DITEC
Data Information Technology & Expert Consulting

Formát dátových objektov pre FO formulár v1.0

v rámci profilu XAdES_ZEP

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Formát dátových objektov pre FO formulár v1.0		
Podnázov	v rámci profilu XAdES_ZEP		
Ref. číslo	GOV_ZEP.71	Verzia	2

Vypracoval	Vojtela Igor, Vittek Róbert	Podpis	Dátum 23. 3. 2010
Preveril	Major Marián	Podpis	Dátum
Schválil	Dobias Ján	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	Formát dátových objektov pre FO formulár v1.0	
Referencia	GOV_ZEP.71 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. 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 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, v3.0 (2010-01-17)

[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 – formát ZEP na báze XAdES, v1.0, DITEC, a.s., 2008

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

[25] W3C IETF Recommendation: "Extensible Stylesheet Language (XSL) Version 1.0", v2001-10-15,

[26] 602XML – Elementy a atributy přípustné v podepisovaném formuláři s redukovaným formátováním, v2.7, vztaženo k verzi 602XML Core 2.5, Software602, 16. 7. 2009

[27] XML Form Technical Specification, v2.2, Related to 602XML Filler and 602XML Designer applications v2.59, Software602, 15. 8. 2009

[28] Metodika návrhu FO formulárov, v1.02, Software602, 12. 2. 2010

3. Úvod

Tento dokument je prílohou dokumentov profilu XAdES_ZEP – formát ZEP na báze XAdES [23][24] (ďalej len XAdES_ZEP) a stanovuje požiadavky na štruktúru a obsah podpisovaných dátových objektov pre XML dáta FO formulárov a príslušných dátových objektov s verifikačnými údajmi. Zároveň sú tu bližšie profilované niektoré elementy špecifikácie formátu elektronického podpisu XAdES_ZEP, týkajúce sa podpisovaných dátových objektov pre XML dáta FO formulárov a príslušných dátových objektov s verifikačnými údajmi.

Tento dokument stanovuje požiadavky na:

- štruktúru elementu ds:Object a obaľujúceho koreňového elementu dátového objektu pre XML dáta FO formulára,
- štruktúru a obsah dátového objektu s referenciami verifikačných údajov pre FO formulár:
    - ⇒ podpísaná referencia XML schémy dát FO formulára,
    - ⇒ podpísaná referencia uzamknutej vizualizácie FO formulára (pozri kapitolu 4),
- obsah príslušných xades:DataObjectFormat elementov v rámci xades:SignedDataObjectProperties elementu profilu XAdES_ZEP,
- obsah príslušných ds:Reference elementov v rámci ds:Manifest elementov profilu XAdES_ZEP,
- spracovanie dátových objektov pre FO formuláre a príslušných verifikačných dát pred vytvorením archívneho podpisu.

4. FO formuláre

XML dokumenty vo všeobecnosti neobsahujú informácie o spôsobe prezentácie dát, ktoré obsahujú. Spôsob prezentácie XML dát je možné definovať prostredníctvom jazyka XSL, ktorý slúži na definovanie tzv. *štýlov*.

Špecifikácia XSL v1.0 [25] sa skladá z dvoch častí:

- XSLT – jazyka pre transformáciu XML dokumentov,
- XSL:FO – slovníka formátovacích objektov pre špecifikáciu platformovo nezávislého formátovania XML dokumentov[1].

XSL Stylesheet (definícia štýlov) potom definuje spôsob prezentácie triedy XML dokumentov, t.j. popisuje, ako je potrebné transformovať inštanciu danej triedy XML dokumentov na XML dokument, ktorý už obsahuje aj informáciu o formátovaní XML dokumentu s využitím štýlov. Výsledný XML dokument je možné prostredníctvom tzv. *formátovača* pre dané cieľové prostredie spracovať, t.j. sformátovať do tvaru vhodného pre prezentáciu v príslušnom cieľovom prostredí (obrazovka, tlačiareň, web prehliadač a pod.)

FO formuláre sú založené na špecifikácii XSL v1.0, konkrétne na formátovacom jazyku XSL:FO. Jazyk XSL:FO je plne v súlade so štandardom XML, jednotlivé XSL:FO formátovacie objekty (blocks, tables, ...) spolu s ich atribútmi sú takisto definované vo formáte XML. Prehľad elementov (a príslušných atribútov) formátovacieho jazyka XSL:FO, ktoré sa môžu vyskytovať v FO formulári je uvedený v dokumentoch [26] a [27].

FO formulár môže byť v jednej z nasledujúcich foriem:

- štandardný FO formulár – plnohodnotný FO formulár, umožňujúci editáciu dát, ktorý môže navyše obsahovať aktívne prvky (aktívne tlačidlá, funkcie pre validáciu polí formulára a pod.); tento typ formulára môže alebo nemusí mať k sebe pripojené XML dáta,
- uzamknutý FO formulár – neumožňuje editáciu k nemu pripojených XML dát, len ich vizualizáciu; neobsahuje žiadne aktívne prvky (aktívne tlačidlá, funkcie pre validáciu polí formulára a pod.); XML dáta nie sú oddelené od FO formulára,
- uzamknutá vizualizácia FO formulára – neumožňuje editáciu XML dát, len ich vizualizáciu; neobsahuje žiadne aktívne prvky (aktívne tlačidlá, funkcie pre validáciu polí formulára a pod.); XML dáta sú oddelené od FO formulára; FO formulár a XML dáta sú pripravené na podpísanie elektronickým podpisom.

Formy uzamknutý FO formulár a uzamknutá vizualizácia FO formulára sa nazývajú aj FO formuláre s redukovaným formátovaním. Štandardný FO formulár

[1] Teda formátovania, ktoré je nezávislé na cieľovom výstupnom zariadení alebo prostredí – obrazovka, tlačiareň, web prehliadač atď.

je možné prostredníctvom 602XML SDK previesť do niektorej z foriem FO formulárov s redukovaným formátovaním. Ak je požadovaný prevod FO formulára do formy uzamknutej vizualizácie FO formulára, je potrebné, aby už pri návrhu formulára bola do formulára zaradená aj jeho uzamknutá vizualizácia (element <fm:visualization/>). Prevod FO formulára do formy uzamknutého FO formulára je možný len v aplikácii na to určenej bez zásahu designéra formulára.

Procesy návrhu FO formulárov a zásady návrhu FO formulárov, ktoré umožňujú naplnenie bezpečnostných požiadaviek vyplývajúcich z dokumentov [11] – [22], upravuje dokument Metodika návrhu FO formulárov [28].

4.1. Požiadavky na štruktúru a obsah podpisovaných FO formulárov

Táto špecifkácia formátu dátových objektov pre FO formulár vyžaduje, aby bol FO formulár pred vytvorením elektronického podpisu vo formáte XAdES_ZEP vo forme uzamknutej vizualizácie s oddelenými XML dátami FO formulára.

FO formulár nesmie tiež obsahovať žiadne prílohy, tie musia byť pred vytvorením elektronického podpisu vo formáte XAdES_ZEP extrahované z FO formulára a môžu byť prípadne podpísané v rámci vytváranej štruktúry XAdES_ZEP ako samostatné dátové objekty. XML dáta oddelené od vizualizácie FO formulára môžu obsahovať údaje, ktoré popisujú alebo referencujú takto oddelené prílohy FO formulára.

4.2. Uloženie FO formulára v rámci štruktúry elektronického podpisu

Pri vytvorení elektronického podpisu vo formáte XAdES_ZEP budú v rámci štruktúry elektronického podpisu vytvorené dva dátové objekty ds:Object:

- dátový objekt pre XML dáta FO formulára,
- dátový objekt pre referencie verifikačných údajov pre FO formulár:
  - ⇒ podpísaná referencia XML schémy dát FO formulára – vytvorená pomocou elementu ds:Reference z XML schémy dát FO formulára,
  - ⇒ podpísaná referencia vizualizácie FO formulára – vytvorená pomocou elementu ds:Reference z uzamknutej vizualizácie FO formulára.

Aplikačná vrstva na strane podpisovateľa musí mať pre vytvorenie uvedených referencií k dispozícii obsah príslušnej XML schémy dát FO formulára a takisto príslušnú uzamknutú vizualizáciu FO formulára. Rovnaké údaje pre overenie týchto referencií musí mať k dispozícii aplikačná vrstva na strane overovateľa.

5. Dátový objekt pre XML dáta FO formulára

5.1. Štruktúra dátového objektu pre XML dáta FO formulára

Na štruktúru a obsah samotných dátových objektov pre XML dáta FO formulára nie sú v rámci tohto dokumentu stanovené žiadne ďalšie požiadavky okrem tých, ktoré sú uvedené v dokumentoch [23] a [24], v kapitole 4.2.4.

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 pre XML dáta FO formulárov.

5.2. 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 pre XML dáta FO formulára 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. URI príslušnej XML schémy dát FO formulára),
- MIME Type – string, hodnota "application/vnd.software602.filler.form+xml" (aby bolo možné na aplikačnej úrovni identifikovať, že ide o XML dáta, ktoré je potrebné vizualizovať prostredníctvom FO formulára).

5.3. Referencia dátového objektu v rámci profilu XAdES_ZEP

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

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

6. Verifikačné údaje pre FO formulár

Prednosťou FO formulára ako špeciálneho typu XML elektronického dokumentu je možnosť vyjadrenia jeho štruktúry a definovania jednoduchých aj komplexných údajových typov jeho jednotlivých polí pomocou XML schémy (XSD – http://www.w3.org/XML/Schema/).

Na základe definovanej XML schémy je možné automaticky overovať správnosť štruktúry dokumentu. Správna štruktúra FO formulára 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 vytvorením samotného podpisu.

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

Z týchto dôvodov je potrebné podpisované XML dáta FO formulára opatriť doplňujúcou podpísanou informáciou, ktorá deklaruje XML schému použitú pre overenie správnosti štruktúry podpisovaných XML dát FO formulára pred samotným vytvorením elektronického podpisu.

Overovateľ elektronického podpisu musí overiť použitie správnej XML schémy pre overenie správnosti štruktúry podpísaných XML dát FO formulára.

Zákon č. 215/2002 Z.z. definuje požiadavku zobrazenia (vizualizácie) podpisovaného elektronického dokumentu podpisovateľovi skôr, ako sa spustí procedúra na vyhotovenie zaručeného elektronického podpisu. XML dáta sú vo väčšine prípadov pre bežného používateľa nečitateľné, preto je potrebné zabezpečiť ich vizualizáciu inými prostriedkami. Vizualizáciu FO formulárov a k nim pripojených XML dát do čitateľnej formy zabezpečuje prostredníctvom implementácie technológií XSL transformácie a XSL:FO formátovacie objekty napr. komponent 602XML SDK od spoločnosti Software 602.

Zodpovednosť za vydávanie a zverejňovanie aktuálnych uzamknutých vizualizácií FO formulárov je na správcovi komunikačného scenára, v rámci ktorého sa požaduje spracovanie FO formulárov podpísaných elektronickým podpisom. Zodpovednosť za použitie dôveryhodnej a správnej vizualizácie FO formulára je na podpisovateľovi XML dát príslušného FO formulára.

K podpisovaným XML dátam FO formulára je potrebné pripojiť doplňujúcu informáciu, ktorá deklaruje, aká vizualizácia FO formulára bola použitá pre zobrazenie XML dát podpisovaného FO formulára pred samotným vytvorením elektronického podpisu.

Overovateľ elektronického podpisu musí overiť použitie správnej vizualizácie pre zobrazenie XML dát podpísaného FO formulára.

6.1. Štruktúra verifikačných údajov pre FO formuláre

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

Dátový objekt s referenciami verifikačných údajov pre FO formulár musí obsahovať:

- element s referenciou XML schémy, ktorá bola použitá pre overenie štruktúry XML dát podpisovaného FO formulára,
- element s referenciou uzamknutej vizualizácie FO formulára, ktorá bola použitá pre zobrazenie podpisovaného FO formulára podpisovateľovi.

Štruktúra objektu s referenciami verifikačných údajov FO formulára 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_fo/v1.0"
targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep_fo/v
1.0">

<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 = "FOVerificationDataReferences">
      <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 podpisovaných XML dát FO formulára a vizualizáciu FO formulára 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 pre referencie verifikačných údajov FO formulára musia byť súčasťou príslušného komponentu SCVA aplikácie.

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

6.2. 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 FO formulár musia mať nasledujúce elementy xades:DataObjectFormat elementu nasledovné hodnoty:

- Description – string, obsahuje popis, ktorý bližšie definuje typ dátového objektu verifikačné údaje pre FO formulár (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_fo/v1.0"
- MimeType – string, hodnota "application/xml".

6.3. Referencia dátového objektu s referenciami verifikačných údajov

Dátový objekt s referenciami verifikačných údajov pre FO formulár 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.

7. Požiadavky pre vytvorenie archívneho podpisu

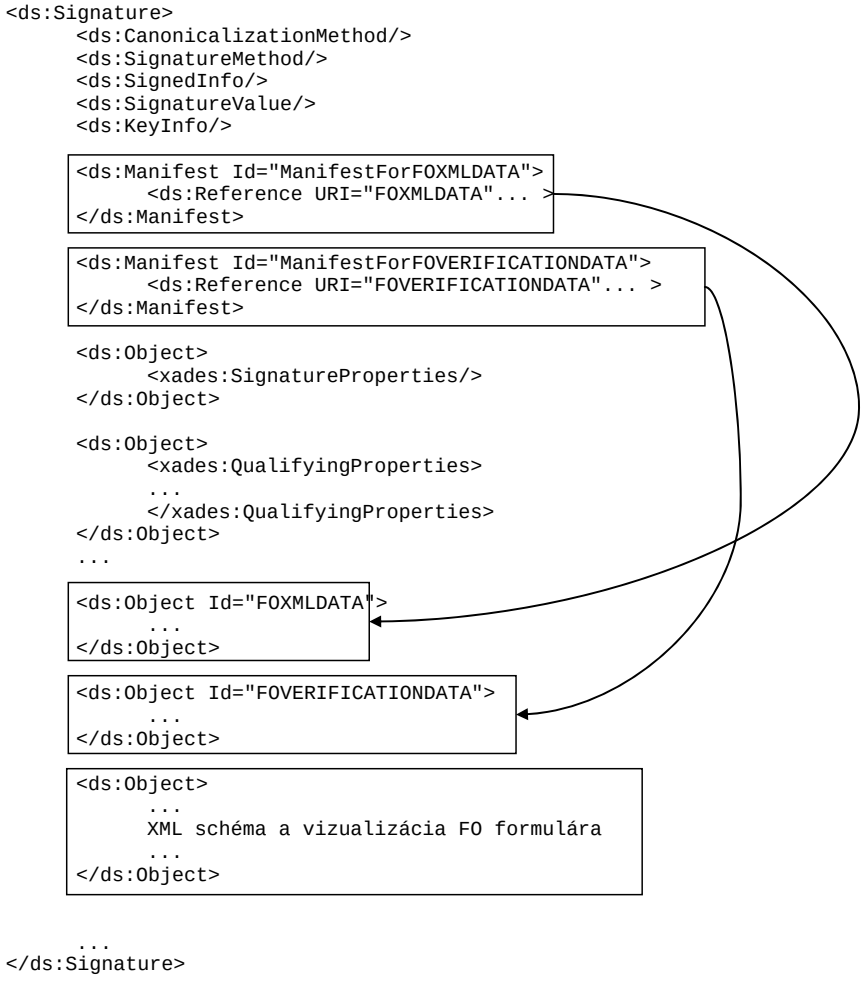
Podľa požiadaviek profilu XAdES_ZEP musia byť pred vytvorením archívneho podpisu zahrnuté pod ds:Signature element

- 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 referencie verifikačných údajov pre podpísaný FO formulár.

Pred vytvorením archívneho podpisu musí teda SCVA aplikácia vykonať pre dátové objekty pre FO formulár nasledujúce činnosti:

- vytvoriť ds:Object s hodnotami verifikačných údajov, t.j. vytvoriť pre objekty XML schémy pre XML dáta FO formulára a uzamknutej vizualizácie FO formulára štruktúru ds:Object, do ktorej vloží príslušnú XML schému dát formulára a vizualizáciu FO formulára, ktoré sú referencované v rámci verifikačných údajov.
- vložiť ako *child* elementy do štruktúry ds:Signature nasledujúce ds:Object elementy:
  - ⇒ ds:Object pre XML dáta FO formulára,
  - ⇒ ds:Object s referenciami verifikačných údajov pre FO formulár,
  - ⇒ ds:Object pre XML schému dát formulára a vizualizáciu FO formulára, teda objekt s hodnotami verifikačných údajov.

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



Obr. 1 Zaradenie podpísaných XML dát FO formulára a verifikačných údajov pre FO formulár a ich referencií do štruktúry ds:Signature.

Štruktúra objektu s hodnotami verifikačných údajov pre FO formulár 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_fo/v1.0"
targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep_fo/v
1.0">

<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 = "FOVerificationDataValues">
      <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 vizualizácie FO formulára v objekte s referenciami verifikačných údajov pre FO formulár.

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.