DITEC
Data Information Technology & Expert Consulting

Formát dátových objektov typu XML dokument v2.0

v rámci profilu XAdES_ZEP

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Formát dátových objektov typu XML dokument v2.0		
Podnázov	v rámci profilu XAdES_ZEP		
Ref. číslo	GOV_ZEP.125	Verzia	3

Vypracoval	Vittek Róbert	Podpis	Dátum 23.12.2015
Preveril	Major Marián	Podpis	Dátum
Schválil	Dobias Ján	Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 13.10.2005

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 v2.0		
Referencia	GOV_ZEP.125	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. 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) v1.4.2

[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] Smernica Európskej únie č. 1999/93/EC z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[26] 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

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

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

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

3. Úvod

Tento dokument tvorí prílohu dokumentov profilu XAdES_ZEP – formátu ZEP na báze XAdES [23][24][25] (ďalej len XAdES_ZEP) 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,
- na štruktúru a obsah dátového objektu pre referencie verifikačných údajov pre dátový objekt typu XML dokument:
  - ⇒ podpísaná referencia XML schémy,
  - ⇒ podpísaný typ XML transformácie pre vizualizáciu XML dokumentu,
  - ⇒ podpísaná referencia XML transformácie pre vizualizáciu XML dokumentu,
- na obsah príslušných xades:DataObjectFormat elementov v rámci xades:SignedDataObjectProperties elementu profilu XAdES_ZEP,
- na obsah príslušných ds:Reference elementov v rámci ds:Manifest, resp. ds:SignedInfo elementov v súlade s príslušným profilom XAdES_ZEP,
- na spracovanie XML dokumentov a verifikačných dát pre XML dokumenty pred vytvorením archívneho podpisu.

V rámci tohto dokumentu sú kvôli prehľadnosti a jednoznačnosti elementy z nasledujúcich namespacov prefixované nasledovne:

- XML Signature:
  xmlns:ds = "http://www.w3.org/2000/09/xmldsig#",
- XAdES, v1.3.2:
  xmlns:xades = "http://uri.etsi.org/01903/v1.3.2#".

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) [16].

4.1. Uloženie XML dokumentu v rámci štruktúry podpisu

V rámci profilu XAdES_ZEP musí byť XML dokument bez XML Declaration vložený priamo do elementu ds:Object, ktorý musí obsahovať nasledujúce atribúty:

- Id – identifikátor elementu ds:Object.

4.2. Štruktúra a obsah XML dokumentov

Dátový objekt typu XML dokument nesmie obsahovať vnorenú štruktúru elektronického podpisu. XML dokument nesmie tiež obsahovať referencie znakových entít v tvare &#xD, &#xA, &#13 a &#10. Na štruktúru a obsah samotných dátových objektov typu XML dokument nie sú v rámci tohto dokumentu stanovené žiadne ďalšie požiadavky okrem tých, ktoré sú uvedené v dokumentoch [23][24] a [25], v kapitole Dátové objekty.

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.

4.3. 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 2014"),
- ObjectIdentifier – URI, obsahuje identifikátor, ktorý bližšie definuje typ podpísaného dátového objektu (napr. URI príslušnej XML schémy),

- MimeType – string, hodnota "application/xml".[1]

4.4. Referencia dátového objektu v rámci profilu XAdES_ZEP

Dátový objekt typu XML dokument musí byť podľa profilov XAdES_ZEP [23][24][25] referencovaný z príslušného ds:Reference elementu v rámci ds:Manifest, resp. ds:SignedInfo elementu. V rámci tohto dokumentu sa požaduje, aby táto 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,

[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.

5. Verifikačné údaje pre dátový objekt typu XML

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. [12] 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 [28] požaduje, aby povinnou prezentáciou pre podpisovanie a pre iný spôsob autorizácie elektronického formulára (ďalej len „podpisová prezentácia“) bol formát HTML alebo XHTML, a ak ide o elektronické formuláre s viac ako 50 procesnými krokmi, prezentáciou pre podpisovanie môže byť aj formát Plain 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 alebo TXT používa jazyk XSL Transformations 1.0 (XSLT).

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 alebo XHTML 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.

Požiadavky na prezentácie XML dokumentov pre podpisovanie sú mimo rámca tejto špecifikácie a sú definované v samostatnom dokumente [29]. 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.

5.1. 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:Object element, ktorý je referencovaný z ds:Manifest, resp. ds:SignedInfo elementu v súlade s požiadavkami profilov XAdES_ZEP [23][24][25].

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 typom XML transformácie pre vizualizáciu 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/v2.0"
targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep_xml/
v2.0">

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

<xsd:element name="VisualTransformType">
      <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                  <xsd:enumeration value="TXT"/>
                  <xsd:enumeration value="HTML"/>
```

```
                    <xsd:enumeration value="PDF"/>[2]
                </xsd:restriction>
            </xsd:simpleType>
        </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.

Atribút DataTarget slúži na previazanie dátového objektu s verifikačnými údajmi s daným dátovým objektom typu XML dokument a obsahuje URI dátového objektu, ku ktorému sa vzťahujú verifikačné údaje.

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 2014"),
- ObjectIdentifier – URI identifikátor, ktorý definuje typ dátového objektu verifikačné údaje pre XML dokument, hodnota: "http://www.ditec.sk/ep/signature_formats/xades_zep_xml/v2.0"
- MimeType – string, hodnota "application/xml".

[2] Možnosť vizualizácie XML dokumentu do formátu PDF bola zrušená novelou výnosu MF SR o štandardoch č. 276/2014 Z.z.

5.3. Referencia dátového objektu s referenciami verifikačných údajov

Dátový objekt typu referencie verifikačných údajov pre XML dokument musí byť v súlade s príslušným profilom XAdES_ZEP referencovaný z ds:Reference elementu uloženého v rámci ds:Manifest, resp. ds:SignedInfo elementu. V rámci tohto dokumentu sa požaduje, aby referencia tohto 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

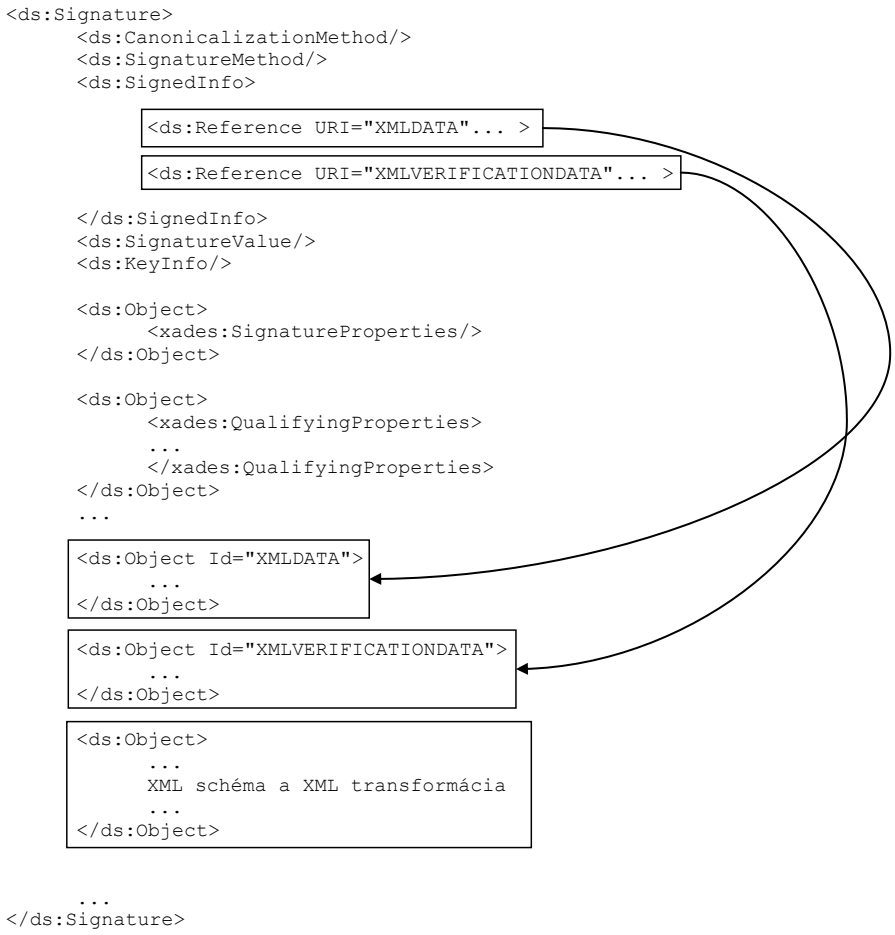
Podľa požiadaviek profilu XAdES_ZEP musia byť pred vytvorením archívneho podpisu zahrnuté pod ds:Signature element

- všetky dátové objekty ds:Object, ktoré sú referencované z niektorého z ds:Reference elementu v rámci príslušného ds:Manifest, resp. ds:SignedInfo elementu,
- všetky externé objekty, referencované pomocou ds:Reference elementu z niektorého z podpísaných dátových objektov, teda aj z objektu obsahujúceho referencie 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/v2.0"
targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep_xml/
v2.0">

<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>

</xsd:schema>
```

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.