autorizáciou. Doručenka sa elektronicky doručuje do elektronickej schránky odosielateľa elektronickej správy, ktorej doručenie doručenka potvrdzuje.

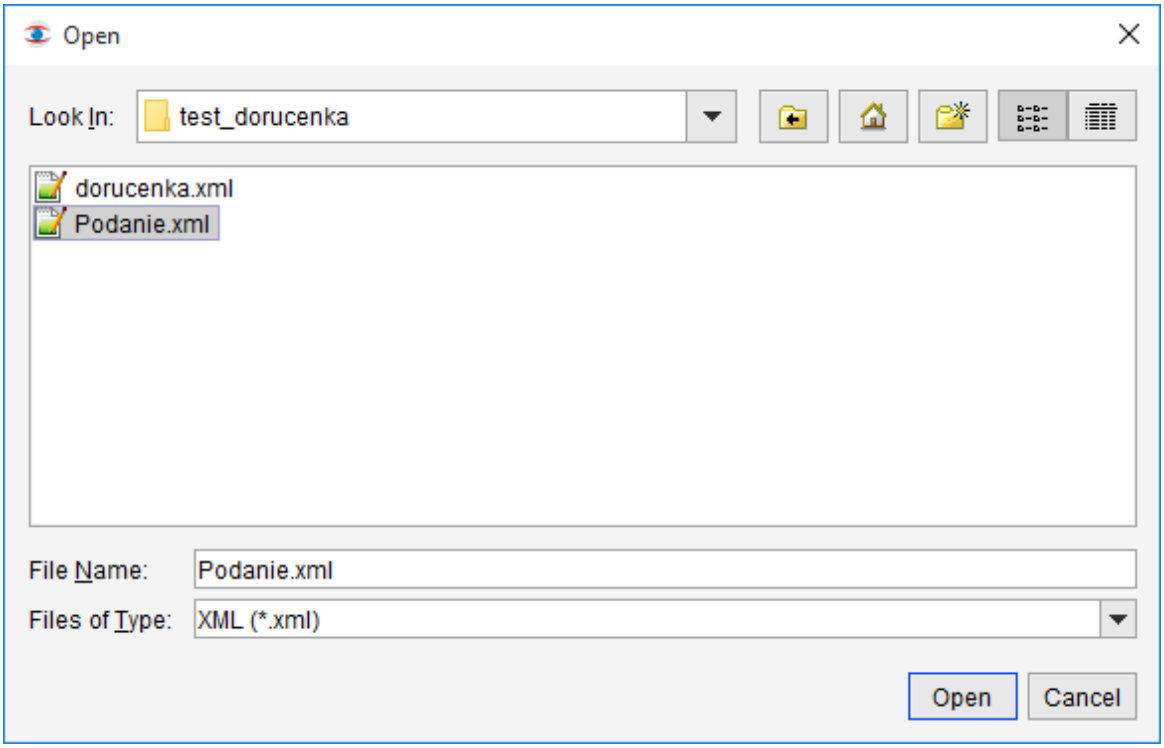
Doručenka sa používateľovi zobrazuje v rámci kontajnera elektronickej správy ako podpísaný dokument s URI identifikátorom http://schemas.gov.sk/form/ED.DeliveryReport/1.9/form.xsd.



Ak kontajner elektronickej správy obsahuje Doručenku, kliknutím pravým tlačidlom myši na položku Doručenky v strome zobrazenej dátovej štruktúry sa používateľovi sprístupní operácia Overiť podanie vzhľadom k doručenke.

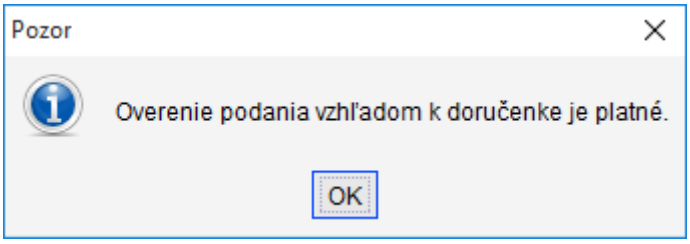


Po potvrdení operácie Overiť podanie vzhľadom k doručenke sa zobrazí dialógové okno pre výber súboru elektronického podania v rámci operačného systému používateľa.

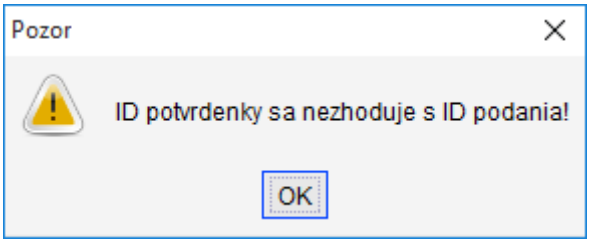


Používateľ vyberie súbor elektronického podania (MessageContainer). Aplikácia následne použije transformáciu a hash funkciu uvedenú v doručenke, vyráta digitálny odtlačok podania a vykoná porovnanie s digitálnym odtlačkom v doručenke.

Ak je digitálny odtlačok v doručenke zhodný s digitálnym odtlačokm podania, používateľovi sa zobrazí hláška.

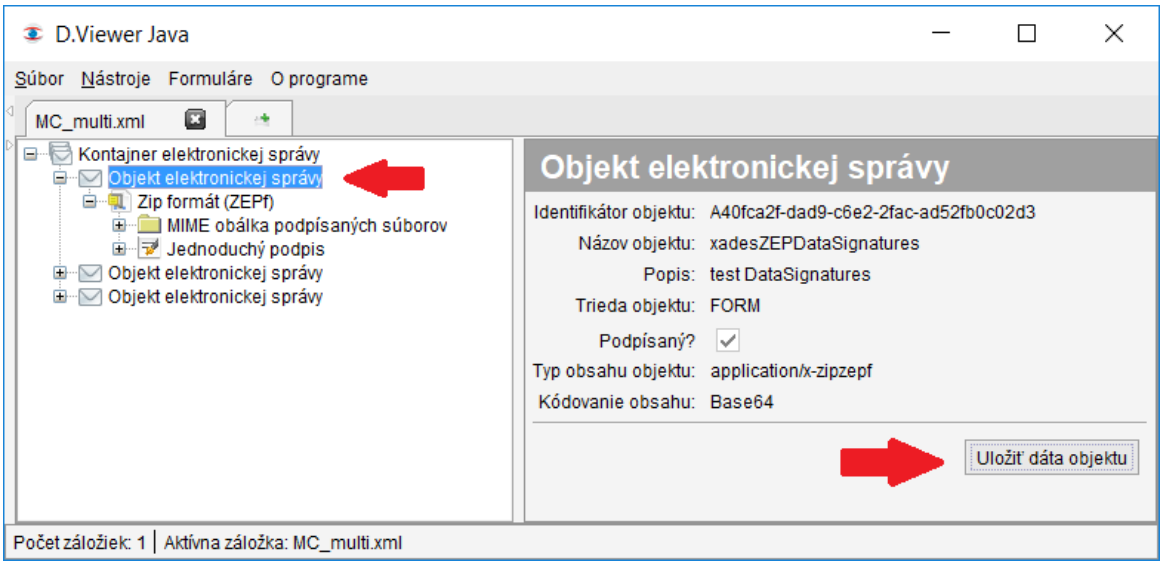


Ak digitálny odtlačok v doručenke nie je zhodný s digitálnym odtlačkom podania, používateľovi sa zobrazí hláška.

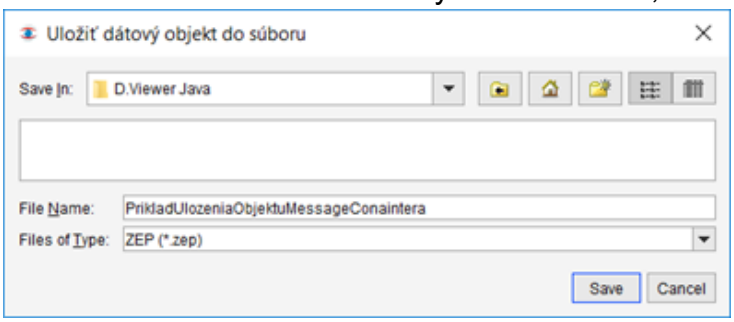


6.2.2. Uloženie vybraného objektu elektronickej správy

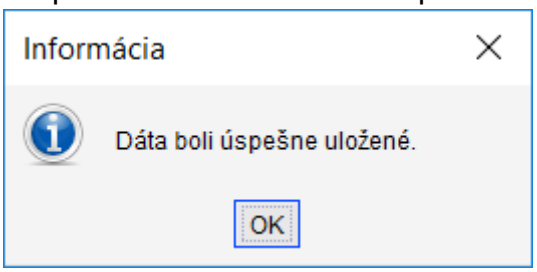
MessageContainer môže obsahovať viaceré objekty elektronickej správy, pričom aplikácia D.Viewer Java umožňuje uložiť objekty do samostatných súborov na disk.



V následnom okne uloženia objektu do súboru je možné vybrať cestu k uloženému súboru na disku a zvoliť vlastný názov súboru, do ktorého budú dáta uložené.



Po potvrdení a zrealizovaní operácie bude zobrazené informačné okno.



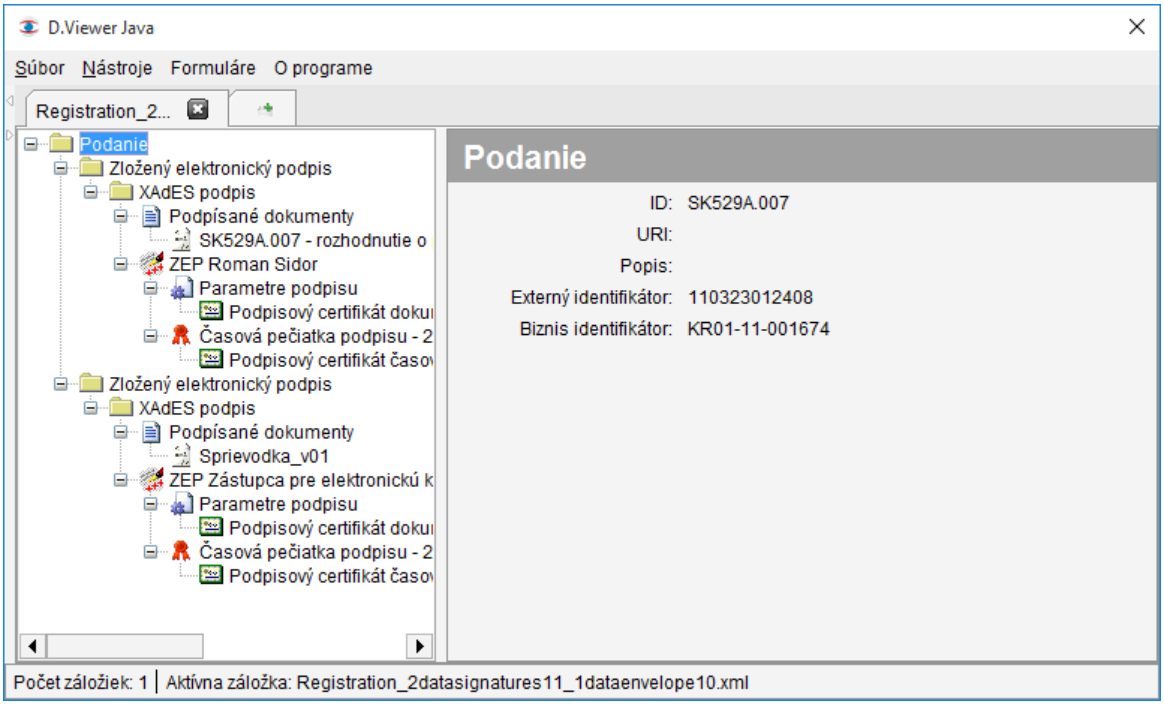
6.3. Registration

Kontajner elektronického podania (Registration) je dátový prvok, ktorý môže obsahovať viaceré objekty elektronickej správy. Aplikácia D.Viewer Java zobrazuje

dátový prvok Registration pod názvom Podanie a v rámci detailu sa zobrazujú atribúty:

- ID - reťazec slúžiaci ako jednoznačný identifikátor typu elektronického podania,
- URI - bližšia identifikácia elektronického podania. Z pohľadu spracovania nie je vyžadovaný ani inak kontrolovaný, pokiaľ to nie je explicitne vyžadované správcom biznisu,
- popis - bližšia identifikácia elektronického podania,
- externý identifikátor - identifikácia externého systému v pripade komunikácie podateľňa-podateľňa,
- biznis identifikátor - identifikátor biznis prípadu. Umožňuje odosielateľovi prideliť vlastný identifikátor k zaslanému podaniu. Odpovede viažúce sa k danému podaniu budú mať vyplnený tento identifikátor za účelom párovania odpovede.

Príklad zobrazenia Elektronického podania (Registration), obsahujúceho dva Zložené elektronické podpisy.



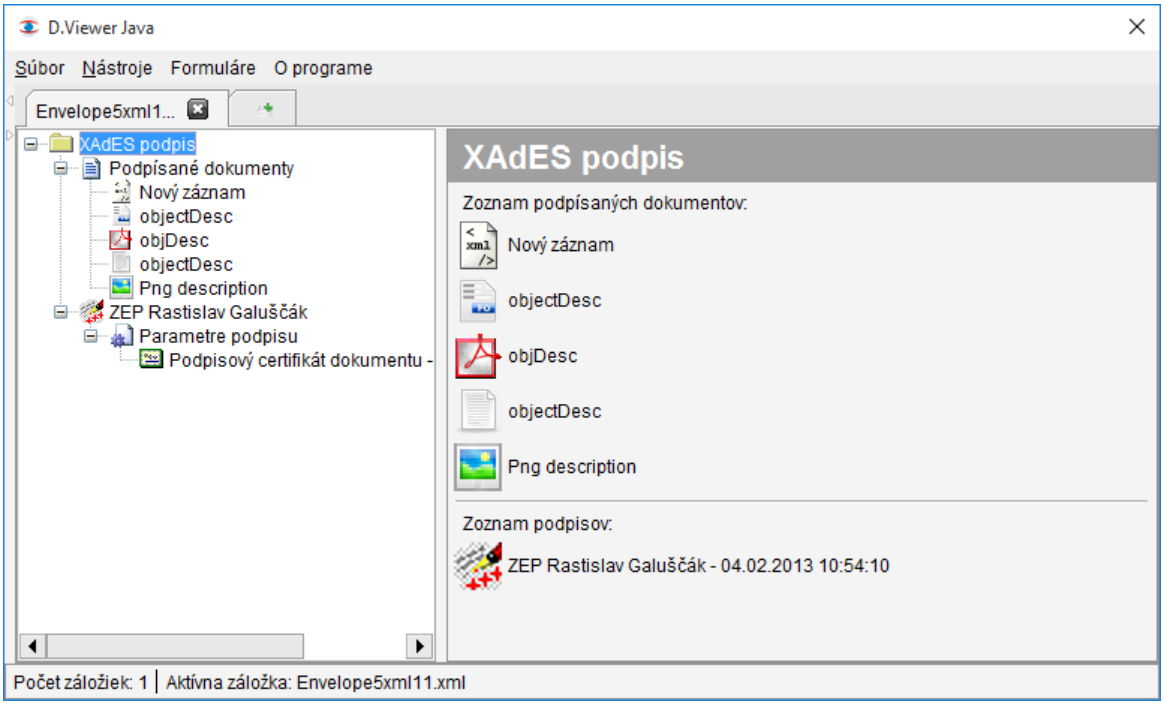
6.4. XAdES_ZEP

XAdES_ZEP [4] [5] [6] a XAdES_ZEPbp [7] je formát elektronického podpisu definovaný v súlade so špecifikáciou XAdES a zároveň platnou legislatívou Slovenskej republiky pre oblasť elektronického podpisu, pre vytváranie a overovanie zaručeného elektronického podpisu, resp. zaručenej elektronickej pečate, nad množinou povolených formátov dátových objektov (XML, FO, PDF, PNG, TXT).

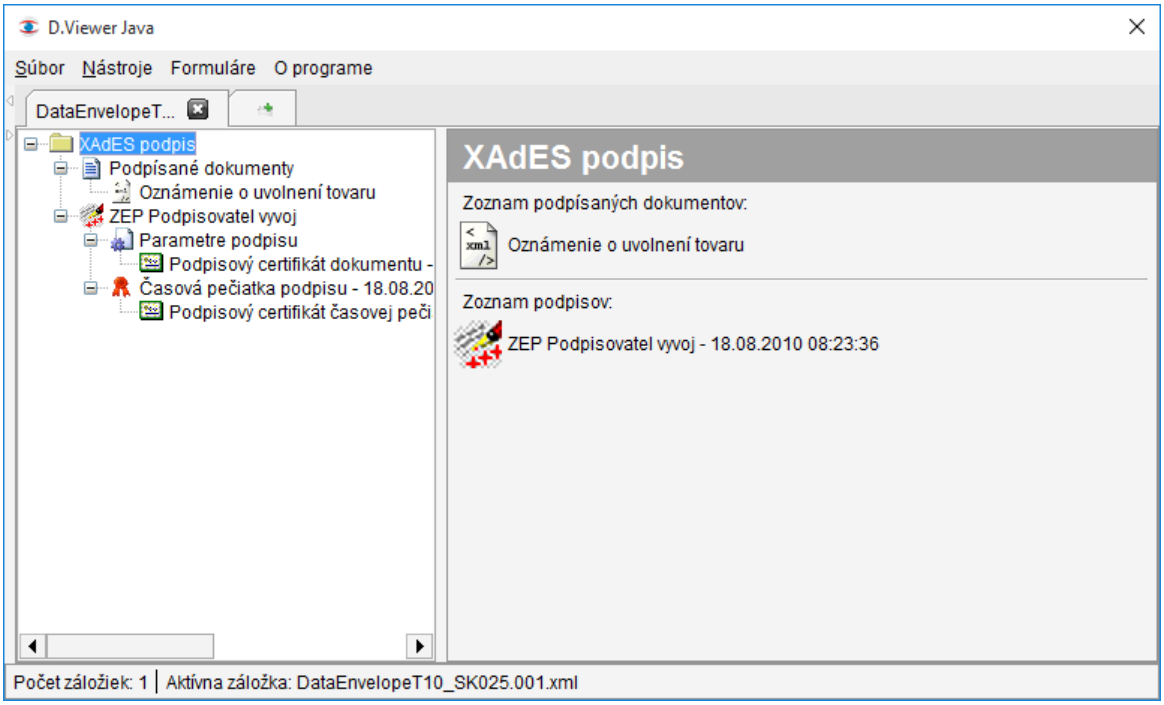
Aplikácia D.Viewer Java zobrazuje elektronický podpis, resp. elektronickú pečať vo formáte XAdES_ZEP pod názvom XAdES podpis. V hierarchickej stromovej štruktúre sa v rámci XAdES podpisu zobrazujú dátové objekty:

- Podpísané dokumenty – podpísaných môže byť jeden alebo viac elektronických dokumentov vo formátoch XML, FO, PDF, PNG, TXT
- Podpis – vo formáte XAdES_ZEP
  - ⇒ Časová pečiatka podpisu – povinné pre formát podpisu XAdES-T, XAdES-X type 1, XAdES-A
  - ⇒ Časová pečiatka referencií validačných dát – povinné pre formát podpisu XAdES-X type 1, nepovinné pre formát podpisu XAdES-A
  - ⇒ Referencie certifikátov - povinné pre formát podpisu XAdES-X type 1, nepovinné pre formát podpisu XAdES-A
  - ⇒ Referencie informácií o revokácii - povinné pre formát podpisu XAdES-X type 1, nepovinné pre formát podpisu XAdES-A
  - ⇒ Časová pečiatka archívna – povinné pre formát podpisu XAdES-A
  - ⇒ Certifikáty – povinné pre formát podpisu XAdES-A
  - ⇒ Informácia o revokácii - povinné pre formát podpisu XAdES-A

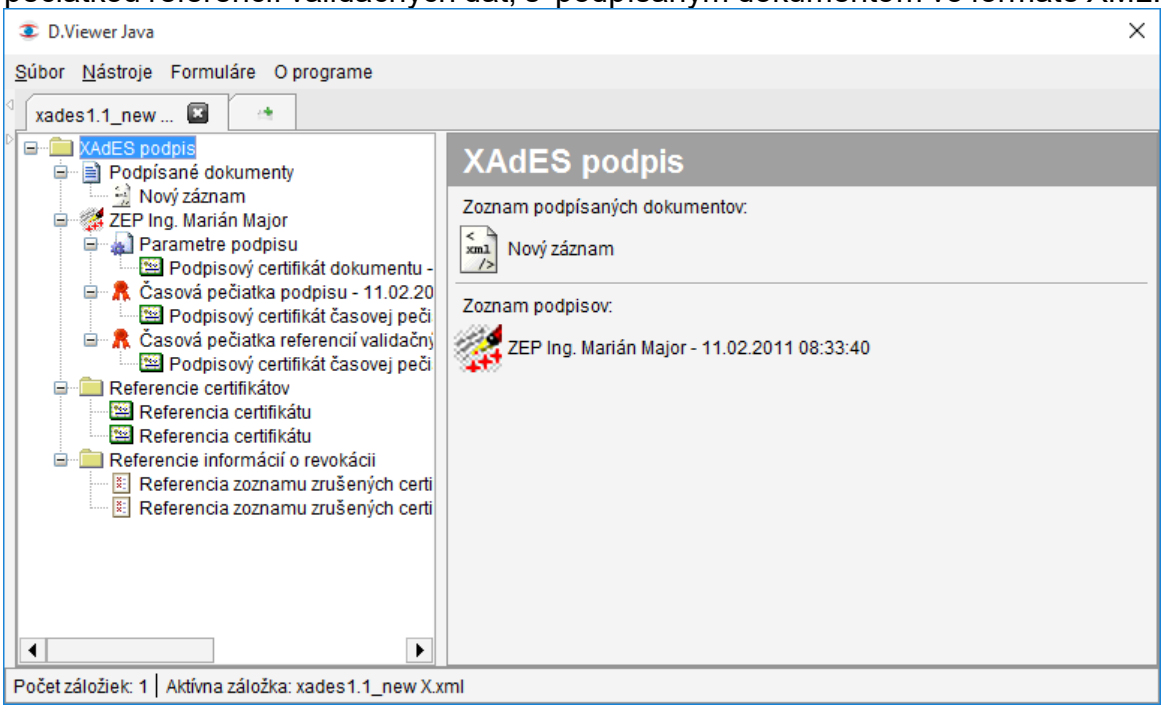
Príklad zobrazenia elektronického podpisu vo formáte XAdES_ZEP_EPES (bez časovej pečiatky), s piatimi podpísanými dokumentami.



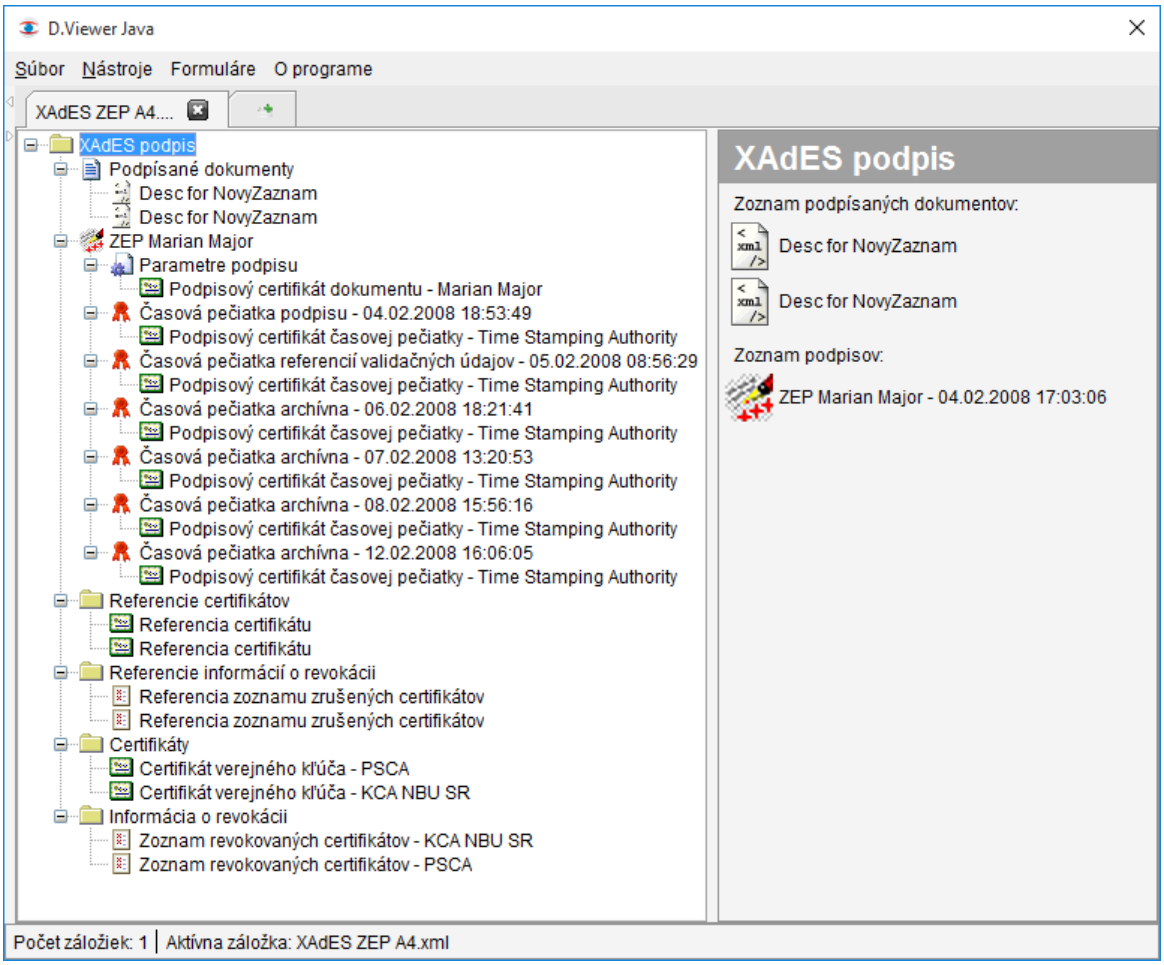
Príklad zobrazenia elektronického podpisu vo formáte XAdES_ZEP_T s časovou pečiatkou podpisu, s podpísaným dokumentom vo formáte XML.



Príklad zobrazenia elektronického podpisu vo formáte XAdES_ZEP_X1 s časovou pečiatkou referencií validačných dát, s podpísaným dokumentom vo formáte XML.



Príklad zobrazenia elektronického podpisu vo formáte XAdES_ZEP_A so štyrmi archívnymi časovými pečiatkami, s dvoma podpísanými dokumentami vo formáte XML.



6.5. DataSignatures

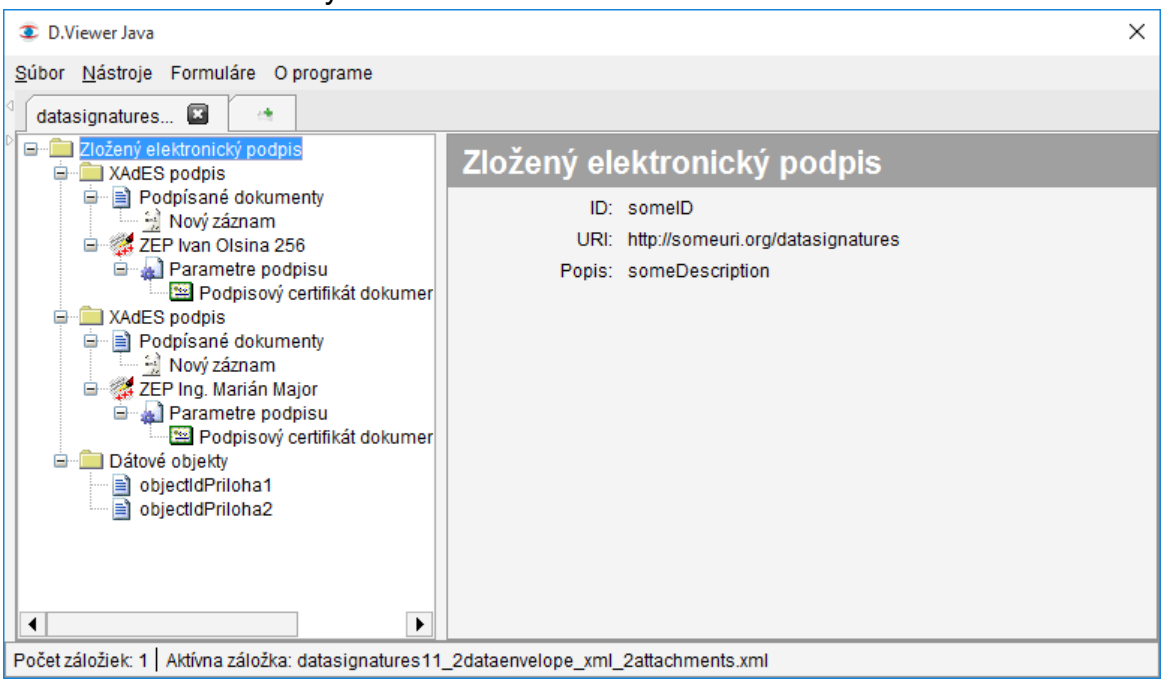
DataSignatures je formát zloženého elektronického podpisu, pozostávajúceho z viacerých samostatných elektronických podpisov XAdES_ZEP. V rámci zloženého elektronického podpisu je možné spojiť niekoľko nezávislých elektronických podpisov, ktoré boli vytvorené v súlade s profilom XAdES_ZEP, prípadne nad tými istými dátovými objektami. Príslušnosť jednotlivých dátových objektov a samotných štruktúr elektronických podpisov je zabezpečená pomocou referencií cez Id atribúty.

Aplikácia D.Viewer Java zobrazuje zložený elektronický podpis pod názvom Zložený elektronický podpis a v rámci detailu sa zobrazujú atribúty:

- ID - identifikátor danej inštancie vytvoreného zloženého elektronického podpisu,
- URI - jednoznačný identifikátor profilu dátovej štruktúry zloženého elektronického podpisu,

- Popis - popis inštancie alebo profilu zloženého elektronického podpisu
- V hierarchickej stromovej štruktúre v rámci Zloženého elektronického podpisu sa zobrazujú dátové objekty:
- Podpísaná zložka – jeden alebo viac elektronických podpisov vo formáte XAdES_ZEP
- Dátové objekty – nepovinné, jeden alebo viacero nepodpísaných elektronických dokumentov

Príklad zobrazenia zloženého elektronického podpisu DataSignatures, ktorý obsahuje dva elektronické podpisy vo formáte XAdES_ZEP a dva nepodpísané elektronické dokumenty.



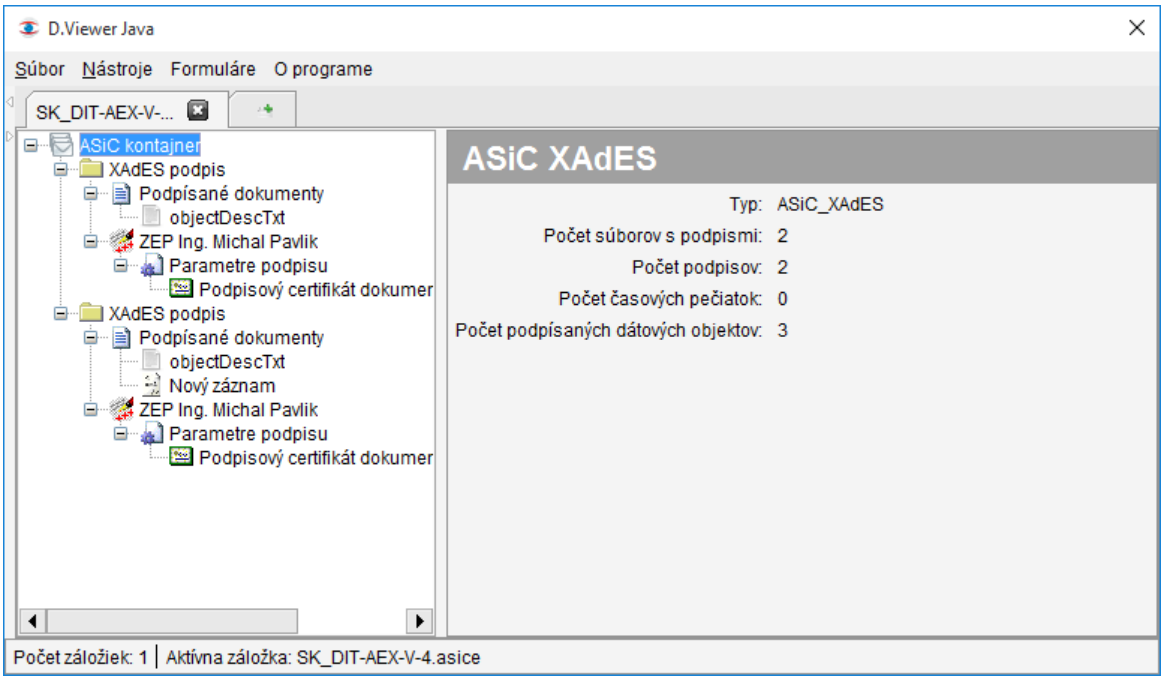
6.6. ASiC Baseline Profile

Associated Signature Containers (ASiC) je dátový kontajner spájajúci podpísané dátové objekty s elektronickými podpismi.

Aplikácia D.Viewer Java zobrazuje ASiC obálku pod názvom ASiC kontajner a v rámci detailu sa zobrazujú atribúty:

- Typ – typ podpisov zabalených v rámci ASiC kontajnera,
- Počet súborov s podpismi – celkový počet podpísaných súborov v rámci ASiC kontajnera,
- Počet podpisov – celkový počet zabalených podpisov v kontajnery,
- Počet časových pečiatok - celkový počet zabalených časových pečiatok v kontajnery,
- Počet podpísaných dátových objektov – celkový počet zabalených podpísaných dátových objektov v kontajnery.

Príklad zobrazenia ASiC kontajnera, ktorý obsahuje dva XAdES podpisy, pričom jeden podpisuje jeden textový dátový objekt, druhý naviac aj dátový objekt typu XML.



6.7. CAdES_ZEP

CAdES_ZEP [9] [10] je formát elektronického podpisu definovaný v súlade so špecifikáciou CAdES a zároveň platnou legislatívou Slovenskej republiky pre oblasť elektronického podpisu, pre vytváranie a overovanie zaručeného elektronického podpisu, resp. zaručenej elektronickej pečate, nad množinou povolených formátov dátových objektov (XML, PDF, PNG, TXT). Podpisované dátové objekty sú štandardne vložené do S/MIME obálky, v prípade integritného podpisu je podpisovaný textový súbor obsahujúci referencie dát chránených integritným podpisom.

Aplikácia D.Viewer Java zobrazuje elektronický podpis, resp. elektronickú pečať vo formáte CAdES_ZEP pod názvom CAdES podpis. V hierarchickej stromovej štruktúre sa v rámci CAdES podpisu zobrazujú dátové objekty:

- Vnorené podpísané dáta – položka sa zobrazuje iba v prípade interného podpisu. V prípade externého podpisu nie sú podpísané dáta vložené do CMS štruktúry podpisu,
- Certifikáty – zoznam obsahuje povinne všetky podpisové certifikáty a nepovinne certifikáty z certifikačnej cesty podpisových certifikátov,
- Informácia o revokácii – zoznam(y) revokovaných certifikátov (CRL) a OCSP odpovedí,
- Podpis – CMS štruktúra CAdES podpisu môže obsahovať jeden alebo viacero podpisov (SignerInfo) vo formáte CAdES_ZEP,

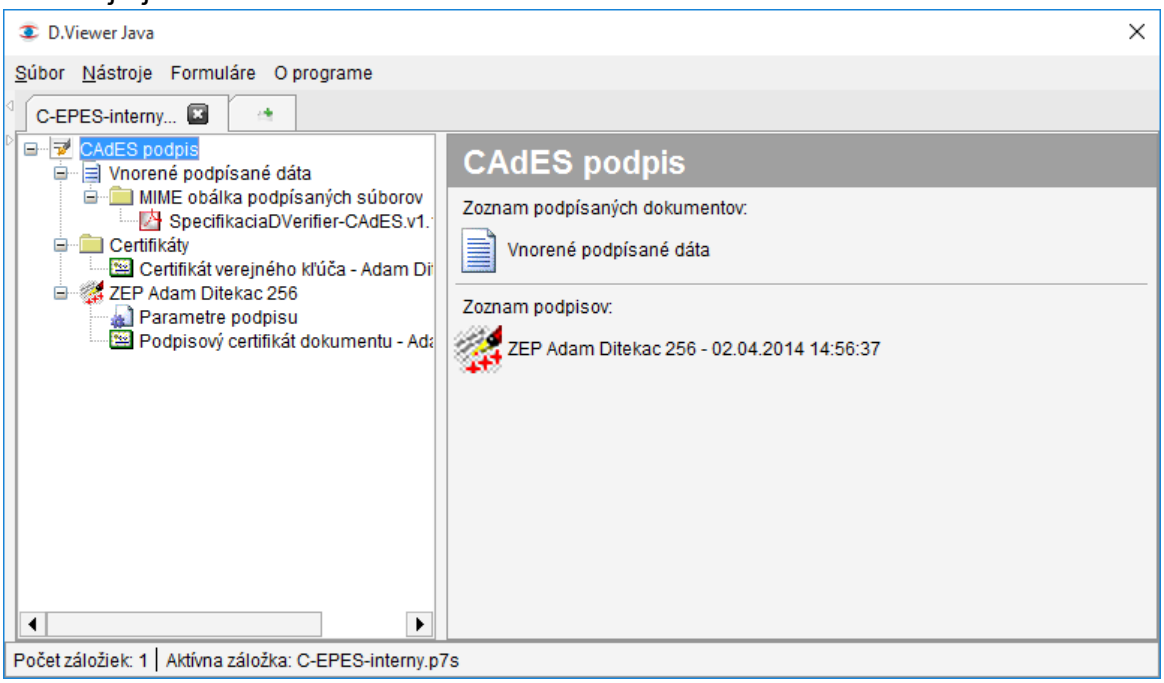
⇒ Časová pečiatka podpisu – povinné pre formát podpisu CAdES-T a vyššie formy pdopisu,

⇒ Časová pečiatka archívna – povinné pre formát podpisu CAdES-A,

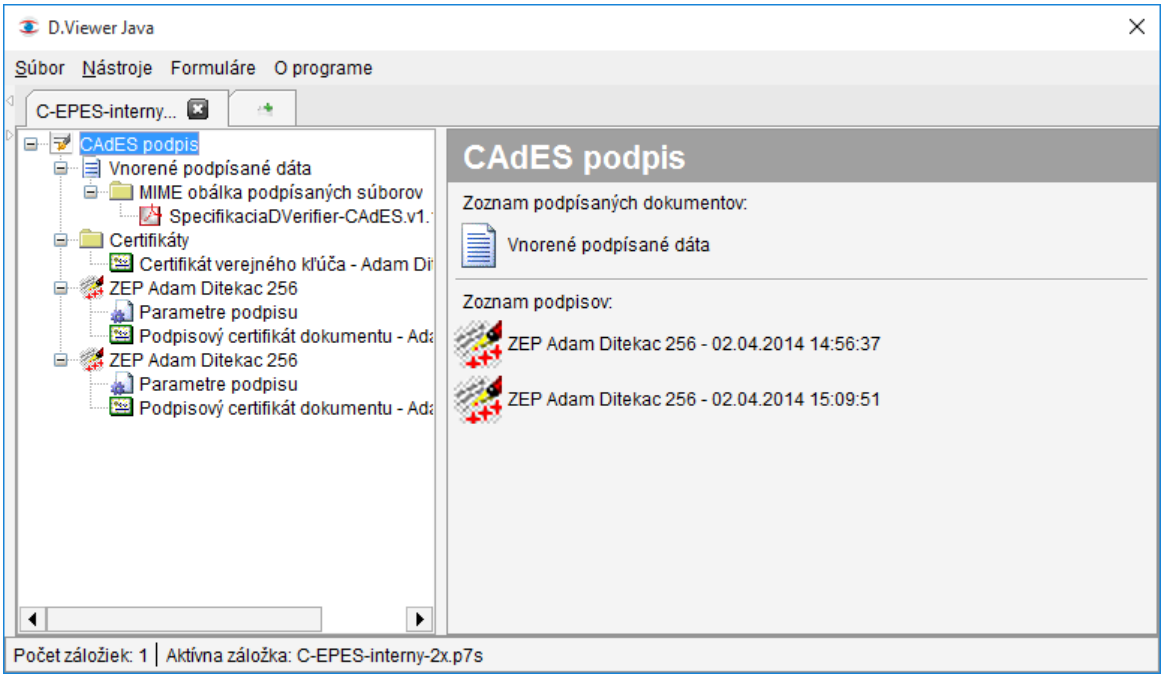
⇒ Certifikáty – nepovinný zoznam certifikátov, ak je uvedený, len tieto certifikáty sú použité pri overovaní,

⇒ Informácie o revokácii – povinné pre formát podpisu CAdES-C a vyššie formy pdopisu.

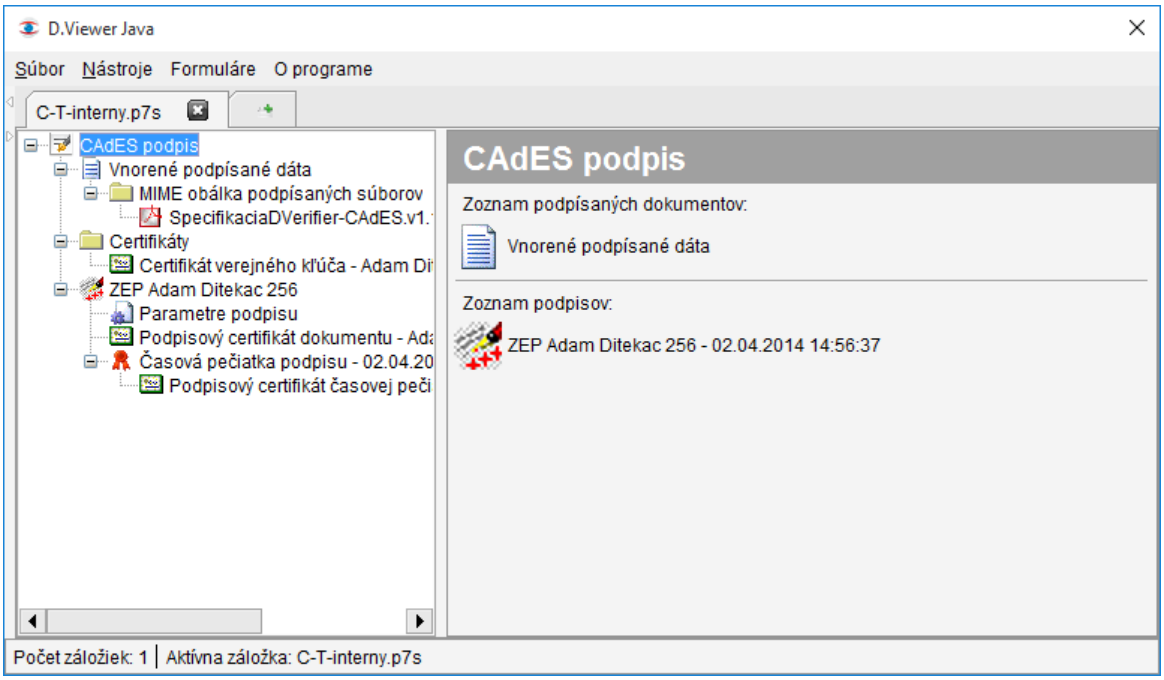
Príklad zobrazenia interného elektronického podpisu vo formáte CAdES_ZEP_EPES (bez časovej pečiatky), s podpísanou S/MIME obálkou, ktorá obsahuje jedent súbor vo formáte PDF.



Príklad zobrazenia dvojitého interného elektronického podpisu vo formáte CAdES_ZEP_EPES (bez časovej pečiatky), s podpísanou S/MIME obálkou, ktorá obsahuje jeden súbor vo formáte PDF. CMS štruktúra v tomto príklade obsahuje dva podpisy (dve sekcie SignerInfo).



Príklad zobrazenia interného elektronického podpisu vo formáte CAdES_ZEP_T (s časovou pečiatkou), s podpísanou S/MIME obálkou, ktorá obsahuje jeden súbor vo formáte PDF.



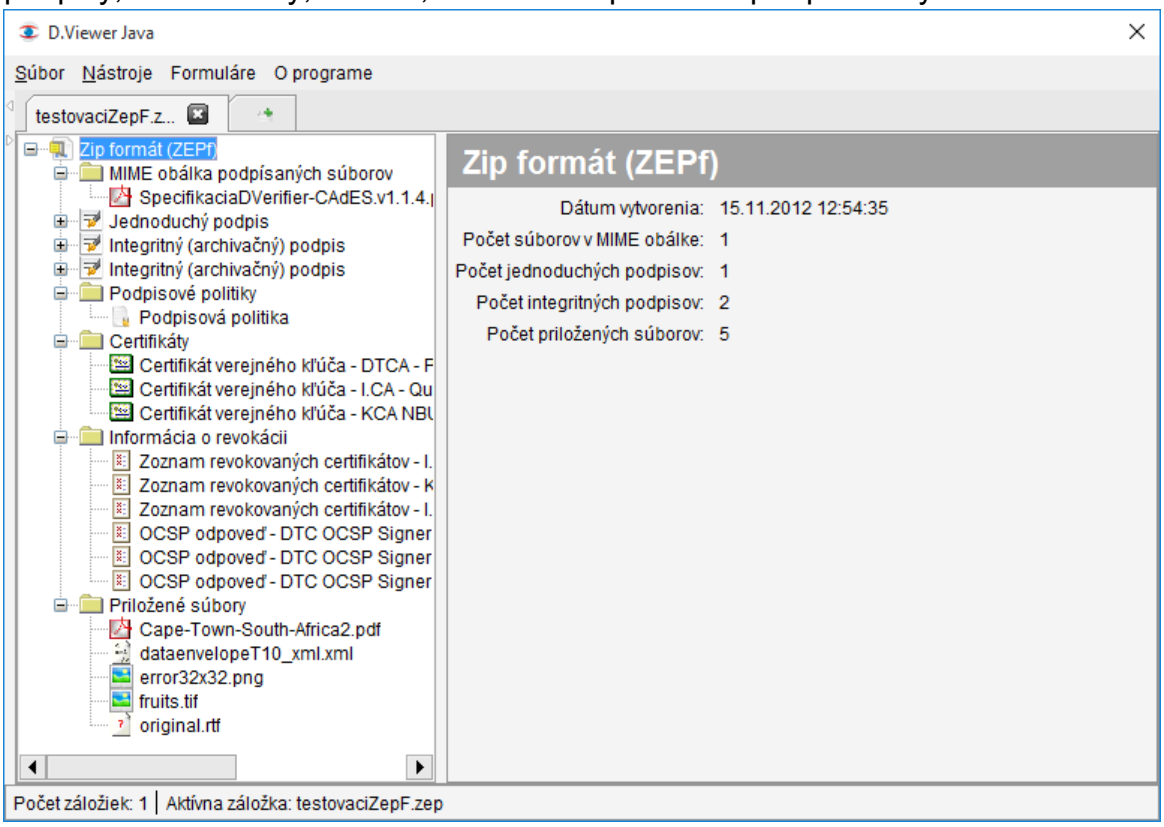
6.8. ZIP formát súboru (ZEPf)

Podpisovaný dokument, jeho podpisy, informácie potrebné na overenie podpisu dokumentu a ďalšie dokumenty súvisiace s podpisovaným dokumentom je potrebné spojiť do formátu, ktorého spracovanie je jednoduché a bežne dostupné. Medzi takéto bežne dostupné formáty patrí aj ZIP.

Aplikácia D.Viewer Java zobrazuje ZEPfZIP obálku pod názvom ZIP formát súboru (ZEPf). V hierarchickej stromovej štruktúre v rámci ZEPfZIP obálky sa zobrazujú dátové objekty:

- MIME obálka podpísaných súborov – v prípade externého CAdES podpisu sú podpisované dátové objekty (XML, PDF, PNG, TXT, etc.) štandardne vložené do S/MIME obálky,
- Jednoduchý podpis – ZEPfZIP obálka môže nepovinne obsahovať jeden alebo viacero jednoduchých CAdES podpisov, pozri kapitola 6.6 CAdES ZEP,
- Integritný (archivačný) podpis - ZEPfZIP obálka môže nepovinne obsahovať jeden alebo viacero integritných (archivačných) CAdES podpisov, pozri kapitola 6.6 CAdES ZEP,
- Podpisové politiky – nepovinne jedna alebo viac podpisových politík,
- Certifikáty - nepovinne jeden alebo viac certifikátov,
- Informácia o revokácii – nepovinne zoznam(y) revokovaných certifikátov (CRL) a OCSP odpovedí,
- Priložené súbory – nepovinne zoznam priložených súborov.

Príklad zobrazenia ZIP formátu súboru (ZEPf), ktorý obsahuje MIME obálku s vloženým PDF súborom, jeden jednoduchý podpis, dva integritné (archivačné) podpisy, tri certifikáty, tri CRL, tri OCSP odpovede a päť priložených súborov.



6.9. Vizualizácia súčastí dátových štruktúr

Dátové štruktúry uvedené v predchádzajúcom texte môžu obsahovať rôzne typy dátových objektov a táto kapitola popisuje spôsob ich vizualizácie v rámci aplikácie D.Viewer Java.

6.9.1. Podpis

V dátovej štruktúre XAdES_ZEP (XAdES podpis) sa nachádza vždy jeden podpis, v dátovej štruktúre CAdES_ZEP (CAdES podpis) sa môže nachádzať jeden alebo viacero podpisov.

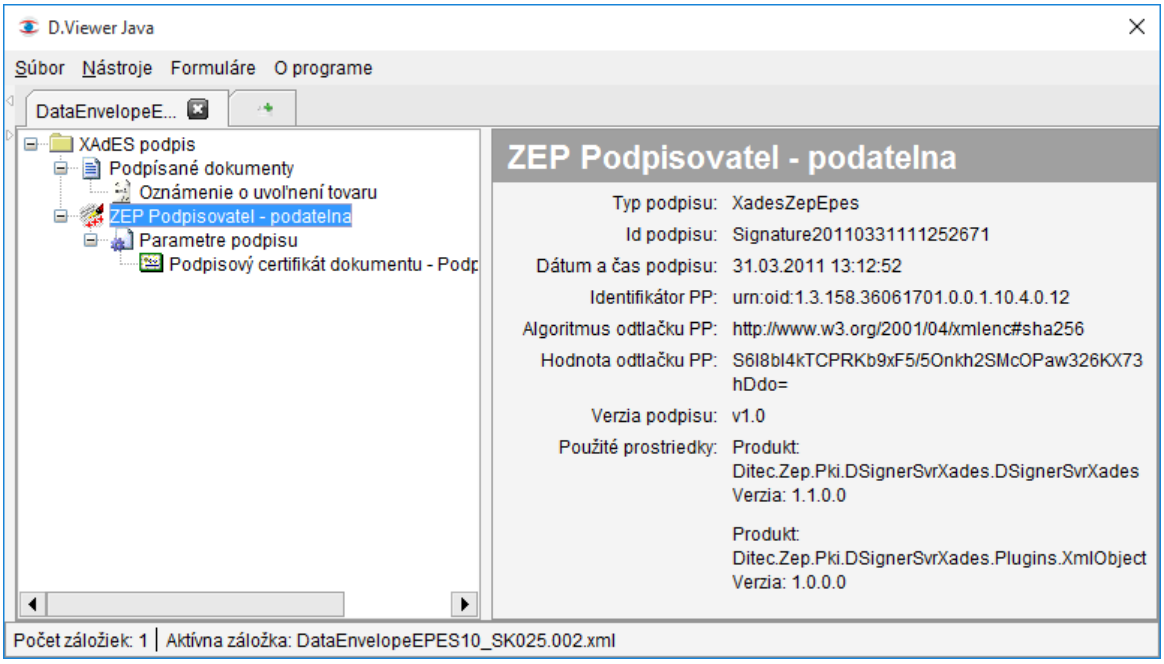
6.9.1.1. XAdES podpis

V rámci detailu XAdES podpisu sa zobrazujú atribúty:

- Typ podpisu,
- ID podpisu,
- Dátum a čas podpisu,
- Identifikátor podpisovej politiky,
- Algoritmus odtlačku podpisovej politiky,

- Hodnota odlačku podpisovej politiky,
- Verzia podpisu,
- Použité prostriedky.

Príklad zobrazenia detailu podpisu XAdESZEPEpes.

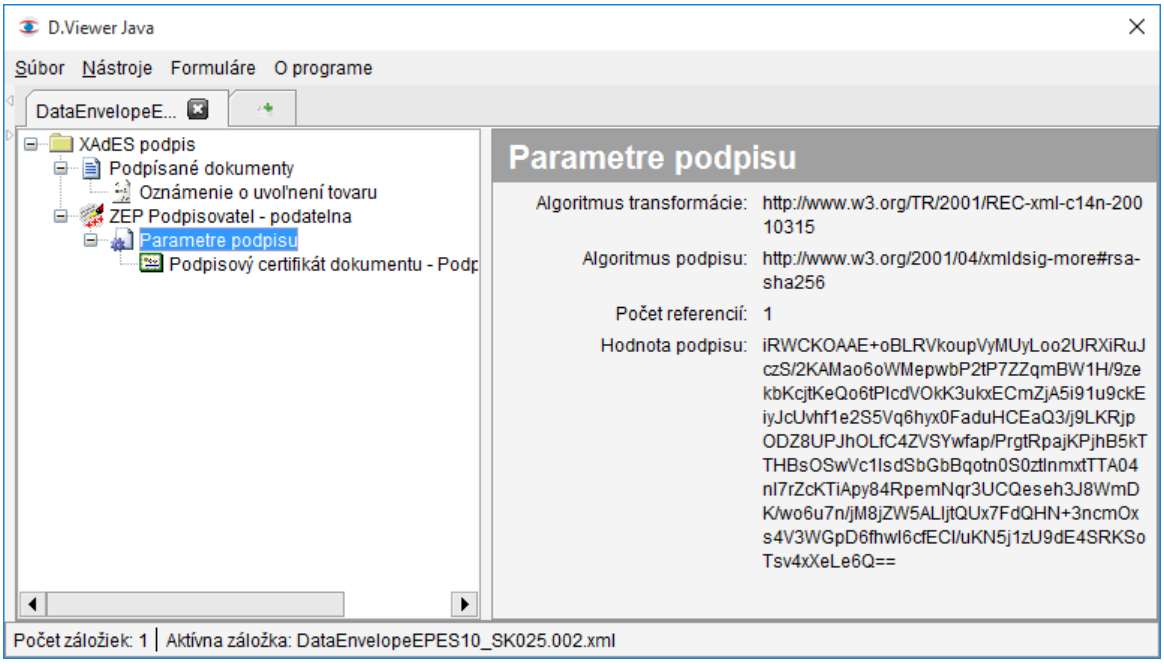


6.9.1.1.1. Parametre podpisu

V rámci detailu parametrov XAdES podpisu sa zobrazujú atribúty:

- Algoritmus transformácie,
- Algoritmus podpisu,
- Počet referencií,
- Hodnota podpisu.

Príklad zobrazenia parametrov XAdES podpisu.

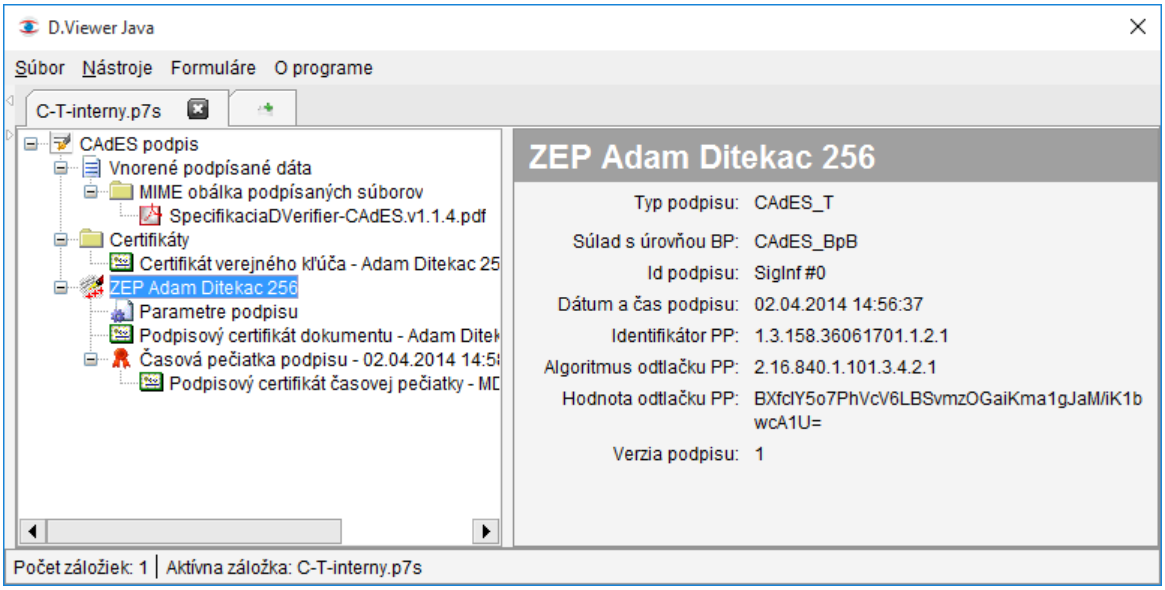


6.9.1.2. CAdES podpis

V rámci detailu CAdES podpisu sa zobrazujú atribúty:

- Typ podpisu,
- Súlad s úrovňou BP,
- ID podpisu,
- Dátum a čas podpisu,
- Identifikátor podpisovej politiky,
- Algoritmus odtlačku podpisovej politiky,
- Hodnota odlačku podpisovej politiky,
- Verzia podpisu.

Príklad zobrazenia detailu podpisu CAdES_EPES.

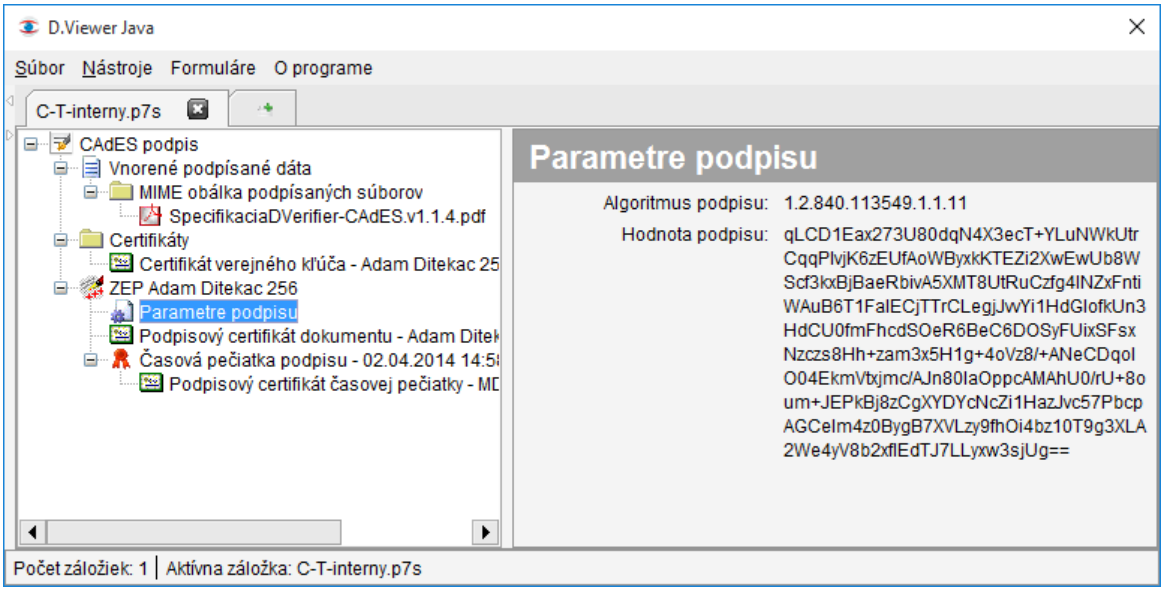


6.9.1.2.1. Parametre podpisu

V rámci detailu parametrov CAdES podpisu sa zobrazujú atribúty:

- Algoritmus podpisu,
- Hodnota podpisu.

Príklad zobrazenia parametrov CAdES podpisu.



6.9.2. MIME obálka

MIME obálka podpísaných súborov sa môže zobrazovať v rámci ZEPfZIP obálky (ako externe podpísané dáta ku všetkým Jednoduchým podisom v ZEPfZIP

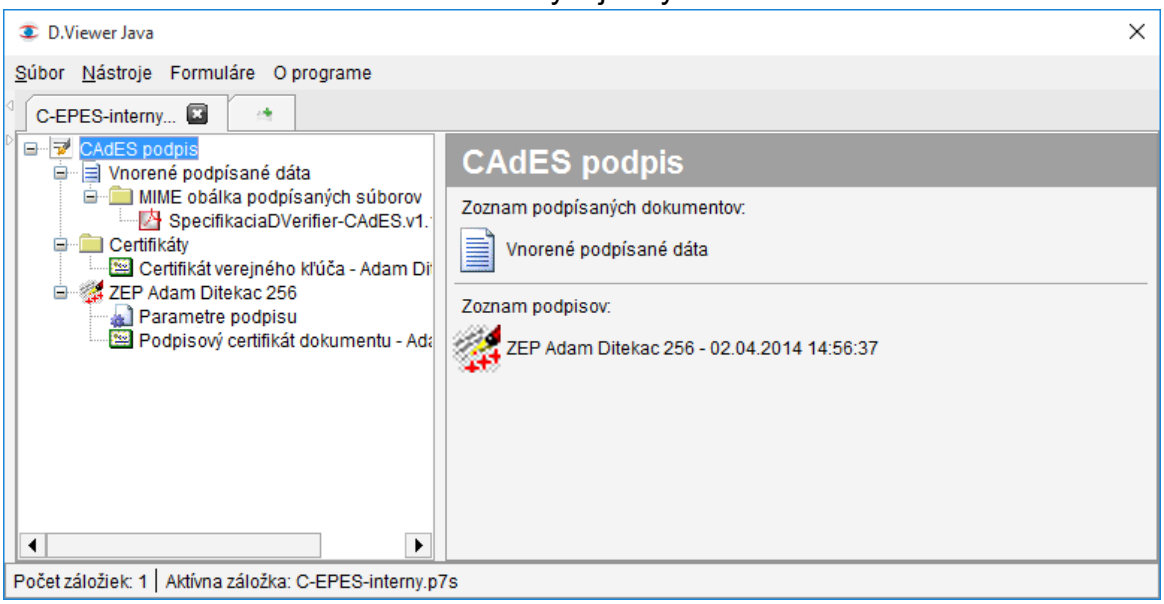
obákle) alebo v rámci interného CAdES podpisu pod položkou Vnorené podpísané dáta.

V rámci detailu MIME obálky podpídaných súborov sa zobrazuje atribút:

- Počet súborov v MIME obálke.

V rámci hierarchickej stromovej štruktúty sa pod MIME obálkou podpísaných súborov zobrazujú súbory vložené do obálky (XML, PDF, PNG, TXT, etc.)

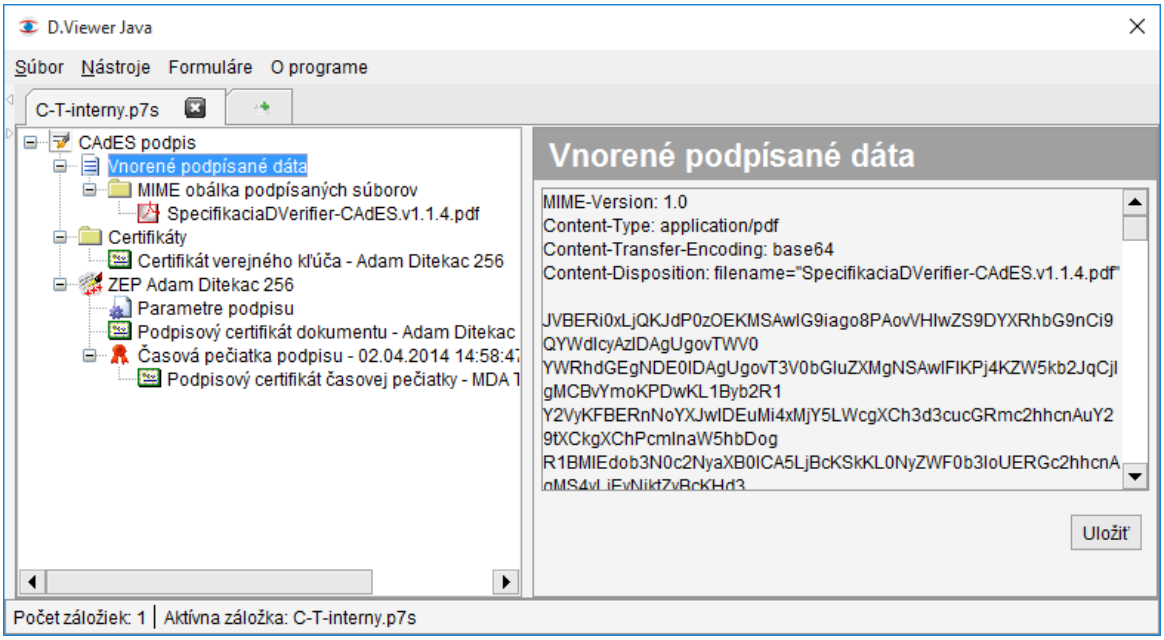
Príklad zobrazenia detailu MIME obálky s jedným PDF súborom.



6.9.3. Vnorené podpísané dáta

Položka vnorené podpísané dáta sa zobrazuje v hierarchickej stromovej štruktúre v rámci interného CAdES podpisu. V prípade jednoduchého CAdES podpisu sa pod položkou vnorené podpísané dáta nachádza MIME obálka (pozri kapitolu 6.8.2 MIME obálka). V prípade integritného CAdES podpisu je podpísaný textový súbor obsahujúci referencie dát, ktorých integrita je podpisom chránená.

Príklad zobrazenia detailu vnorených podpísaných dát integritného CAdES podpisu.



6.9.4. Certifikát

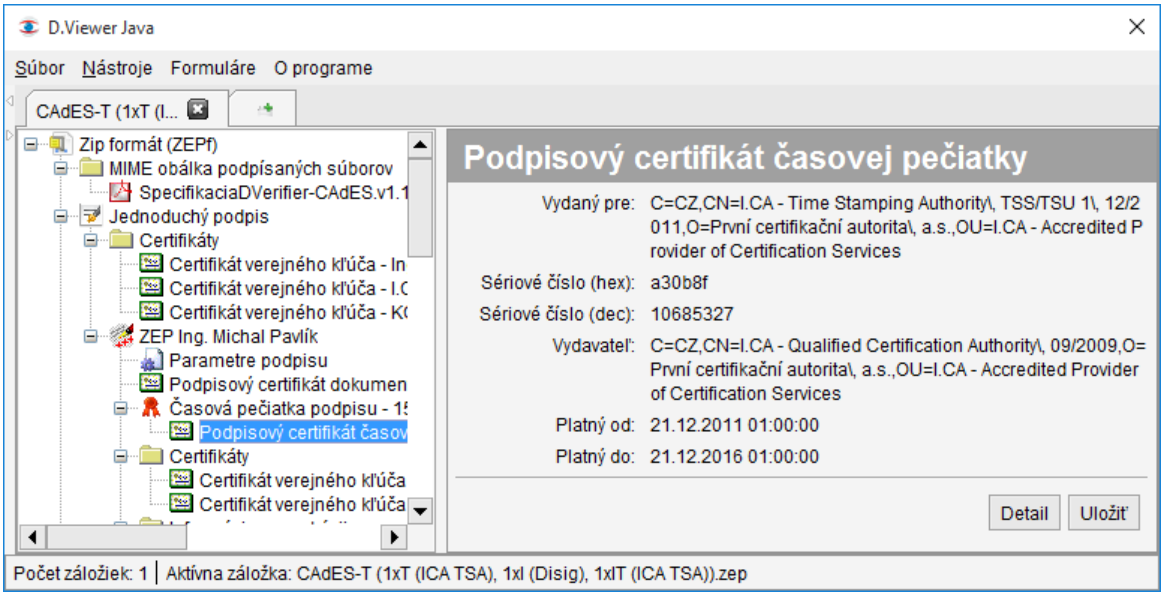
Vo vyššie popísaných ZEP štruktúrach sa môže zobrazovať:

- Podpisový certifikát dokumentu,
- Podpisový certifikát časovej pečiatky,
- Certifikát verejného kľúča.

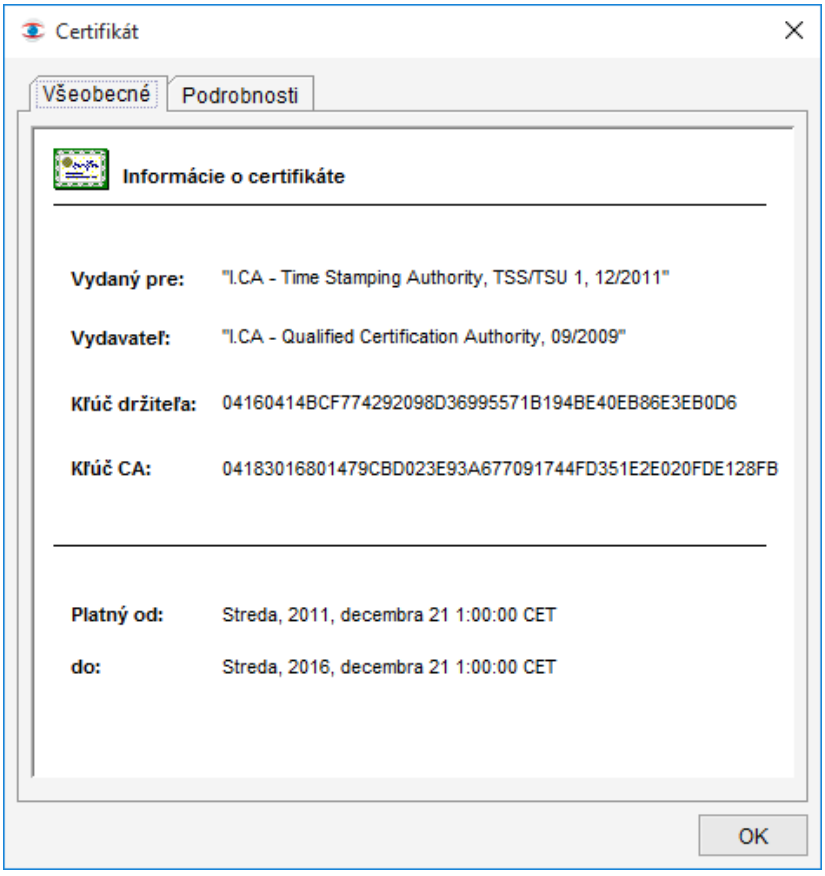
Pri zobrazení detailu certifikátu sa zobrazujú atribúty:

- Vydaný pre,
- Sériové číslo (hex),
- Sériové číslo (dec),
- Vydavateľ,
- Platný od,
- Platný do.

Príklad zobrazenia detailu podpisového certifikátu časovej pečiatky.



Kliknutím na tlačidlo Detail sa v modálnom dialógovom okne zobrazí detail certifikátu. Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie certifikátu v rámci operačného systému používateľa.



6.9.5. Časová pečiatka

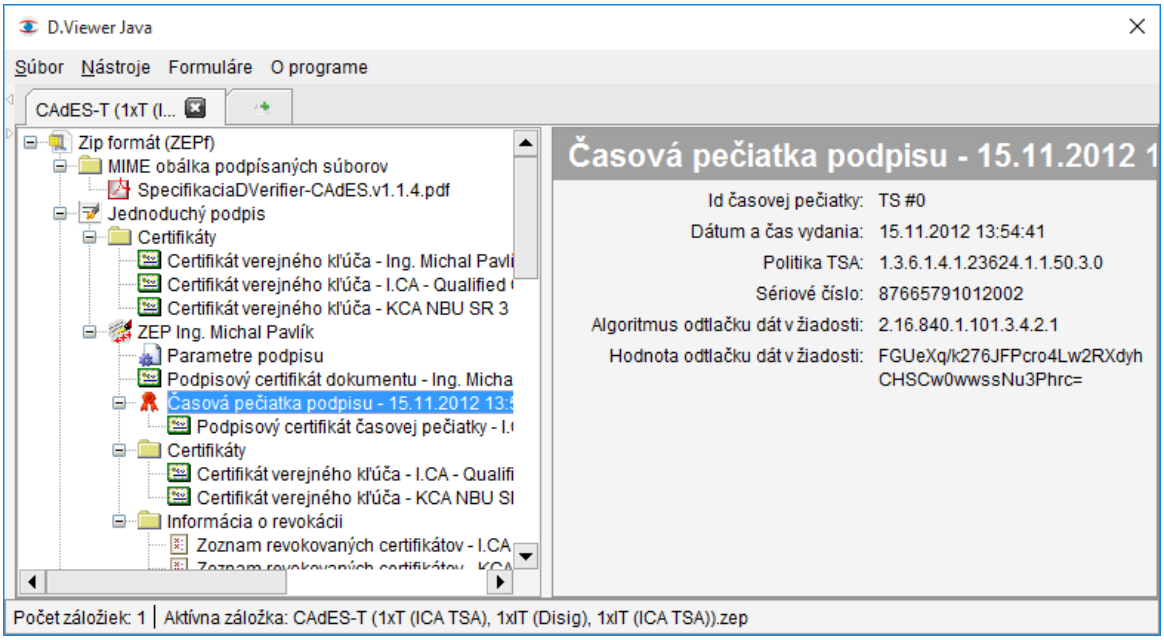
Vo vyššie popísaných ZEP štruktúrach sa môže zobrazovať:

- Časová pečiatka podpisu,
- Časová pečiatka archívna.

Pri zobrazení detailu časovej pečiatky sa používateľovi zobrazujú atribúty:

- ID časovej pečiatky,
- Dátum a čas vydania,
- Politika TSA,
- Sériové číslo,
- Algoritmus odtlačku dát v žiadosti,
- Hodnota odtlačku dát v žiadosti.

Príklad zobrazenia detailu časovej pečiatky.

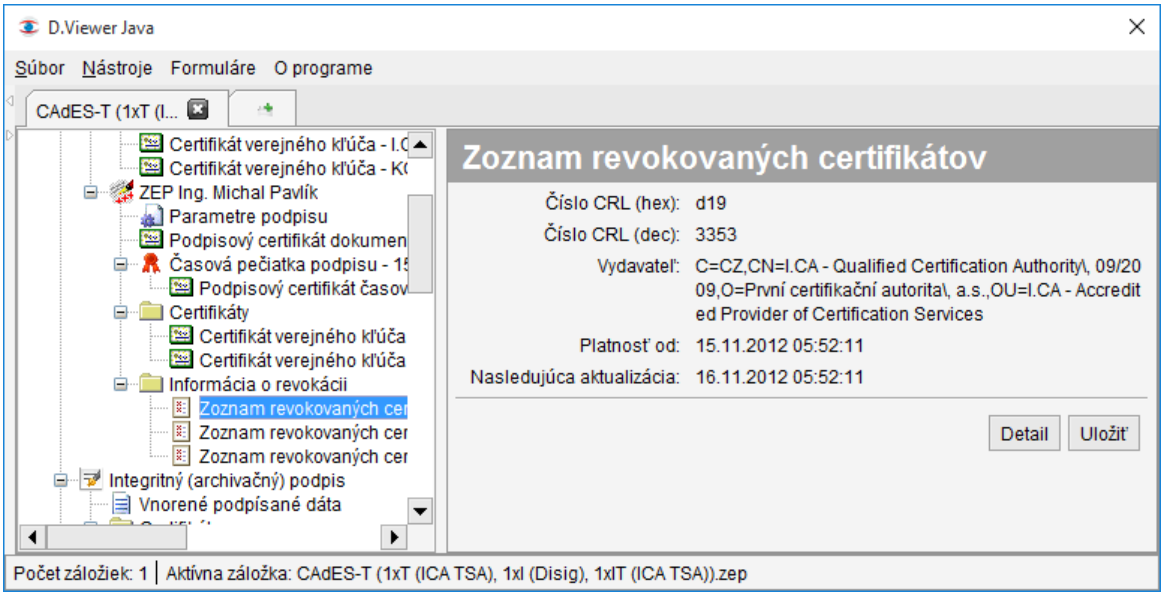


6.9.6. Zoznam revokovaných certifikátov

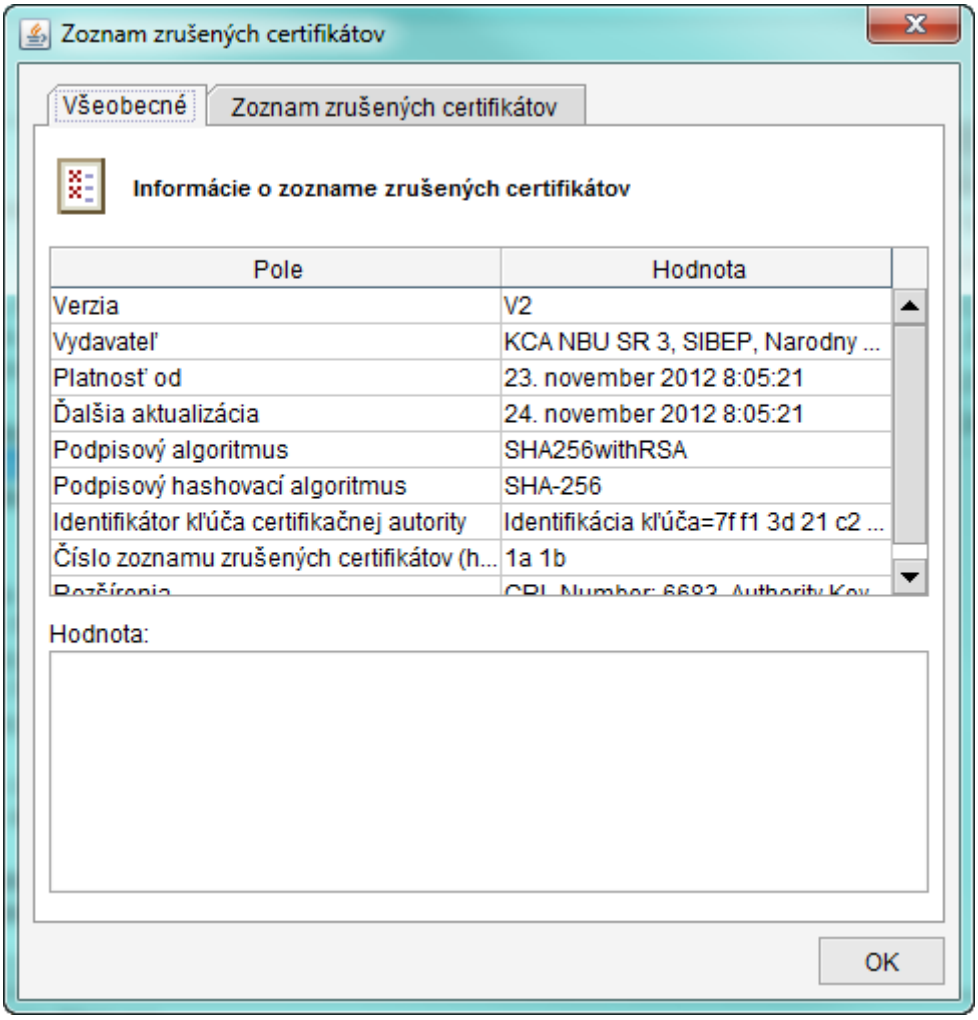
Pri zobrazení detailu zoznamu revokovaných certifikátov (CRL) sa zobrazujú atribúty:

- Číslo CRL (hex),
- Číslo CRL (dec),
- Vydavateľ,
- Platnosť od,
- Nasledujúca aktualizácia.

Príklad zobrazenia detailu zoznamu revokovaných certifikátov (CRL).



Kliknutím na tlačidlo Detail sa v modálnom dialógovom okne zobrazí detail CRL. Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie CRL v rámci operačného systému používateľa.



6.9.7. OCSP odpoveď

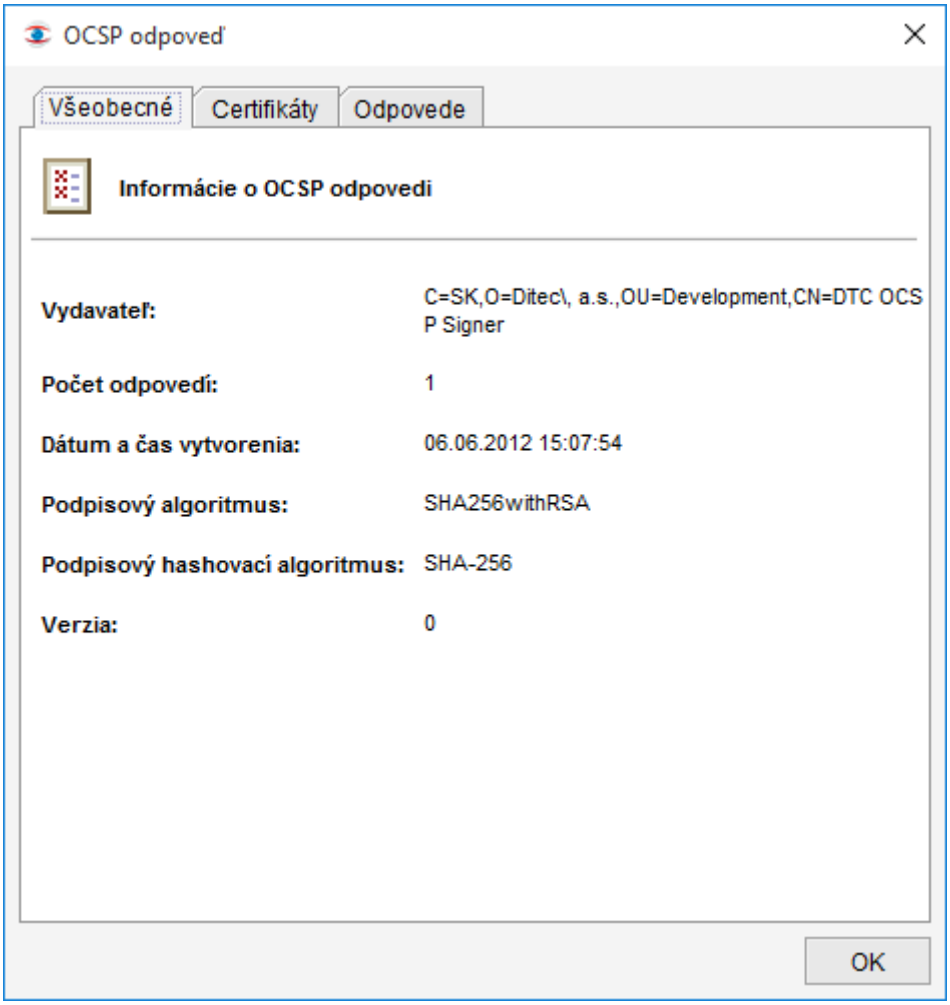
Pri zobrazení detailu OCSP odpovede sa zobrazujú atribúty:

- Vydavateľ,
- Dátum a čas vytvorenia,
- Počet odpovedí.

Príklad zobrazenia detailu OCSP odpovede.



Kliknutím na tlačidlo Detail sa v modálnom diálogovom okne zobrazí detail OCSP odpovede. Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie OCSP odpovede v rámci operačného systému používateľa.

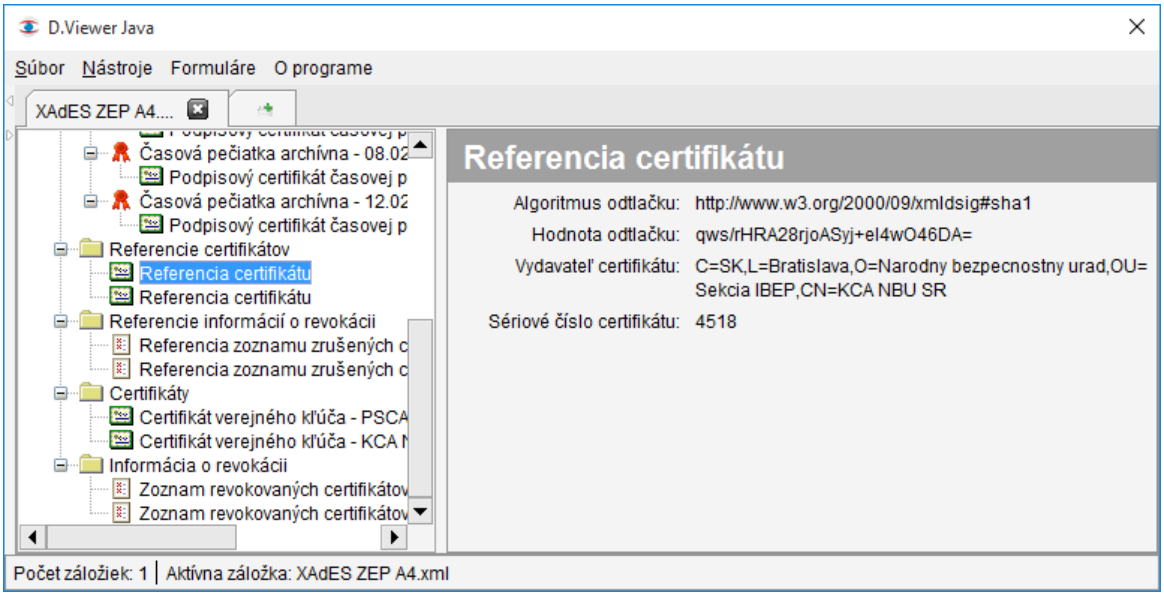


6.9.8. Referencia certifikátu

Pri zobrazení detailu referencie certifikátu sa zobrazujú atribúty:

- Algoritmus odtlačku,
- Hodnota odtlačku,
- Vydavateľ certifikátu,
- Sériové číslo certifikátu.

Príklad zobrazenia detailu referencie certifikátu.

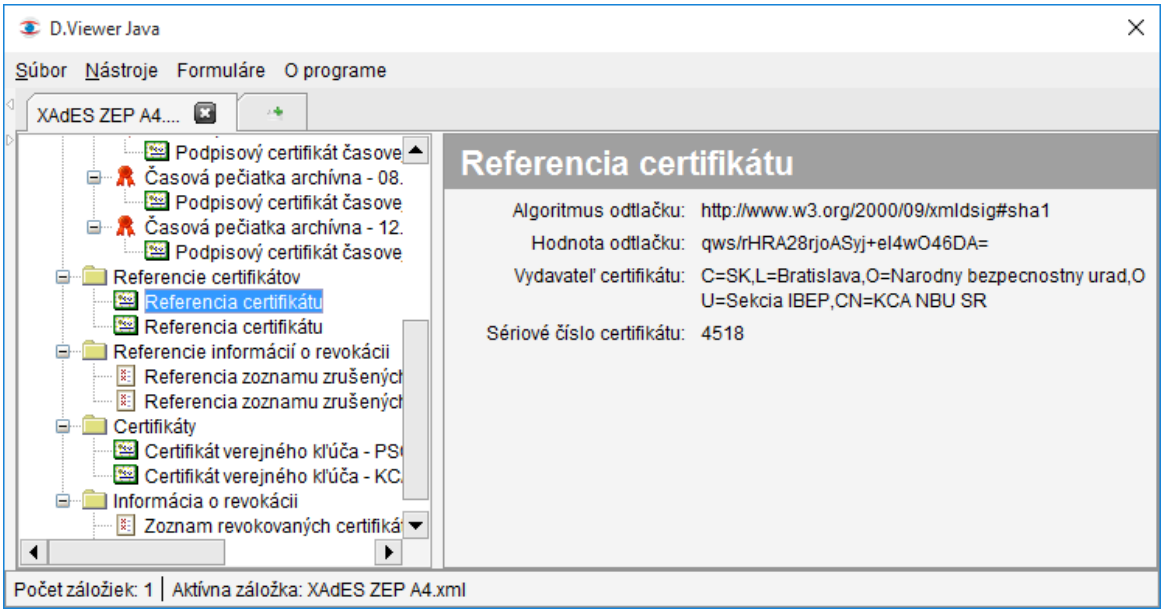


6.9.9. Referencia zoznamu zrušených certifikátov

Pri zobrazení detailu referencie zoznamu revokovaných certifikátov (CRL) sa zobrazujú atribúty:

- Algoritmus odtlačku,
- Hodnota odtlačku,
- Vydavateľ,
- Dátum a čas vydania,
- Číslo CRL.

Príklad zobrazenia detailu referencie zoznamu revokovaných certifikátov (CRL).

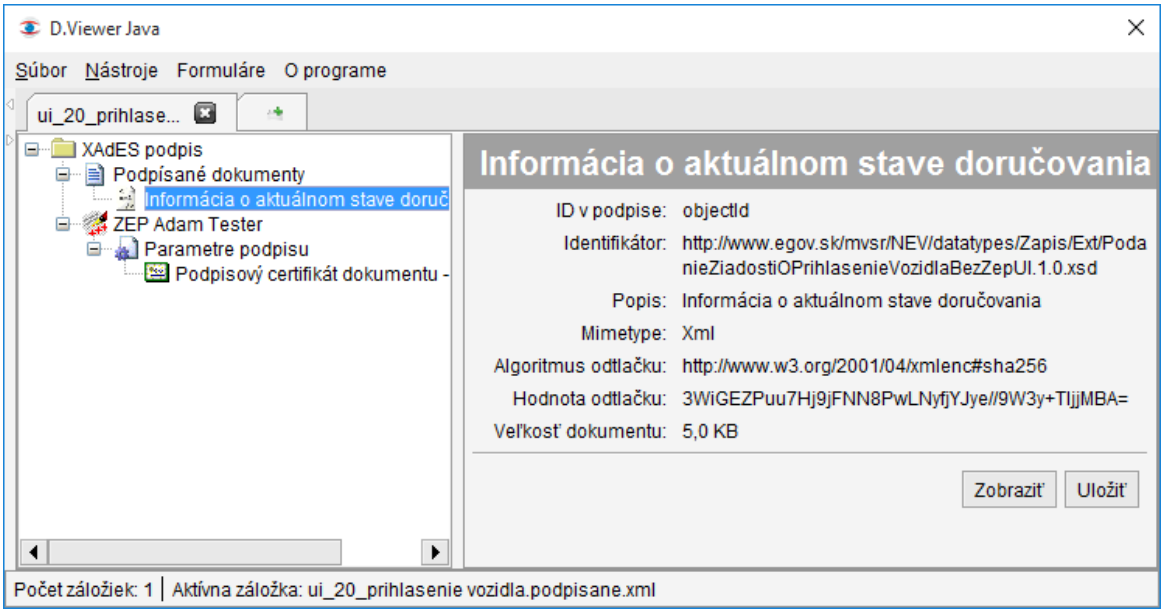


6.9.10. Podpísané dokumenty

Pri zobrazení detailu podpísaného dokumentu okrem objektu typu XDC (pozri kapitola 6.8.10.1 Podpísaný objekt typu XMLDataContainer) sa zobrazujú atribúty:

- ID v podpise,
- Identifikátor,
- Popis,
- MimeType,
- Algoritmus odtlačku,
- Hodnota odlačku,
- Veľkosť dokumentu.

Príklad zobrazenia detailu podpísaného XML dokumentu.



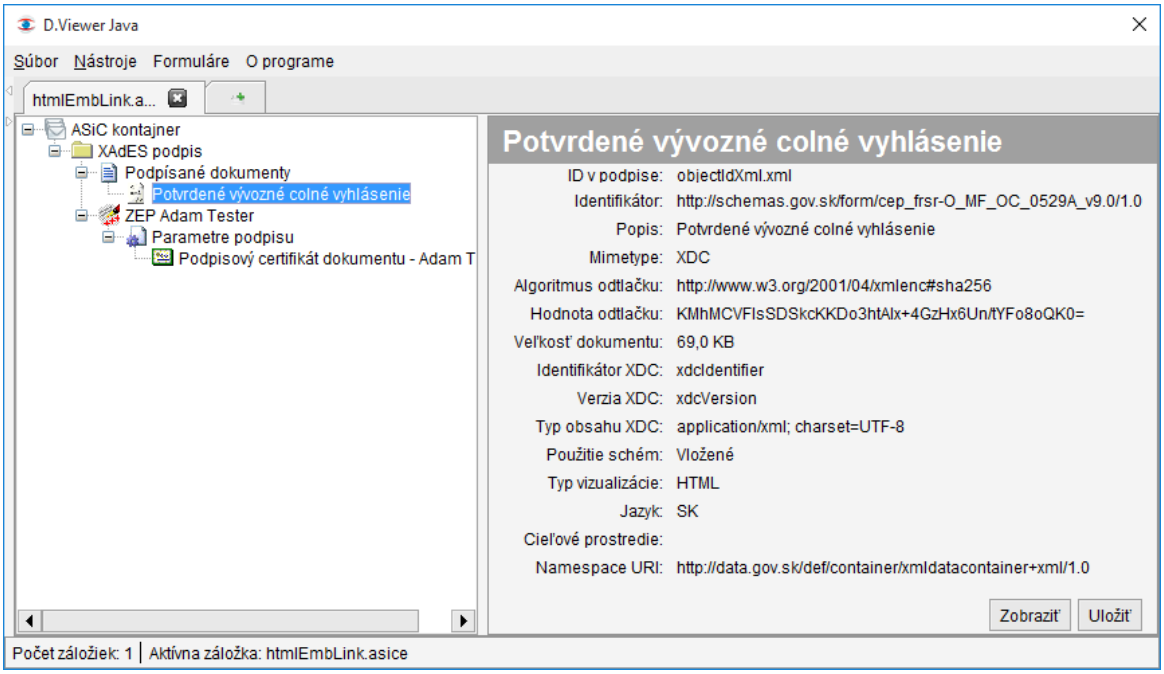
Kliknutím na tlačidlo Zobraziť sa vizualizuje obsah podpísaného dokumentu (pozri kapitola 6.8.10.2 Vizualizácia obsahu podpísaných dokumentov. Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie dokumentu v rámci operačného systému používateľa.

6.9.10.1. Podpísaný objekt typu XMLDataContainer

Pri zobrazení detailu podpísaného dátového objektu typu XMLDataContainer [1] sa zobrazujú atribúty:

- ID v podpise,
- Identifikátor,
- Popis,
- MimeType,
- Algoritmus odtlačku,
- Hodnota odlačku,
- Veľkosť dokumentu,
- Identifikátor XDC,
- Verzia XDC,
- Typ obsahu,
- Použitie schém,
- Typ vizualizácie,
- Jazyk,
- Cieľové prostredie,
- Namespace URI.

Príklad zobrazenia detailu podpísaného dátového objektu typu XMLDataContainer.



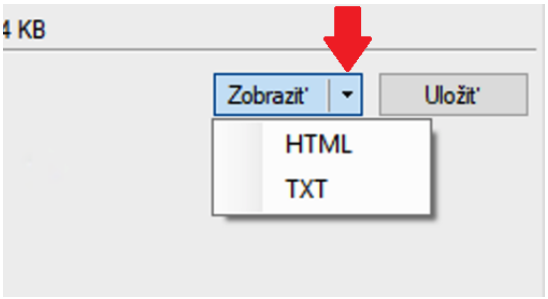
Kliknutím na tlačidlo Zobraziť sa vizualizuje obsah podpísaného dokumentu (pozri kapitola 6.8.10.2 Vizualizácia obsahu podpísaných dokumentov). Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie dokumentu v rámci operačného systému používateľa.

6.9.10.2. Vizualizácia obsahu podpísaných dokumentov

Dátové objekty PDF, PNG, TXT sa zobrazujú v asociovanom programe (podľa koncovky) v rámci operačného systému používateľa.

Dátove objekty XDC, XML alebo FO formuláre sa zobrazujú podľa nasledovných pravidiel. Vizualizácia môže byť priamo súčasťou dátového objektu typu XMLDataContainer [1], alebo ak je v rámci dátového objektu typu XMLDataContainer referencovaná alebo podpisovaný dátový objekt typu XML (resp. typu FO formulár) je súčasťou štruktúry XAdES_ZEP [4] [5] [6], tak musí existovať v rámci konfigurácie aplikácie D.Viewer Java – v číselníku visualizations.xml.

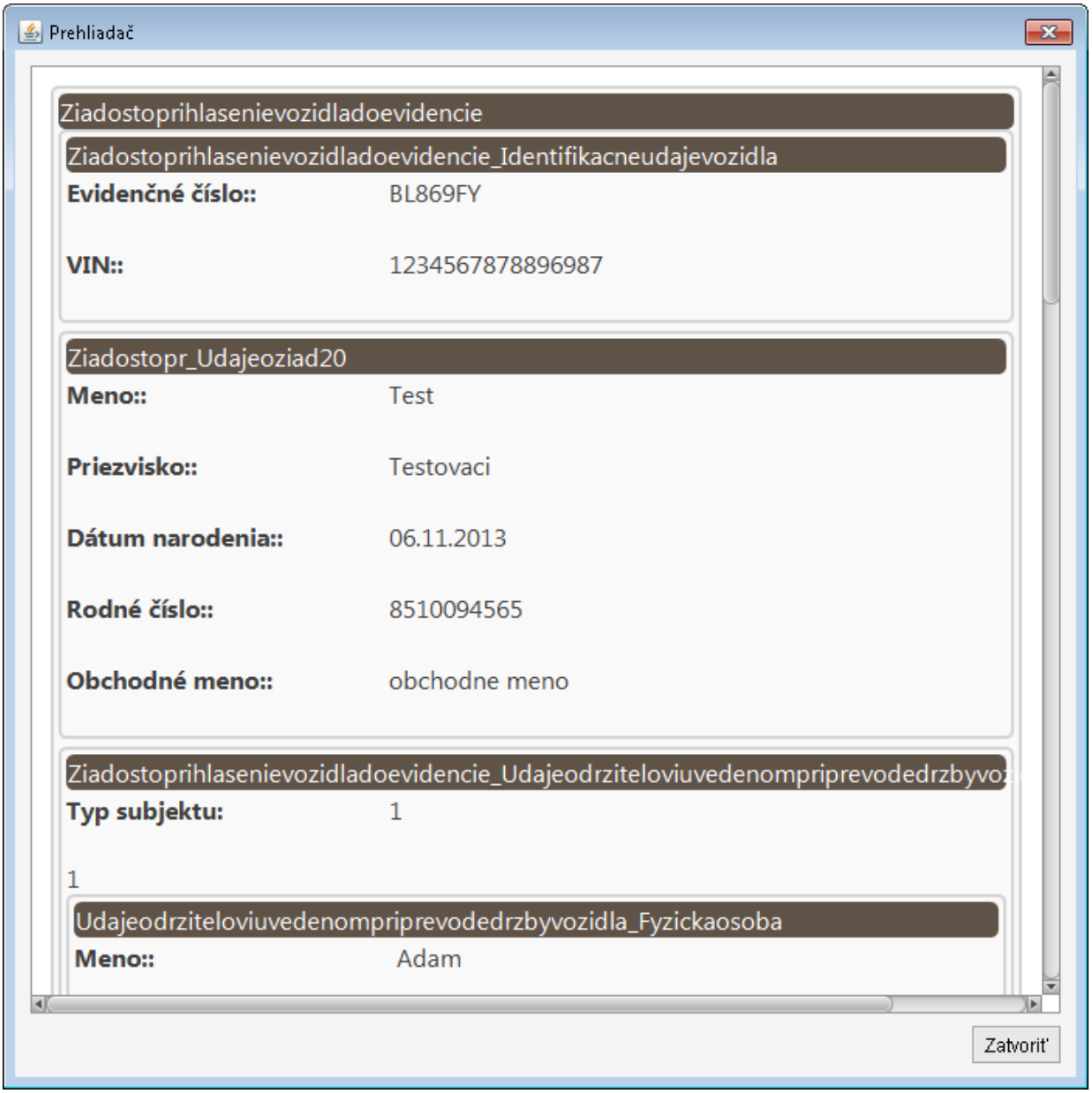
Ak existuje v číselníku visualizations.xml viacero typov vizualizácií, je tlačidlo Zobraziť rozšírené o rozbaľovací zoznam, pomocou ktorého si používateľ môže zvoliť typ vizualizácie pre zobrazenie.



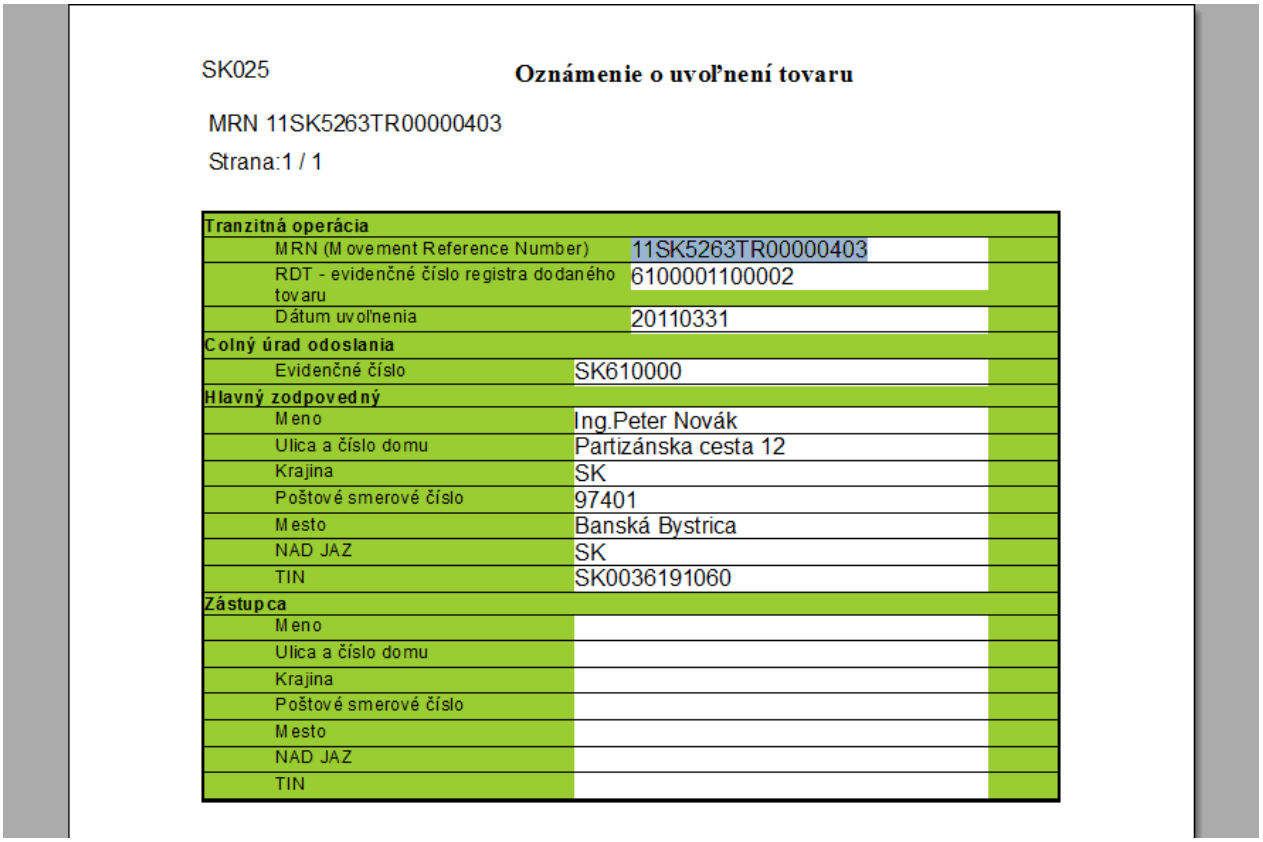
V opačnom prípade alebo kliknutím na Zobraziť D.Viewer Java zobrazuje podpísaný dátový objekt typu XML, resp. FO formulár podľa nasledujúcich pravidiel:

- dátový objekt typu FO formulár:
  - ⇒ vizualizácia XML pomocou aplikácie 602 Filler a pomocou uzamknutej FO vizualizácie, ktorá je referencovaná v rámci štruktúry podpisu,
  - ⇒ inak v asociovanej aplikácii (podľa prípony .xml),
- dátový objekt typu XML v1.0 v rámci profilov XAdES_ZEP:
  - ⇒ ak existuje v číselníku visualizations.xml uzamknutá FO vizualizácia, tak pomocou aplikácie 602 Filler a pomocou danej FO vizualizácie,
  - ⇒ ak existuje v číselníku visualizations.xml HTML vizualizácia, tak pomocou danej HTML vizualizácie,
  - ⇒ ak existuje v číselníku visualizations.xml TXT vizualizácia, ktorá je referencovaná v štruktúre podpisu, tak pomocou danej TXT vizualizácie,
  - ⇒ inak v asociovanej aplikácii (podľa prípony .xml),
- dátový objekt typu XML v2.0 v rámci profilov XAdES_ZEP:
  - ⇒ pomocou vizualizácie referencovanej v štruktúre podpisu, ak taká existuje v rámci číselníka visualizations.xml,
  - ⇒ inak v asociovanej aplikácii (podľa prípony .xml).

Príklad vizualizácie podpísaného XML dokumentu do HTML.



Príklad vizualizácie podpísaného XML dokumentu pomocou FormFillera a FO vizualizácie.



SK025

Oznámenie o uvoľnení tovaru

MRN 11SK5263TR00000403

Strana:1 / 1

Tranzitná operácia		
	MRN (Movement Reference Number)	11SK5263TR00000403
	RDT - evidenčné číslo registra dodaného tovaru	6100001100002
	Dátum uvoľnenia	20110331
Colný úrad odoslania		
	Evidenčné číslo	SK610000
Hlavný zodpovedný		
	Meno	Ing.Peter Novák
	Ulica a číslo domu	Partizánska cesta 12
	Krajina	SK
	Poštové smerové číslo	97401
	Mesto	Banská Bystrica
	NAD JAZ	SK
	TIN	SK0036191060
Zástupca		
	Meno	
	Ulica a číslo domu	
	Krajina	
	Poštové smerové číslo	
	Mesto	
	NAD JAZ	
	TIN	

7. Podpora pre nevidiacich pomocou NVDA

Komponent D.Viewer Java má zapracovanú podporu pre nevidiacich pomocou technológie NVDA (NonVisual Desktop Access). NVDA je voľne šíriteľný open-source čítač obrazovky pre operačný systém Windows. Pomocou hlasového a hmatového výstupu umožňuje nevidiacim a zrakovo postihnutým používateľom pristupovať k PC so systémom Windows a k aplikáciám so zapracovanou podporou. Vývoj NVDA zastrešuje organizácia NV Access (http://www.nvaccess.org/).

7.1. Systémové požiadavky pre NVDA

- 32 aj 64 bitové verzie systémov Windows Vista alebo novších,
- 50 MB voľného miesta na disku,
- žiadne ďalšie požiadavky na hardware mimo požiadaviek kladených operačným systémom.

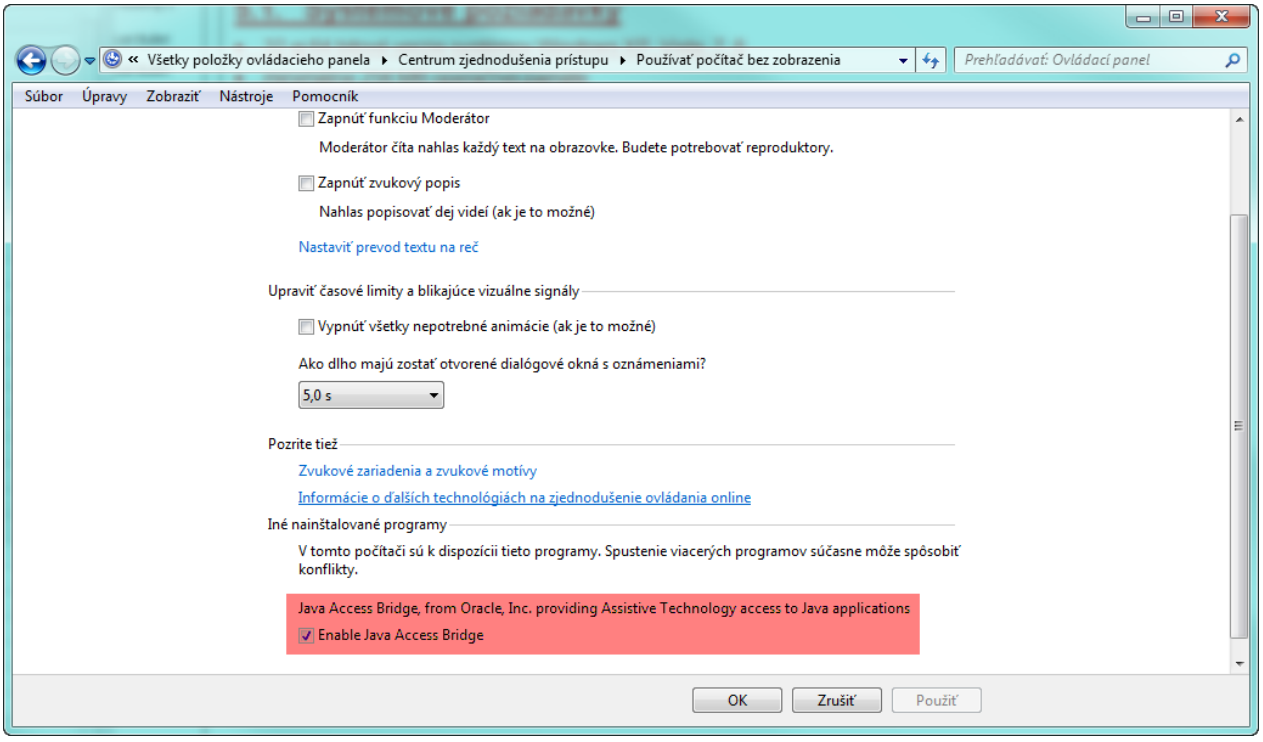
pozn: Uvedené sú systémové požiadavky pre NVDA, ktoré boli aktuálne v čase písania integračnej príručky.

7.1.1. Aktivácia Java Access Bridge

Java Access Bridge je zahrnutý vo verzii Java 7 Update 6 a vo vyšších verziách. Pre aktiváciu Java Acess Bridge, spustite nasledovný príkaz (kde `%JRE_HOME%` je adresár JRE): `%JRE_HOME%\bin\jabswitch -enable`

Alternatívne, vo Windows Vista a neskorších verziách, môžete aktivovať Java Access Bridge cez Ovládací panel (Control Panel):

1) Štart (Start) > Ovládací panel (Control Panel) > Centrum zjednodušeného prístupu (Ease of Access Center)
2) Vyberte Používať počítač bez zobrazenia (Use the computer without a display)
3) V sekcii Iné nainštalované programy (Other programs installed), označte check box Enable Java Access Bridge.


« Všetky položky ovládacieho panela ▸ Centrum zjednodušenia prístupu ▸ Používať počítač bez zobrazenia
Prehľadávať: Ovládací panel
Súbor Úpravy Zobraziť Nástroje Pomocník
Zapnúť funkciu Moderátor
Moderátor číta nahlas každý text na obrazovke. Budete potrebovať reproduktory.
Zapnúť zvukový popis
Nahlas popisovať dej videí (ak je to možné)
Nastaviť prevod textu na reč
Upraviť časové limity a blikajúce vizuálne signály
Vypnúť všetky nepotrebné animácie (ak je to možné)
Ako dlho majú zostať otvorené dialógové okná s oznámeniami?
5,0 s
Pozrite tiež
Zvukové zariadenia a zvukové motívy
Informácie o ďalších technológiách na zjednodušenie ovládania online
Iné nainštalované programy
V tomto počítači sú k dispozícii tieto programy. Spustenie viacerých programov súčasne môže spôsobiť konflikty.
Java Access Bridge, from Oracle, Inc. providing Assistive Technology access to Java applications
Enable Java Access Bridge
OK
Zrušiť
Použiť