DITEC
Data Information Technology & Expert Consulting

Formát dátových objektov typu XML dokument

v rámci profilu XAdES_ZEP

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Formát dátových objektov typu XML dokument		
Podnázov	v rámci profilu XAdES_ZEP		
Ref. číslo	GOV_ZEP.3	Verzia	1

Vypracoval	Vittek Róbert	Podpis	Dátum 14. 11. 2007
Preveril	Major Marián	Podpis	Dátum 14. 11. 2007
Schválil	Dobias Ján	Podpis	Dátum 14. 11. 2007

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	Formát dátových objektov typu XML dokument		
Referencia	GOV_ZEP.3	Verzia	1

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. Zoznam použitých skratiek

CA – certifikačná autorita
CMS – Cryptographic Message Syntax
CRL – Certificate Revocation List
HTML – HyperText Markup Language
NBÚ – Národný bezpečnostný úrad
PDF – Portable Document Format
PKI – Public Key Infrastructure
PNG – Portable Network Graphics
RTF – Rich Text Format
SCA – Signature Creation Application
SCVA – Signature Creation and Validation Application
SVA – Signature Validation Application
TIFF – Tagged Image File Format, formát obrazových súborov
TSA – Autorita vydávajúca časové pečiatky
XAdES – XML Advanced Electronic Signatures
XML – eXtended Markup Language
XSD – XML Schema Definition
XSL – eXtensible Stylesheet Language
XSLT– XSL Transformation
ZEP – Zaručený elektronický podpis

2. 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) v1.3.2

[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 3280 – 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 (novelizovaný zákonom č. 275/2006 Z.z.)

[12] Vyhláška NBÚ č. 537/2002 Z.z., o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu...

[13] Vyhláška NBÚ č. 538/2002 Z.z., o formáte a obsahu kvalifikovaného certifikátu, o správe kvalifikovaných certifikátov a o formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o kvalifikovaných certifikátoch)

[14] Vyhláška NBÚ č. 542/2002 Z.z. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku (novelizovaná vyhláškou NBÚ NBÚ č. 233/2007 Z.z.)

[15] NBÚ Formáty kvalifikovaných certifikátov, v2.1 (2007-09-18)

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

[17] NBÚ Formáty zaručených elektronických podpisov, v2.0 (2007-07-22)

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

[19] CWA 14170:2001 E – Security Requirements for Signature Creation Applications

[20] CWA 14171:2001 E – Procedures for Electronic Signature Verification

3. Úvod

Tento dokument tvorí prílohu dokumentu Profil XAdES_ZEP – formát ZEP na báze XAdES a stanovuje požiadavky na štruktúru a obsah dátových objektov typu XML dokument a objektov s verifikačnými údajmi pre podpisované XML dokumenty. V rámci tohto dokumentu sú zároveň bližšie profilované niektoré elementy špecifikácie formátu elektronického podpisu XAdES_ZEP, týkajúce sa podpisovaných dátových objektov pre XML dokumenty.

Tento dokument:

- stanovuje požiadavky na štruktúru elementu ds:Object a obaľujúceho koreňového elementu pre dátový objekt typu XML dokument,
- stanovuje požiadavky na štruktúru a obsah dátového objektu pre referencie verifikačných údajov pre dátový objekt typu XML dokument:
  - ⇒ podpísaná referencia XML schémy,
  - ⇒ podpísaná referencia XML transformácie pre vizualizáciu XML dokumentu,
- stanovuje požiadavky na obsah príslušných xades:DataObjectFormat elementov v rámci xades:SignedDataObjectProperties elementu profilu XAdES_ZEP,
- stanovuje požiadavky na obsah príslušných ds:Reference elementov v rámci ds:Manifest elementov profilu XAdES_ZEP,
- stanovuje požiadavky na spracovanie XML dokumentov a verifikačných dát pre XML dokumenty pred vytvorením archívneho podpisu.

4. Dátový objekt typu XML dokument

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).

4.1. Štruktúra XML dokumentov

Na štruktúru a obsah samotných dátových objektov typu XML dokument nie sú v rámci tohto dokumentu stanovené žiadne požiadavky.

V nasledujúcich kapitolách sú uvedené požiadavky bližšie profilujúce obsah niektorých z požadovaných elementov a atribútov elementov špecifikácie formátu elektronického podpisu XAdES_ZEP pre účely podpisovania dátových objektov typu XML dokument.

4.2. Typ dátového objektu

V rámci štruktúry elektronického podpisu podľa profilu XAdES_ZEP je potrebné identifikovať typ podpisovaného dátového objektu pomocou podpísaného elementu xades:DataObjectFormat.

Pre podpisovaný dátový objekt typu XML dokument musia mať nasledujúce elementy xades:DataObjectFormat elementu nasledovné hodnoty:

- Description – string, obsahuje popis, ktorý bližšie definuje typ podpísaného dátového objektu (napr. "DPPO 2007"),
- ObjectIdentifier – URI, obsahuje identifikátor, ktorý bližšie definuje typ podpísaného dátového objektu (napr. URL príslušnej XML schémy),
- MimeType – string, hodnota "application/xml".[1]

[1] Rozdiel medzi "application/xml" a "text/xml" je popísaný v rámci RFC 3023, "If a text/xml entity is received with the charset parameter omitted, MIME processors and XML processors MUST use the default charset value of "us-ascii". Táto default hodnota pre kódovanie má väčšiu váhu ako kódovanie špecifikované v deklariách XML alebo ako default kódovania pre XML dokumenty UTF-8 a UTF-16, čiže vynechanie parametra charset pre "text/xml" entitu môže viesť k nepredvídateľným výsledkom. Identifikátor "application/xml" je vhodnejší aj z dôvodu, že obsah pôvodného XML dokumentu nemusí byť čitateľný bežnými používateľmi.

4.3. Referencia dátového objektu v rámci profilu XAdES_ZEP

Dátový objekt typu XML dokument musí byť v rámci profilu XAdES_ZEP referencovaný z príslušného ds:Manifest elementu. V rámci tohto dokumentu sa požaduje, aby referencia dátového objektu typu XML dokument obsahovala:

- element ds:Transforms – hodnota musí byť Canonical XML (omits comments) http://www.w3.org/TR/2001/REC-xml-c14n-20010315,

5. Verifikačné údaje pre dátový objekt typu XML

Jednou 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. 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.

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. Vhodným formátom pre zobrazovanie obsahu dokumentu (vzhľadom na technickú realizovateľnosť aj vzhľadom na dostatočnú vypovedaciu schopnosť) je jednoduchý textový formát (Plain Text). Základom pre úplné a správne

zobrazenie dokumentu pred podpisovaním je kontrola XML dokumentu vzhľadom na XML schému.

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

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

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

5.1. Štruktúra verifikačných údajov pre XML dokumenty

Dátový objekt s referenciami verifikačných údajov pre XML dokument je podpisovaný dátový objekt, čiže v rámci štruktúry elektronického podpisu musí pre neho existovať ds:Manifest element, ktorý je referencovaný z ds:SignedInfo podľa požiadaviek profilu XAdES_ZEP.

Dátový objekt s referenciami verifikačných údajov pre XML dokument musí obsahovať:

- element s referenciou XML schémy, ktorá bola použitá pre overenie štruktúry podpisovaného XML dokumentu,
- element s referenciou XML transformácie, ktorá bola použitá pre zobrazenie podpisovaného dokumentu podpisovateľovi.

Štruktúra objektu s referenciami verifikačných údajov pre XML dokument je popísaná v rámci nasledujúcej XML schémy:

```
<?xml version="1.0"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns="http://www.ditec.sk/ep/signature_formats/xades_zep_xml/v1.0"
targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep_xml/
v1.0">

<xsd:import
      namespace = "http://www.w3.org/2000/09/xmldsig#"
      schemaLocation = "http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"
/>

<xsd:element name = "XMLVerificationDataReferences">
      <xsd:complexType>
            <xsd:sequence>
```

```
                  <xsd:element ref = "SchemaReference"/>
                  <xsd:element ref = "VisualTransformReference"/>
            </xsd:sequence>
            <xsd:attribute name="DataTarget" type="xsd:anyURI"
                  use="required"/>
      </xsd:complexType>
</xsd:element>

<xsd:element name = "SchemaReference">
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:element ref = "ds:Reference"/>
            </xsd:sequence>
      </xsd:complexType>
</xsd:element>

<xsd:element name = "VisualTransformReference">
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:element ref = "ds:Reference"/>
            </xsd:sequence>
      </xsd:complexType>
</xsd:element>

</xsd:schema>
```

Jednotlivé referencie pre XML schému a XML transformáciu musia obsahovať:

- atribút URI – úplná a jednoznačná referencia daného objektu,
- element ds:Transforms – hodnota musí byť Canonical XML (omits comments) http://www.w3.org/TR/2001/REC-xml-c14n-20010315,
- element ds:DigestMethod – algoritmus pre výpočet hodnoty odtlačku daného objektu, musí byť použitý algoritmus, ktorý je podporovaný v rámci profilu XAdES_ZEP,
- element ds:DigestValue – hodnota odtlačku daného objektu po transformácii.

XML schéma a XML transformácia pre vizualizáciu dátového objektu typu referencie verifikačných údajov pre XML dokument musia byť súčasťou príslušného komponentu SCVA aplikácie.

5.2. Typ dátového objektu s referenciami verifikačných údajov

V rámci štruktúry elektronického podpisu podľa profilu XAdES_ZEP je potrebné identifikovať typ podpisovaného dátového objektu pomocou podpísaného elementu xades:DataObjectFormat.

Pre podpisovaný dátový objekt typu referencie verifikačných údajov pre XML dokument musia mať nasledujúce elementy xades:DataObjectFormat elementu nasledovné hodnoty:

- Description – string, obsahuje popis, ktorý bližšie definuje typ dátového objektu verifikačné údaje pre XML dokument (napr. "Verifikačné údaje pre DPPO 2007"),
- ObjectIdentifier – URI identifikátor, ktorý definuje typ dátového objektu verifikačné údaje pre XML dokument, hodnota: "http://www.ditec.sk/ep/signature_formats/xades_zep_xml/v1.0"
- MimeType – string, hodnota "application/xml".

5.3. Referencia dátového objektu s referenciami verifikačných údajov

Dátový objekt typu refrencie verifikačných údajov pre XML dokument musí byť v rámci profilu XAdES_ZEP referencovaný z príslušného ds:Manifest elementu. V rámci tohto dokumentu sa požaduje, aby referencia takého dátového objektu obsahovala:

- element ds:Transforms – hodnota musí byť Canonical XML (omits comments) http://www.w3.org/TR/2001/REC-xml-c14n-20010315,

6. Požiadavky pre vytvorenie archívneho podpisu

Podľa požiadaviek profilu XAdES_ZEP musia byť pred vytvorením archívneho podpisu zahrnuté pod ds:Signature element

- všetky dátové objekty ds:Object, ktoré sú referencované z niektorého z ds:Manifest elementov v rámci ds:Signature,
- všetky externé objekty, referencované pomocou ds:Reference elementu z niektorého z podpísaných dátových objektov, teda aj z objektu obsahujúceho refrencie verifikačných údajov pre podpísaný XML dokument.

Pred vytvorením archívneho podpisu musí teda SCVA aplikácia vykonať pre dátové objekty typu XML dokument nasledujúce činnosti:

- vytvoriť ds:Object s hodnotami verifikačných údajov, t.j. vytvoriť pre objekty XML schémy a XML transformácie štruktúru ds:Object, do ktorej vloží príslušnú XML schému a XML transformáciu, ktoré sú referencované v rámci verifikačných údajov.
- vložiť ako *child* elementy do štruktúry ds:Signature nasledujúce ds:Object elementy:
  - ⇒ ds:Object pre XML dokument,
  - ⇒ ds:Object s referenciami verifikačných údajov pre XML dokument,
  - ⇒ ds:Object pre XML schému a XML transformáciu teda objekt s hodnotami verifikačných údajov.

Takýmto spôsobom budú tieto dáta zahrnuté do výpočtu hodnoty odtlačku pre archívnu časovú pečiatku.

Obr. 1 Zaradenie podpísaného XML dokumentu, verifikačných údajov pre XML dokument a ich referencií do štruktúry ds:Signature.

Štruktúra objektu s hodnotami verifikačných údajov pre XML dokument je popísaná v rámci nasledujúcej XML schémy:

```
<?xml version="1.0"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns="http://www.ditec.sk/ep/signature_formats/xades_zep_xml/v1.0"
targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep_xml/
v1.0">

<xsd:import
      namespace = "http://www.w3.org/2000/09/xmldsig#"
      schemaLocation = "http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd"
/>

<xsd:element name = "XMLVerificationDataValues">
```

```
      <xsd:complexType>
            <xsd:sequence>
                  <xsd:element ref = "SchemaValue"/>
                  <xsd:element ref = "VisualTransformValue"/>
            </xsd:sequence>
      </xsd:complexType>
</xsd:element>

<xsd:element name = "SchemaValue">
      <xsd:complexType>
            <xsd:simpleContent>
                  <xsd:extension base="xsd:string">
                        <xsd:attribute name="URI" type="xsd:anyURI"
                              use="required"/>
                  </xsd:extension>
            </xsd:simpleContent>
      </xsd:complexType>
</xsd:element>

<xsd:element name = "VisualTransformValue">
      <xsd:complexType>
            <xsd:simpleContent>
                  <xsd:extension base="xsd:string">
                        <xsd:attribute name="URI" type="xsd:anyURI"
                              use="required"/>
                  </xsd:extension>
            </xsd:simpleContent>
      </xsd:complexType>
</xsd:element>
```

Povinný atribút URI musí mať hodnotu URI z príslušnej referencie XML schémy alebo XML transformácie v objekte s referenciami verifikačných údajov pre XML dokument.

V prípade, že by mali byť pod ds:Signature element zahrnuté viaceré identické dátové objekty s tými istými hodnotami verifikačných údajov, stačí, ak bude vytvorený a do štruktúry ds:Signature vložený len jeden taký dátový objekt.