DITEC
Data Information Technology & Expert Consulting

Používateľská príručka
D.Viewer .NET v3.1

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Podnázov	D.Viewer .NET v3.1		
Ref. číslo	GOV_ZEP.185	Verzia	2

Vypracoval	Peter Obeda	Podpis	Dátum 15.2.2016
Preveril		Podpis	Dátum
Schválil		Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 17.5.2005

Projekt	GOV_ZEP		A3019_002
Dokument	Používateľská príručka		
Referencia	GOV_ZEP.185	Verzia	2

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

D.Viewer .NET 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 .NET je, že nepracuje len ako Win32 aplikácia, ale jeho komponenty možno využiť pri tvorbe webových stránok.

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

2. Systémové požiadavky a inštalácia

2.1. Systémové požiadavky

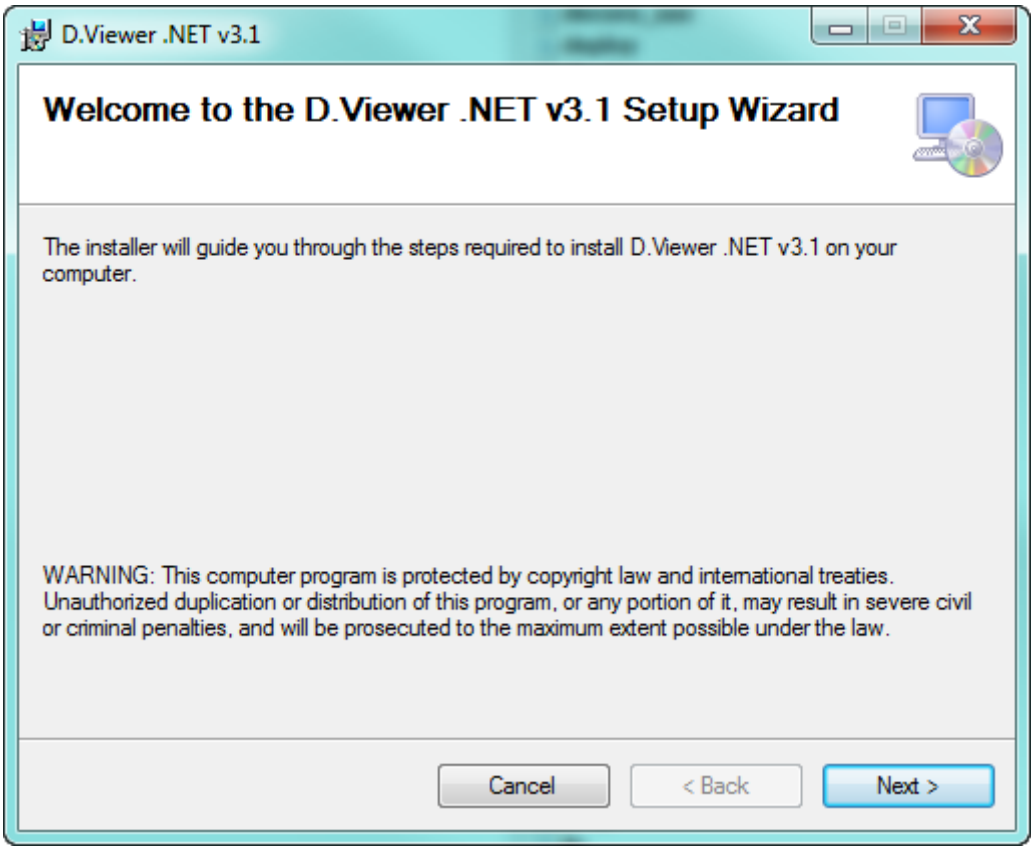
Systémové požiadavky aplikácie D.Viewer .NET sú nasledujúce:

- operačný systém MS Windows Vista alebo novší,
- .NET Framework 2.0 až 3.5 (http://www.microsoft.com),
- web prehliadač – MS Internet Explorer 7 alebo vyšší, Firefox v3.x, Google Chrome v12.x – v44, Opera v10.x, Safari 5.1 alebo vyššia.

2.2. Postup inštalácie

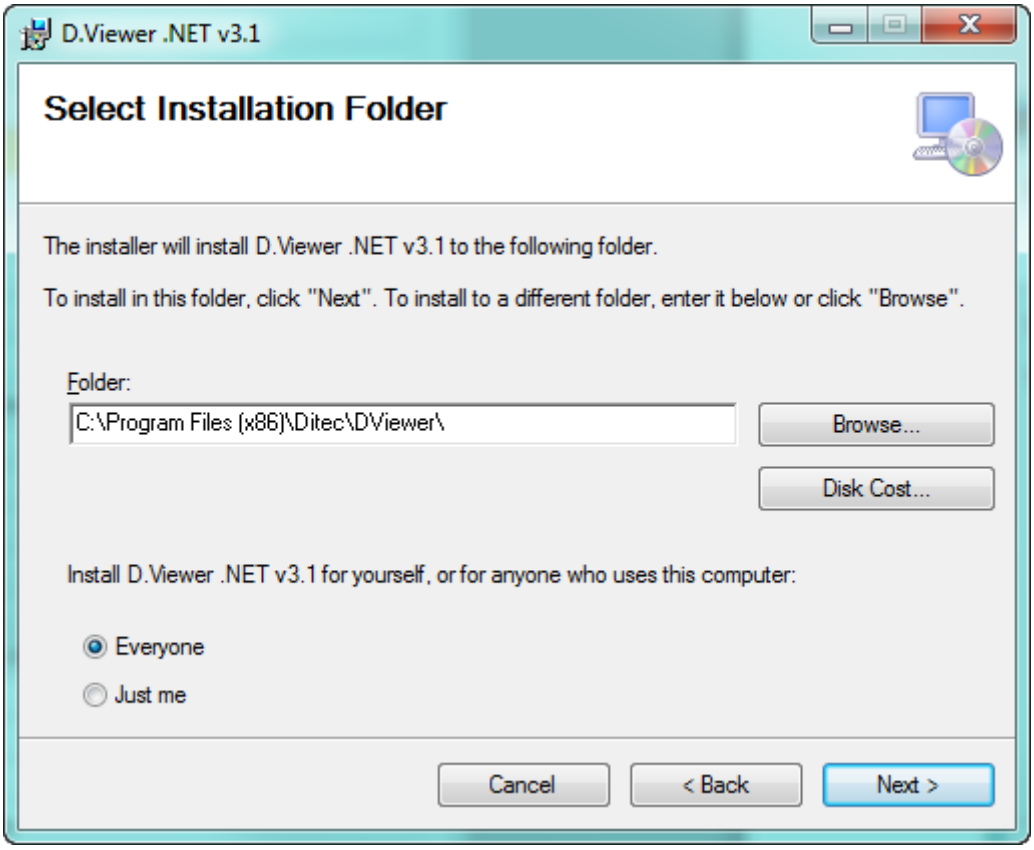
Pred inštaláciou aplikácie D.Viewer .NET v3.1 je potrebné mať nainštalovaný .NET Framework 2.0 až 3.5 (http://www.microsoft.com).

Inštaláciu zahájime spustením súboru setup.exe z inštalačného adresára (CD).



obr. 2.2.1

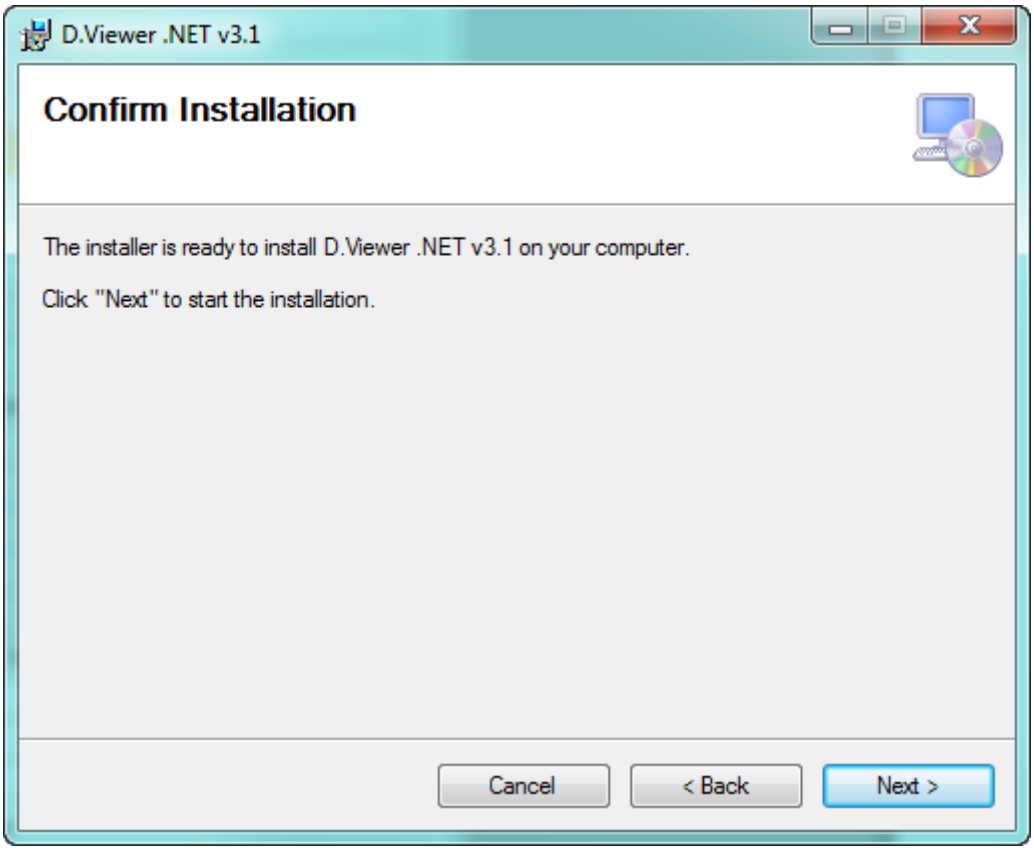
Sprievodca inštaláciou zobrazí uvítaciu obrazovku (obr. 2.2.1). Pokračujeme kliknutím na tlačidlo Next.



obr. 2. 2.2

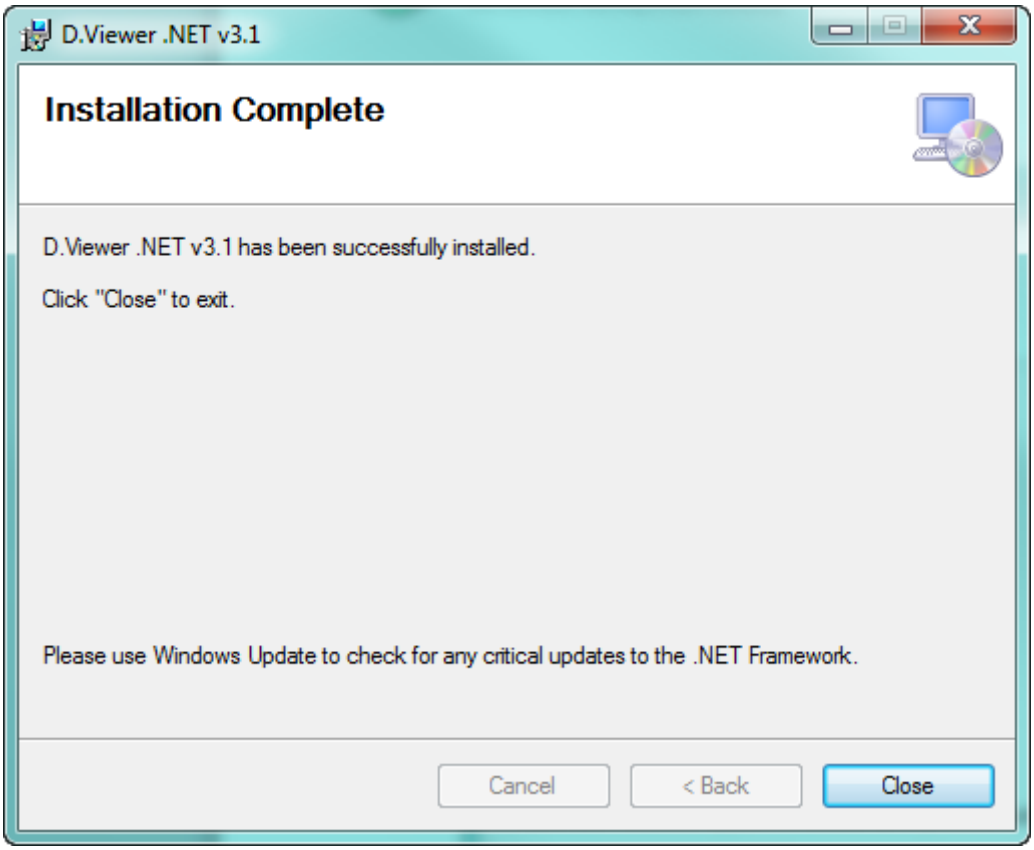
V okne na obr. 2.1.2 nám sprievodca inštaláciou ponúkne predvolený cieľový inštalačný adresár. Ak chceme, môžeme ho zmeniť kliknutím na Browse.

V dolnej časti obrazovky vyberieme, či sa má D.Viewer .NET inštalovať pre každého používateľa počítača (Everyone), alebo len pre práve prihláseného používateľa (Just me).



obr. 2.2.3

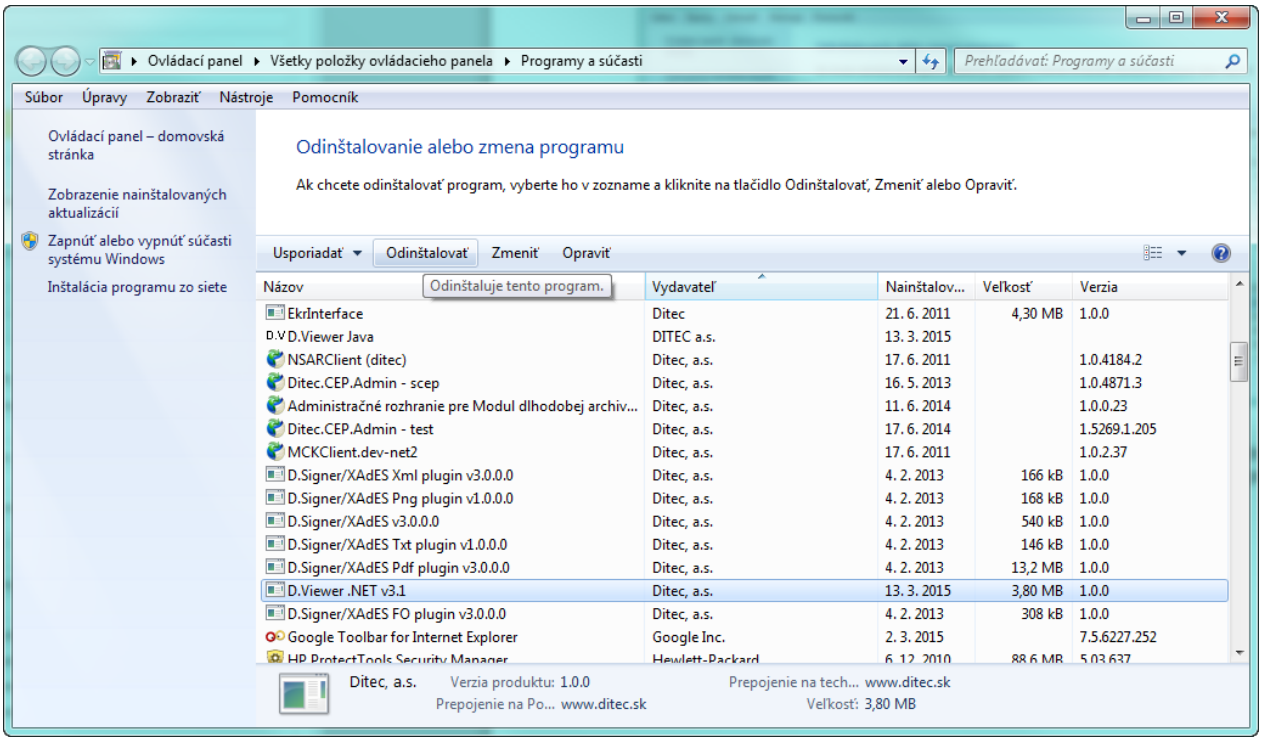
V okne na obr. 2.2.3 si sprievodca inštaláciou od nás vyžiada súhlas s inštaláciou. Potvrdíme tlačidlom Next.



obr. 2.2.4

O úspešnom ukončení inštalácie nás sprievodca informuje v okne na obr. 2.2.4. Stlačením Close ukončíme sprievodcu inštaláciou.

2.3. Odinštalovanie

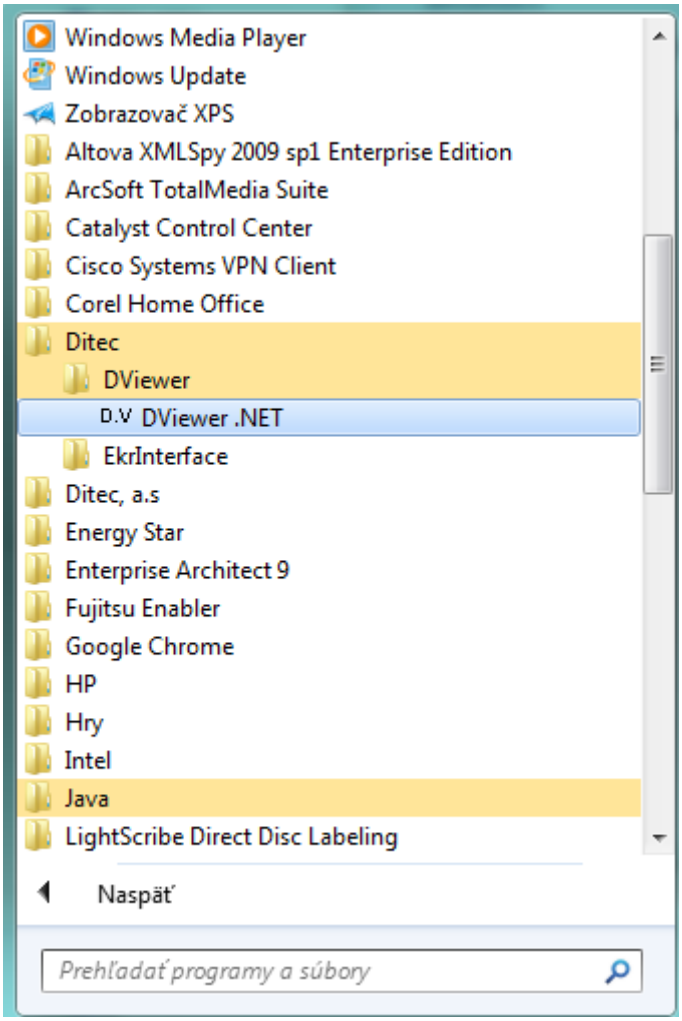


obr. 2.3.1

Na odinštalovanie aplikácie sa využíva štandardný postup na obr. 2.3.1 – Ovládací panel (Control panel)/Odinštalovať program (Add or remove programs) , označením aplikácie a potvrdením voľby Odinštalovať (Remove).

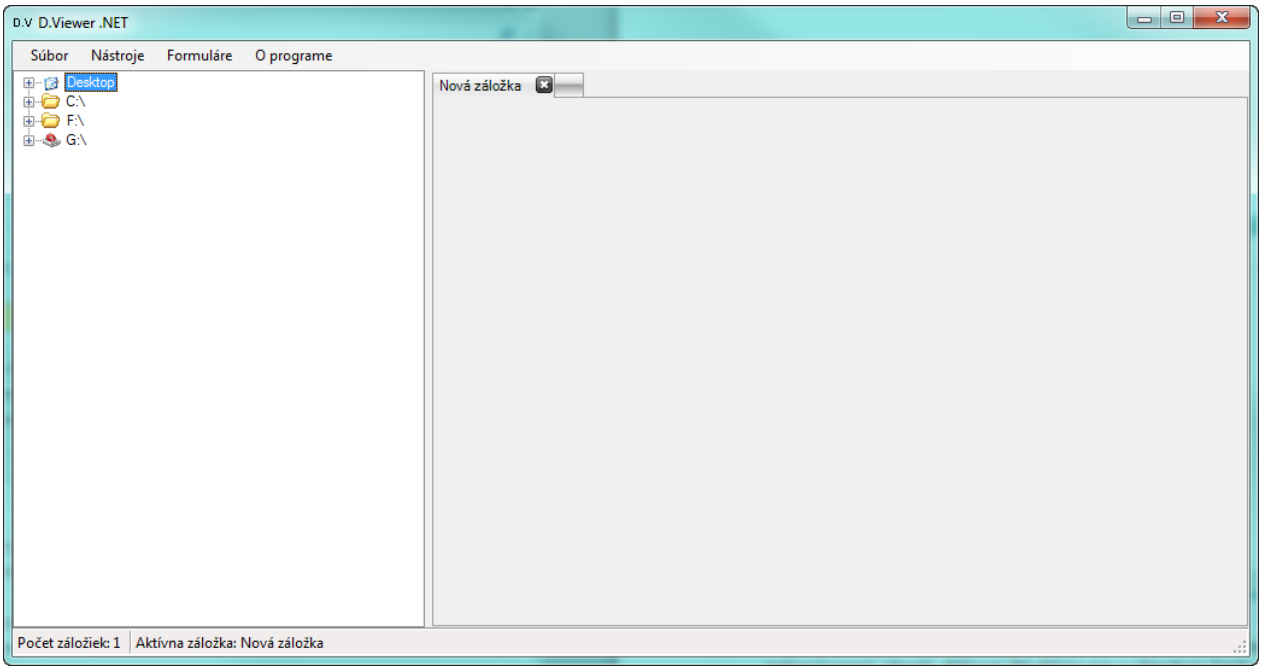
3. Práca s aplikáciou

Aplikáciu spustíme z menu Štart –> Programy –> Ditec –> D.Viewer –> D.Viewer .NET (obr. 3.1).



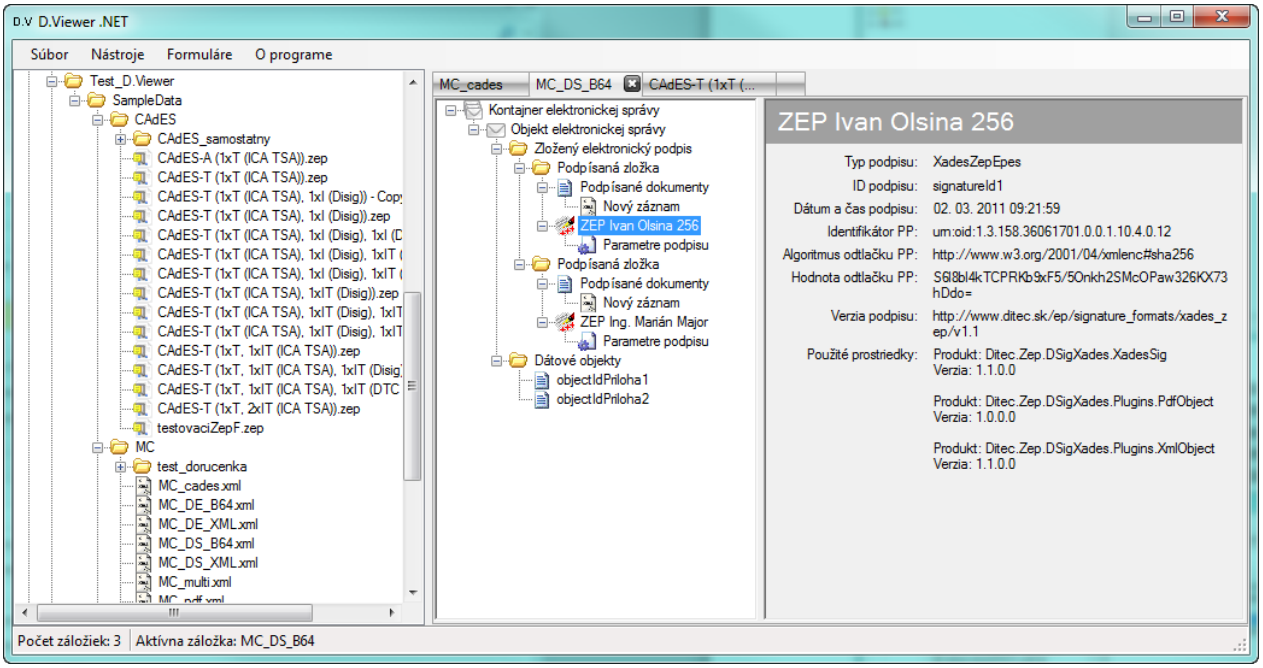
obr. 3.1

Po spustení sa zobrazí základná obrazovka aplikácie (obr. 3.2).



obr. 3.2

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 (obr. 3.3).



obr. 3.3

3.1. Menu aplikácie

Menu aplikácie D.Viewer .NET má štruktúru podľa obr. 3.1.1.

obr. 3.1.1

Popis jednotlivých príkazov menu:

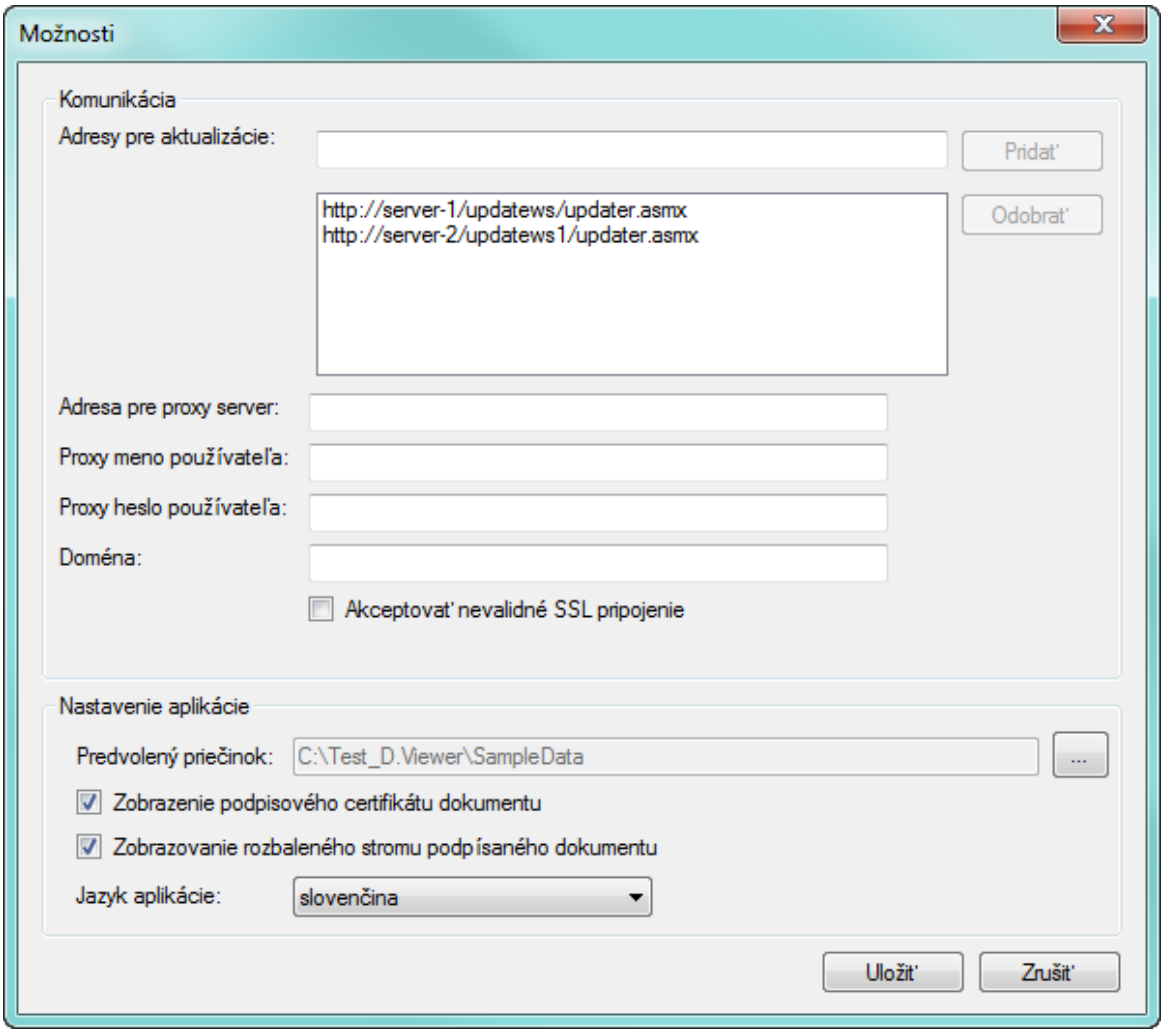
Súbor –> Otvoriť – otvorí dialógové okno Windows pre otvorenie XML súboru. Po vybraní je tento súbor otvorený v novej záložke.

Súbor –> Zavrieť – zatvorí aktuálnu záložku.

Súbor –> Zavrieť všetky – zatvorí všetky záložky

Súbor –> Koniec – ukončí aplikáciu

Nástroje –> Možnosti – zobrazí okno konfiguračných nastavení (obr. 3.1.2)



obr. 3.1.2

Okno je rozdelené na dve časti. V horne časti obrazovky sú komunikačné nastavenia pre aktualizáciu vizualizácií elektronických dokumentov, v dolnej časti sú lokálne nastavenia aplikácie. Zmeny v konfiguračných nastaveniach aplikácie sa prejavia až po uložení a reštartovaní aplikácie.

Komunikačné nastavenia:

Pre aktualizáciu vizualizácií je možné nastaviť viacero serverov, podľa toho, s akými elektronickými formulármi chce používateľ pracovať.

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.

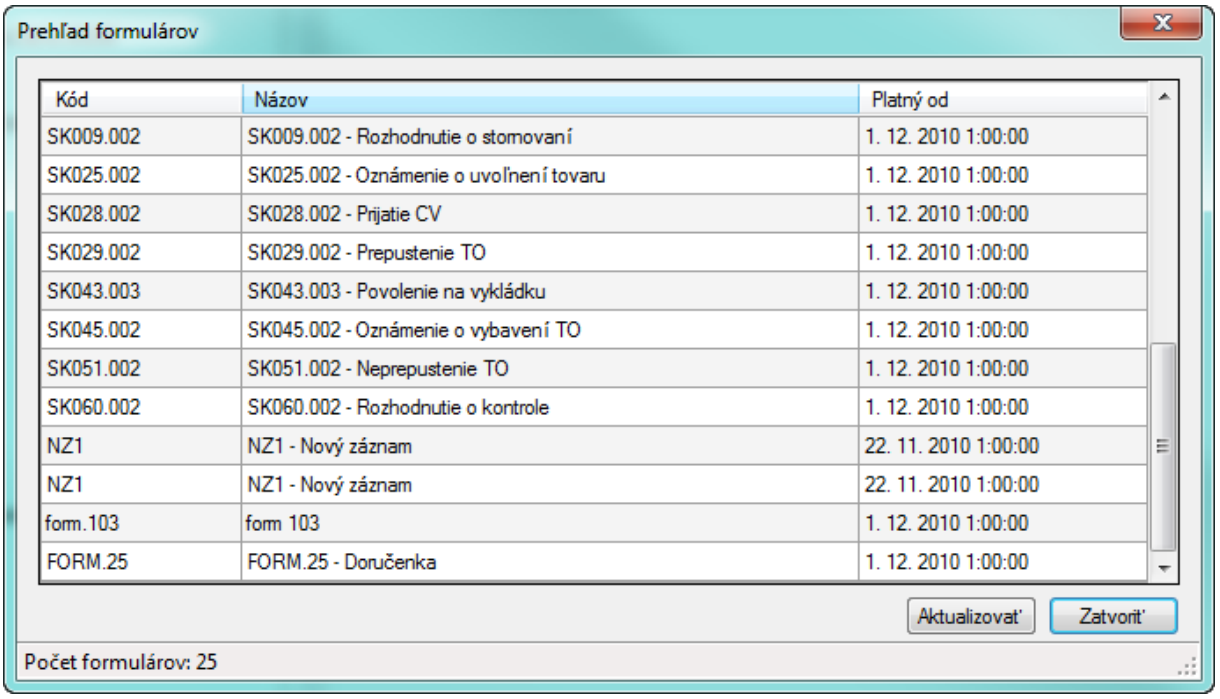
Zobrazovanie rozbaleného stromu podpísaného dokumentu – prepína zobrazovanie rozbaleného/zbaleného stromu dátovej štruktúry po otvorení súboru.

Jazyk aplikácie – nastavenie slovenského alebo anglického jazyka.

Nástroje –> Otvoriť konfiguračný priečinok – otvorí adresár konfiguračných nastavení aplikácie, v ktorom sa nachádza konfiguračný súbor a adresár vizualizačných schém elektronických formulárov.

Nástroje –> Zobraziť/skryť strom priečinok – zobrazí alebo skryje strom pre výber súborov v rámci operačného systému používateľa v ľavej časti obrazovky.

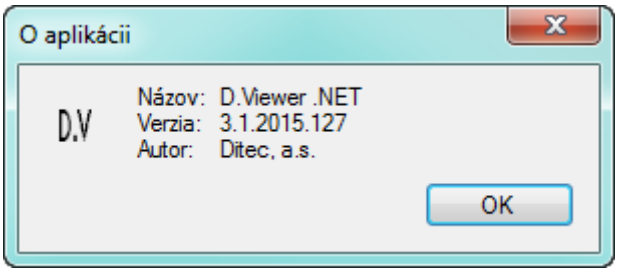
Formuláre – zobrazí okno prehľadu formulárov (obr. 3.1.3)



obr. 3.1.3

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 (obr. 3.1.4)


O aplikácii
D.V
Názov: D.Viewer .NET
Verzia: 3.1.2015.127
Autor: Ditec, a.s.
OK

obr. 3.1.4

4. Vizualizácia dátových štruktúr

D.Viewer .NET v3.1 podporuje vizualizáciu nasledovných dátových štruktúr:

- formát elektronickej správy podľa výnosu ministerstva financií Slovenskej republiky o jednotnom formáte elektronických správ vytváraných a odosielaných prostredníctvom prístupových miest a o podrobnostiach elektronických formulárov elektronických podaní a elektronických úradných dokumentov
  - ⇒ MessageContainer
- formát elektronického podania
  - ⇒ Registration v1.0, http://www.ditec.sk/ekr/registration/v1.0
- formát zaručeného elektronického podpisu na báze XAdES
  - ⇒ 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
- formát zloženého elektronického podpisu, pozostávajúceho z viacerých samostatných elektronických podpisov XAdES_ZEP
  - ⇒ DataSignatures v1.0, http://www.ditec.sk/ep/signature_formats/xades_zep/v1.0
  - ⇒ DataSignatures v1.1, http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1
  - ⇒ DataSignatures v2.0, http://www.ditec.sk/ep/signature_formats/xades_zep/v2.0
- formát zaručeného elektronického podpisu na báze CAdES
  - ⇒ CAdES_ZEP v1.0, http://www.ditec.sk/ep/signature_formats/cades_zep/v1.0
- ZIP obálka pre CAdES podpis(y) a ďalšie informácie súvisiace s podpisovaným dokumentom
  - ⇒ ZIP formát súboru (ZEPf), http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/schvalene-formaty/formaty_zep.pdf

4.1. MessageContainer

V nasledujúcej tabuľke je uvedený popis súčastí dátového prvku Kontajner elektronickej správy, resp. Elektronické podanie (MessageContainer):

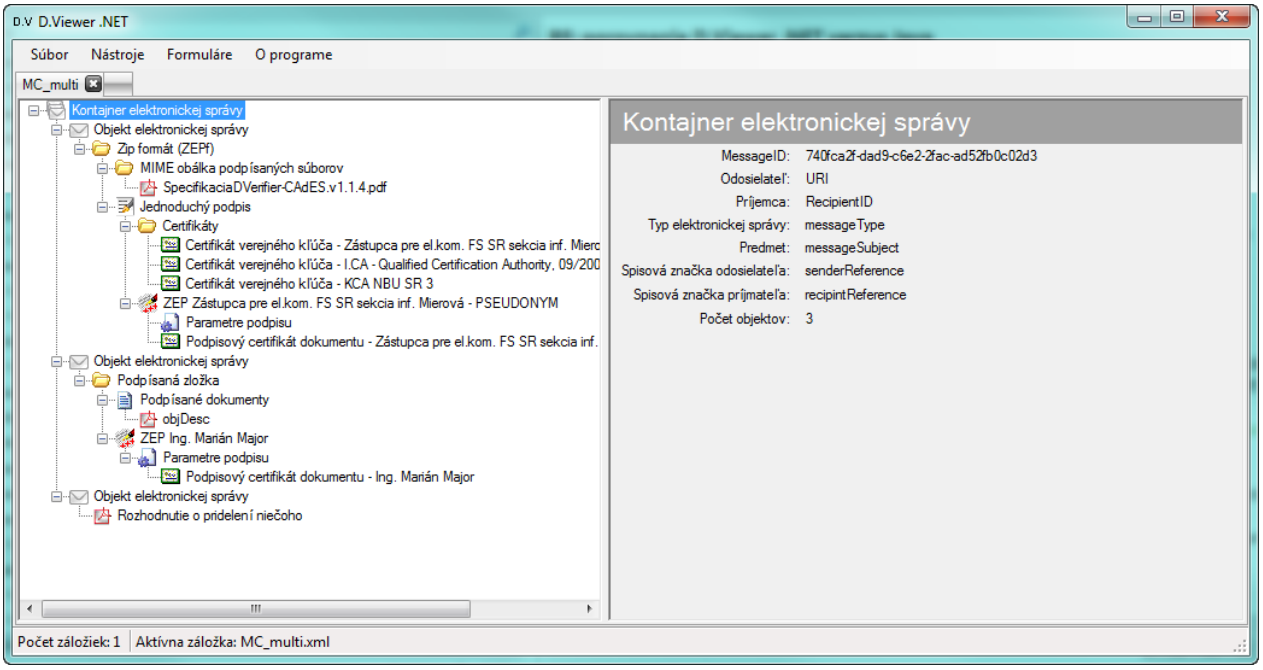
Atribút	Názov elementu / atribútu	Poznámka
Identifikátor elektronickej správy	MessageId	Jednoznačný identifikátor elektronickej správy. [Stav: Povinný.] [Formát reprezentácie: Guid.] [Hodnoty: Hodnota je generovaná.]
Odosielateľ elektronickej správy	SenderId	Jednoznačný identifikátor odosielateľa elektronickej správy. [Formát reprezentácie: Unified Resource Identifier (URI) v tvare referencovateľného identifikátora.] [Hodnoty: type=„IdIdentity“ – nemenná hodnota.] [Stav: Povinný.] [Poznámky: Referencovateľný identifikátor má tvar Unified Resource Identifier (URI), pričom posledná časť reťazca {referencia} reprezentuje samotnú hodnotu identifikácie.]
Príjemca elektronickej správy	RecipientId	Jednoznačný identifikátor prijímateľa elektronickej správy. [Stav: Povinný.] [Formát reprezentácie: Unified Resource Identifier (URI) v tvare referencovateľného identifikátora.] [Hodnoty: type=„IdIdentity“ – nemenná hodnota.] [Poznámky: Referencovateľný identifikátor mátvar Unified Resource Identifier (URI), pričom posledná časť reťazca {referencia} reprezentuje samotnú hodnotu identifikácie.]

Typ elektronickej správy	MessageType	Identifikuje typ podania, rozhodnutia a podobne. [Stav: Povinný.] [Formát reprezentácie: Textový reťazec.]
Predmet elektronickej správy	MessageSubject	Stručný popis predmetu elektronickej správy. [Stav: Nepovinný.] [Formát reprezentácie: Textový reťazec.] [Hodnoty: Nemá predpísaný obsah.] [Poznámky: Môže byť definovaný podľa typu elektronickej správy. Podanie vytvorené prostredníctvom ústredného portálu verejnej správy používa kód služby, zadaný pri registrácii elektronickej služby príslušným orgánom verejnej moci. Podľa tohto kódu sa vykonáva automatické spracovanie.]
Značka odosielateľa elektronickej správy	SenderBusinessReference	Spisová značka odosielateľa elektronickej správy. [Stav: Nepovinný.] [Formát reprezentácie: Textový reťazec.] [Hodnoty: Nemá predpísaný obsah.]
Značka prijímateľa elektronickej správy	RecipientBusinessReference	Spisová značka prijímateľa elektronickej správy. [Stav: Nepovinný.] [Formát reprezentácie: Textový reťazec.] [Hodnoty: Nemá predpísaný obsah.]
Objekt elektronickej správy	Object	Dátový prvok pre jeden objekt obsahu elektronickej správy. [Stav: Povinný] [Hodnoty: Vnorený elektronický formulár vo formáte XML alebo iný typ súboru.] [Poznámky: Môže byť použitý viackrát, pretože elektronická správa môže obsahovať viac objektov. Príklad použitia: Elektronický formulár.

		Príloha1. Príloha 2.] Atribúty: Id, Name, Description, Class, IsSigned, MimeType, Encoding
	Id	Reťazec slúžiaci ako jednoznačný identifikátor objektu elektronickej správy. [Stav: Povinný.] [Formát reprezentácie: Guid.] [Hodnoty: Hodnota je generovaná.] [Poznámky: Cieľom použitia je možnosť referencovania.]
	Name	Názov objektu, spravidla názov pôvodného súboru. [Stav: Nepovinný.] [Hodnoty: Nemá predpísaný obsah. Príklady použitia: RozhodnutieUPSVAR_RP_131_priloha.pdf. Ziadost_stavebne_povolenie_15.xml.]
	Description	Popis objektu, určený na zobrazenie. [Stav: Nepovinný.] [Hodnoty: Nemá predpísaný obsah. Príklady použitia: Rozhodnutie o pridelení rodičovského príspevku príloha 1, Žiadosť o stavebné povolenie.]
	Class	Trieda objektu, slúži na identifikovanie typu / účelu použitia objektu. [Stav: Povinný.] [Hodnoty: Vypĺňa sa v súlade s číselníkom ústredného portálu verejnej správy OBJECT_CLASS. Prípustné hodnoty sú: „AA_TOKEN“, ak je objektom autorizačný token, „ATTACHMENT“, ak je objektom všeobecná príloha, ktorá nie je elektronickým formulárom, „AUTHORIZATION“, ak je objektom

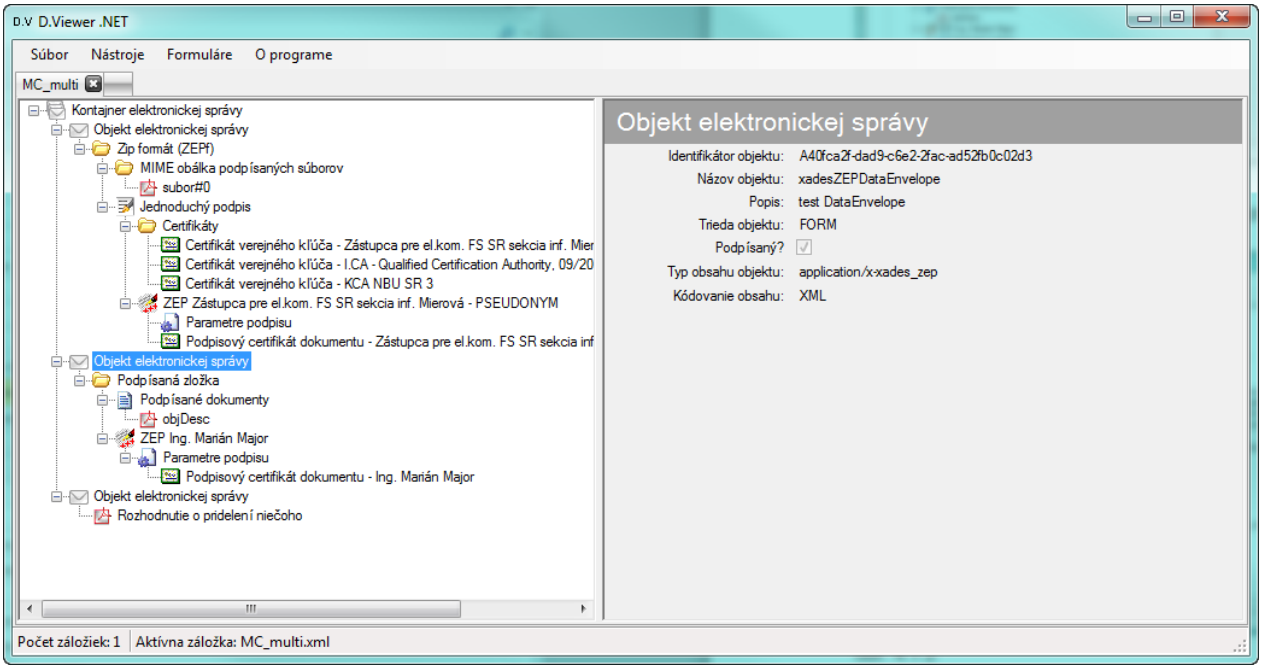
		technická forma splnomocnenia, „FORM“, ak je objektom elektronický formulár, „NOTIFY_TEMPLATE“, ak je objektom notifikačná šablóna.]
	IsSigned	Príznak, či je objekt elektronicky podpísaný. [Stav: Nepovinný.] [Hodnoty: „true“ Znamená, že objekt je elektronicky podpísaný. „false“ Znamená, že objekt nie je elektronicky podpísaný.]
	MimeType	Typ obsahu objektu, určuje dátový formát objektu.

Na obrázku 4.1.1 je uvedený príklad zobrazenia dátového prvku Kontajner elektronickej správy (MessageContainer), obsahujúceho tri objekty elektronickej správy.



obr. 4.1.1

Na obrázku 4.1.2 je uvedený príklad zobrazenia detailu objektu elektronickej správy.

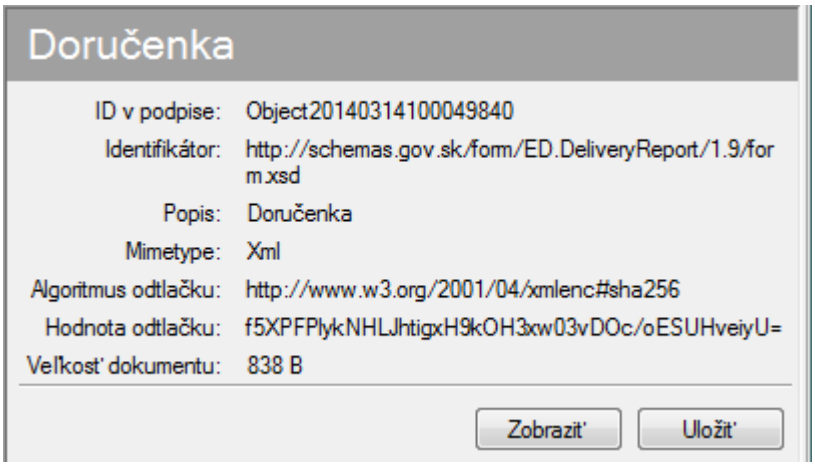


obr. 4.1.2

4.1.1. Overenie podania voči doručenke

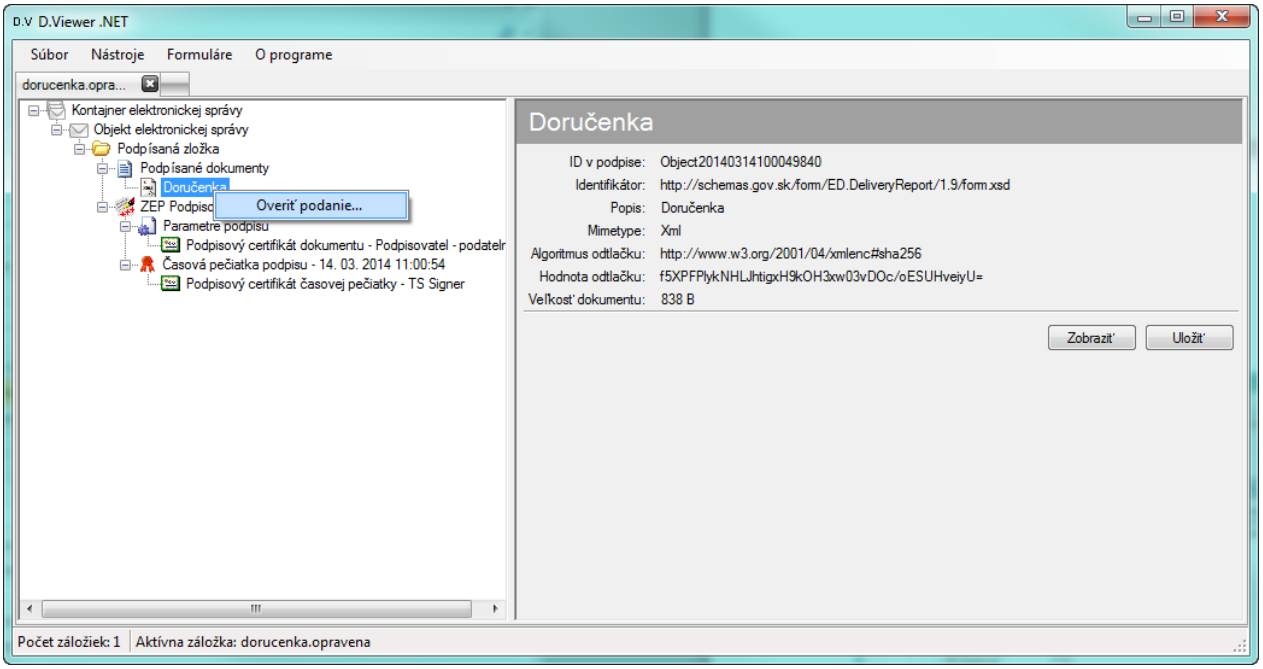
Doručenka je elektronický dokument, obsahujúci údaj o dni, hodine, minúte a sekunde elektronického doručenia, identifikátor osoby prijímateľa, identifikátor osoby odosielateľa a identifikáciu elektronickej správy a elektronických dokumentov, ktoré sa elektronicky doručujú. Ak je adresátom orgán verejnej 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 identifikátorom http://schemas.gov.sk/form/ED.DeliveryReport/1.9/form.xsd (obr. 4.1.1.1).



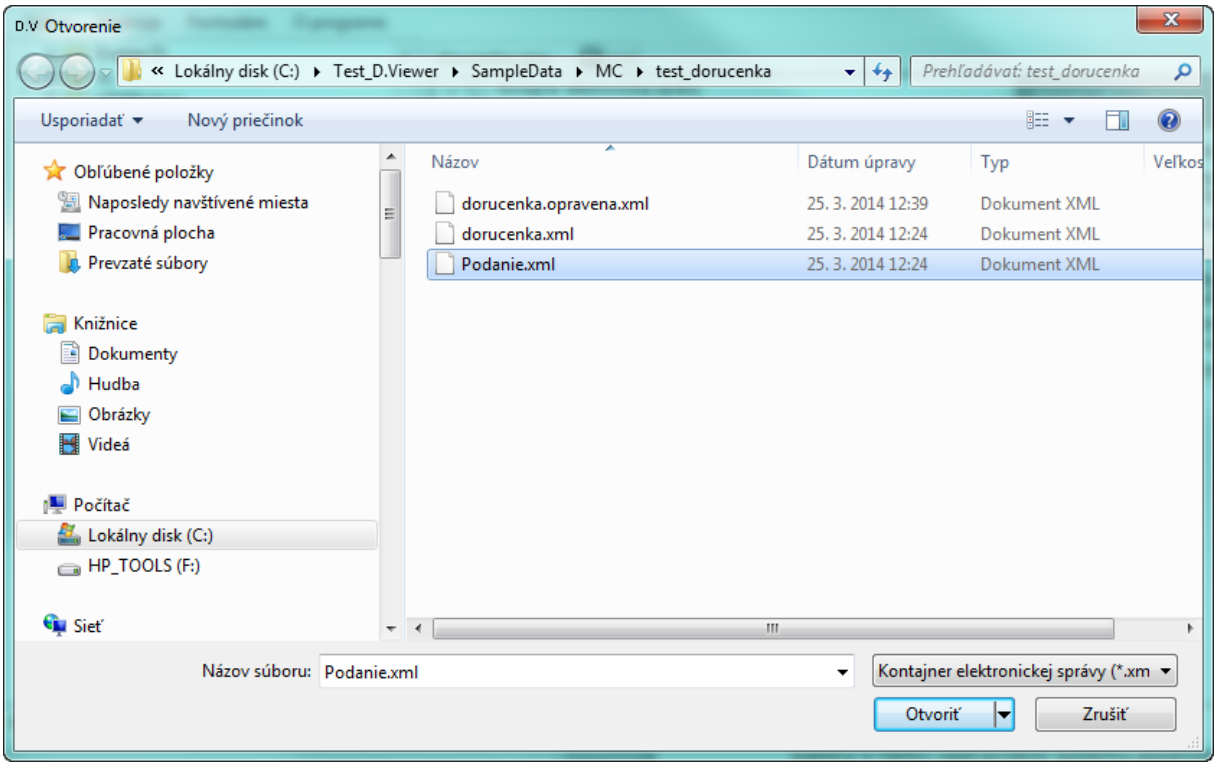
obr. 4.1.1.1

Ak kontajner elektronickej správy obsahuje Doručenku, kliknutím pravým tlačidlom myši na položku Doručenky v strome zobrazenej dátovej štruktúry sa používateľovi sprístupní operácia Overiť podanie (obr. 4.1.1.2).



obr. 4.1.1.2

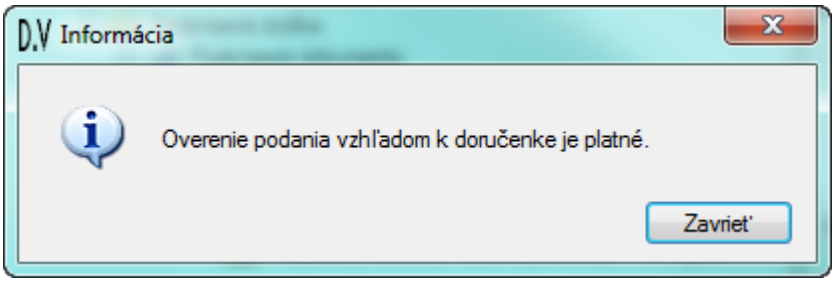
Po potvrdení operácie Overiť podanie sa zobrazí dialógové okno pre výber súboru elektronického podania v rámci operačného systému používateľa (obr. 4.1.1.3).



obr. 4.1.1.3

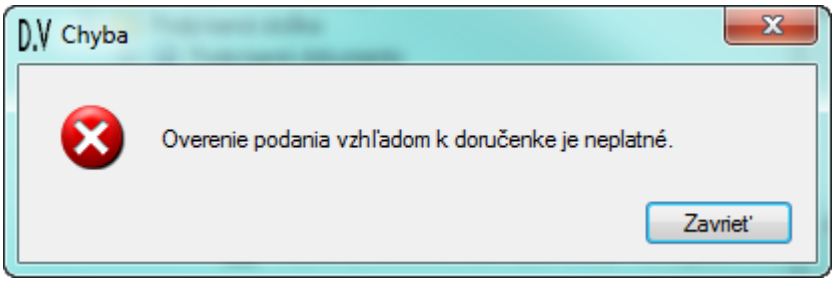
Používateľ vyberie súbor elektronického podania (MessageContainer). Aplikácia následne použije transformáciu a hash funkciu uvedenú v doručenke, vyráta digitálny odtlačok podania a vykoná porovnanie s digitálnym odtlačkom v doručenke.

Ak je digitálny odtlačok v doručenke zhodný s digitálnym odtlačkom podania, používateľovi sa zobrazí hláška (obr. 4.1.1.4).



obr. 4.1.1.4

Ak digitálny odtlačok v doručenke nie je zhodný s digitálnym odtlačkom podania, používateľovi sa zobrazí hláška (obr. 4.1.1.5).



obr. 4.1.1.5

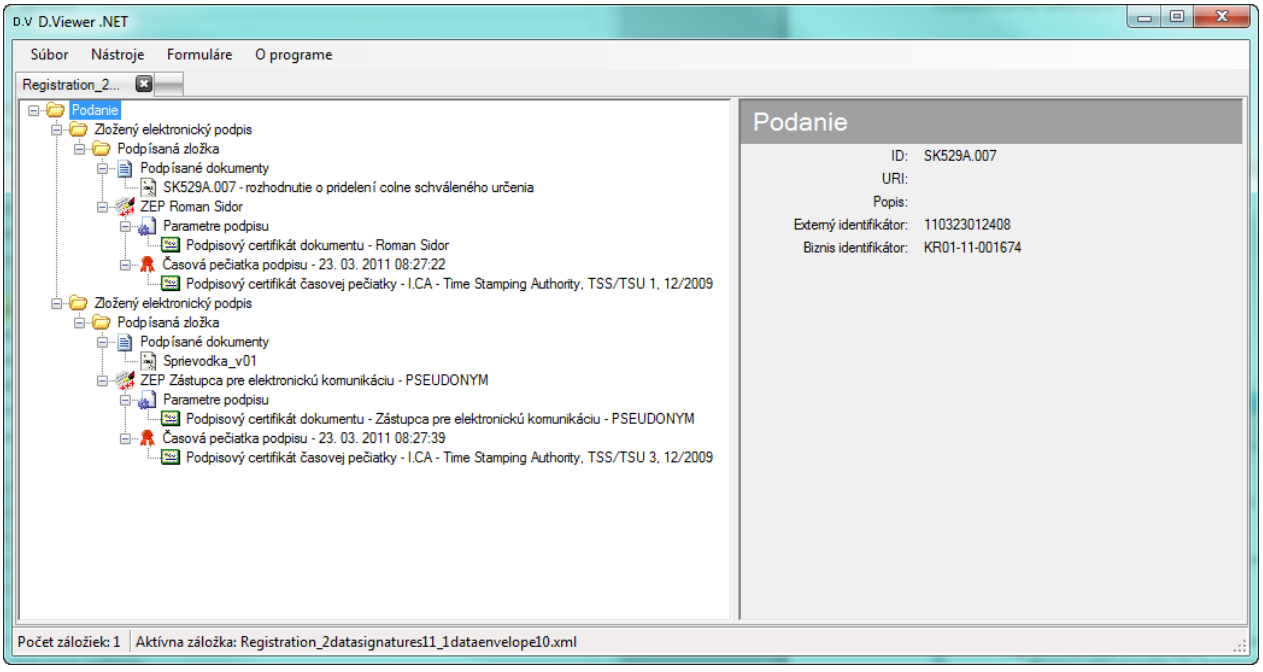
4.2. Registration

V nasledujúcej tabuľke je uvedený popis súčastí dátového prvku Elektronické podanie (Registration):

Atribút	Názov elementu / atribútu	Poznámka
Podanie	Registration	Dátový prvok elektronického podania. [Stav: Povinný] [Hodnoty: Napríklad dokument zloženého el. podpisu alebo dokument bez autorizácie.] [Poznámky: Elektronické podanie môže obsahovať viac objektov.]
URI	URI	Bližšia identifikácia elektronického podania. Z pohľadu spracovania nie je vyžadovaný ani inak kontrolovaný, pokiaľ to nie je explicitne vyžadované správcom biznisu. [Formát reprezentácie: Unified Resource Identifier (URI) v tvare referencovateľného identifikátora.] [Stav: Nepovinný.]
Identifikátor typu podania	ID	Reťazec slúžiaci ako jednoznačný identifikátor typu elektronického podania. [Stav: Nepovinný.] [Hodnoty: Nemá predpísaný obsah.]
Popis	Description	Bližšia identifikácia elektronického podania. [Stav: Nepovinný.] [Hodnoty: Nemá predpísaný obsah.]
Externý	ExternalIdentifier	Identifikácia externého systému v pripade

identifikátor		komunikácie podateľňa-podateľňa. [Stav: Nepovinný.] [Hodnoty: Nemá predpísaný obsah.]
Identifikátor biznis prípadu	BusinessIdentifier	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. [Stav: Nepovinný.] [Hodnoty: Nemá predpísaný obsah.]

Na obrázku 4.2.1 je uvedený príklad zobrazenia Elektronického podania (Registration), obsahujúceho dva Zložené elektronické podpisy.



obr. 4.2.1

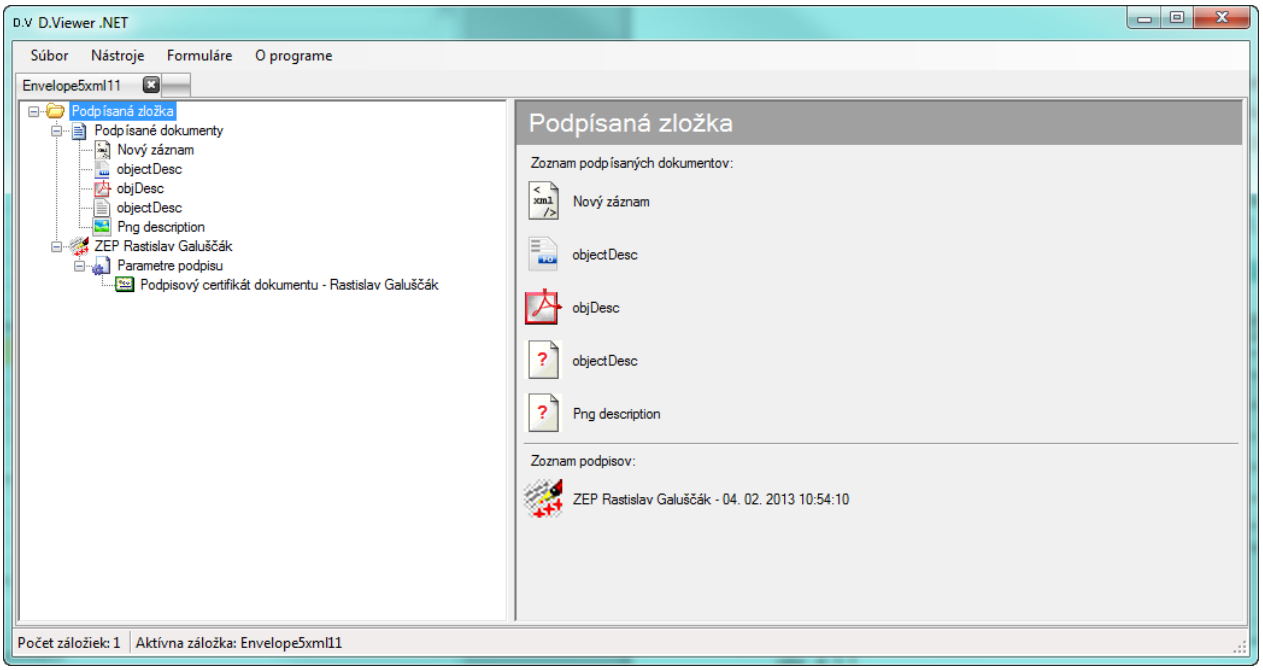
4.3. XAdES_ZEP

XAdES_ZEP 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 rôznych formátov dát (XML, FO, PDF, PNG, TXT).

Aplkácia D.Viewer .NET zobrazuje elektronický podpis, resp. elektronickú pečať vo formáte XAdES_ZEP pod názvom Podpísaná zložka. V hierarchickej stromovej štruktúre v rámci Podpísanej zložky sa zobrazujú dátové objekty:

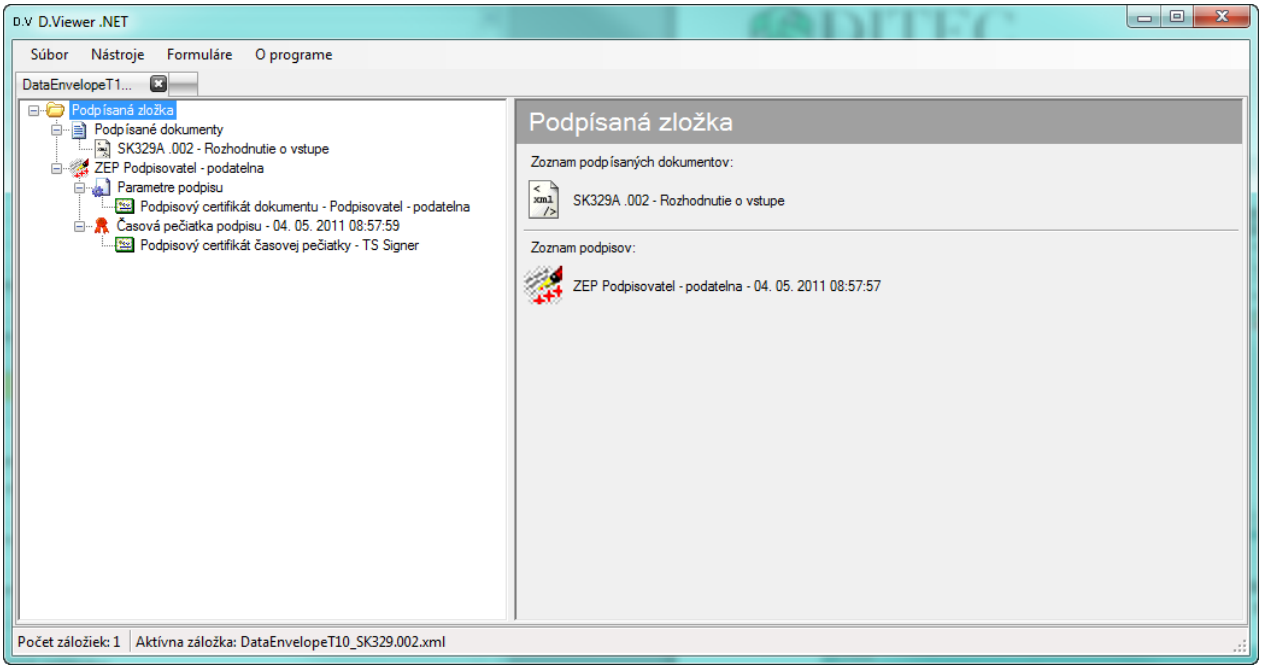
- Podpísané dokumenty – podpísaných môže byť jeden alebo viac elektronických dokumentov vo formátoch XML, FO, PDF, PNG, TXT
- Podpis – vo formáte XAdES_ZEP
    - ⇒ Časová pečiatka podpisu – povinné pre formát podpisu XAdES-T, XAdES-X type 1, XAdES-A
    - ⇒ Časová pečiatka referencií validačných dát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

Na obrázku 4.3.1 je uvedený príklad zobrazenia elektronického podpisu vo formáte XAdES_ZEP_EPES (bez časovej pečiatky), s piatimi podpísanými dokumentami (XML, FO, PDF, PNG, TXT).



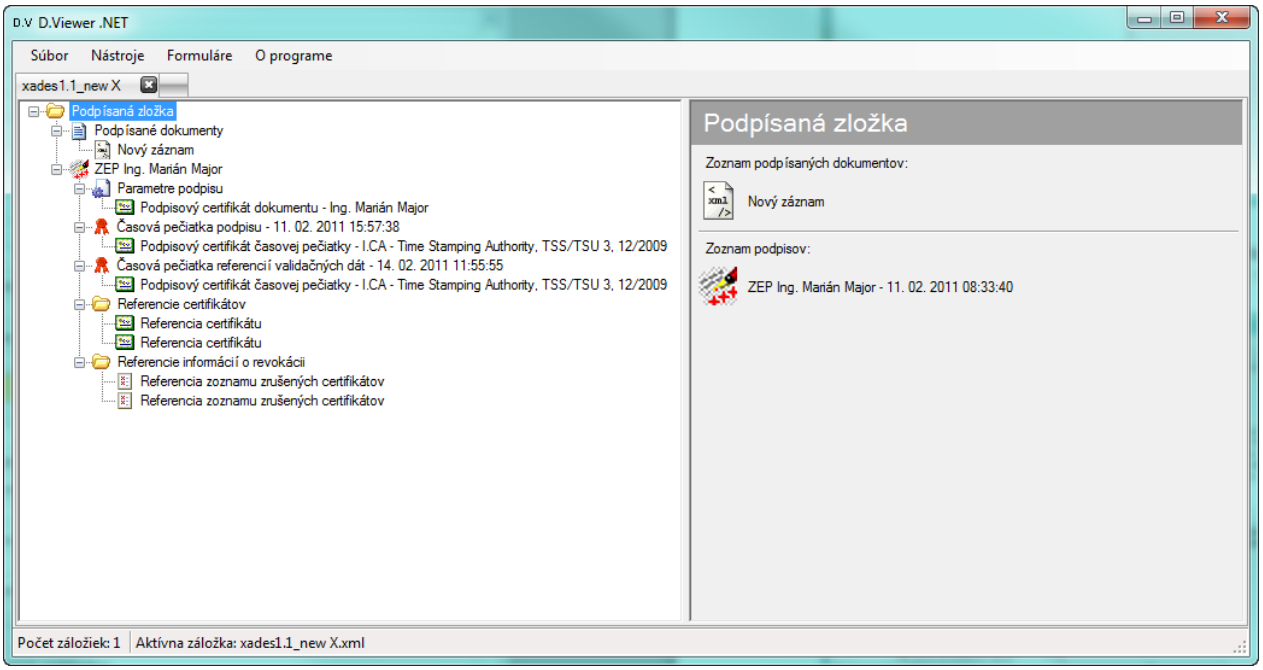
obr. 4.3.1

Na obrázku 4.3.2 je uvedený príklad zobrazenia elektronického podpisu vo formáte XAdES_ZEP_T s časovou pečiatkou podpisu, s podpísaným dokumentom vo formáte XML.



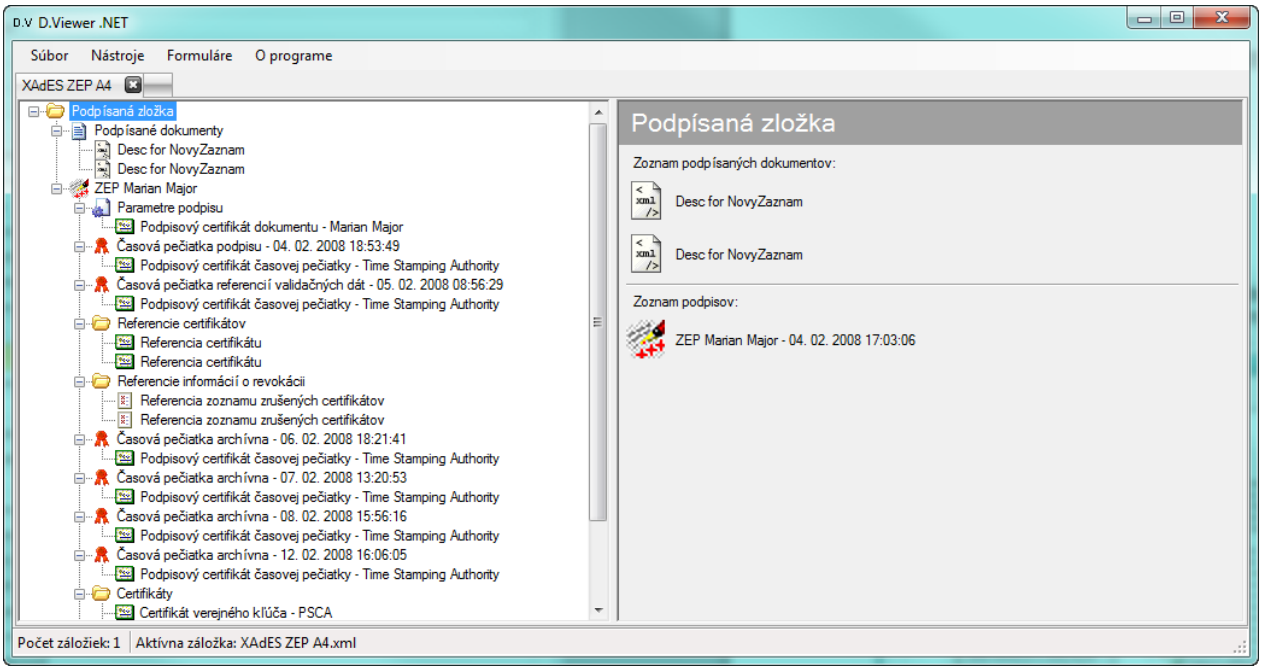
obr. 4.3.2

Na obrázku 4.3.3 je uvedený príklad zobrazenia elektronického podpisu vo formáte XAdES_ZEP_X1 s časovou pečiatkou referencií validačných dát, s podpísaným dokumentom vo formáte XML.



obr. 4.3.3

Na obrázku 4.3.4 je uvedený príklad zobrazenia elektronického podpisu vo formáte XAdES_ZEP_A so štyrmi archívnymi časovými pečiatkami, s dvoma podpísanými dokumentami vo formáte XML.



obr. 4.3.4

4.4. DataSignatures

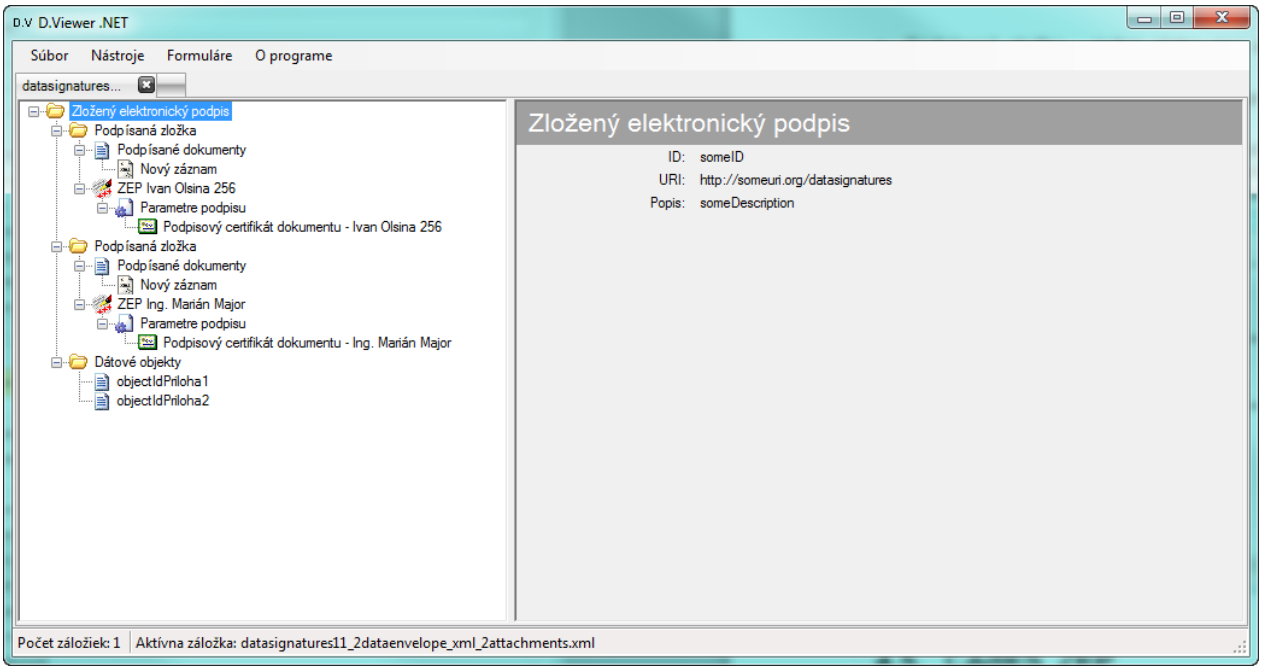
DataSignatures je formát zloženého elektronického podpisu, pozostávajúceho z viacerých samostatných elektronických podpisov XAdES_ZEP. V rámci zloženého elektronického podpisu je možné spojiť niekoľko nezávislých elektronických podpisov, ktoré boli vytvorené v súlade s profilom XAdES_ZEP, prípadne nad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

Aplkácia D.Viewer .NET 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

Na obrázku 4.4.1 je uvedený príklad zobrazenia zloženého elektronického podpisu DataSignatures, ktorý obsahuje dva elektronické podpisy vo formáte XAdES_ZEP a dva nepodpísané elektronické dokumenty.



obr. 4.4.1

4.5. CAdES_ZEP

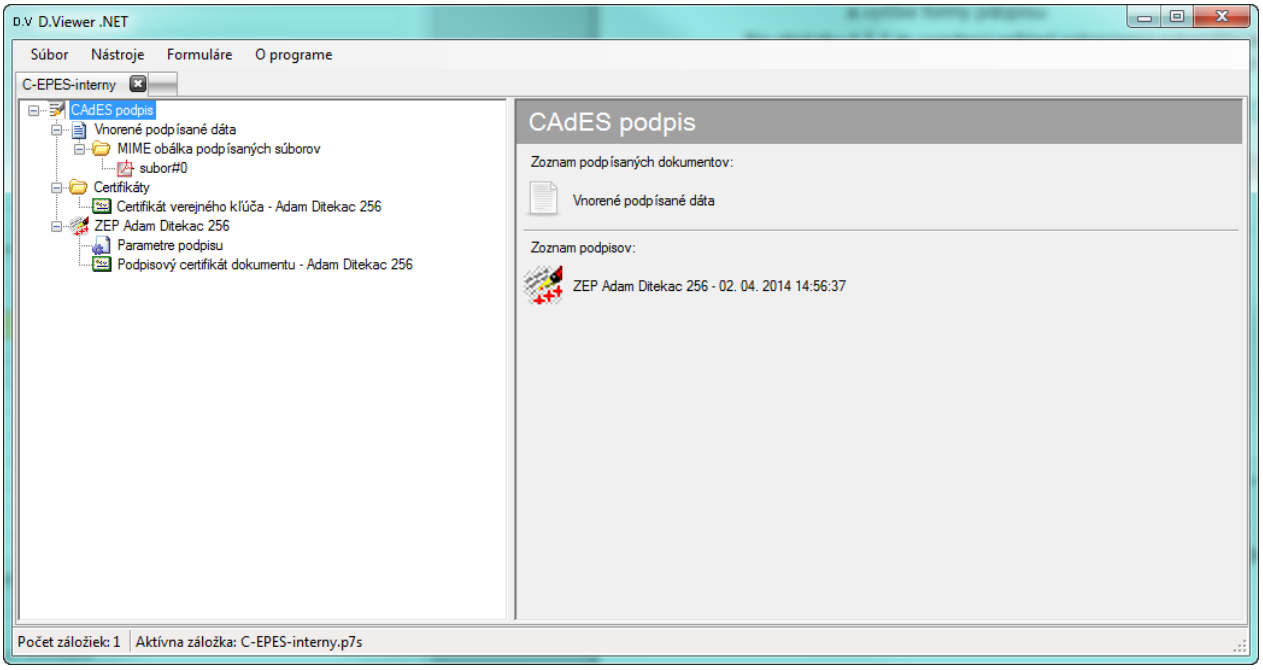
CAdES_ZEP je formát elektronického podpisu definovaný v súlade so špecifikáciou CAdES a zároveň platnou legislatívou Slovenskej republiky pre oblasť elektronického podpisu, pre vytváranie a overovanie zaručeného elektronického podpisu, resp. zaručenej elektronickej pečate, nad množinou rôznych formátov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

Aplkácia D.Viewer .NET zobrazuje elektronický podpis, resp. elektronickú pečať vo formáte CAdES_ZEP pod názvom CAdES podpis. V hierarchickej stromovej štruktúre v rámci CAdES podpisu sa 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.

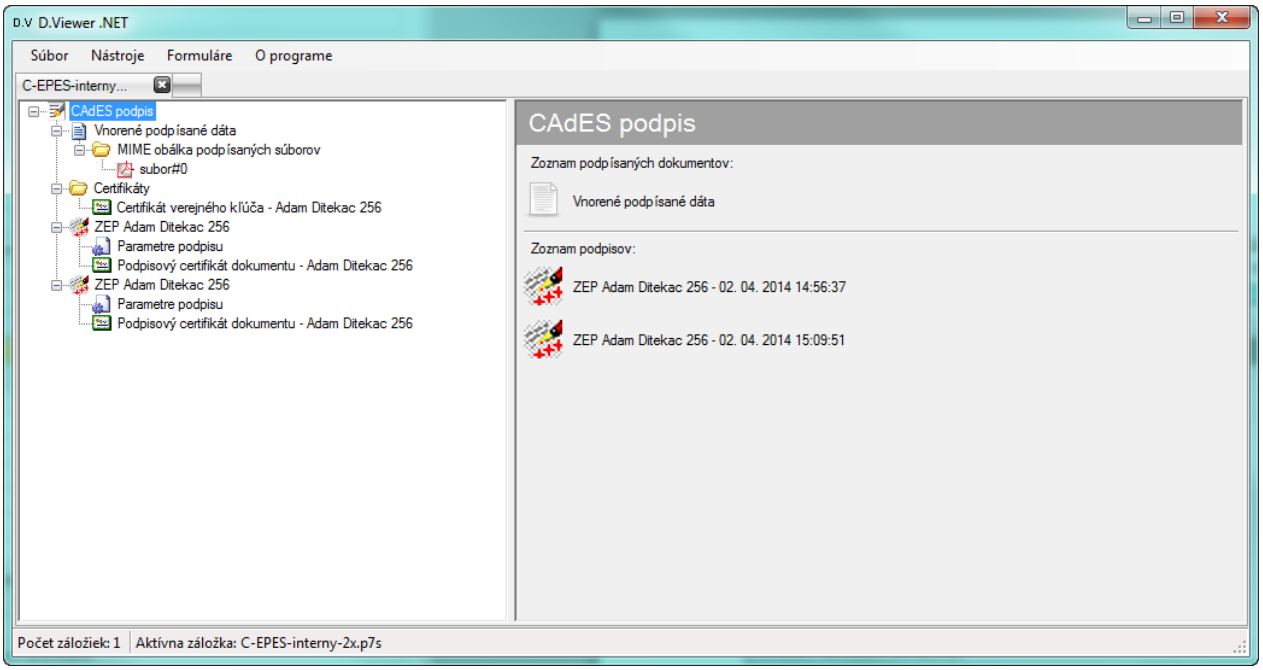
- Certifikáty – zoznam obsahuje povinne všetky podpisové certifikáty a nepovinne certifikáty z certifikačnej cesty podpisových certifikátov
- Informácia o revokácii – zoznam(y) revokovaných certifikátov (CRL) a OCSP odpovedí
- Podpis – CMS štruktúra CAdES podpisu môže obsahovať jeden alebo viacero podpisov (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

Na obrázku 4.5.1 je uvedený príklad zobrazenia interného elektronického podpisu vo formáte CAdES_ZEP_EPES (bez časovej pečiatky), s podpísanou S/MIME obálkou, ktorá obsahuje jeden súbor vo formáte PDF.



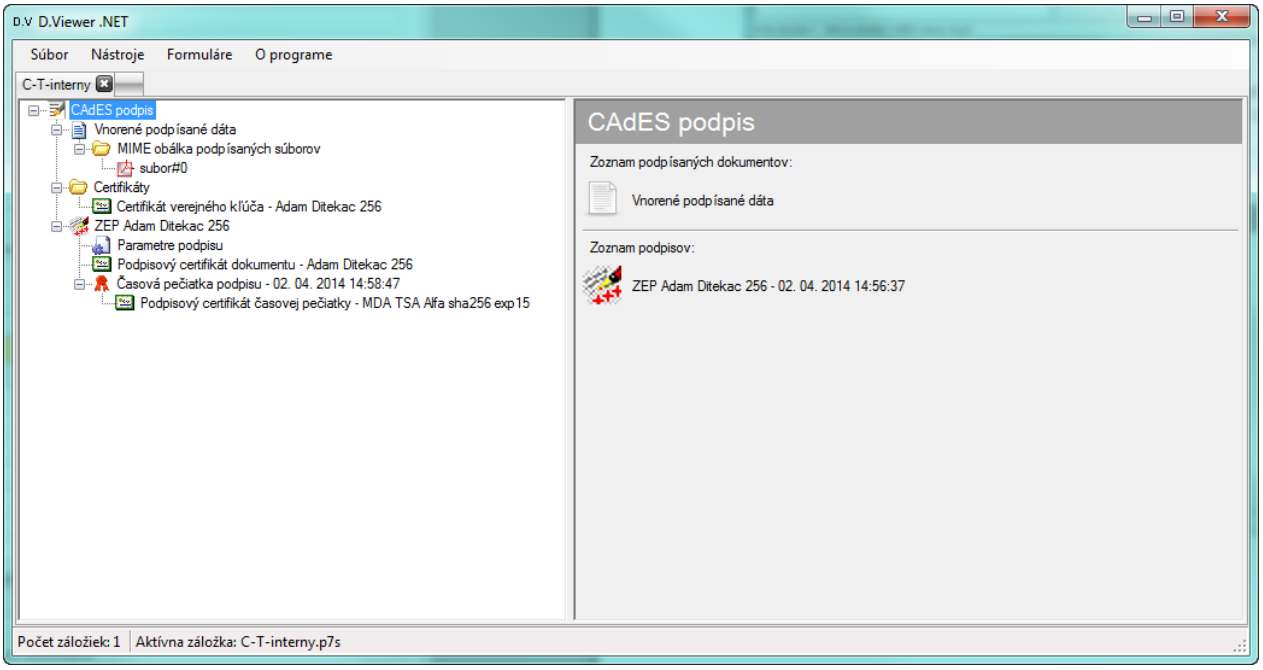
obr. 4.5.1

Na obrázku 4.5.2 je uvedený príklad zobrazenia dvojitého interného elektronického podpisu vo formáte CAdES_ZEP_EPES (bez časovej pečiatky), s podpísanou S/MIME obálkou, ktorá obsahuje jedent súbor vo formáte PDF. CMS štruktúra v tomto príklade obsahuje dva podpisy (dve sekcie SignerInfo).



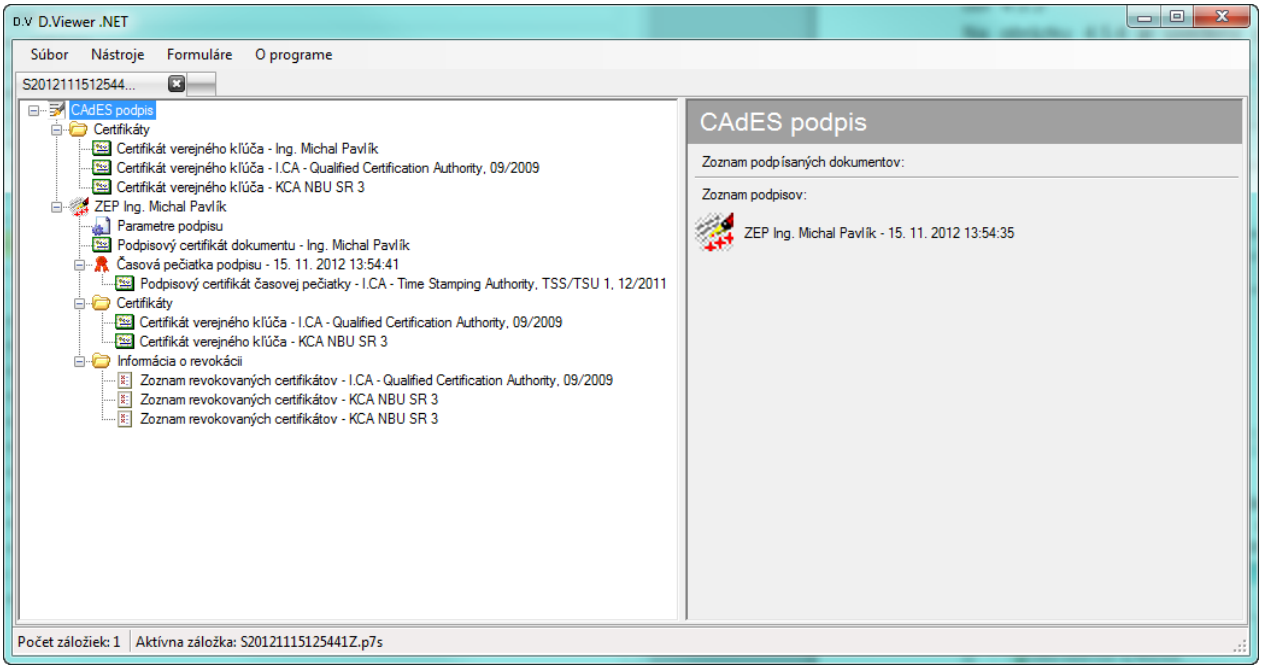
obr. 4.5.2

Na obrázku 4.5.3 je uvedený príklad zobrazenia interného elektronického podpisu vo formáte CAdES_ZEP_T (s časovou pečiatkou), s podpísanou S/MIME obálkou, ktorá obsahuje jedent súbor vo formáte PDF.



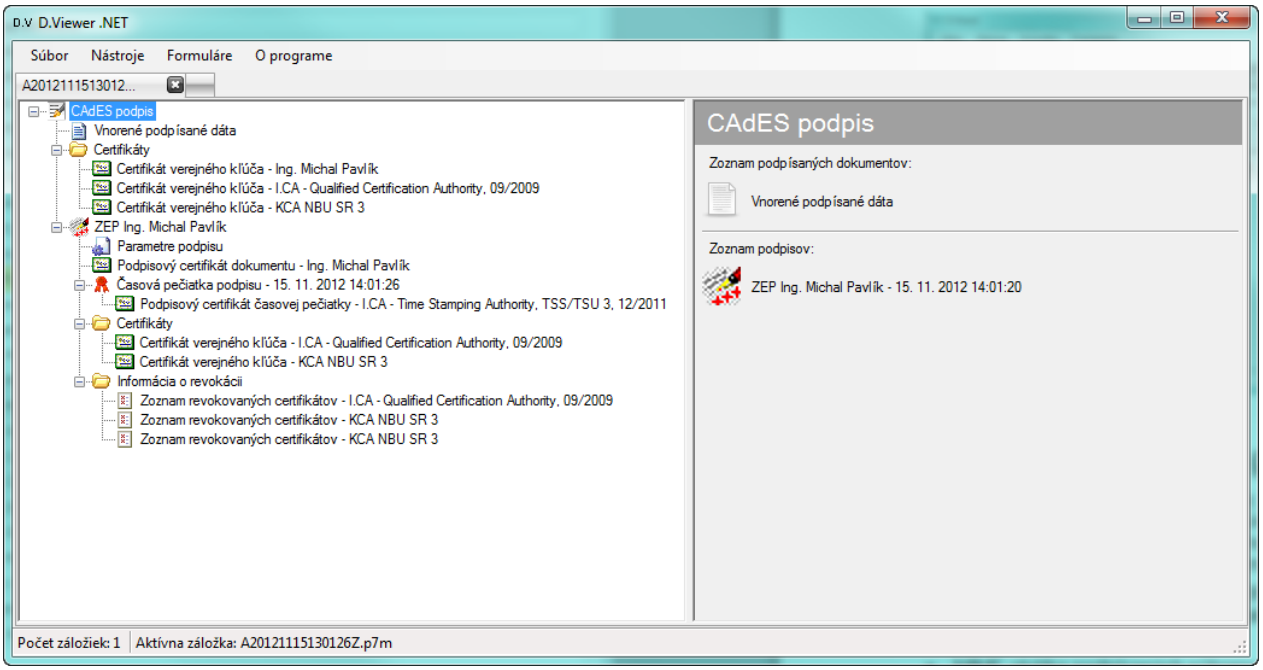
obr. 4.5.3

Na obrázku 4.5.4 je uvedený príklad zobrazenia externého elektronického podpisu vo formáte CAdES_ZEP_T (s časovou pečiatkou).



obr. 4.5.4

Na obrázku 4.5.5 je uvedený príklad zobrazenia interného elektronického podpisu vo formáte CAdES_ZEP_A (s archívnou časovou pečiatkou), s vnorenými podpísanými dátami (textový súbor).



obr. 4.5.5

4.6. ZIP formát súboru (ZEPf)

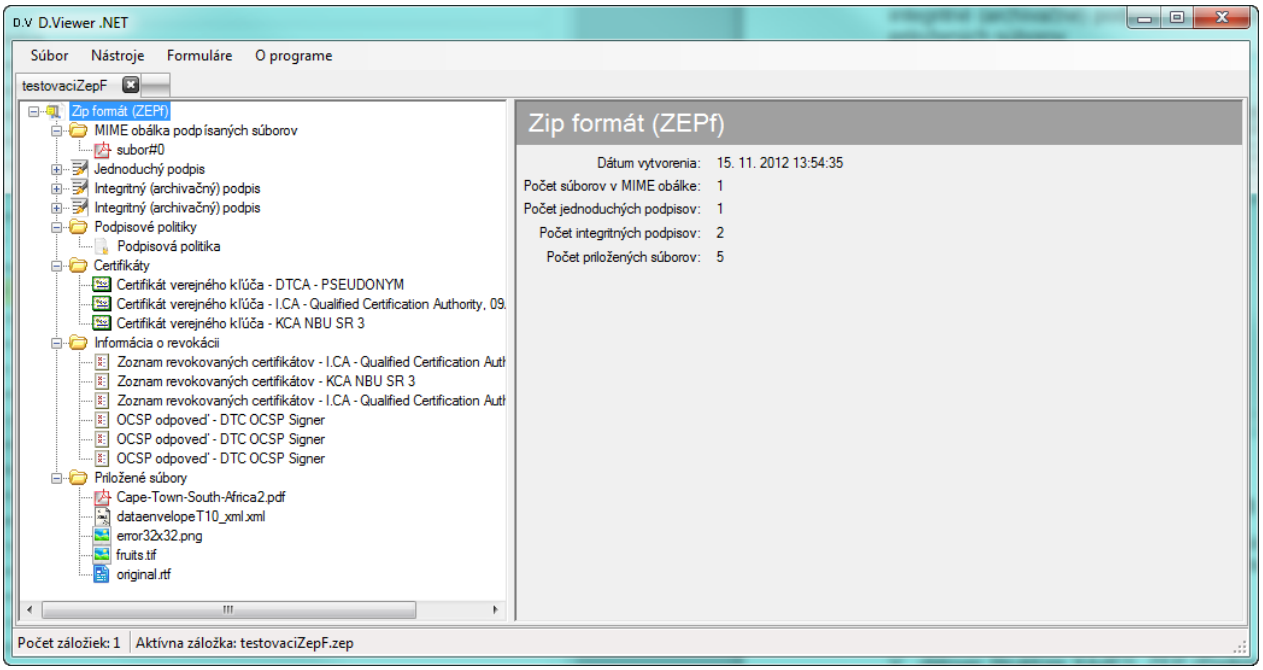
Podpisovaný dokument, jeho podpisy, informácie potrebné na overenie podpisu dokumentu a ďalšie dokumenty súvisiace s podpisovaným dokumentom je potrebné spojiť do formátu, ktorého spracovanie je jednoduché a bežne dostupné. Medzi takéto bežne dostupné formáty patrí aj ZIP.

Aplkácia D.Viewer .NET 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 4.5 CAdES_ZEP
- Integritný (archivačný) podpis - ZEPfZIP obálka môže nepovinne obsahovať jeden alebo viacero integritných (archivačných) CAdES podpisov, pozri kapitola 4.5 CAdES_ZEP
- Podpisové politiky – nepovinne jedna alebo viac podpisových politík
- Certifikáty - nepovinne jeden alebo viac certifikátov

- Infromácia o revokácii – nepovinne zoznam(y) revokovaných certifikátov (CRL) a OCSP odpovedí
- Priložené súbory – nepovinne zoznam priložených súborov

Na obrázku 4.6.1 je uvedený 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.



obr. 4.6.1

4.7. 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 .NET.

4.7.1. Podpis

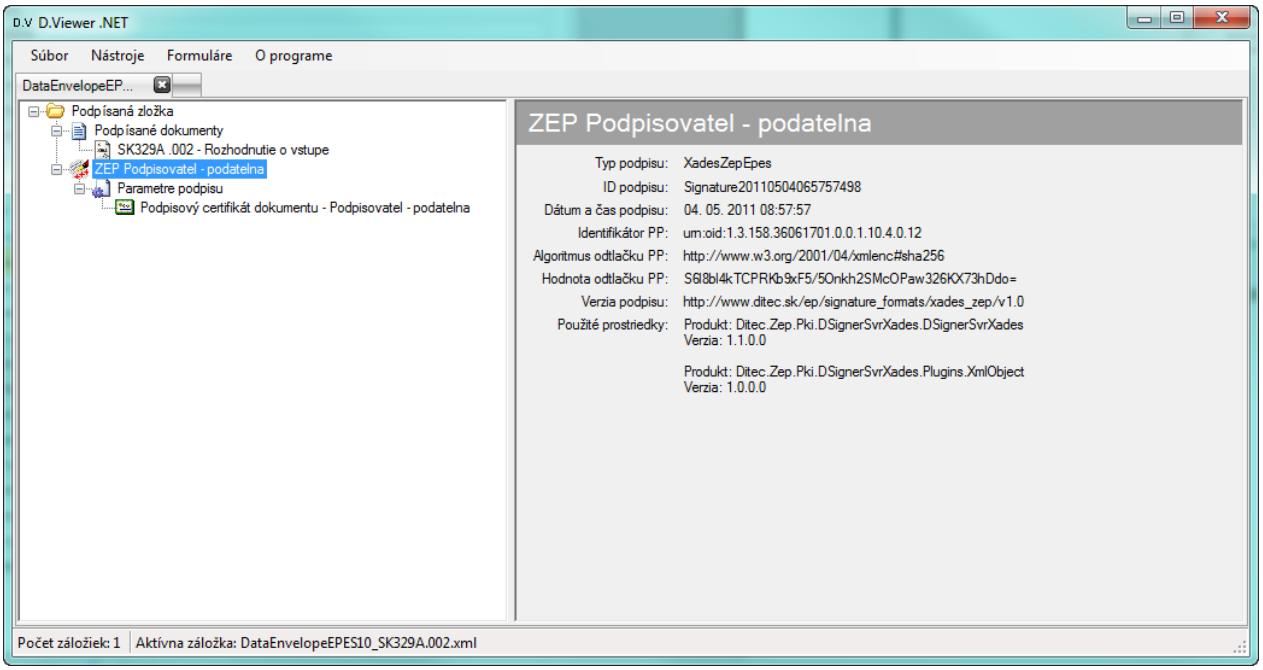
V dátovej štruktúre XAdES_ZEP (Podpísaná zložka) sa nachádza vždy jeden podpis, v dátovej štruktúre CAdES_ZEP (CAdES podpis) sa môže nachádzať jeden alebo viacero podpisov.

V rámci detailu podpisu sa zobrazujú atribúty:

- Typ podpisu

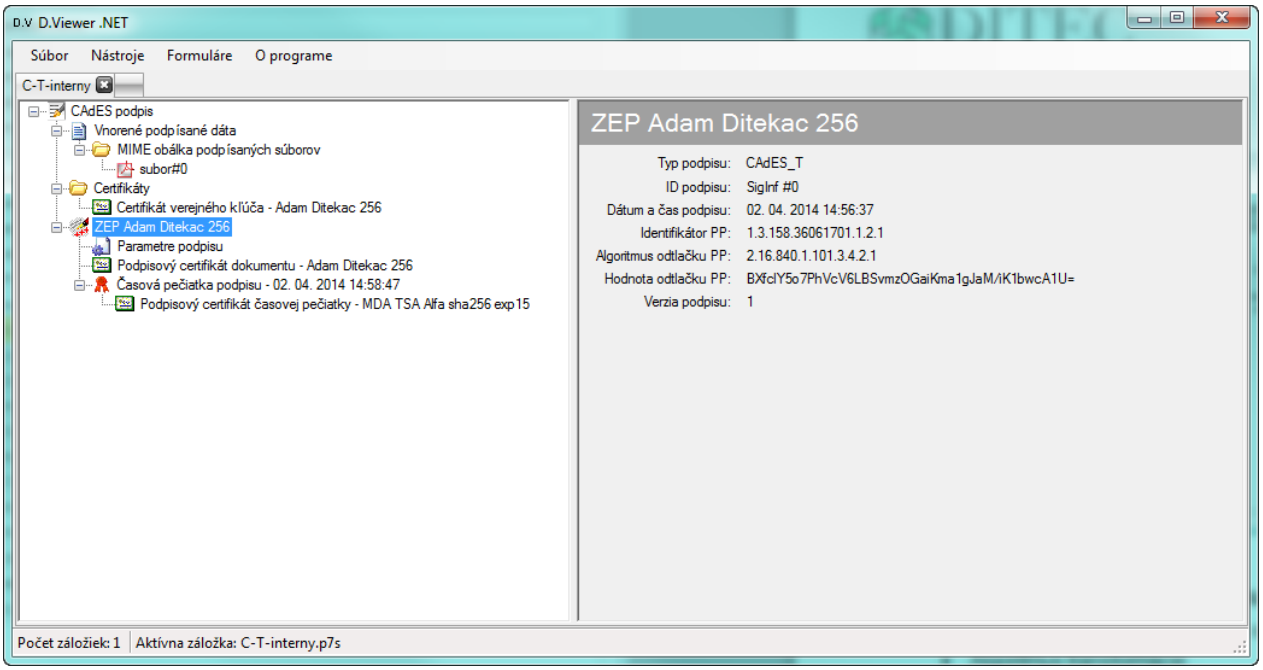
- ID podpisu
- Dátum a čas podpisu
- Identifikátor podpisovej politiky
- Algoritmus odtlačku podpisovej politiky
- Hodnota odlačku podpisovej politiky
- Verzia podpisu
- Použité prostriedky

Na obrázku 4.7.1.1 je uvedený príklad zobrazenia detailu podpisu XAdESZEPEpes.



obr. 4.7.1.1

Na obrázku 4.7.1.2 je uvedený príklad zobrazenia detailu podpisu CAdES_EPES.



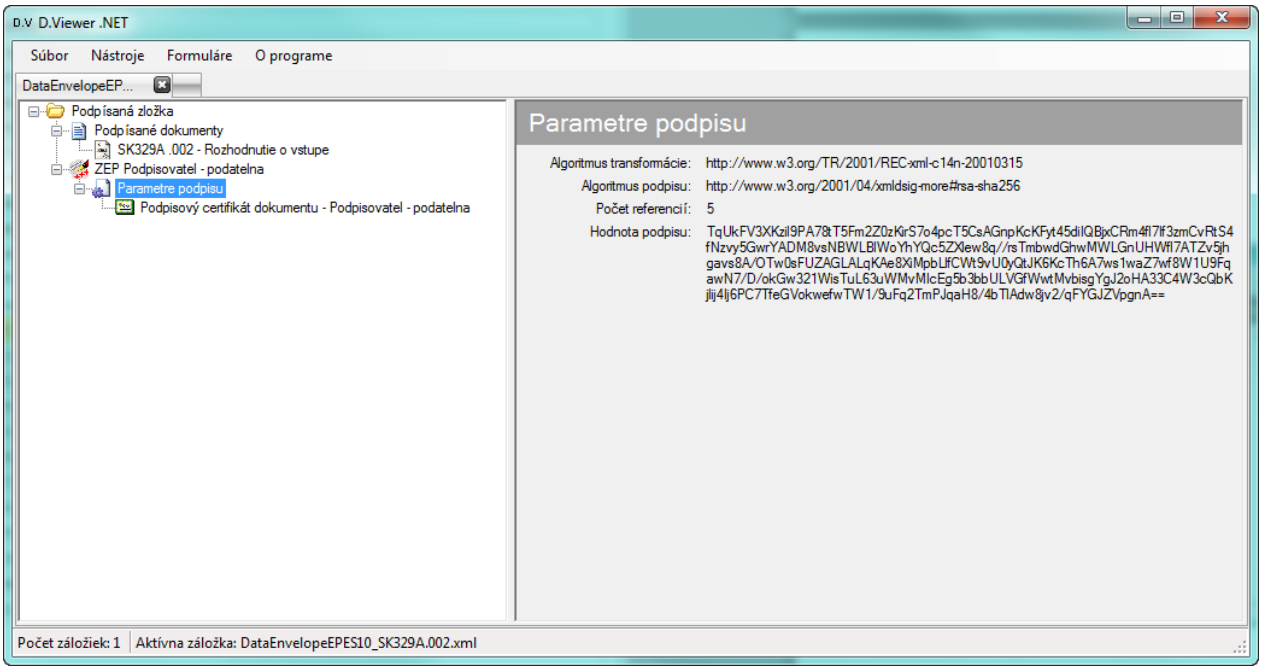
obr. 4.7.1.2

4.7.2. Parametre podpisu

V rámci detailu parametrov podpisu sa zobrazujú atribúty:

- Algoritmus transformácie
- Algoritmus podpisu
- Počet referencií
- Hodnota podpisu

Na obrázku 4.7.2.1 je uvedený príklad zobrazenia parametrov podpisu.



obr. 4.7.2.1

4.7.3. MIME obálka

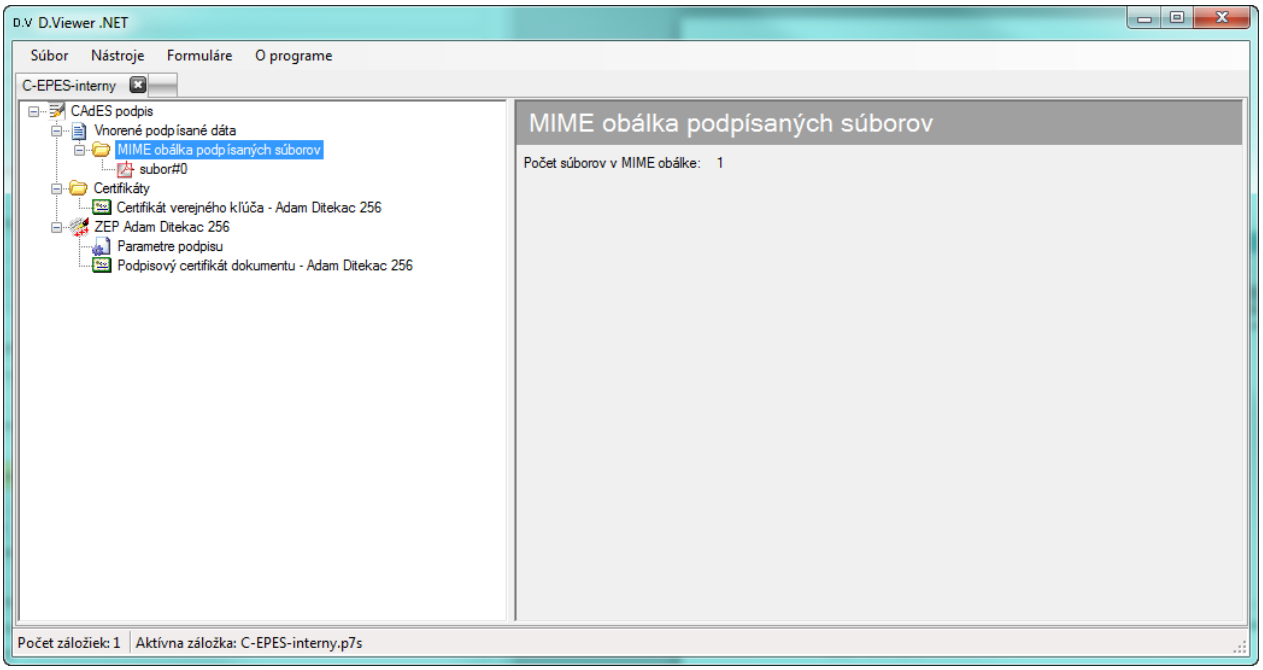
MIME obálka podpísaných súborov sa môže zobrazovať v rámci ZEPfZIP obákly (ako externe podpísané dáta ku všetkým Jednoduchým podisom v ZEPfZIP obákle) alebo v rámci interného CAdES podpisu pod položkou Vnorené podpísané dáta.

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.)

Na obrázku 4.7.3.1 je uvedený príklad zobrazenia detailu MIME obálky s jedným PDF súborom.

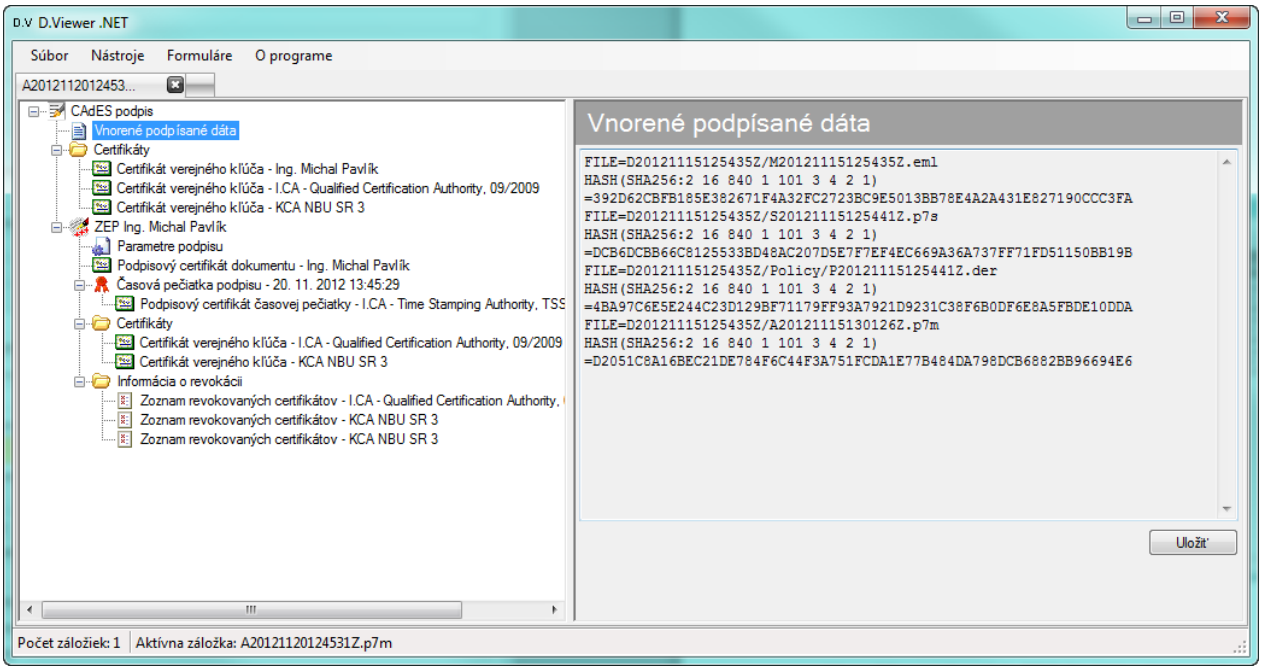


obr. 4.7.3.1

4.7.4. 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 4.7.3 MIME obálka). V prípade integritného CAdES podpisu je podpísaný textový súbor obsahujúci referencie dát, ktorých integrita je podpisom chránená.

Na obrázku 4.7.4.1 je uvedený príklad zobrazenia detailu vnorených podpísaných dát integritného CAdES podpisu.



obr. 4.7.4.1

4.7.5. Certifikát

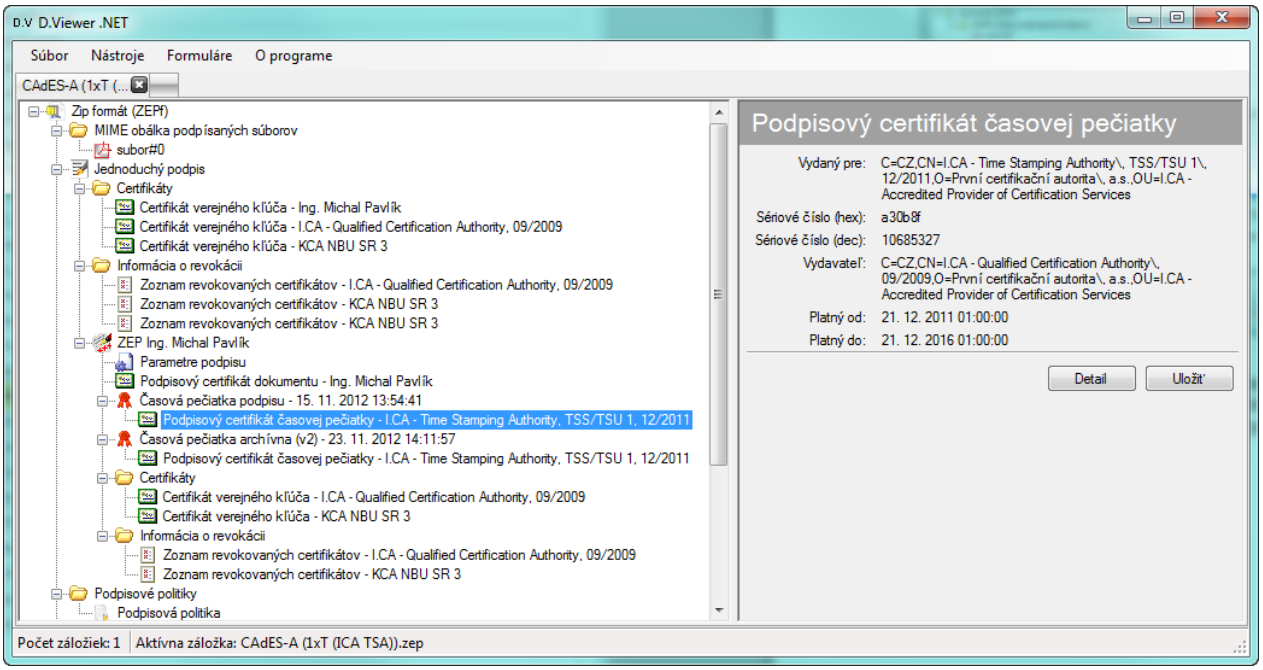
Vo vyššie popísaných ZEP štruktúrach sa môže zobrazovať:

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

Pri zobrazení detailu certifikátu sa zobrazujú atribúty:

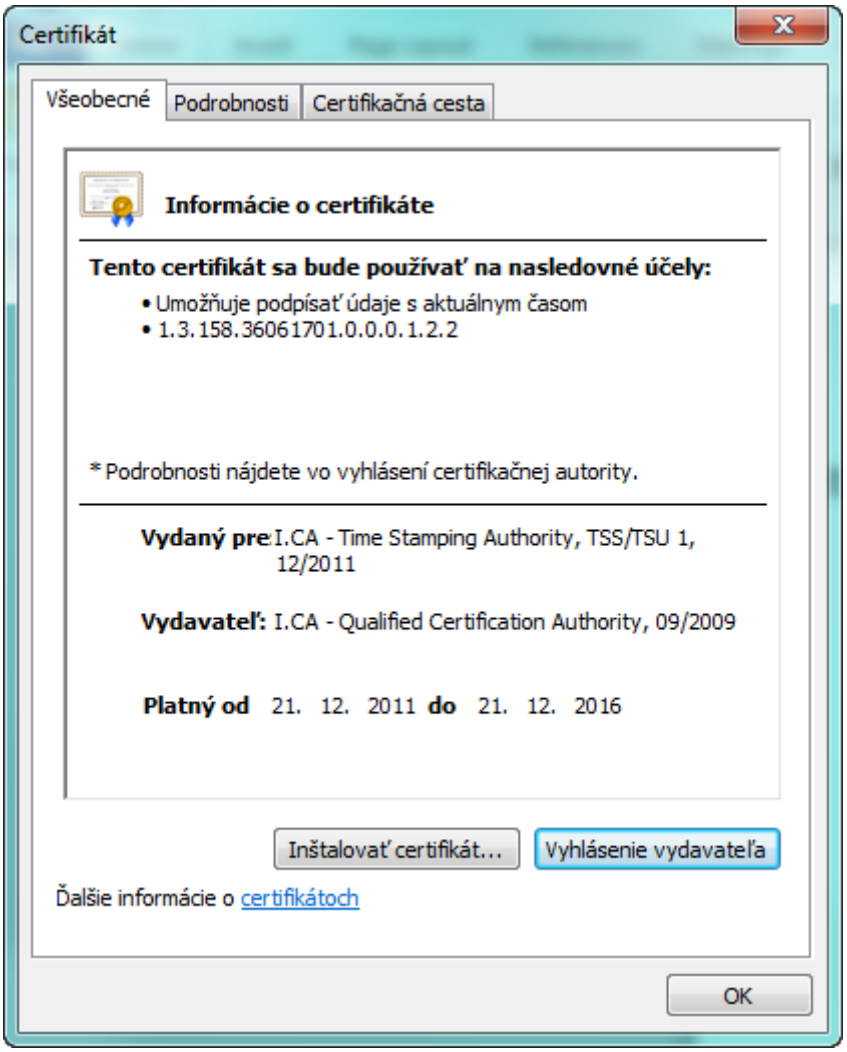
- Vydaný pre
- Sériové číslo (hex)
- Sériové číslo (dec)
- Vydavateľ
- Platný od
- Platný do

Na obrázku 4.7.5.1 je uvedený príklad zobrazenia detailu podpisového certifikátu časovej pečiatky.



obr. 4.7.5.1

Kliknutím na tlačidlo Detail sa v štandardnom okne operačného systému zobrazí detail certifikátu (obr. 4.7.5.2). Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie certifikátu v rámci operačného systému používateľa.



obr. 4.7.5.2

4.7.6. Časová pečiatka

Vo vyššie popísaných ZEP štruktúrach sa môže zobrazovať:

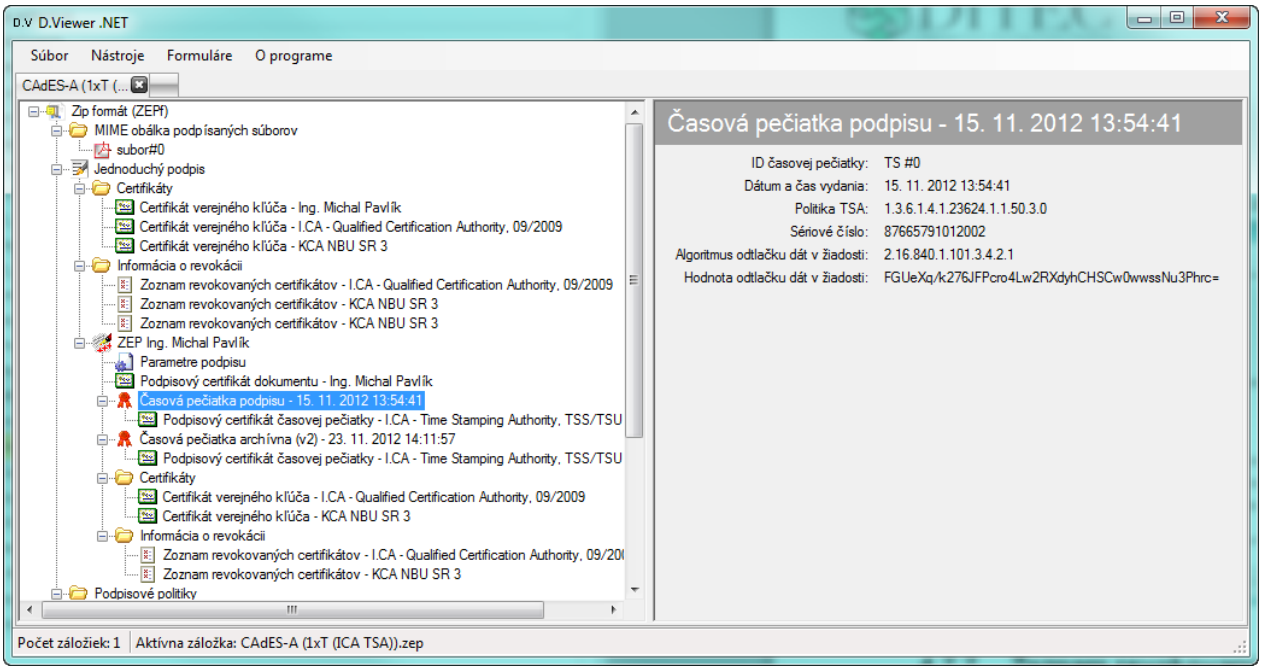
- Časová pečiatka podpisu
- Časová pečiatka archívna

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

Na obrázku 4.7.6.1 je uvedený príklad zobrazenia detailu časovej pečiatky.



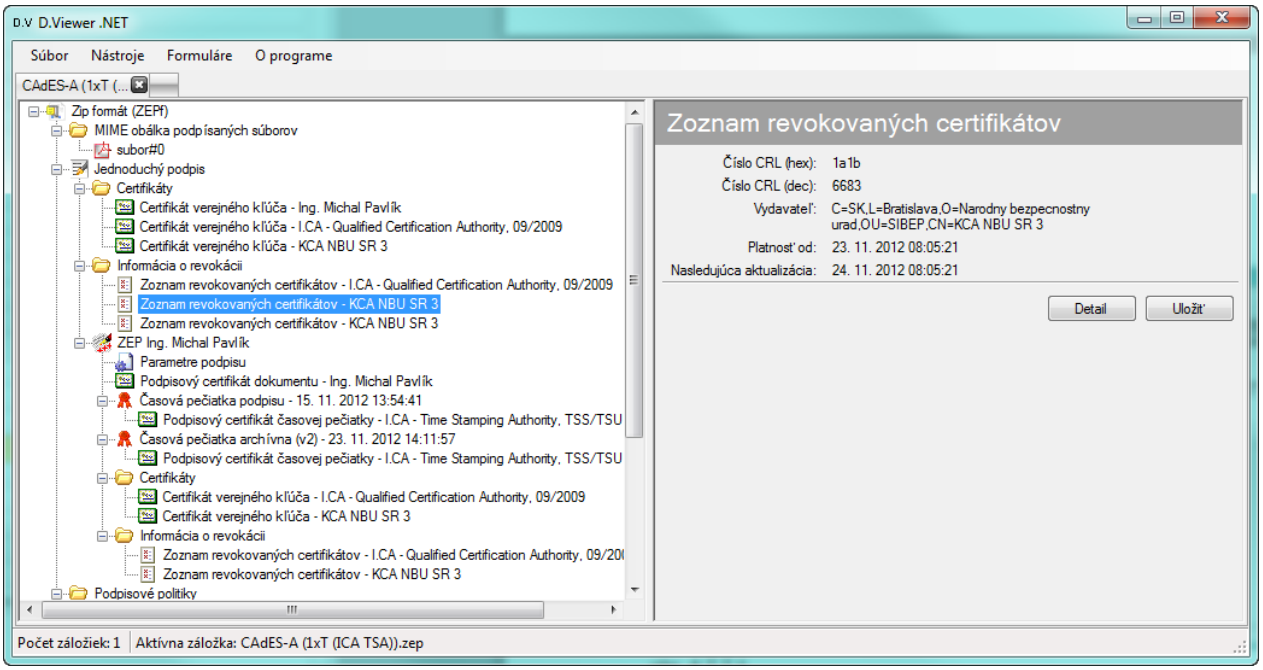
obr. 4.7.6.1

4.7.7. Zoznam revokovaných certifikátov

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

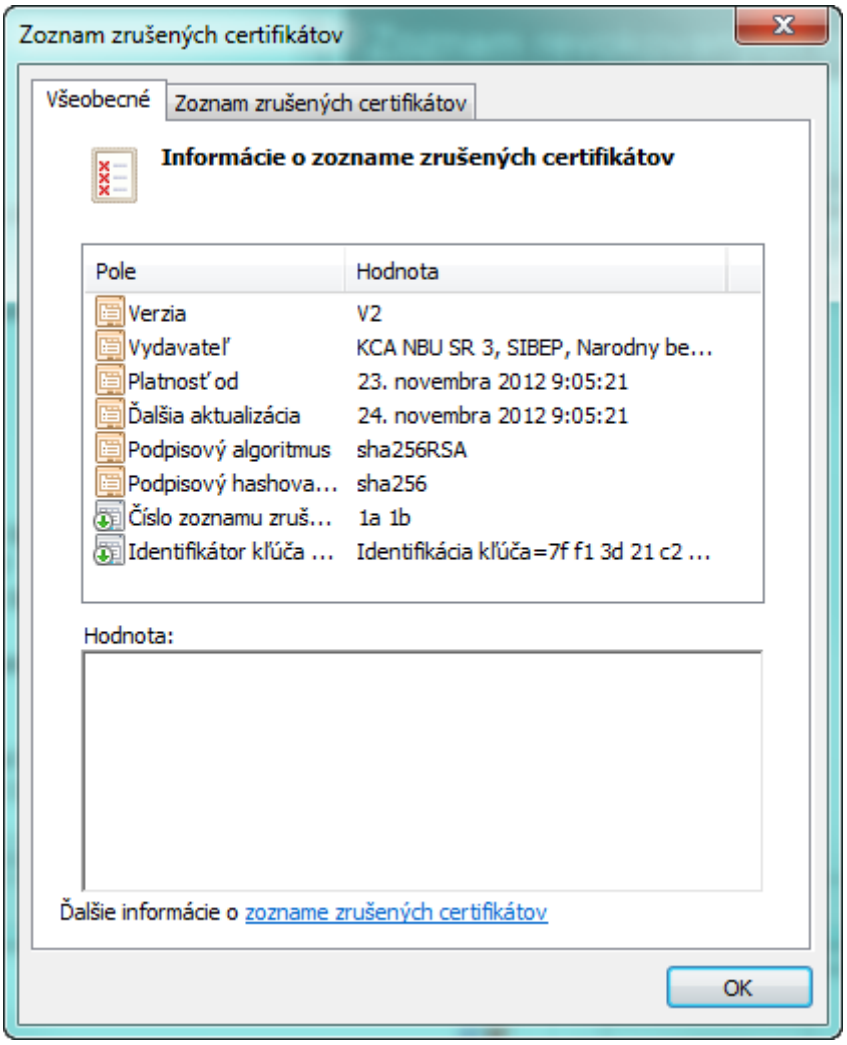
- Číslo CRL (hex)
- Číslo CRL (dec)
- Vydavateľ
- Platnosť od
- Nasledujúca aktualizácia

Na obrázku 4.7.7.1 je uvedený príklad zobrazenia detailu zoznamu revokovaných certifikátov (CRL).



obr. 4.7.7.1

Kliknutím na tlačidlo Detail sa v štandardnom okne operačného systému zobrazí detail CRL (obr. 4.7.7.2). Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie CRL v rámci operačného systému používateľa.



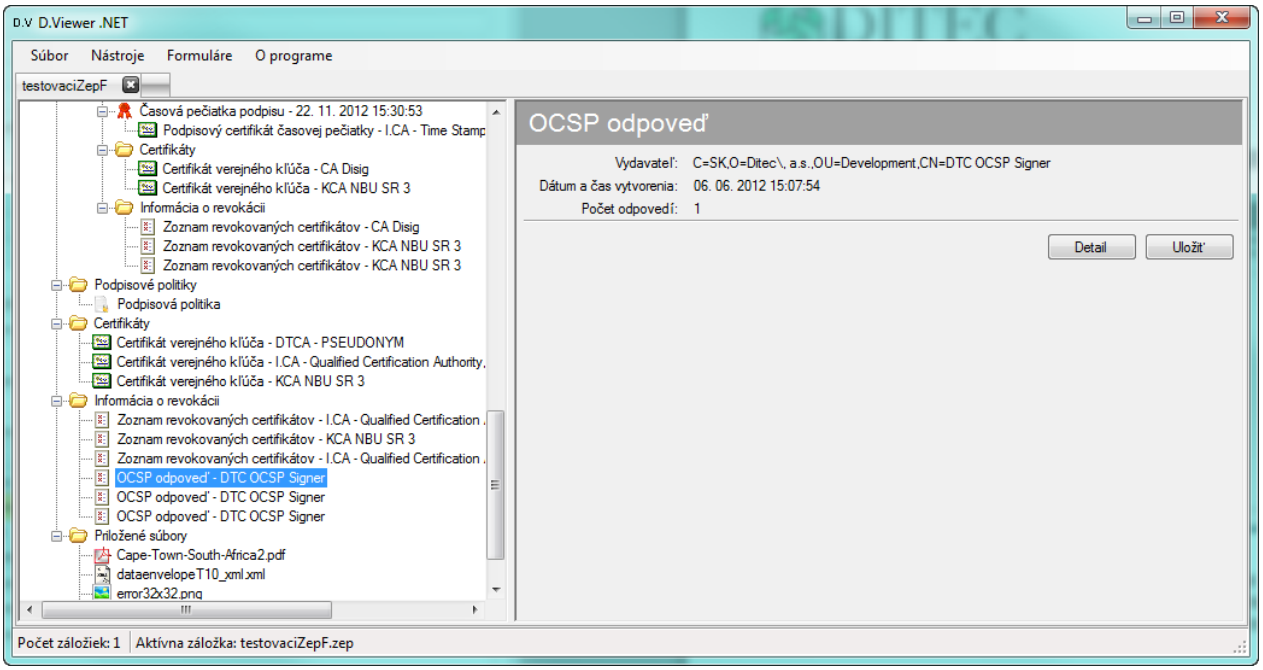
obr. 4.7.7.2

4.7.8. OCSP odpoveď

Pri zobrazení detailu OCSP odpovede sa zobrazujú atribúty:

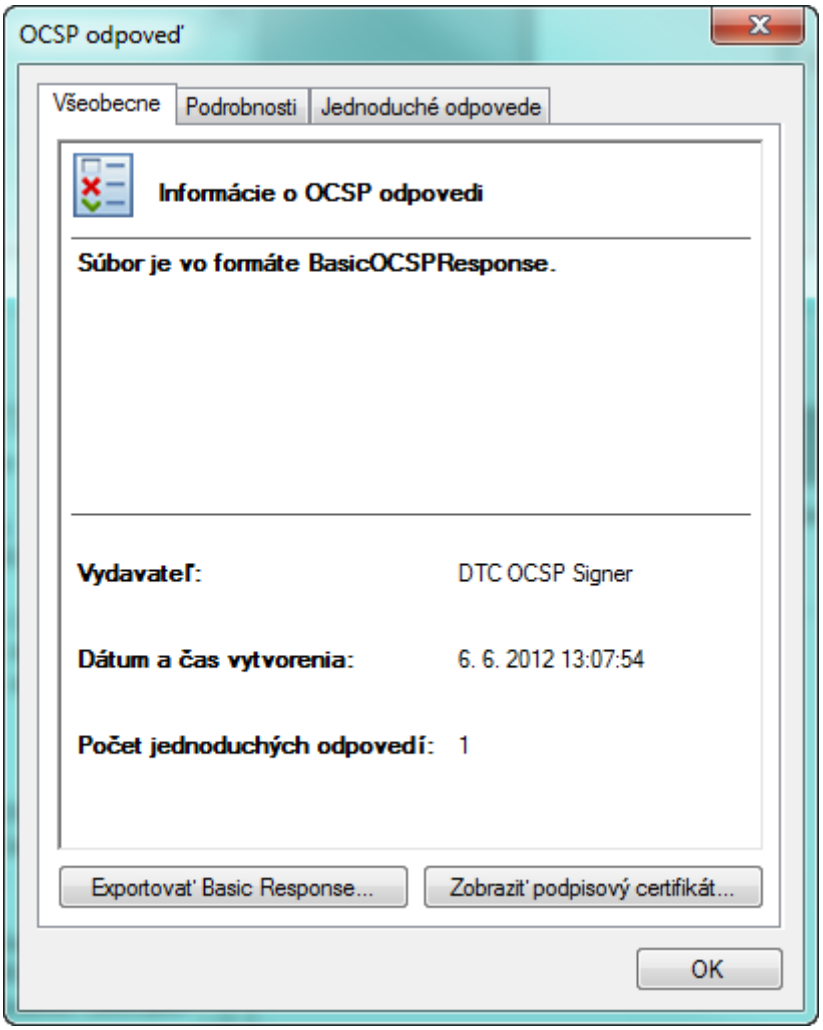
- Vydavateľ
- Dátum a čas vytvorenia
- Počet odpovedí

Na obrázku 4.7.8.1 je uvedený príklad zobrazenia detailu OCSP odpovede.



obr. 4.7.8.1

Kliknutím na tlačidlo Detail sa v modálnom okne zobrazí detail OCSP odpovede (obr. 4.7.7.2). Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie OCSP odpovede v rámci operačného systému používateľa.



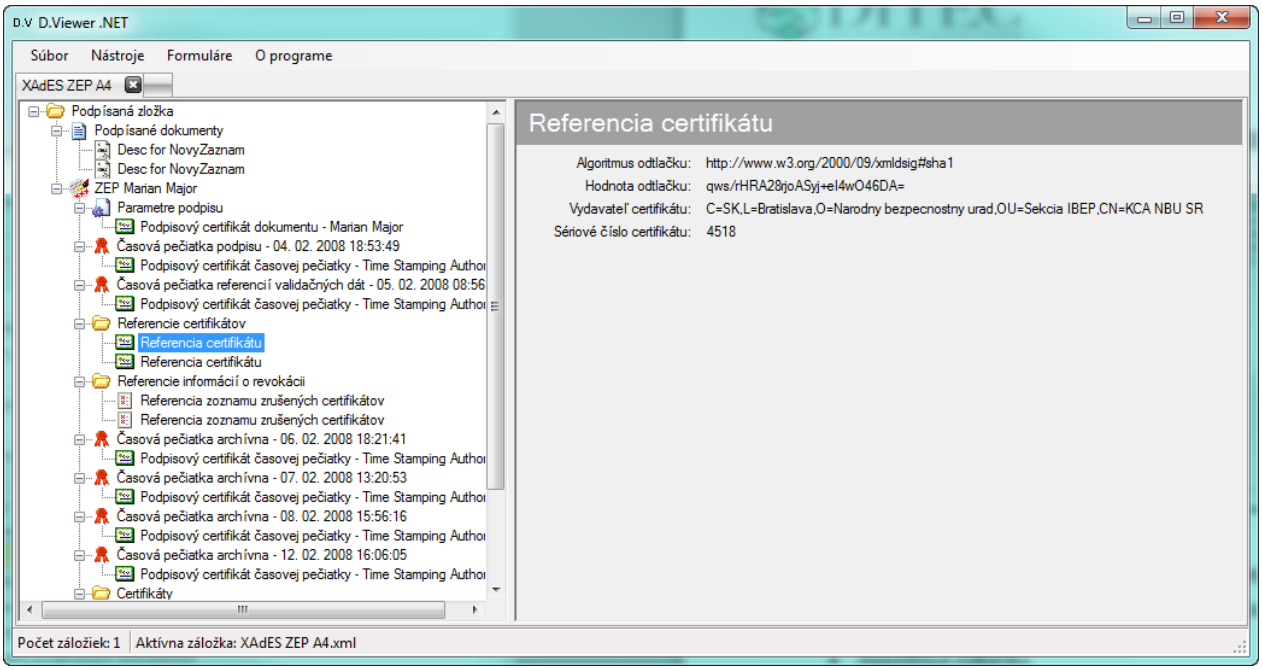
obr. 4.7.8.2

4.7.9. Referencia certifikátu

Pri zobrazení detailu referencie certifikátu sa zobrazujú atribúty:

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

Na obrázku 4.7.9.1 je uvedený príklad zobrazenia detailu referencie certifikátu.



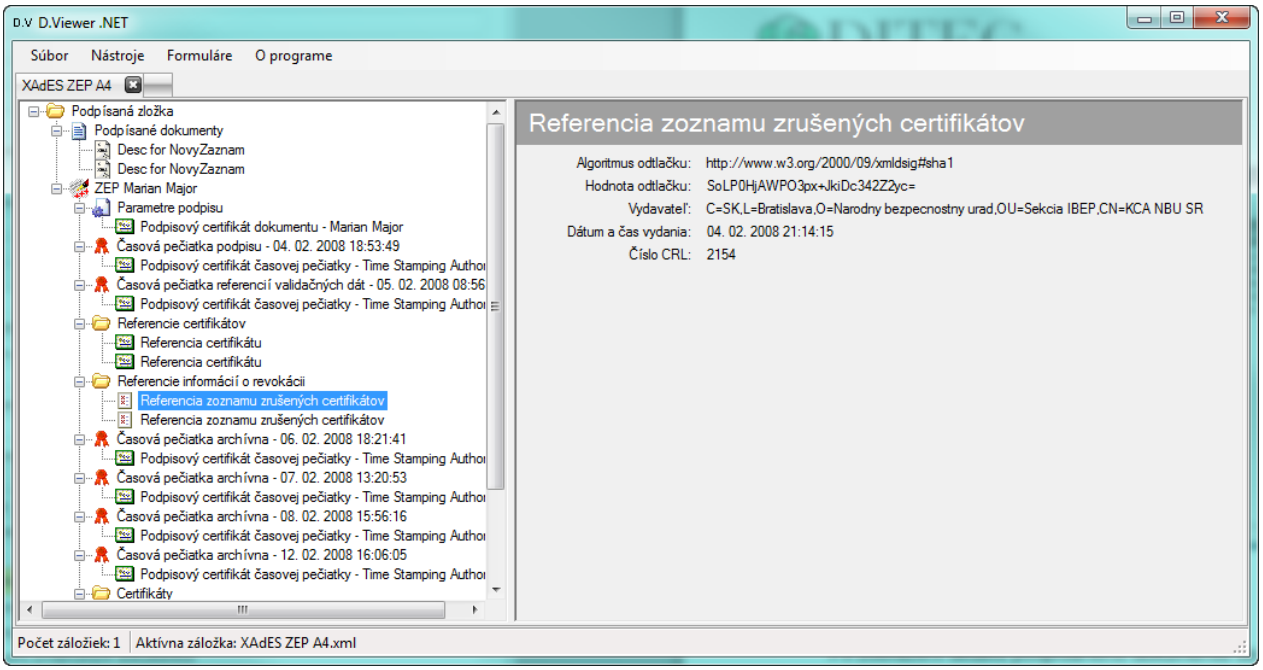
obr. 4.7.9.1

4.7.10. 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

Na obrázku 4.7.10.1 je uvedený príklad zobrazenia detailu referencie zoznamu revokovaných certifikátov (CRL).



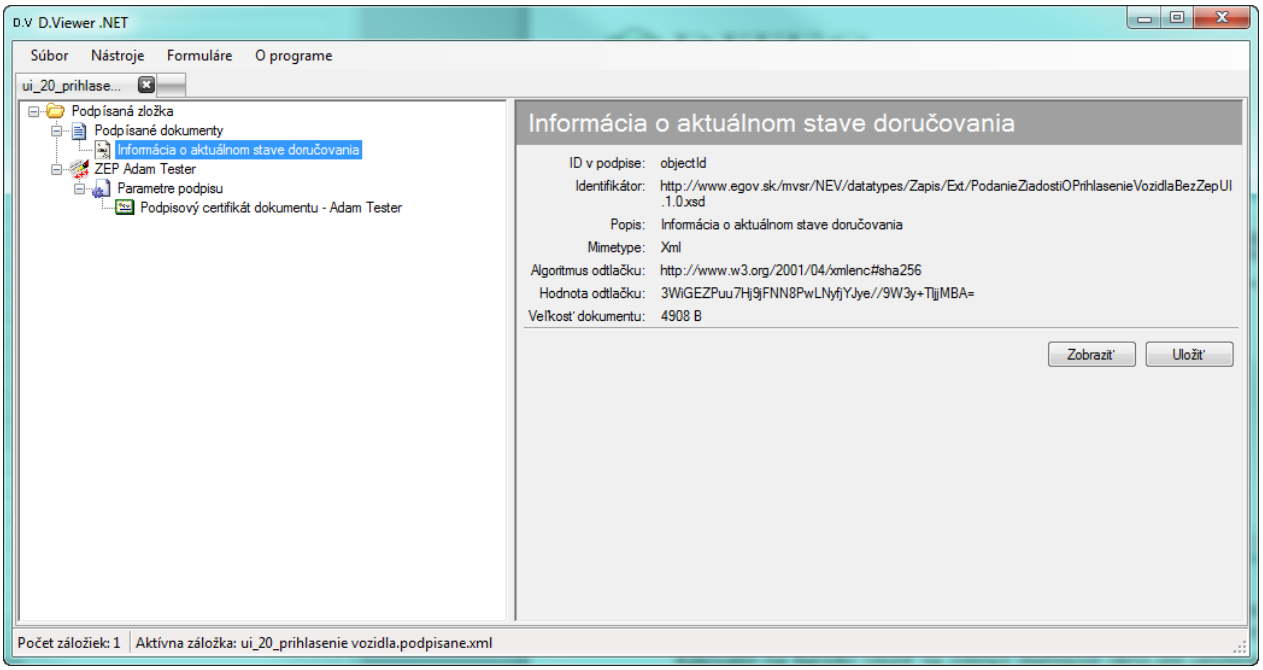
obr. 4.7.10.1

4.7.11. Podpísané dokumenty

Pri zobrazení detailu podpísaného dokumentu sa zobrazujú atribúty:

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

Na obrázku 4.7.11.1 je uvedený príklad zobrazenia detailu podpísaného XML dokumentu.



obr. 4.7.11.1

Kliknutím na tlačidlo Zobraziť sa vizualizuje obsah podpísaného dokumentu (pozri kapitola 4.7.11.1 Vizualizácia obsahu podpísaných dokumentov).

Kliknutím na tlačidlo Uložiť sa zobrazí dialógové okno pre uloženie dokumentu v rámci operačného systému používateľa.

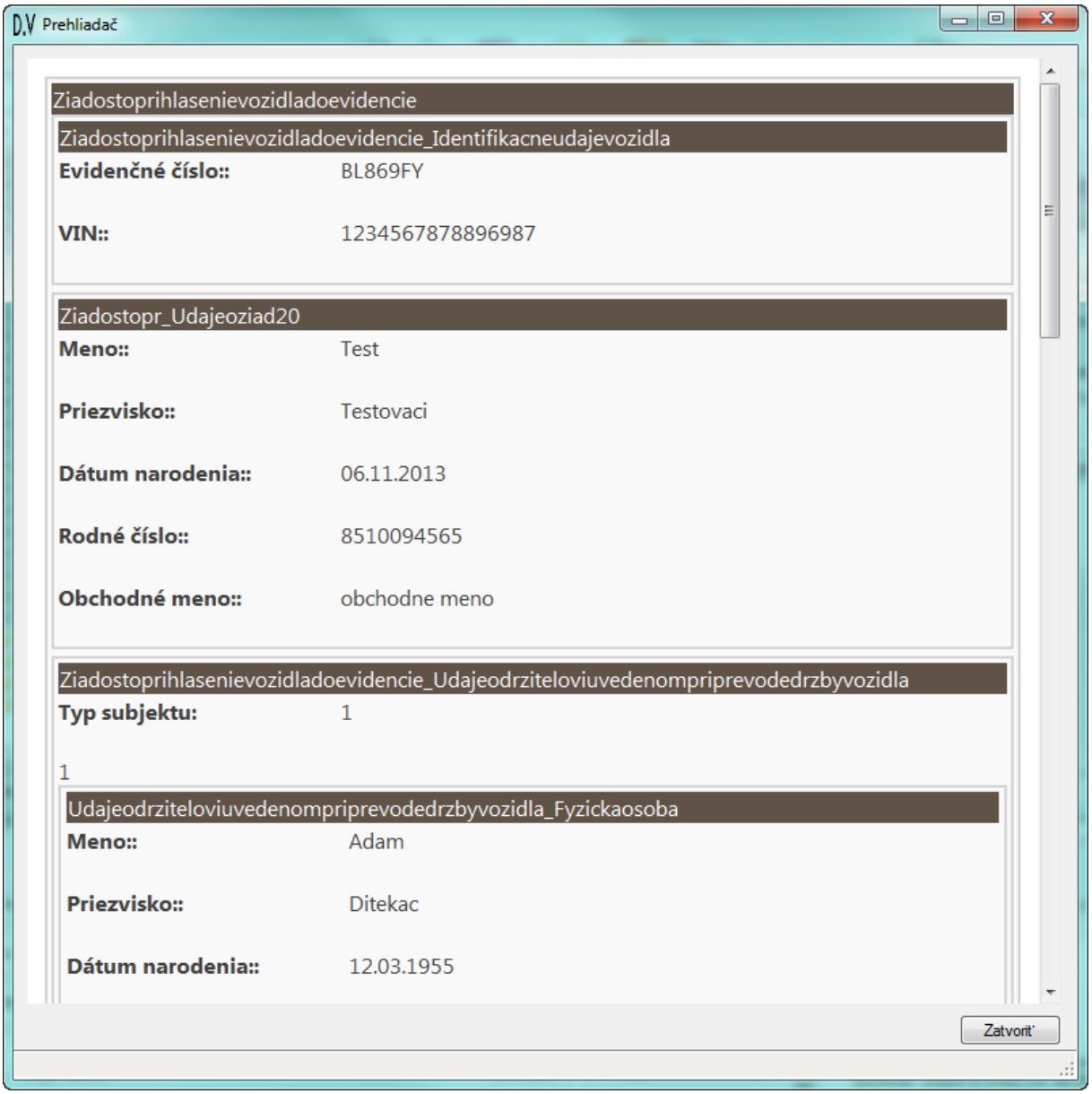
4.7.11.1. Vizualizácia obsahu podpísaných dokumentov

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

Dátove objekty XML alebo FO formuláre sa zobrazujú podľa nasledovných pravidiel:

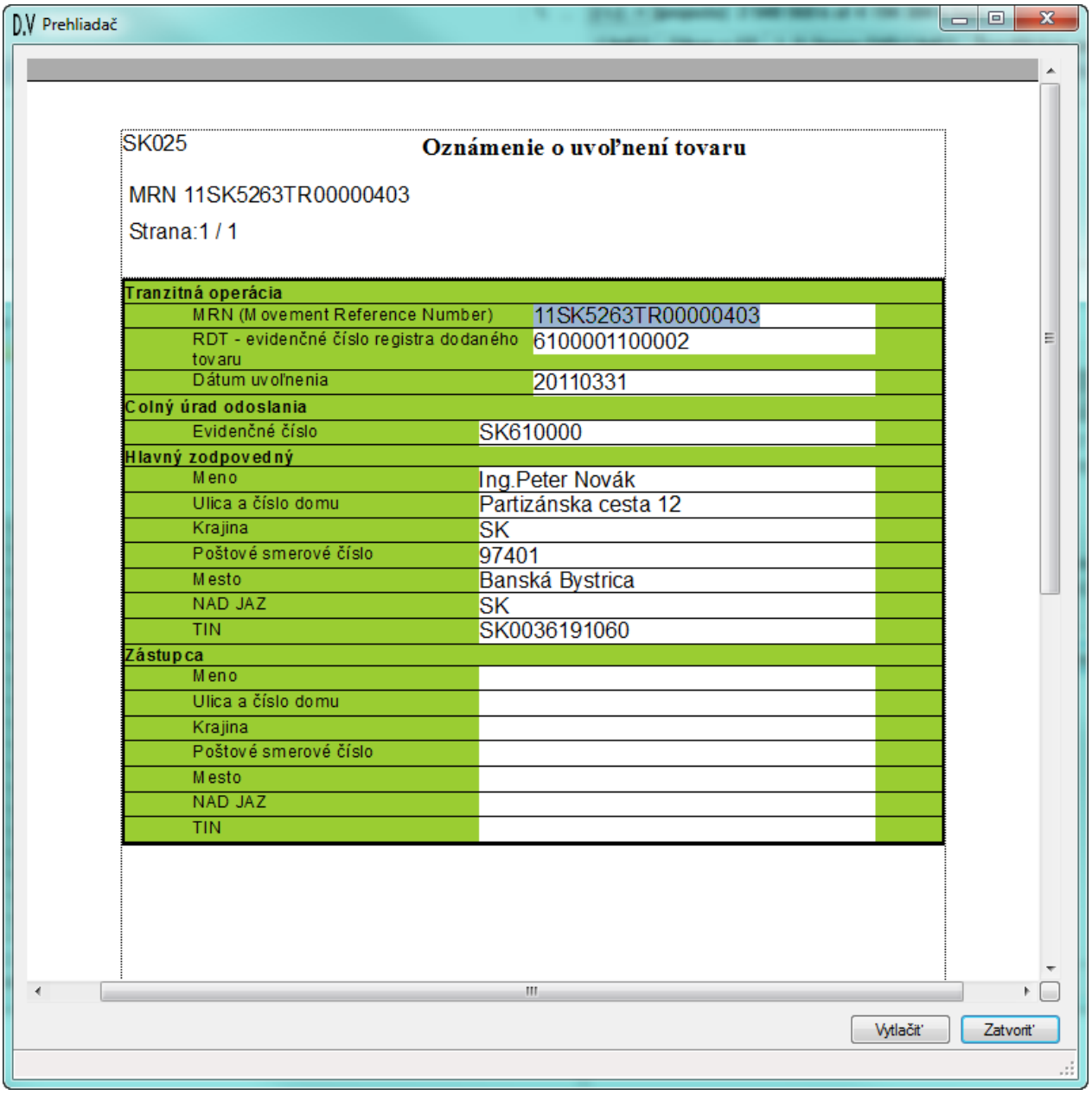
- ak podľa konfigurácie D.Viewera existuje FO vizualizácia pre dané XML a používateľ má nainštalovanú aplikáciu FormFiller (http://www.602.cz/produkty/form_filler/download), tak sa XML zobrazí pomocou FormFillera a FO vizualizácie, inak sa XML zobrazí v asociovanej aplikácii
- ak podľa konfigurácie D.Viewera existuje TXT/HTML vizualizácia pre dané XML, tak sa XML zobrazí v textovej forme po transformácii cez XSLT, inak sa XML zobrazí v asociovanej aplikácii

Na obrázku 4.7.11.1.1 je uvedený príklad vizualizácie podpísaného XML dokumentu do HTML.



obr. 4.7.11.1.1

Na obrázku 4.7.11.1.2 je uvedený príklad vizualizácie podpísaného XML dokumentu pomocou FormFillera a FO vizualizácie.


D.V Prehliadač
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
Vytlačiť
Zatvoriť

obr. 4.7.11.1.2

5. Podpora pre nevidiacich pomocou NVDA

Aplikácia D.Viewer 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/).

5.1. Systémové požiadavky pre NVDA

- 32 aj 64 bitové verzie systémov Windows XP, Vista, 7, 8
- minimálne 256 MB operačnej pamäte
- výkonnosť procesora minimálne 1 GHZ
- 50 MB voľného miesta na disku

pozn: Uvádzame systémové požiadavky pre NVDA, ktoré boli aktuálne v čase písania používateľskej príručky.