DITEC
Data Information Technology & Expert Consulting

Integračná príručka
D.Signer/XAdES .NET - XML Plugin, v3.0

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Integračná príručka		
Podnázov	D.Signer/XAdES .NET - XML Plugin, v3.0		
Ref. číslo	GOV_ZEP.155	Verzia	3

Vypracoval	Vittek Róbert	Podpis	Dátum 13.6.2014
Preveril		Podpis	Dátum
Schválil		Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 14.10.2005

Akceptované dňa : <Dátum akceptácie>

Za <Objednávateľa>: Za <Dodávateľa>.:

<Meno zodpovednej osoby> < Meno zodpovednej osoby >

Projekt	GOV_ZEP		A3019_002
Dokument	Integračná príručka		
Referencia	GOV_ZEP.155	Verzia	3

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

Tento dokument popisuje funkcionalitu a integračné API komponentu D.Signer/XAdES .NET – XML Plugin a tvorí prílohu Integračnej príručky aplikácie D.Signer/XAdES .NET.

Aplikácia D.Signer/XAdES .NET predstavuje riešenie pre vytváranie zaručeného elektronického podpisu (ZEP) vo formáte XAdES_ZEP nad množinou rôznych formátov dokumentov, resp. typov dát (XML dokumenty, PDF dokumenty atď.), prípadne nad ľubovoľnou kombináciou podporovaných formátov dát, ktoré spolu vytvárajú tzv. *multipart* dokument. Funkcionalita SCA je v rámci aplikácie D.Signer/XAdES .NET rozdelená do samostatných modulov, ktoré je možné pri nasadení aplikácie kombinovať podľa požiadaviek zákazníka. Aplikáciu D.Signer/XAdES .NET tvorí sada knižníc, ktoré poskytujú pre klientské aplikácie nasledujúce integračné rozhrania:

- .Net API – pre .Net aplikácie,
- COM API – wrapper nad .Net API pre iné ako .Net aplikácie,
- COM API (prostredníctvom ATL knižnice) – wrapper nad COM API (primárne pre Internet Explorer)
- NP API – wrapper pre volanie služieb komponentu D.Signer/XAdES .NET z prehliadačov s podporou NPAPI rozhrania (je odvodené z .Net API komponentu D.Signer/XAdES .NET a jeho pluginov).

Aby bolo možné postupne budovať podporu pre ďalšie typy dátových objektov, medzi hlavným modulom D.Signer/XAdES .NET a pluginmi bolo takisto navrhnuté abstraktné API, ktoré musí každý plugin implementovať. Hlavný modul komunikuje s jednotlivými pluginmi prostredníctvom tohto rozhrania. Architektúra aplikácie D.Signer/XAdES .NET je podrobne popísaná v Integračnej príručke D.Signer/XAdES .NET.

Každý plugin aplikácie D.Signer/XAdES .NET musí pre typ dátového objektu, pre ktorý je určený, definovať triedu, ktorá predstavuje integračné API pluginu. Všeobecné požiadavky na integračné API pluginov, ktoré vyplývajú z architektúry aplikácie D.Signer/XAdES .NET, sú definované v Integračnej príručke D.Signer/XAdES .NET. Trieda integračného API pluginu môže navyše poskytovať svojmu okoliu ďalšie metódy a atribúty, ktoré sú špecifické pre príslušný typ podporovaného dátového objektu.

2. Zoznam použitých skratiek

DHC – Data Hashing Component

DTBS – Data To Be Signed

DTBSF – Data To Be Signed Formatted, resp. komponent Data To Be Signed Formatter

DTBSR – Data To Be Signed Representation

NBÚ – Národný bezpečnostný úrad

SAC – Signer's Authentication Component

SCA – Signature Creation Application

SCDev – Signature Creating Device

SCVA – Signature Creation and Validation Application

SDOC – Signed Data Object Composer

SDP – Signer's Document Presentation

SIC – Signer Interaction Component

SLC – Signature Logging Component

SSA – SCDev/SCA Authenticator

SSC – SCDev/SCA Communicator

SSCD – Secure Signature Creating Device

SVA – Signature Validation Application

XML – eXtended Markup Language

XSD – XML Schema Definition

XSL – eXtensible Stylesheet Language

XSLT – XSL Transformation

XAdES – XML Advanced Electronic Signatures

XAdES_ZEP – profil špecifikácie formátu elektronického podpisu XAdES pre ZEP

ZEP – Zaručený elektronický podpis

3. Referencie

[1] W3C/IETF Recommendation: "XML-Signature Syntax and Processing" v2002-02-12 (XMLDSIG)

[2] ETSI TS 101 733 – CMS Advanced Electronic Signatures (CAdES) v1.6.3

[3] ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES) v1.4.2

[4] RFC 3125 – Electronic Signature Policies

[5] RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol

[6] RFC 3279 – Algorithms and Identifiers for the Internet X.509 PKI

[7] RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[8] RFC 3548 – The Base16, Base32, and Base64 Data Encodings

[9] RFC 3852 – Cryptographic Message Syntax (CMS)

[10] RFC 4051 – Additional XML Security Uniform Resource Identifiers

[11] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

[12] Vyhláška NBÚ č. 131/2009 Z.z. o certifikátoch a kvalifikovaných certifikátoch

[13] Vyhláška NBÚ č. 134/2009 Z.z. o produktoch elektronického podpisu

[14] Vyhláška NBÚ č. 135/2009 Z.z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky

[15] Vyhláška NBÚ č. 136/2009 Z.z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku

[16] NBÚ Formáty certifikátov a kvalifikovaných certifikátov, v3.0 (2009-06-30)

[17] NBÚ Formáty zoznamu zrušených kvalifikovaných certifikátov, v1.2 (2005-11-06)

[18] NBÚ Formáty zaručených elektronických podpisov, v3.0 (2009-08-12)

[19] NBÚ Upresnenia obsahu a formálne špecifikácie formátov dokumentov pre ZEP, v1.0 (2007-07-24)

[20] CWA 14170:2004 E – Security requirements for signature creation applications

[21] CWA 14171:2004 D/E/F – General guidelines for electronic signature verification

[22] XMLENC – XML Encryption Syntax and Processing", J. Reagle, D. Eastlake, December 2002. http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[23] Koncepcia všeobecného formátu XML podpisu a aplikácie SCVA, DITEC, a.s., 2006

[24] Profil XAdES_ZEP – formát ZEP na báze XAdES, v1.0, DITEC, a.s., 2008

[25] Profil XAdES_ZEP – formát ZEP na báze XAdES, v1.1, DITEC, a.s., 2009

[26] Profil XAdES_ZEP – formát ZEP na báze XAdES, v2.0, DITEC, a.s., 2011

[27] Formát dátových objektov typu XML dokument v rámci profilu XAdES_ZEP, v1.0, DITEC, a.s., 2013

[28] Formát dátových objektov typu XML dokument v rámci profilu XAdES_ZEP, v2.0, DITEC, a.s., 2013

[29] Integračná príručka D.Signer-XAdES .NET, v3.0, DITEC, a.s., 2014

[30] Rozhodnutie komisie 2011/130/EU, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu

[31] ETSI TS 103 171 – Electronic Signatures and Infrastructures (ESI) XAdES Baseline Profile, v2.1.1

[32] Extensible Markup Language (XML) 1.0 (Fifth Edition) – http://www.w3.org/TR/2008/REC-xml-20081126/

[33] Výnos MF SR č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy

[34] Požiadavky na prezentácie XML dokumentov pre podpisovanie, DITEC, a.s., 2014

4. Formát XML

Formát XML v súčasnosti predstavuje rozšírený a podporovaný štandard pre elektronickú komunikáciu a výmenu dát medzi rôznymi systémami v heterogénnych prostrediach, pričom umožňuje jednoznačnú definíciu štruktúry, jednoznačnú interpretáciu obsiahnutých údajov, ako aj ich jednoduché automatické spracovanie. Formát XML má navyše oporu v legislatíve ako jeden z dátových formátov, nad ktorými je možné vytvárať zaručený elektronický podpis (ZEP) [15].

Jednou z výhod XML formátu elektronického dokumentu je možnosť vyjadrenia štruktúry a definovania údajových typov (jednoduchých aj komplexných) pomocou XML schémy (XSD – http://www.w3.org/XML/Schema/).

Na základe definovanej XML schémy je možné automaticky overovať správnosť štruktúry dokumentu. Správna štruktúra XML dokumentu je základnou požiadavkou pre akceptovanie podpisovaného dokumentu príjemcom. Správnosť dokumentu umožňuje jeho ďalšie automatizované spracovanie (záruka správnosti štruktúry a typu obsahu) a tiež korektnú vizualizáciu obsahu dokumentu. Preto je vhodné požadovať overenie správnosti štruktúry dokumentu pred samotným podpisom.

Zodpovednosť za vydávanie a zverejňovanie aktuálnych XML schém je na správcovi príslušného komunikačného scenára, v rámci ktorého sa požaduje spracovanie XML dokumentov podpísaných zaručeným elektronickým podpisom. Zodpovednosť za použitie dôveryhodnej a správnej XML schémy je na podpisovateľovi príslušného XML dokumentu.

Z týchto dôvodov je potrebné podpisovaný XML dokument opatriť doplňujúcou podpísanou informáciou, ktorá deklaruje XML schému použitú pre overenie správnosti štruktúry podpisovaného XML dokumentu pred samotným vytvorením elektronického podpisu.

Overovateľ elektronického podpisu musí overiť použitie správnej XML schémy pre overenie správnosti štruktúry podpísaného XML dokumentu.

Zákon č. 215/2002 Z.z. [11] definuje požiadavku zobrazenia (vizualizácie) podpisovaného elektronického dokumentu podpisovateľovi ešte predtým, ako sa spustí procedúra na vyhotovenie zaručeného elektronického podpisu. XML dokument obsahuje štruktúrované dáta, ktoré sú vo väčšine prípadov pre bežného používateľa nečitateľné, preto je vhodné realizovať samotné zobrazenie XML dokumentu podpisovateľovi pomocou transformácie XML dokumentu do čitateľnej formy. Príloha č. 3 Výnosu MF SR o štandardoch pre informačné systémy verejnej správy [33] požaduje, aby povinnou prezentáciou pre podpisovanie a pre iný spôsob autorizácie elektronického formulára (ďalej len „podpisová prezentácia“) bol formát HTML, XHTML alebo PDF minimálne vo verzii 1.3 a maximálne vo verzii 1.5, a ak sa jedná o elektronické formuláre s viac ako päťdesiatimi procesnými krokmi, prezentáciou pre podpisovanie môže byť aj

formát Text Format (.txt) v kódovaní UTF-8, pričom môžu existovať aj ďalšie podpisové prezentácie v iných formátoch. V prezentačnej schéme sa pre transformáciu dátových prvkov do prezentácie vo formátoch HTML, XHTML, TXT alebo PDF používa jazyk XSL Transformations 1.0 (XSLT) a na opis formátovania prezentácie vo formáte PDF sa používa značkovací jazyk Extensible Stylesheet Language - Formatting Objects (XSL-FO) vo verzii 1.0 podľa World Wide Web Consortium (W3C).

Na vyjadrenie ľubovoľnej transformácie XML dokumentu existuje štandard pre XML transformácie (XSLT – http://www.w3.org/TR/xslt/), pomocou ktorého možno definovať pravidlá pre transformáciu XML dokumentu do požadovaného formátu. Možnosti XSLT sú pomerne rozsiahle, preto pravidlá transformácie podpisovaného XML dokumentu musia byť definované tak, aby zaručili zobrazenie úplného obsahu XML dokumentu v zrozumiteľnej forme.

Najjednoduchšou alternatívou pre zobrazenie obsahu XML dokumentu (vzhľadom na technickú realizovateľnosť, aj vzhľadom na dostatočnú vypovedaciu schopnosť) je jednoduchý textový formát (Plain Text). Vizualizácia do TXT umožňuje zároveň realizovať vizualizáciu aj extrémne veľkých XML dokumentov (rádovo desaťtisíce strán), pri ktorých by vizualizácia do HTML, XHTML alebo PDF mohla byť v súčasnosti technicky problematická kvôli pamäťovým nárokom.

Vizualizácia do HTML (XHTML) na druhej strane poskytuje oveľa väčšie možnosti formátovania XML dokumentu a priblíženie sa vzhľadu pôvodného formuláru. Pri vizualizácii do HTML je však potrebné zvážiť použitie takých HTML prvkov, ktoré môžu spôsobiť odchýlky v zobrazení výslednej HTML prezentácie XML dokumentu v rôznych prehliadačoch. Takisto je potrebné riešiť možnosť použitia aktívneho kódu vo výslednej HTML prezentácii (javascript, applety), ako aj referencovanie externého obsahu (CSS štýly, obrázky), ktorý nie je súčasťou podpisovaných dát a ktorého zmena môže významne ovplyvniť HTML prezentáciu XML dokumentu podpisovateľovi.

Vizualizácia XML dokumentu do formátu PDF sa realizuje prostredníctvom štandardov XSLT (http://www.w3.org/TR/xslt) a XSL-FO vo verzii 1.0 (http://www.w3.org/TR/2001/REC-xsl-20011015/). Vizualizáciu do formátu PDF je možné využiť, ak je už napríklad definovaná pre daný typ XML dokumentov pre účely tlače, kvalitatívne však oproti vizualizácii do HTML nič nové neprináša. Rovnako, ako pri vizualizácii do HTML, je aj tu potrebné riešiť možnosť použitia aktívneho kódu vo výslednej PDF prezentácii (javascript), ako aj referencovanie externého obsahu (fonty, externé linky), ktorý nie je súčasťou podpisovaných dát a ktorého zmena môže významne ovplyvniť PDF prezentáciu XML dokumentu podpisovateľovi. Vizualizácia XML dokumentu do formátu PDF nie je v rámci XML Pluginu pre aplikáciu D.Signer/XAdES .NET podporovaná.

Požiadavky na prezentácie XML dokumentov pre podpisovanie sú mimo rámca tejto špecifikácie a sú definované v samostatnom dokumente [34]. Základom pre úplné a správne zobrazenie dokumentu pred podpisovaním je validácia XML dokumentu vzhľadom na XML schému.

Zodpovednosť za vydávanie a zverejňovanie aktuálnych, úplných a správnych transformačných schém na prezentáciu XML dokumentov pre podpisovanie je na správcovi komunikačného scenára, v rámci ktorého sa požaduje spracovanie XML dokumentov podpísaných zaručeným elektronickým podpisom. Zodpovednosť za použitie dôveryhodnej a správnej prezentácie XML pre podpisovanie je na podpisovateľovi príslušného XML dokumentu.

Podpisovaný XML dokument je teda potrebné opatriť tiež doplňujúcou podpísanou informáciou, ktorá deklaruje XML prezentáciu použitú pre zobrazenie obsahu podpisovaného XML dokumentu pred samotným vytvorením elektronického podpisu.

Overovateľ elektronického podpisu musí overiť použitie správnej XML prezentácie pre zobrazenie obsahu podpísaného XML dokumentu.

5. Architektúra XML Pluginu

V rámci tejto kapitoly je popísaná architektúra XML Pluginu pre aplikáciu D.Signer/XAdES .NET, ktorá vychádza z dokumentov:

- Koncepcia všeobecného formátu XML podpisu a aplikácie SCVA [23]
- CWA14170:2004 E – Security requirements for signature creation applications [20].

5.1. Postavenie komponentu v rámci prevádzkového prostredia a aplikácie D.Signer/XAdES .NET

XML Plugin pre aplikáciu D.Signer/XAdES .NET je realizovaný ako samostatný komponent, ktorý môže byť nasadený ako súčasť aplikácie D.Signer/XAdES .NET v rámci rozsiahlejších systémov, napr. pre elektronickú výmenu dokumentov medzi rôznymi subjektami, v rámci ktorých je potrebné zabezpečiť:

- jednoznačnú identifikáciu pôvodcu dokumentu a neodmietnuteľnosť autorstva,
- integritu (prenášaných) dokumentov.

V rámci aplikácie D.Signer/XAdES .NET zabezpečuje XML Plugin činnosti potrebné pre spracovanie a vizualizáciu dát typu XML dokument pred spustením procedúry vytvorenia ZEP a vytvorenie príslušných XML štruktúr pre formát podpisu v súlade s profilom XAdES_ZEP.

Komponent XML Plugin poskytuje pre klientské aplikácie nasledujúce integračné rozhrania – API:

- .Net API – umožňuje volanie funkcií komponentu priamo z .Net prostredia,
- COM API – wrapper nad .Net API, ktorý umožňuje volanie funkcií komponentu z iných prostredí (kontainerov),
- ATL COM API – wrapper nad COM API (primárne pre Internet Explorer).

Pre interakciu s podpisovateľom poskytuje komponent XML Plugin GUI rozhranie, v rámci ktorého je realizované:

- zobrazenie obsahu podpisovaných XML dokumentov,
- zobrazenie obsahu verifikačných údajov pre podpisované XML dokumenty (XML schéma, XSL transformácia),
- zobrazenie ostatných relevantných parametrov ZEP (napr. použité algoritmy pre digitálne odtlačky a ich hodnoty)

pred spustením procedúry vytvorenia ZEP.

Komponent XML Plugin zároveň poskytuje implementáciu abstraktného API rozhrania pre integráciu s aplikáciou D.Signer/XAdES .NET, ktoré je definované v rámci dokumentu Integračná príručka D.Signer/XAdES .NET.

Komponent XML Plugin nevykonáva kryptografické operácie ani nekomunikuje s SSCD zariadením. Pre tento účel volá funkcie rozhrania samostatnej knižnice, ktorá takisto tvorí súčasť aplikácie D.Signer/XAdES .NET.

5.2. Funkčná dekompozícia komponentu

Vnútorná architektúra komponentu XML Plugin pre D.Signer/XAdES .NET vychádza a je v súlade s funkčným komponentovým modelom dokumentu CWA14170:2004 E – Security requirements for signature creation applications [20].

Z pohľadu funkčného komponentového modelu SCA sú v rámci komponentu XML Plugin pre D.Signer/XAdES .NET implementované nasledujúce dôveryhodné komponenty:

- SDP – Signer's Document Presentation Component – zabezpečuje zobrazenie podpisovaných XML dokumentov podpisovateľovi, kontrolu výslednej vizualizácie XML dokumentov na nepovolený obsah,
- SAV – Signature Attributes Viewer – zabezpečuje zobrazenie príslušných verifikačných údajov pre XML dokument a ďalších atribútov vytváraného ZEP podpisovateľovi,
- DTBSF – Data To Be Signed Formatter – zabezpečuje sformátovanie a tranformáciu vstupných XML dokumentov a ďalších parametrov podpisu do kanonickej formy a vytvorenie štruktúry DTBSF,
- SIC – Signer Interaction Component – GUI rozhranie pre vizualizáciu XML dokumentov, príslušných verifikačných údajov a ďalších atribútov ZEP a pre interakciu medzi podpisovateľom a aplikáciou D.Signer/XAdES .NET.

XML Plugin pre D.Signer/XAdES .NET obsahuje nasledujúce aplikačne závislé komponenty všeobecnej architektúry SCA:

- SDOC – Signed Data Object Composer – modul pre vytvorenie príslušných XML fragmentov výsledného ZEP vo formáte XAdES_ZEP zo vstupných XML dokumentov a ďalších vstupných parametrov.

Obrázok funkčnej dekompozície aplikácie D.Signer/XAdES .NET na jednotlivé komponenty SCA ako aj pohľad na jednotlivé vrstvy architektúry sa nachádza v dokumente Integračná príručka D.Signer/XAdES .NET [29], kapitola 6.2.

6. Špecifikácia funkčnosti

6.1. Popis činnosti

Komponent XML Plugin pre aplikáciu D.Signer/XAdES .NET zabezpečuje nasledujúce činnosti:

- vytvorenie dátového objektu typu XML dokument pre aplikáciu D.Signer/XAdES .NET pre .Net aplikácie pomocou .Net API, resp. pre iné ako .Net aplikácie pomocou COM alebo COM ATL API,
- spracovanie vstupných dátových objektov typu XML dokument, validáciu voči XML schéme a aplikovanie príslušných transformácií pre vytyvorenie DTBSF (kanonikalizácia, XSLT),
- vizualizácia XML dokumentu, príslušných verifikačných údajov (XML schémy a XSL transformácie) a ďalších atribútov vytváraného ZEP podpisovateľovi v plain text formáte alebo HTML/XHTML,
- podľa typu výslednej vizualizácie zároveň vykoná validáciu výslednej vizualizácie XML dokumentu nasledovne:
  - ⇒ vizualizácia do plain text (TXT) – kontrola na nepovolené znaky (viď povolené znaky pre entitu Char – http://www.w3.org/TR/2008/REC-xml-20081126/#charsets [32]),
  - ⇒ vizualizácia do HTML – kontrola nepovolených HTML tagov: applet, script, iframe, link, object.
- v prípade, že výsledná vizualizácia obsahuje nepovolený obsah, tak sa XML dokument nezobrazí a aplikácia vypíše upozornenie,
- vytvorenie príslušných fragmentov výslednej štruktúry ZEP podľa profilu XAdES_ZEP a prílohy Formát dátových objektov typu XML dokument a ich poskytnutie aplikácii D.Signer/XAdES .NET.

Popis činnosti komponentu v rámci aplikácie D.Signer/XAdES .NET je špecifikovaný v rámci dokumentu Integračná príručka D.Signer/XAdES .NET [29], kapitola 7.

7. Špecifikácia API

Komponent XML Plugin pre D.Signer/XAdES .NET tvorí DLL knižnica, ktorá pre klientské aplikácie poskytuje nasledujúce integračné rozhrania:

- .Net API – pre .Net aplikácie,
- COM API – wrapper nad .Net API pre iné ako .Net aplikácie,
- COM API (prostredníctvom ATL knižnice) – wrapper nad COM API (primárne pre Internet Explorer).

XML Plugin definuje v rámci integračného API triedu pre typ dátového objektu XML dokument, ktorá reprezentuje:

- podpisovaný XML dokument,
- verifikačné údaje pre daný XML dokument – XML schéma a XSL transformácia – a ich atribúty.

XML Plugin pre D.Signer/XAdES .NET implementuje abstraktné API pre komunikáciu s hlavnou aplikáciou D.Signer/XAdES .NET.

V nasledujúcich kapitolách sú popísané jednotlivé rozhrania.

7.1. Integračné API pluginu

7.1.1. .Net API

Pre .Net aplikácie XML Plugin pre aplikáciu D.Signer/XAdES .NET publikuje:

Triedu:

```
Ditec.Zep.DSigXades.Plugins.XmlPlugin
```

Metódy a premenné:

```
object CreateObject
(     string objectId
,     string objectDescription
,     string sourceXml
,     string sourceXsd
,     string namespaceUri
,     string xsdReference
,     string sourceXsl
,     string xslReference
);

object CreateObject2
(     string objectId
,     string objectDescription
,     string sourceXml
,     string sourceXsd
,     string namespaceUri
,     string xsdReference
,     string sourceXsl
,     string xslReference
,     string transformType
);

string ErrorMessage { get;}
```

7.1.2. COM API

Pre iné prostredia ako .Net XML Plugin pre aplikáciu D.Signer/XAdES .NET publikuje nasledujúce COM rozhranie:

ProgId:

```
<DSig.XmlPlugin>
```

Funkcie a premenné:

```
VARIANT CreateObject
(     [in] BSTR objectId
,     [in] BSTR objectDescription
,     [in] BSTR sourceXml
,     [in] BSTR sourceXsd
,     [in] BSTR namespaceUri
,     [in] BSTR xsdReference
,     [in] BSTR sourceXsl
,     [in] BSTR xslReference
);

VARIANT CreateObject2
(     [in] BSTR objectId
,     [in] BSTR objectDescription
,     [in] BSTR sourceXml
,     [in] BSTR sourceXsd
,     [in] BSTR namespaceUri
,     [in] BSTR xsdReference
,     [in] BSTR sourceXsl
,     [in] BSTR xslReference
,     [in] BSTR transformType
);

[propget] BSTR ErrorMessage();
```

7.1.3. COM API prostredníctvom ATL knižnice

Aby bolo možné v rámci MS Internet Explorer identifikovať v rámci AddOns výrobcu pluginu pre daný typ dátových objektov, XML Plugin pre aplikáciu D.Signer/XAdES .NET publikuje popísané COM rozhranie aj prostredníctvom ATL knižnice.

ProgId:

```
<DSig.XmlPluginAtl>
```

Funkcie a premenné:

```
VARIANT CreateObject
(     [in] BSTR objectId
,     [in] BSTR objectDescription
,     [in] BSTR sourceXml
,     [in] BSTR sourceXsd
,     [in] BSTR namespaceUri
,     [in] BSTR xsdReference
,     [in] BSTR sourceXsl
,     [in] BSTR xslReference
);

VARIANT CreateObject2
(     [in] BSTR objectId
,     [in] BSTR objectDescription
,     [in] BSTR sourceXml
,     [in] BSTR sourceXsd
,     [in] BSTR namespaceUri
,     [in] BSTR xsdReference
,     [in] BSTR sourceXsl
,     [in] BSTR xslReference
,     [in] BSTR transformType
);

[propget] BSTR ErrorMessage();
```

7.1.4. Popis funkcií a premenných API pluginu

7.1.4.1. CreateObject

Umožňuje vytvoriť dátový objekt typu XML dokument v1.0 pre aplikáciu D.Signer/XAdES .NET.

Parametre:

objectId – XML Id daného objektu v rámci výslednej XML štruktúry podľa XAdES_ZEP, povolené znaky: a..z, A..Z, 0..9, „.“ (bodka), „-“ (pomlčka), „_“ (podčiarkovník),

objectDescription – popis obsahu daného XML objektu, napr: "DPPO 2007",

sourceXml – samotný vstupný XML dokument,

sourceXsd – XML schéma pre vstupný XML dokument,

namespaceUri – namespace URI vstupného XML dokumentu,

xsdReference – URI referencia XML schémy,

sourceXsl – XSL transformácia vstupného XML dokumentu do plain textu,

xslReference – URI referencia XSL transformácie.

7.1.4.2. CreateObject2

Umožňuje vytvoriť dátový objekt typu XML dokument v2.0 pre aplikáciu D.Signer/XAdES .NET.

Parametre:

objectId – XML Id daného objektu v rámci výslednej XML štruktúry podľa XAdES_ZEP, povolené znaky: a..z, A..Z, 0..9, „.“ (bodka), „-“ (pomlčka), „_“ (podčiarkovník),

objectDescription – popis obsahu daného XML objektu, napr: "DPPO 2007",

sourceXml – samotný vstupný XML dokument,

sourceXsd – XML schéma pre vstupný XML dokument,

namespaceUri – namespace URI vstupného XML dokumentu,

xsdReference – URI referencia XML schémy,

sourceXsl – XSL transformácia vstupného XML dokumentu do plain textu, HTML/XHTML alebo XSL:FO[1],

xslReference – URI referencia XSL transformácie.

transformType – typ výslednej vizualizácie XML dokumentu, povolené hodnoty sú "TXT", "HTML".

7.1.4.3. ErrorMessge

V prípade výskytu chyby v rámci procesu vytvárania dátového objektu typu XML dokument bude obsahovať príslušnú chybovú správu.

[1] Pozn. Tento typ transformácie a následné spracovanie XSL:FO do formátu PDF nebude v rámci komponentu D.Signer/XAdES .NET – XML Plugin podporované.