DITEC
Data Information Technology & Expert Consulting

Formát zloženého elektronického podpisu v1.0

príloha formátu XAdES_ZEP

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Formát zloženého elektronického podpisu v1.0		
Podnázov	príloha formátu XAdES_ZEP		
Ref. číslo	GOV_ZEP.58	Verzia	3

Vypracoval	Vittek Róbert	Podpis	Dátum 16. 8. 2009
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 zloženého elektronického podpisu v1.0		
Referencia	GOV_ZEP.58	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
XMLDSIG – XML Digital Signature
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, 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] Profil XAdES_ZEP v1.0 – formát ZEP na báze XAdES, DITEC, a.s., 2008

3. Úvod

Zo súčasného rozvoja používania (zaručeného) elektronického podpisu, najmä v rámci procesov elektronickej komunikácie s orgámi štátnej správy SR vyplýva požiadavka definovať formát a štruktúru tzv. zloženého elektronického podpisu, pozostávajúceho z viacerých samostatných elektronických podpisov.

Špecifikácie XML Signature – XMLDSIG [1] a XAdES [3] definujú prostriedky pre vytvorenie tzv. *multiple electronic signature* – zloženého elektronického podpisu, ktorý môžu tvoriť:

- nezávislé podpisy – sú to paralelne vytvorené elektronické podpisy, pričom ich poradie nie je dôležité. Výpočet týchto podpisov je vykonaný nad tými istými dátami (dokumentami) s využitím rôznych privátnych kľúčov,
- kontrasigntúry (countersignatures) – tieto podpisy sú aplikované jeden po druhom a používajú sa v prípade, keď poradie vytvorenia elektronických podpisov je v rámci daného procesu dôležité, napr. prvý elektronický podpis podpisuje samotné dáta (dokument), každý ďalší podpis (kontrasignatúra) môže podpisovať pôvodné dáta a/alebo tiež predchádzajúce elektronické podpisy.

Špecifikácia XAdES [3] poskytuje mechanizmy pre vytvorenie rôznych schém kontrasignatúr prostredníctvom elementu xades:CounterSignature a zavedením URI pre Type atribút referencie iného (kvalifikovaného) elektronického podpisu "http://uri.etsi.org/01903#CountersignedSignature".[1] Uvedené špecifikácie [1] a [3] sa však nezaoberajú definovaním kontajnera (obálky) pre štruktúru viacerých nezávislých elektronických podpisov.

Tento dokument tvorí prílohu dokumentu špecifikácie formátu XAdES_ZEP [21] a definuje formát a štruktúru obálky zloženého elektronického podpisu, vytvoreného z viacerých nezávislých elektronických podpisov vo formáte XAdES_ZEP.

Ako najvhodnejší formát pre zabezpečenie prenosu štruktúrovaných dát medzi subjektami v rámci elektronickej komunikácie je v súčasnosti považovaný formát XML. Vzhľadom k tomu, že zložený elektronický podpis bude tvoriť štruktúru vytvorenú nad XML štruktúrami profilu XAdES_ZEP, bol ako nosný dátový formát pre zložený elektronický podpis zvolený tiež formát XML.

Tento dokument:

- definuje štruktúru obálky zloženého elektronického podpisu – elementu xzepds:DataSignatures,

[1] Profil XAdES_ZEP, v1.0 tieto mechanizmy nepodporuje.

- popisuje postup vytvorenia zloženého elektronického podpisu z viacerých nezávislých elektronických podpisov, ktoré sú v súlade s profilom XAdES_ZEP,
- popisuje postup vytvorenia samostatných elektronických podpisov vo formáte XAdES_ZEP zo zloženého elektronického podpisu, ktorý je v súlade s touto špecifikáciou.

4. Špecifikácia formátu zloženého podpisu

4.1. Štruktúra zloženého podpisu

Profil XAdES_ZEP [21] definuje štruktúru pre (zaručený) elektronický podpis na báze formátu XAdES [3], ktorý je možné vytvárať nad rôznymi formátmi vstupných dokumentov (XML, PDF apod.) V tejto kapitole sú definované a popísané elementy XML schémy pre zložený elektronický podpis, pričom boli zohľadnené nasledujúce požiadavky:

- potreba definovať obálku pre navzájom nezávislé elektronické podpisy vytvorené podľa profilu XAdES_ZEP,
- potreba identifikovať profil a obsah obálky zloženého elektronického podpisu na aplikačnej úrovni,
- efektívne uloženie elektronických podpisov a podpísaných dátových objektov (dokumentov) v rámci obálky pre zložený elektronický podpis,
- možnosť pripojiť k obálke zloženého elektronického podpisu ďalšie sprievodné dáta (XML štruktúry) pre potreby aplikačnej úrovne.

V nasledujúcom texte je uvedená XML schéma pre zložený elektronický podpis.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xzepds="http://www.ditec.sk/ep/signature_formats/
        xades_zep_data_signatures/v1.0"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    targetNamespace="http://www.ditec.sk/ep/signature_formats/
        xades_zep_data_signatures/v1.0"
    version="1.0"
    elementFormDefault="qualified">
  <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="DataSignatures" type="xzepds:DataSignaturesType" />
  <xsd:complexType name="DataSignaturesType">
    <xsd:sequence>
      <xsd:element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element ref="ds:Signature" minOccurs="1"
        maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
    <xsd:attribute name="Description" type="xsd:string" use="optional"/>
```

```
  </xsd:complexType>
</xsd:schema>
```

V rámci zloženého elektronického podpisu je teda 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.

Zložený elektronický podpis môže teda obsahovať:

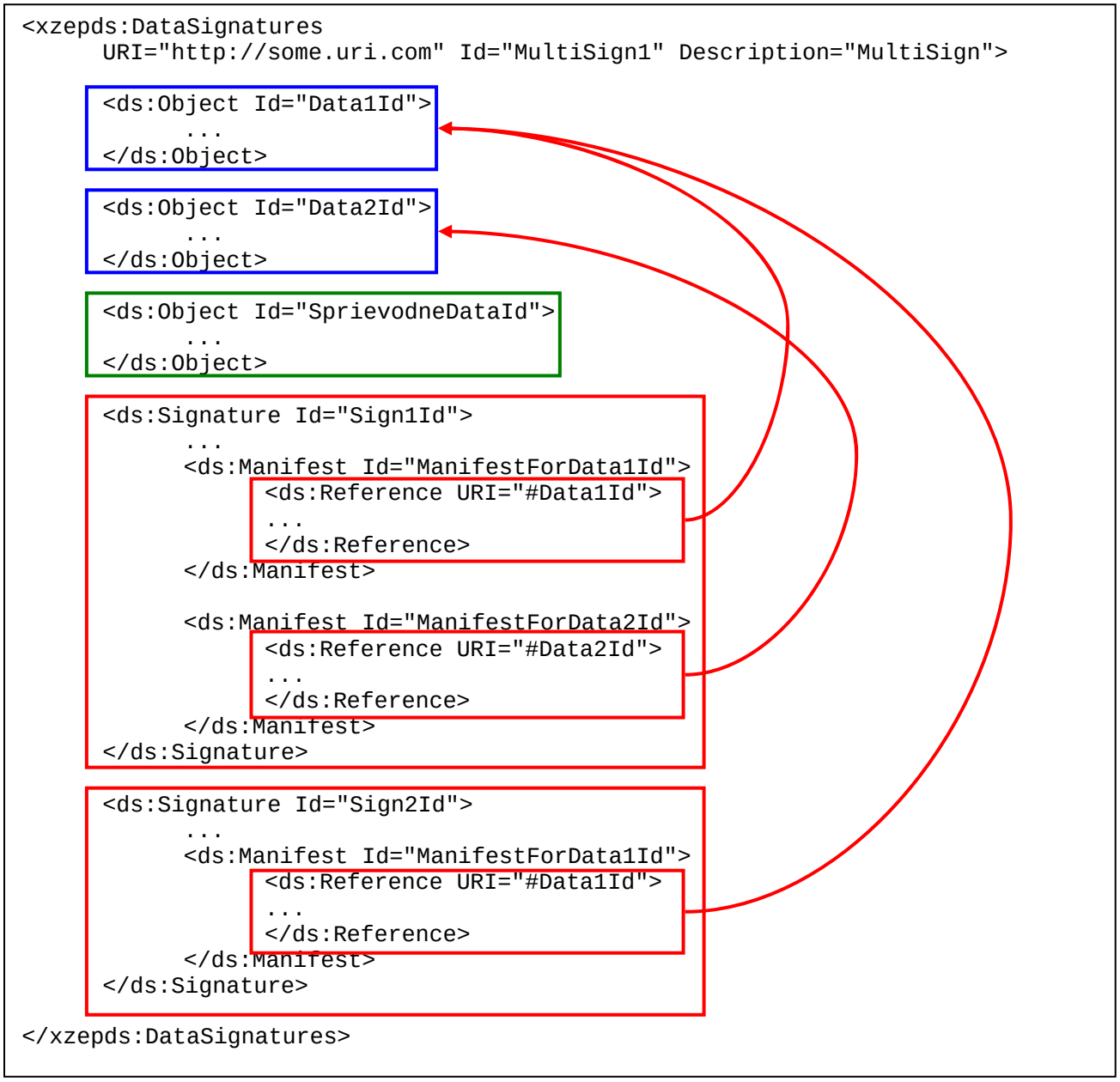
- niekoľko elementov ds:Object – dátových objektov, resp. dokumentov, ktoré sú referencované z niektorého z pripojených elektronických podpisov (ds:Signature elementov),
- niekoľko elementov ds:Object – dátových objektov, ktoré nie sú referencované zo žiadneho z pripojených elektronických podpisov (ds:Signature elementov) a obsahujú sprievodné dáta,
- jeden alebo viac ds:Signature elementov extrahovaných z elektronických podpisov vytvorených v súlade s profilom XAdES_ZEP,
- atribút URI – jednoznačný identifikátor profilu dátovej štruktúry zloženého elektronického podpisu (mal by byť definovaný v rámci príslušného procesu špecifikácie dátových štruktúr na aplikačnej úrovni),
- atribút Id – nepovinný atribút, identifikátor danej inštancie vytvoreného zloženého elektronického podpisu,
- atribút Description – nepovinný atribút, popis inštancie alebo profilu zloženého elektronického podpisu.

Elementy ds:Object, ktoré obsahujú podpísané dátové objekty a elementy ds:Signature musia spĺňať požiadavky profilu XAdES_ZEP [21].

Elementy ds:Object, ktoré obsahujú nepodpísané (sprievodné) dáta musia spĺňať nasledujúce požiadavky:

- element ds:Object musí obsahovať atribút Id,
- koreňový element samotného dátového objektu musí obsahovať atribút xmlns – namespace pre elementy použité v rámci dátového objektu.

Na nasledujúcom obrázku je uvedený príklad štruktúry zloženého elektronického podpisu.



Uvedený príklad štruktúry zloženého elektronického podpisu teda obsahuje:

- dva podpísané dátové objekty s identifikátormi Data1Id a Data2Id,
- dva ds:Signature elementy z dvoch nezávislých elektronických podpisov vytvorených podľa profilu XAdES_ZEP, pričom
  - ⇒ v rámci podpisu s id=Sign1Id sú referencované oba dátove objekty,
  - ⇒ v rámci podpisu s id=Sign2Id je referencovaný len dátový objekt s id=Data1Id,

- jeden nepodpísaný dátový objekt s Id=SprievodneDataId.

Vzhľadom k tomu, že oba elektronické podpisy referencujú ten istý dátový objekt s Id=Data1Id, nachádza sa tento dátový objekt v štruktúre podpisu len raz. Zlúčením oboch elektronických podpisov vznikla zložená štruktúra dvoch *detached* elektronických podpisov.

Pozn.: Pri vytváraní zloženého elektronického podpisu z archívneho formátu XAdES_ZEP-A nie je možné vyextrahovať podpísané dátové objekty mimo príslušný ds:Signature element.

4.2. Postup vytvorenia zloženého elektronického podpisu

Vstupy:

- kolekcia nezávislých elektronických podpisov vo formáte XAdES_ZEP,
- kolekcia dátových objektov so sprievodnými dátami,
- URI profilu štruktúry zloženého elektronického podpisu,
- Id inštancie zloženého elektronického podpisu,
- Popis inštancie alebo profilu zloženého elektronického podpisu.

Výstup:

- zložený elektronický podpis v súlade s touto špecifikáciou.

Premenné:

currentSignature – aktuálne pridávaný elektronický podpis,

currentDataObject – aktuálne pridávaný dátový objekt,

dataObjects – kolekcia pridávaných dátových objektov ds:Object,

signatureObjects – kolekcia pridávaných objektov ds:Signature,

Postup:

Pre každý vstupný elektronický podpis vo formáte XAdES_ZEP:

1) vyextrahuj zo vstupného elektronického podpisu element ds:Signature a ulož ho do premennej currentSignature,
2) ak daná štruktúra podpisu currentSignature nie je archívny podpis XAdES_ZEP-A, tak z obálky vstupného elektronického podpisu xzep:DataEnvelope vyextrahuj všetky *detached* dátové objekty ds:Object,
3) pre každý vyextrahovaný dátový objekt currentDataObject:
   A) skontroluj pred pridaním do kolekcie dátových objektov dataObjects jednoznačnosť Id,
   B) ak v kolekcii dataObjects už existuje dátový objekt s daným Id, tak skontroluj hodnotu jeho referencie (odtlačku):

l) ak odtlačok currentDataObject nie je rovnaký, ako odtlačok príslušného dátového objektu v kolekcii dataObjects, skonči s chybou,

C) ak v kolekcii dataObjects neexistuje dátový objekt s daným Id, tak pridaj currentDataObject do kolekcie dataObjects,

4) ak v rámci kolekcie signatureObjects už existuje elektronický podpis s Id rovnakým, ako je Id podpisu uloženého v premennej currentSignature, skonči s chybou,

5) inak pridaj do kolekcie signatureObjects podpis uložený v premennej currentSignature.

Pre každý dátový objekt z kolekcie dátových objektov so sprievodnými dátami:

6) skontroluj pred pridaním do kolekcie dátových objektov dataObjects jednoznačnosť Id,

7) ak v kolekcii dataObjects neexistuje dátový objekt s daným Id, tak pridaj daný dátový objekt so sprievodnými dátami do kolekcie dataObjects, inak skonči s chybou.

Nakoniec vyskladaj štruktúru zloženého elektronického podpisu na základe:

- kolekcie pridávaných dátových objektov – dataObjects,
- kolekcia pridávaných objektov – signatureObjects,
- vstupných parametrov:
  - ⇒ URI profilu štruktúry zloženého elektronického podpisu,
  - ⇒ Id inštancie zloženého elektronického podpisu,
  - ⇒ Popis zloženého elektronického podpisu.

Pozn.: Id atribúty všetkých elementov v rámci výslednej XML štruktúry zloženého elektronického podpisu musia byť jednoznačné.

4.3. Postup dekompozície zloženého elektronického podpisu

Vstup:

- zložený elektronický podpis v súlade s touto špecifikáciou.

Výstupy:

- kolekcia nezávislých elektronických podpisov vo formáte XAdES_ZEP,
- kolekcia dátových objektov so sprievodnými dátami,
- URI profilu štruktúry zloženého elektronického podpisu,
- Id inštancie zloženého elektronického podpisu,
- Popis zloženého elektronického podpisu.

Premenné:

dataObjects – kolekcia všetkých dátových objektov ds:Object zahrnutých v zloženom elektronickom podpise,

signatureObjects – kolekcia všetkých objektov ds:Signature zahrnutých v zloženom elektronickom podpise,

Postup:

Vytvor na základe vstupného zloženého elektronického podpisu:

- dataObjects – kolekciu všetkých zahrnutých dátových objektov, elementov ds:Object,
- signatureObjects – kolekciu všetkých zahrnutých objektov elektronických podpisov ds:Signature,

Pre každý element ds:Signature v kolekcii signatureObjects:

1) ak daná štruktúra nie je archívny podpis XAdES_ZEP-A, tak pre všetky referencie ds:Manifest, nájdi príslušný dátový objekt v kolekcii dataObjects a nastav príznak, že daný dátový objekt je referencovaný z niektorého z elektronických podpisov,
2) z nájdených ds:Object elementov a aktuálneho ds:Signature elementu vyskladaj elektronický podpis vo formáte XAdES_ZEP a pridaj ho do výstupnej kolekcie nezávislých elektronických podpisov vo formáte XAdES_ZEP,
3) ak daná štruktúra je archívny podpis XAdES_ZEP-A, tak vytvor pre neho len obálku xzep:DataEnvelope a výsledný elektronický podpis pridaj do výstupnej kolekcie nezávislých elektronických podpisov vo formáte XAdES_ZEP,

Pre všetky nereferencované dátové objekty v kolekcii dataObjects:

4) pridaj daný dátový objekt do výstupnej kolekcie dátových objektov so sprievodnými dátami.

Nastav hodnoty výstupných parametrov:

- URI profilu štruktúry zloženého elektronického podpisu,
- Id inštancie zloženého elektronického podpisu,
- Popis zloženého elektronického podpisu.