

# **Profil XAdES\_ZEP v1.1**

## **formát zaručeného elektronického podpisu na báze XAdES**

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

# Copyright

Všetky práva vyhradené

Tento dokument je vlastníctvom spoločnosti DITEC, a. s. Žiadna jeho časť sa nesmie akýmkoľvek spôsobom (elektronickým, mechanickým) poskytnúť tretej strane, rozmnožovať, kopírovať, vrátane spätného prevodu do elektronickej podoby, bez písomného povolenia spracovávateľa.

## Popisné charakteristiky dokumentu

|            |  |           |
|------------|--|-----------|
| Projekt    | GOV_ZEP  | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1                                  |           |
| Podnázov   | formát zaručeného elektronického podpisu na báze XAdES |           |
| Ref. číslo | GOV_ZEP.2  | Verzia 6  |

|            |               |        |                   |
|------------|---------------|--------|-------------------|
| Vypracoval | Vittek Róbert | Podpis | Dátum 26. 5. 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   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

### Záznamy o zmenách

| Autor | Popis zmien | Dátum | Verzia |
|-------|-------------|-------|--------|
|       |             |       |        |
|       |             |       |        |
|       |             |       |        |

### Pripomienkovanie a kontrola

| Autor | Stanovisko | Dátum | Verzia |
|-------|------------|-------|--------|
|       |            |       |        |
|       |            |       |        |
|       |            |       |        |

### Rozdeľovník

|          | Priezvisko Meno | Firma, Funkcia |
|----------|-----------------|----------------|
| Originál |                 |                |
| Kópia    |                 |                |
| Kópia    |                 |                |
| Kópia    |                 |                |

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

# Obsah

|             |  |           |
|-------------|--|-----------|
| <b>1.</b>   | <b>Zoznam použitých skratiek .....</b>         | <b>6</b>  |
| <b>2.</b>   | <b>Referencie .....</b>                        | <b>7</b>  |
| <b>3.</b>   | <b>Úvod .....</b>                              | <b>8</b>  |
| <b>4.</b>   | <b>Špecifikácia profilu XAdES_ZEP .....</b>    | <b>10</b> |
| <b>4.1.</b> | <b>Podporované pokročilé formy XAdES .....</b> | <b>12</b> |
| <b>4.2.</b> | <b>Štruktúra podpisu .....</b>                 | <b>13</b> |
| 4.2.1.      | Dátová obálka.....                             | 15        |
| 4.2.2.      | ds:Signature element.....                      | 17        |
| 4.2.3.      | ds:Manifest elementy.....                      | 18        |
| 4.2.4.      | Dátové objekty.....                            | 19        |
| 4.2.4.1.    | Dátové objekty s verifikačnými údajmi.....     | 19        |
| 4.2.5.      | ds:SignatureProperties element .....           | 20        |
| 4.2.6.      | XML namespaces.....                            | 21        |
| 4.2.7.      | Id atribúty.....                               | 22        |
| 4.2.8.      | Kódovanie XML .....                            | 22        |
| <b>4.3.</b> | <b>Profil časti XML Signature .....</b>        | <b>22</b> |
| 4.3.1.      | ds:SignedInfo element.....                     | 22        |
| 4.3.1.1.    | ds:CanonicalizationMethod element.....         | 22        |
| 4.3.1.2.    | ds:SignatureMethod element.....                | 23        |
| 4.3.1.3.    | ds:Reference elementy v ds:SignedInfo .....    | 23        |
| 4.3.1.3.1.  | ds:Transforms element.....                     | 24        |
| 4.3.1.3.2.  | ds:DigestMethod element.....                   | 25        |
| 4.3.1.3.3.  | ds:DigestValue element .....                   | 25        |
| 4.3.2.      | ds:SignatureValue element.....                 | 25        |
| 4.3.3.      | ds:KeyInfo element.....                        | 25        |
| 4.3.4.      | ds:Manifest elementy.....                      | 26        |
| 4.3.4.1.    | ds:Transforms element.....                     | 26        |
| 4.3.4.2.    | ds:DigestMethod element.....                   | 27        |
| 4.3.4.3.    | ds:DigestValue element .....                   | 27        |
| <b>4.4.</b> | <b>Profil xades:QualifyingProperties .....</b> | <b>27</b> |
| 4.4.1.      | xades:SignedProperties element.....            | 30        |
| 4.4.2.      | xades:UnsignedProperties element.....          | 30        |
| 4.4.3.      | xades:SignedSignatureProperties element .....  | 31        |

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

|  |           |
|--|-----------|
| 4.4.3.1. xades:SigningTime element .....   | 31        |
| 4.4.3.2. xades:SigningCertificate element .....  | 31        |
| 4.4.3.3. xades:SignaturePolicyIdentifier element .....                                       | 31        |
| 4.4.4. xades:SignedDataObjectProperties element .....  | 32        |
| 4.4.4.1. xades:DataObjectFormat element .....  | 32        |
| 4.4.5. xades:UnsignedSignatureProperties element .....                                       | 33        |
| 4.4.5.1. xades:SignatureTimeStamp element .....  | 33        |
| 4.4.5.2. xades:CompleteCertificateRefs element .....   | 33        |
| 4.4.5.3. xades:CompleteRevocationRefs element .....  | 33        |
| 4.4.5.4. xades:SigAndRefsTimeStamp element .....   | 34        |
| 4.4.5.5. xades:CertificatesValues element .....  | 34        |
| 4.4.5.6. xades:RevocationValues element .....  | 35        |
| 4.4.5.7. xades:ArchiveTimeStamp element .....  | 35        |
| 4.4.5.7.1. Zaradenie referencovaných dátových objektov pod<br>ds:Signature pre XAdES-A ..... | 36        |
| 4.4.6. xades:UnsignedDataObjectProperties element .....                                      | 37        |
| <b>4.5. Podporované kryptografické algoritmy .....</b>                                       | <b>37</b> |

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

# 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

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

## 2. Referencie

- [1] W3C/IETF Recommendation: "XML-Signature Syntax and Processing" v2002-02-12 (XMLDSIG)
- [2] ETSI TS 101 733 – CMS Advanced Electronic Signatures (CAAdES) 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] CWA 14170:2001 E – Security Requirements for Signature Creation Applications
- [22] CWA 14171:2001 E – Procedures for Electronic Signature Verification
- [23] XMLENC – XML Encryption Syntax and Processing", J. Reagle, D. Eastlake, December 2002. <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

## 3. Úvod

Cieľom tohto dokumentu je návrh profilu XAdES\_ZEP – formátu elektronického podpisu na báze špecifikácie XAdES [3] pre vytváranie a overovanie zaručeného elektronického podpisu (ZEP) nad množinou rôznych formátov (resp. typov) dát:

- XML dokumenty,
- HTML stránky,
- PDF súbory,
- RTF dokumenty,
- iné dáta (napr. grafické súbory TIFF, PNG, ...) ap.

ktoré sú definované v rámci dokumentu [16].

Špecifikácia XAdES [3] definuje formáty pre zaručené elektronické podpisy, ktoré umožňujú zachovať ich platnosť pre dlhé časové obdobia, sú v súlade so Smernicou Európskej únie o rámci spoločenstva pre elektronické podpisy [11] a obsahujú ďalšie užitočné informácie pre bežné prípady použitia elektronických podpisov.

Táto špecifikácia profilu XAdES\_ZEP definuje formáty zaručených elektronických podpisov v súlade so špecifikáciou XAdES [3] a zároveň platnou legislatívou Slovenskej republiky pre oblasť elektronického podpisu [12] – [20].

Táto špecifikácia profilu XAdES\_ZEP zároveň nevyklučuje použitie definovaného formátu elektronického podpisu aj pre vytváranie tzv. obyčajného elektronického podpisu, ktorý nespĺňa požiadavky kladené na zaručený elektronický podpis.

Pre konkrétnu business aplikáciu bude možné pomocou tohto profilu definovať komplexné dátové štruktúry, v rámci ktorých bude možné skombinovať ľubovoľné typy dát z podporovanej množiny typov. Pre každý podporovaný typ dát bude možné tiež definovať doplňujúce verifikačné dáta (napr. XML schému a XML transformáciu pre XML dokumenty ap.), ktoré môžu byť potrebné z dôvodu naplnenia ďalších legislatívnych, funkcionálnych alebo bezpečnostných požiadaviek.

Aplikácia SCA pre vytvorenie elektronického podpisu bude môcť pomocou samostatných komponentov (pre jednotlivé formáty, resp. typy dát) pripraviť na podpis a zobrazit' používateľovi pred vytvorením podpisu všetky podpisované dátové objekty. Aplikácia SVA overenie elektronického podpisu bude pomocou rovnakého mechanizmu schopná overiť platnosť všetkých referencií v rámci overovaného elektronického podpisu, prípadne platnosť špeciálnych verifikačných dát pre každý typ aplikačných dát.

Cieľom návrhu tohto formátu podpisu je:

- podpora komponentovej architektúry aplikácií pre vytváranie a overovanie ZEP, ktorá bude umožňovať variabilitu vytvárania/overovania ZEP nad rôznymi dátovými štruktúrami,

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

- umožniť definovanie komplexných dátových štruktúr, obsahujúcich objekty rôznych formátov a typov, nad ktorými bude možné vytvárať ZEP,
- definovať tie atribúty ZEP, ktoré sú spoločné pre rôzne typy aplikácií a podpisovanie/overovanie ktorých je možné riešiť v rámci jadra (core) aplikácií pre vytváranie/overovanie ZEP,
- umožniť pripojenie podpisového certifikátu, referencie podpisovej politiky, časových pečiatok a validačných údajov (CA certifikáty, CRL) k samotnej štruktúre ZEP za účelom dlhodobého overenia ZEP,
- umožniť oddelenie spracovania samotného jadra štruktúry formátu ZEP (t.j. core validation samotného podpisu) od spracovania potenciálne dôverných aplikačných dát (dokumentov zmlúv, daňových priznaní apod.) na strane overovateľa ZEP,
- optimalizácia veľkosti dát, ktoré musia byť zahrnuté do štruktúry formátu podpisu a prenášané spolu so samotným podpisom (ds:Signature element) medzi jednotlivými komponentmi systému na strane overovateľa (vhodné pri potrebe spracovávaní objemovo veľkých dát – rádovo MB.)

Navrhovaný formát podpisu vychádza a je v súlade s nasledujúcimi špecifikáciami a dokumentmi:

- XML-Signature Syntax and Processing [1],
- XAdES – XML Advanced Electronic Signature [3],
- Smernica Európskeho únie o rámci spoločenstva pre elektronické podpisy [11],
- zákon Slovenskej republiky o elektronickom podpise a príslušné vyhlášky a usmernenia NBÚ SR [12].

V rámci tejto koncepcie návrhu formátu ZEP je definovaný profil XAdES\_ZEP všeobecného formátu XAdES (a zároveň XML Signature), ktorého cieľom je naplnenie ďalších požiadaviek (legislatívnych a technologických), ktoré sú kladené na aplikácie pre vytváranie a overovanie ZEP.

Tento profil nenahrádza špecifikácie XML Signature [1] a XAdES [3] ani príslušné legislatívne predpisy Slovenskej republiky. Implementátor tohto profilu musí byť oboznámený s uvedenými špecifikáciami a legislatívnymi predpismi pre ZEP, z ktorých tento profil vychádza.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

## 4. Špecifikácia profilu XAdES\_ZEP

Špecifikácia formátu elektronického podpisu XAdES vychádza zo špecifikácie XML-Signature Syntax and Processing, ktorá poskytuje základnú funkcionálnu pre elektronické podpisovanie viacerých dátových objektov.

Základná štruktúra XML Signature (XMLDSIG) je popísaná nasledovne:

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
      (<Transforms>)?
      <DigestMethod>
      <DigestValue>
    </Reference>)+
  </SignedInfo>
  <SignatureValue>
    (<KeyInfo>)?
    (<Object ID?>)*
</Signature>
```

Elektronický podpis je zviazaný s podpísanými dátovými objektami pomocou URI referencií. Základná štruktúra XML Signature môže byť:

- enveloping – podpis je vytvorený nad dátovými objektami, ktoré sa nachádzajú v rámci XML štruktúry podpisu (teda pod ds:Signature elementom),
- enveloped – podpis je vytvorený nad dátovými objektami, ktoré obalujú XML štruktúru podpisu (t.j. ds:Signature element),
- detached – podpis je vytvorený nad objektami, ktoré sú externé vzhľadom k ds:Signature elementu (napr. externé súbory, sibling XML štruktúry).

Špecifikácia XML Signature obsahuje povinné časti (mandatory requirements), zároveň však poskytuje pre implementátorov niekoľko stupňov voľnosti (optional requirements).

Špecifikácia formátu XAdES je rozšírením XML Signature, pričom:

- špecifikuje XML schémy pre definíciu ďalších XML elementov, ktoré dopĺňajú základnú XMLDSIG štruktúru o ďalšie (kvalifikujúce) informácie, potrebné pre naplnenie požiadaviek, ako napr. zabezpečenie dlhotrvajúcej overiteľnosti ZEP,
- definuje mechanizmy pre zahrnutie uvedených informácií do ZEP,
- špecifikuje pokročilé formáty elektronických podpisov na báze XML umožňujúce dlhotrvajúcu overiteľnosť (v rámci bežných use casov),
- definuje množinu požiadaviek pre vyhodnotenie súladu so špecifikáciou XAdES.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

XAdES pridáva k základnej štruktúre XMLDSIG nový objekt typu ds:Object, ktorý obsahuje uvedené kvalifikujúce informácie (xades:QualifyingProperties). Tieto informácie sú:

- podpísané vlastnosti podpisu – informácie kvalifikujúce samotný elektronický podpis (čas vytvorenia, referencia podpisového certifikátu ap.),
- podpísané vlastnosti dátových objektov – informácie kvalifikujúce podpísané dátové objekty (napr. formát, resp. typ dát),
- nepodpísané vlastnosti podpisu – informácie kvalifikujúce samotný elektronický podpis, ktoré ale nie sú zahrnuté do elektronického podpisu, najmä validačné údaje umožňujúce zabezpečiť dlhotrvajúcu overiteľnosť elektronického podpisu,
- nepodpísané vlastnosti dátových objektov – informácie kvalifikujúce podpísané dátové objekty, ktoré ale nie sú zahrnuté do elektronického podpisu.

Základná štruktúra formátu elektronického podpisu XAdES je popísaná nasledovne:



|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

```

</SignedProperties>
<UnsignedProperties>
  </UnsignedSignatureProperties>
  (CounterSignature)*- - - - - +
  (SignatureTimeStamp)*- - - - - +
  (CompleteCertificateRefs)?
  (CompleteRevocationRefs)?
  (AttributeCertificateRefs)?
  (AttributeRevocationRefs)? - - - - - +
  ((SigAndRefsTimeStamp)* |
  (RefsOnlyTimeStamp)*)? - - - - - +
  (CertificatesValues)
  (RevocationValues)
  (AttrAuthoritiesCertValues)?
  (AttributeRevocationValues)?- - - - - ++
  (ArchiveTimeStamp)+
</UnsignedSignatureProperties>- - - - - +
</UnsignedProperties>
</QualifyingProperties>
</ds:Object>
</ds:Signature>- - - - - +
XAdES-BES (EPES)
XAdES-T
XAdES-C
XAdES-X
XAdES-X-L
XAdES-A

```

Špecifikácia XAdES opäť obsahuje povinné časti (mandatory requirements), zároveň však poskytuje pre implementátorov niekoľko stupňov voľnosti (optional requirements).

V tejto kapitole je popísaný profil XAdES\_ZEP formátu zaručeného elektronického podpisu na báze špecifikácií XML Signature a XAdES.

## 4.1. Podporované pokročilé formy XAdES

V rámci profilu XAdES\_ZEP sú podporované nasledujúce pokročilé formy XML elektronických podpisov:

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

**XAdES-EPES** – rozširuje základnú štruktúru XML Signature o informáciu o čase vzniku ZEP, o explicitnú podpísanú referenciu podpisovej politiky a podpísané informácie o typoch a formátoch podpísaných dátových objektov,

**XAdES-T** – rozširuje XAdES-EPES o časovú pečiatku, ktorá je zviazaná s hodnotou elektronického podpisu a takto poskytuje dôveryhodný čas existencie elektronického podpisu a ochranu proti jeho odmietnutiu alebo neuznaniu (repudiation),

**XAdES-X typ 1** – rozširuje XAdES-T o referencie na množinu validačných dát umožňujúcich overenie elektronického podpisu, t.j. referencie na certifikáty z certifikačnej cesty pre podpisový certifikát a referencie na príslušné informácie o revokácii certifikátov (CRL) a element `xades:SigAndRefsTimeStamp`, ktorý obsahuje časovú pečiatku chrániacu integritu ZEP, časovej pečiatky pre ZEP a referencií na množinu validačných dát,

**XAdES-A** – umožňuje vytvoriť archívny elektronický podpis a tak zabezpečiť jeho ochranu pred hrozbou oslabenia použitých kryptografických funkcií, prípadne pred hrozbou expirácie alebo zneplatnenia niektorého certifikátu z certifikačnej cesty.

## 4.2. Štruktúra podpisu

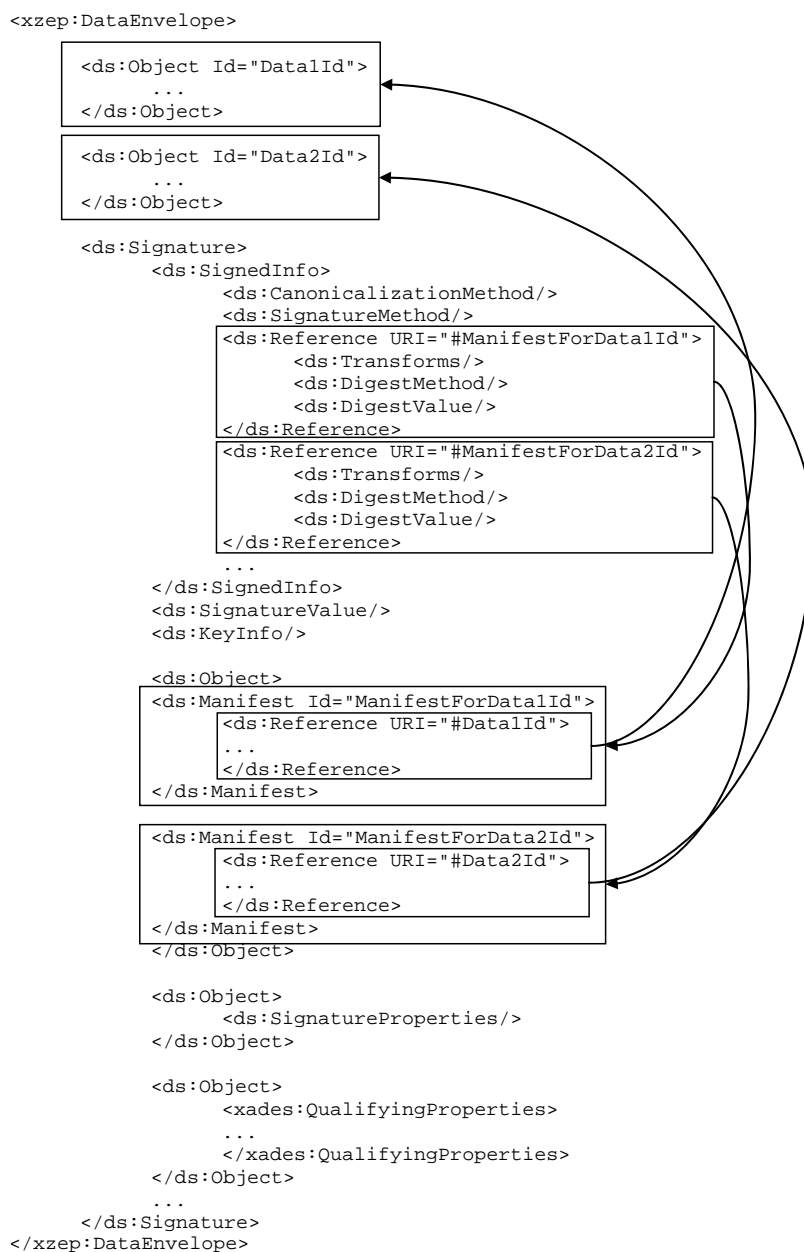
Podporovaný typ štruktúry podpisu v rámci profilu XAdES\_ZEP je:

- **detached** – pre formáty XAdES-EPES, XAdES-T a XAdES-X type 1, t.j. podpísané dátové objekty sú uložené mimo samotnej štruktúry XML Signature (ako sibling elementy v rámci nadradeného XML dokumentu – tzv. dátovej obálky, pozri kapitolu 4.2.1),
- **enveloping** – pre formát XAdES-A, t.j. všetky podpísané dátové objekty a referencované verifikačné údaje pre dátové objekty sú uložené ako *child* elementy v rámci samotnej štruktúry XML Signature<sup>1</sup>.

Podporované typy štruktúr elektronického podpisu v rámci profilu XAdES\_ZEP sú ilustrované na nasledujúcich obrázkoch. Popis (profil) jednotlivých elementov je uvedený v nasledujúcom texte.

<sup>1</sup> Účelom presunu podpísaných dátových objektov do štruktúry XML Signature je, aby aj tieto objekty (nielen referencie na ne) boli zaradené do výpočtu archívnej časovej pečiatky (pozri XAdES [3], kapitola 7.7).

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |



Obr. 1 Príklad *detached* štruktúry podpisu.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |



Obr. 2 Príklad *enveloping* štruktúry podpisu.

#### 4.2.1. Dátová obálka

XML formát je považovaný za najvhodnejšieho kandidáta pre zabezpečenie prenosu štruktúrovaných dát medzi subjektami v rámci elektronickej komunikácie. V rámci jednej elektronickej transakcie môžu byť pomocou XML prenášané dokonca komplexné dátové štruktúry, pozostávajúce z dátových objektov rôznych typov.

- XML dokumentov,

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

- PDF dokumentov,
- RTF dokumentov,
- iných dát (napr. grafických súborov TIFF, PNG ap.)

Tieto dátové objekty môže byť navyše potrebné opatriť zaručeným elektronickým podpisom z dôvodu zabezpečenia:

- integrity prenášaných dát,
- neodmietnuteľnosti pôvodu (autorstva) dát.

Vhodným riešením pre prenos takýchto komplexných dátových štruktúr je ich zabalenie do tzv. dátovej obálky. Jednotlivé súčasti tejto štruktúry môžu byť potom u odosielateľa a prijímateľa spracovávané samostatnými modulmi na základe špecifických procesných, aplikačných, legislatívnych alebo bezpečnostných požiadaviek.

Pre dátovú obálku elektronického podpisu boli identifikované nasledujúce požiadavky:

- potreba definovať obálku pre vytvorenie elektronického podpisu nad množinou dátových objektov rôznych formátov,
- potreba identifikovať profil a obsah obálky elektronického podpisu na aplikačnej úrovni,
- efektívne uloženie podpísaných dátových objektov (dokumentov) v rámci dátovej obálky,
- možnosť pripojiť k obálke elektronického podpisu ďalšie sprievodné dáta (XML štruktúry) pre potreby aplikačnej úrovne.

V rámci profilu XAdES\_ZEP sú stanovené nasledujúce požiadavky na štruktúru dátovej obálky:

- musí obsahovať ds:Signature element – t.j. pripojený elektronický podpis,
- v prípade *detached* štruktúry elektronického podpisu musí obsahovať všetky dátové objekty referencované z pripojeného elektronického podpisu zabalené v rámci príslušných ds:Object elementov,
- koreňový element musí obsahovať atribút `xmlns:xzep="http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1"`,
- koreňový element musí obsahovať atribút `xmlns:ds="http://www.w3.org/2000/09/xmldsig#"`.

Na strane spracovateľa elektronickej transakcie je možné jednotlivé časti dát v rámci dátovej obálky preskupiť tak, aby boli zohľadnené príslušné procesné, aplikačné alebo bezpečnostné požiadavky.<sup>2</sup>

Časť XML schémy profilu XAdES\_ZEP pre štruktúru dátovej obálky je nasledovná:

<sup>2</sup> Napríklad presun štruktúr dátových objektov pod ds:Signature element v prípade vytvárania archívnej formy elektronického podpisu XAdES-A.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

```
<?xml version="1.0"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xzep="http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  targetNamespace="http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1"
  version="1.1"
  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="DataEnvelope" type="xzep:DataEnvelopeType" />
<xsd:complexType name="DataEnvelopeType">
  <xsd:sequence>
    <xsd:element ref="ds:Object" minOccurs="0"
      maxOccurs="unbounded" />
    <xsd:element ref="ds:Signature" />
  </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>
```

Dátová obálka formátu podpisu XAdES\_ZEP teda obsahuje:

- sekvenciu ds:Object elementov pre jednotlivé podpísané dátové objekty,
- element ds:Signature pre vytvorený elektronický podpis,
- nepovinné atribúty:
  - ⇒ URI – obsahuje identifikátor, ktorý identifikuje profil a obsah obálky elektronického podpisu na aplikačnej úrovni (mal by byť definovaný v rámci príslušného procesu špecifikácie dátových štruktúr na aplikačnej úrovni),
  - ⇒ Id – jednoznačný identifikátor inštancie vytvorenej dátovej štruktúry elektronického podpisu,
  - ⇒ Description – string, obsahuje popis inštancie alebo profilu vytvoreného elektronického podpisu.

Žiadne ďalšie požiadavky na štruktúru alebo obsah dátovej obálky nie sú v rámci profilu XAdES\_ZEP stanovené.

#### 4.2.2. ds:Signature element

ds:Signature element je koreňový element XML Signature a XAdES. ds:Signature element musí mať nasledujúce atribúty:

- xmlns:ds = "<http://www.w3.org/2000/09/xmldsig#>" – namespace pre XML Signature elementy,

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

- Id – ds:Signature element je referencovaný z elementu xades:QualifyingProperties, atribút Target.

ds:Signature element musí obsahovať nasledujúce elementy:

- ds:SignedInfo,
- ds:SignatureValue,
- ds:KeyInfo,
- element typu ds:Object pre štruktúru ds:SignatureProperties,
- element typu ds:Object pre štruktúru xades:QualifyingProperties,
- element typu ds:Object pre ds:Manifest elementy.

Pre formát XAdES-A musí tiež obsahovať elementy typu ds:Object pre všetky podpísané dátové objekty, ktoré sú referencované z ds:Manifest elementov alebo z objektov pre verifikačné dáta pre dané dátové objekty.

### 4.2.3. ds:Manifest elementy

Referencie podpísaných dátových objektov a objektov s verifikačnými dátami pre dátové objekty z elementu ds:SignedInfo musia byť realizované prostredníctvom ds:Manifest elementov, ktoré musia byť umiestnené v rámci ds:Signature do jedného spoločného ds:Object elementu.

Overenie referencií v ds:SignedInfo je potrebné vykonať pri každom vyhodnocovaní platnosti elektronického podpisu (predbežné, úplné<sup>3</sup>) v rámci tzv. *core validation*,<sup>4</sup> čo zahŕňa:

- opakovaný prenos všetkých referencovaných objektov v rámci parametrov,
- opakovaný výpočet digitálnych odtlačkov všetkých referencovaných objektov.

ds:Manifest element obsahuje zoznam referencií na podpísané dátové objekty. Overenie týchto referencií nie je zahrnuté do *core validation*, čiže je možné ho vykonať len raz, napr. pri predbežnom overení elektronického podpisu.

Referencie podpisovaných dátových pomocou ds:Manifest elementov teda umožňujú:

- oddelenie spracovania samotného jadra štruktúry formátu XAdES\_ZEP (*core validation*) od spracovania potenciálne dôverných aplikačných dát (dokumentov zmlúv, daňových priznaní apod.) na strane overovateľa ZEP,
- optimalizáciu veľkosti dát, ktoré musia byť zahrnuté do štruktúry formátu podpisu a prenášané spolu so samotným podpisom (ds:Signature element) medzi jednotlivými komponentmi systému na strane overovateľa.

<sup>3</sup> Každý zaručený elektronický podpis je spravidla potrebné vyhodnocovať na niekoľko krát, než je možné zhromaždiť všetky potrebné validačné údaje, ktoré sú potrebné pre jeho úplné overenie.

<sup>4</sup> Pozri dokument [1].

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

V rámci tohto profilu XAdES\_ZEP nie je podporované priame referencovanie podpísaných dátových objektov z elementu ds:SignedInfo.<sup>5</sup> Všetky referencie vyskytujúce sa v rámci štruktúry XAdES\_ZEP musia byť vytvárané a overované pomocou komponentov certifikovanej SCVA aplikácie.

Podrobnejšia špecifikácia profilu ds:Manifest elementov v rámci profilu XAdES\_ZEP je uvedená v kapitole 4.3.4.

#### 4.2.4. Dátové objekty

Každý podpísaný dátový objekt musí byť zabalený v rámci elementu ds:Object, ktorý musí obsahovať atribút:

- Id – ds:Object je referencovaný z príslušného ds:Manifest elementu v rámci ds:Signature, prípadne z príslušného dátového objektu s verifikačnými údajmi (ak sú požadované).

Koreňový element obalujúci samotný dátový objekt musí obsahovať atribút:

- xmlns – namespace pre elementy použité v rámci dátového objektu.

Žiadne ďalšie požiadavky na štruktúru alebo obsah podpísaných dátových objektov nie sú v rámci profilu XAdES\_ZEP stanovené.

Ďalšie požiadavky na štruktúru alebo obsah dátových objektov pre konkrétny dátový typ (XML, PDF, RTF apod.) môžu byť stanovené v rámci príslušných samostatných dokumentov, ktoré tvoria prílohy tohto profilu.

##### 4.2.4.1. Dátové objekty s verifikačnými údajmi

Pre niektoré typy dátových objektov môžu byť definované bezpečnostné požiadavky, ktoré nie je možné naplniť pomocou štruktúr, definovaných v rámci špecifikácií XML Signature alebo XAdES. Preto pre niektoré typy dátových objektov môže vzniknúť potreba doplnenia týchto dátových objektov o verifikačné údaje, reprezentované ako podpísané atribúty, ktoré bližšie určujú dátový objekt, prípadne spôsob jeho vytvorenia alebo spracovania na strane podpisovateľa, resp. overovateľa.

Tieto verifikačné údaje môžu byť zhromaždené v rámci samostatnej XML štruktúry, ktorá môže byť podpísaná pri vytváraní štruktúry elektronického podpisu ako ďalší dátový objekt. V rámci tejto štruktúry je však potrebné identifikovať, ku ktorému dátovému objektu sa dané verifikačné údaje vzťahujú pomocou referencie príslušného dátového objektu.

Každý podpísaný dátový objekt s verifikačnými údajmi musí byť zabalený v rámci elementu ds:Object, ktorý musí obsahovať atribút:

<sup>5</sup> Objekty, ktoré sú referencované z Manifest elementov, nie sú podľa [ref\_XAdES, kapitola 7.7] zahrnuté do výpočtu odtlačku pri vytváraní archívnej časovej pečiatky. Tzn. že obsah takto referencovaných objektov by nebol chránený časovou pečaťou pre prípad oslabenia kryptografie použitej v rámci referencie objektu z Manifest elementu. Preto pri vytváraní XAdES-A je potrebné všetky objekty externé voči Signature elementu presunúť pod Signature element.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

- Id – ds:Object je referencovaný z príslušného ds:Manifest elementu v rámci ds:Signature,

Koreňový element obaľujúci samotný dátový objekt s verifikačnými údajmi musí byť v príslušnej XML schéme definovaný tak, že obsahuje povinné atribúty:

- xmlns – namespace pre elementy použité v rámci dátového objektu s verifikačnými údajmi,
- DataTarget – URI dátového objektu, ku ktorému sa vzťahujú verifikačné údaje.

Príslušná XML schéma pre dátový objekt musí teda pre koreňový element obsahovať nasledujúcu definíciu DataTarget atribútu:

```
<xsd:attribute name="DataTarget" type="xsd:anyURI" use="required"/>
```

Žiadne ďalšie požiadavky na štruktúru alebo obsah podpísaných dátových objektov s verifikačnými údajmi nie sú v rámci profilu XAdES\_ZEP stanovené.

Ďalšie požiadavky na štruktúru alebo obsah dátových objektov s verifikačnými údajmi pre konkrétny dátový typ (XML, PDF, RTF apod.) môžu byť stanovené v rámci príslušných samostatných dokumentov, ktoré tvoria prílohy tohto profilu.

#### 4.2.5. ds:SignatureProperties element

ds:SignatureProperties element môže podľa špecifikácie XML Signature [1] obsahovať doplňujúce informácie, týkajúce sa vytvoreného elektronického podpisu, napr. informácie o použítom kryptografickom hardware, verzii formátu elektronického podpisu apod. Tento element musí byť v rámci štruktúry XML Signature uložený v ds:Object elemente. Podpísanie v ňom uložených informácií podpisovateľom je možné podľa dokumentu [1] zabezpečiť pomocou referencie z elementu ds:SignedInfo.

V rámci profilu XAdES\_ZEP musí existovať práve jeden element ds:SignatureProperties, ktorý musí byť zabalený v samostatnom ds:Object elemente.

Element ds:SignatureProperties musí obsahovať atribút:

- Id – element ds:SignatureProperties musí byť referencovaný z príslušného ds:Reference elementu v rámci ds:SignedInfo.

V rámci elementu ds:SignatureProperties musia existovať ds:SignatureProperty elementy pre nasledujúce informácie:

- xzep:SignatureVersion – obsahuje identifikáciu verzie formátu elektronického podpisu podľa profilu XAdES\_ZEP,
- xzep:ProductInfos – obsahuje identifikáciu produktu (a všetkých jeho komponentov), pomocou ktorého bola vytvorená daná štruktúra elektronického podpisu.

Každý ds:SignatureProperty element musí obsahovať atribút:

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

- Target – URI referencia na Id atribút príslušného ds:Signature elementu.

Časť XML schémy profilu XAdES\_ZEP pre element xzep:SignatureVersion je nasledujúca:

```
<xsd:element name="SignatureVersion" type="xsd:anyURI" />
```

Časť XML schémy profilu XAdES\_ZEP pre element xzep:ProductInfos je nasledujúca:

```
<xsd:element name="ProductInfos" type="xzep:ProductInfosType" />
<xsd:complexType name="ProductInfosType">
  <xsd:sequence>
    <xsd:element ref="xzep:ProductInfo" maxOccurs="unbounded" />
  </xsd:sequence>
</xsd:complexType>

<xsd:element name="ProductInfo" type="xzep:ProductInfoType" />
<xsd:complexType name="ProductInfoType">
  <xsd:sequence>
    <xsd:element name="ProductName" type="xsd:string" />
    <xsd:element name="ProductVersion" type="xsd:string" />
  </xsd:sequence>
</xsd:complexType>
```

## 4.2.6. XML namespaces

Vzhľadom k tomu, že výsledná štruktúra podpisu v rámci dátovej obálky môže zahŕňať elementy a atribúty z rôznych XML štruktúr, je potrebné vyriešiť jednoznačnosť ich názvov.

xzep:DataEnvelope element musí mať špecifikovaný namespace:

- xmlns:xzep = "[http://www.ditec.sk/ep/signature\\_formats/xades\\_zep/v1.1](http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1)"

pričom všetky použité elementy musia mať prefix xzep.

ds:Signature element musí mať špecifikovaný namespace:

- xmlns:ds = "<http://www.w3.org/2000/09/xmldsig#>"

pričom všetky použité elementy musia mať prefix ds

xades:QualifyingProperties element musí mať špecifikované namespaces:

- xmlns:xades = "<http://uri.etsi.org/01903/v1.3.2#>"
- xmlns:ds = "<http://www.w3.org/2000/09/xmldsig#>"

pričom všetky použité elementy z týchto namespaces musia mať príslušný prefix ds alebo xades.

Podpísané dátové objekty (a podpísané objekty s verifikačnými dátami pre dátové objekty) musia mať takisto definovaný atribút namespace (pozri kapitolu 4.2.4), pričom nepovinné prefixovanie názvov elementov zabezpečuje v tomto prípade aplikačná úroveň.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

## 4.2.7. Id atribúty

Id pre jednotlivé elementy v rámci štruktúry elektronického podpisu musia byť jedinečné pre danú inštanciu štruktúry zaručeného elektronického podpisu podľa profilu XAdES\_ZEP. Aplikačná úroveň môže vyžadovať jednoznačnosť Id atribútov v širšom meradle, preto tento profil nestanovuje žiadne ďalšie požiadavky alebo obmedzenia na obsah alebo syntax Id atribútov.

## 4.2.8. Kódovanie XML

Všetky XML štruktúry v rámci inštancie štruktúry zaručeného elektronického podpisu podľa profilu XAdES\_ZEP musia byť kódované pomocou UTF-8.

```
<?xml version="1.0" encoding="UTF-8" ?>
```

## 4.3. Profil časti XML Signature

### 4.3.1. ds:SignedInfo element

ds:SignedInfo element zahŕňa:

- ds:CanonicalizationMethod element – referenciu kanonikalizačného algoritmu,
- ds:SignatureMethod element – referenciu použitej podpisovej schémy,
- ds:Reference elementy – referencie jednotlivých podpisovaných dátových objektov,

V rámci zoznamu referencií v ds:SignedInfo musí byť uvedená referencia na ds:KeyInfo element, pričom atribút Type musí mať hodnotu:

- Type = "<http://www.w3.org/2000/09/xmldsig#Object>".

V rámci zoznamu referencií v ds:SignedInfo musí byť uvedená referencia na ds:SignatureProperties element, pričom atribút Type musí mať hodnotu::

- Type = "<http://www.w3.org/2000/09/xmldsig#SignatureProperties>".

V rámci zoznamu referencií v ds:SignedInfo musí byť uvedená referencia na xades:SignedProperties element, pričom atribút Type musí mať hodnotu::

- Type = "<http://uri.etsi.org/01903#SignedProperties>".

Všetky ostatné referencie v rámci ds:SignedInfo musia byť referenciami na ds:Manifest elementy a musia mať hodnotu atribútu Type:

- Type = "<http://www.w3.org/2000/09/xmldsig#Manifest>".

#### 4.3.1.1. ds:CanonicalizationMethod element

ds:CanonicalizationMethod element špecifikuje kanonikalizačný algoritmus, ktorý je aplikovaný na ds:SignedInfo element pred vytvorením elektronického podpisu.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

V rámci tohto profilu XAdES\_ZEP je jediný podporovaný kanonikalizačný algoritmus pre kanonikalizáciu ds:SignedInfo požadovaný Canonical XML (omits comments) <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>.

ds:CanonicalizationMethod element musí obsahovať atribút:

- Algorithm = "<http://www.w3.org/TR/2001/REC-xml-c14n-20010315>"

#### Príklad:

```
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

#### 4.3.1.2. ds:SignatureMethod element

ds:SignatureMethod element špecifikuje algoritmus, ktorý je použitý pri vytváraní a overovaní elektronického podpisu, spolu so všetkými ďalšími použitými kryptografickými operáciami (digest, padding apod.), t.j. podpisovú schému.

ds:SignatureMethod element musí obsahovať atribút:

- Algorithm = použitá podpisová schéma pre elektronický podpis.

Podporované podpisové schémy pre elektronický podpis sú špecifikované v kapitole 4.5.

#### Príklad:

```
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
```

#### 4.3.1.3. ds:Reference elementy v ds:SignedInfo

Každý ds:Reference element obsahuje nasledujúce elementy a atribúty:

- elementy:
  - ⇒ ds:Transforms – transformácie, ktoré je potrebné aplikovať na podpisovaný objekt pred vytvorením jeho odtlačku (digest),
  - ⇒ ds:DigestMethod – identifikácia algoritmu pre výpočet odtlačku,
  - ⇒ ds:DigestValue – hodnota odtlačku podpisovaného objektu,
- atribúty:
  - ⇒ Id – ds:Reference element je referencovaný z elementu xades:DataObjectType,
  - ⇒ Type – typ referencovaného podpisovaného objektu,
  - ⇒ URI – referencia manifestu podpisovaného objektu.

Referencia elementu ds:KeyInfo musí mať hodnotu atribútu Type:

Type = "<http://www.w3.org/2000/09/xmldsig#Object>".

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

Referencia elementu ds:SignatureProperties musí mať hodnotu atribútu Type:

- Type = "<http://www.w3.org/2000/09/xmldsig#SignatureProperties>".

Referencia elementu xades:SignedProperties musí mať hodnotu atribútu Type:

Type = "<http://uri.etsi.org/01903#SignedProperties>".

Všetky ostatné podpísané objekty musia mať hodnotu atribútu Type:

Type = "<http://www.w3.org/2000/09/xmldsig#Manifest>".

To znamená, že všetky podpisované dátové objekty sú referencované nepriamo prostredníctvom ds:Manifest elementov (pozri kapitolu 4.3.4).

URI atribút obsahuje referenciu podpísaného ds:Manifest elementu.

#### 4.3.1.3.1. ds:Transforms element

ds:Transforms element obsahuje zoznam transformácií, ktoré je potrebné aplikovať na referencovaný ds:Manifest element pred vytvorením jeho odtlačku. Tieto transformácie popisujú ako podpisovateľ získal dáta pre výpočet odtlačku.

Výstup z každej transformácie slúži ako vstup pre nasledujúce transformáciu. Vstupom pre prvú transformáciu je výsledok dereferencovania príslušného URI atribútu ds:Reference elementu. Výstup z poslednej transformácie je vstup pre algoritmus pre výpočet odtlačku (ds:DigestMethod).

V rámci tohto profilu XAdES\_ZEP je podporovaná jediná transformácia ds:Manifest elementu:

- Canonicalization – Canonical XML (omits comments) <http://www.w3.org/TR/2001/REC-xml-c14n-20010315> – bude použitá, ak referencovaný objekt je komplexná XML štruktúra (ktorá však môže obsahovať aj base64 kódované dáta). Vstup je algoritmom kanonikalizovaný na kanonické XML.

Ostatné odporúčané algoritmy pre transformácie nie sú podporované z nasledujúcich dôvodov:

- base64 – referencovaný ds:Manifest neobsahuje element s base64 kódovanými dátami,
- XPath Filtering – primárny význam tejto transformácie je umožniť vynechanie určitých elementov vstupného XML dokumentu pred výpočtom príslušnej referencie, pre ktoré sú možné špecifické zmeny aj po vytvorení elektronického podpisu. Vzhľadom na požiadavky zákona [12] stanovené pre vytváranie a overovanie ZEP (najmä par. 24, odsek 5, písmeno c) nemá podpora tejto transformácie praktický význam,
- Enveloped Signature Transform – enveloped typ podpisu nie je v rámci tohto profilu XAdES\_ZEP podporovaný,
- XSLT – môže dochádzať k sémantickej zmene, navyše na rôznych platformách poskytuje odlišné výstupy (napr. odriadkovanie CRLF vs. LF apod.)

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

Vzhľadom k tomu, že v rámci jadra formátu podpisu (XML Signature) nie je vhodné riešiť špecifiká jednotlivých podporovaných dátových typov, žiadne ďalšie *user-specific* algoritmy pre transformácie nie sú podporované.

#### 4.3.1.3.2. ds:DigestMethod element

ds:DigestMethod je požadovaný element, ktorý identifikuje algoritmus výpočtu odtlačku, ktorý má byť aplikovaný na podpisovaný objekt po aplikovaní poslednej transformácie.

Podporované algoritmy pre výpočet digitálneho odtlačku sú špecifikované v kapitole 4.5.

#### 4.3.1.3.3. ds:DigestValue element

ds:DigestValue element obsahuje base64 kódovanú hodnotu odtlačku referencovaného objektu.

### 4.3.2. ds:SignatureValue element

ds:SignatureValue element obsahuje skutočnú hodnotu elektronického podpisu a musí byť kódovaný v base64.

ds:SignatureValue element musí obsahovať nasledujúce atribúty:

- Id – element ds:SignatureValue je referencovaný z elementu xades:SignatureTimeStamp.

### 4.3.3. ds:KeyInfo element

ds:KeyInfo element obsahuje referenciu podpisového certifikátu, a zároveň teda verejného kľúča, ktorý má byť použitý pre overenie ZEP. V rámci tohto profilu XAdES\_ZEP je ds:KeyInfo element povinný.

Implementovaný mechanizmus pre získanie verejného kľúča pre overenie ZEP v rámci ds:KeyInfo je element ds:X509Data<sup>6</sup>, ktorý obsahuje elementy:

- ds:X509Certificate,
- ds:X509IssuerSerial,
- ds:X509SubjectName.

ds:KeyInfo element obsahuje len referenciu podpisového certifikátu, nesmú sa v ňom nachádzať žiadne ďalšie referencie iných certifikátov alebo CRL.

ds:KeyInfo element musí obsahovať atribút:

- Id – element ds:KeyInfo je referencovaný z elementu ds:SignedInfo.

<sup>6</sup> Pozor! Aj keď špecifikácia XML Signature [1] vyžaduje: Aplikácie, ktoré sú v súlade s XML Signature musia implementovať ds:KeyValue a mali by implementovať ds:RetrievalMethod, špecifikácia XAdES [3] stanovuje iné požiadavky na ds:KeyInfo element: ds:KeyInfo element musí zahŕňať element ds:X509Data, ktorý obsahuje ds:X509Certificate. Vzhľadom k tomu, že nie je dôvod v rámci jedného elektronického podpisu referencovať verejný kľúč vzájomne redundantnými mechanizmami, tento profil vyžaduje len zahrnutie elementu ds:X509Data.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

#### 4.3.4. ds:Manifest elementy

ds:Manifest element môže vo všeobecnosti obsahovať zoznam referencií na podpísané dátové objekty. Overenie týchto referencií nie je zahrnuté do tzv. *core validation*<sup>7</sup> v rámci overenia ds:Signature. Referencie na ds:Manifest elementy z ds:SignedInfo musia byť overené v rámci *core validation* pri overovaní platnosti ZEP. Všetky referencie vyskytujúce sa v rámci štruktúry XAdES\_ZEP musia byť vytvárané a overované pomocou komponentov certifikovanej SCVA aplikácie.

V rámci inštancie profilu XAdES\_ZEP musí pre každý podpísaný dátový objekt a pre každý objekt s verifikačnými dátami pre dátový objekt existovať samostatný ds:Manifest element, ktorý obsahuje práve jednu referenciu na príslušný objekt.

ds:Manifest element musí mať povinný atribút:

- Id – ds:Manifest element je referencovaný z elementu ds:Reference v rámci elementu ds:SignedInfo.

Referencia v rámci ds:Manifest elementu musí obsahovať nasledujúce elementy a atribúty:

- elementy:
  - ⇒ ds:Transforms – transformácie, ktoré je potrebné aplikovať na podpisovaný objekt pred vytvorením jeho odtlačku (digest),
  - ⇒ ds:DigestMethod – identifikácia algoritmu pre výpočet odtlačku,
  - ⇒ ds:DigestValue – hodnota odtlačku podpisovaného objektu,
- atribúty:
  - ⇒ Type – typ podpisovaného objektu,
  - ⇒ URI – referenciu podpisovaného objektu.

Type atribút definuje typ podpisovaného objektu ako ds:Object a musí mať hodnotu:

Type = "<http://www.w3.org/2000/09/xmlsig#Object>".

URI atribút obsahuje referenciu podpisovaného dátového objektu.

Všetky ds:Manifest elementy musia byť v rámci ds:Signature umiestnené do jedného spoločného ds:Object elementu.

##### 4.3.4.1. ds:Transforms element

ds:Transforms element obsahuje zoznam transformácií, ktoré je potrebné aplikovať na podpisovaný objekt pred vytvorením jeho odtlačku. Tieto transformácie popisujú ako podpisovateľ získal dáta, pre výpočet odtlačku.

Výstup z každej transformácie slúži ako vstup pre nasledujúcu transformáciu. Vstupom pre prvú transformáciu je výsledok dereferencovania URI atribútu

<sup>7</sup> Pozri dokument [1].

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

príslušného ds:Reference elementu. Výstup z poslednej transformácie je vstup pre algoritmus pre výpočet odtlačku (ds:DigestMethod).

V rámci tohto profilu XAdES\_ZEP sú podporované len nasledujúce transformácie:

- Canonicalization – Canonical XML (omits comments) <http://www.w3.org/TR/2001/REC-xml-c14n-20010315> – bude použitá, ak referencovaný objekt je komplexná XML štruktúra (ktorá však môže obsahovať aj base64 kódované dáta). Vstup je algoritmom kanonikalizovaný na kanonické XML,
- Base64 – <http://www.w3.org/2000/09/xmlsig#base64> – bude použitá, ak referencovaný objekt obsahuje len element s base64 kódovanými dátami, pričom vstup je algoritmom dekódovaný na pôvodné binárne dáta.

Ostatné odporúčané algoritmy pre transformácie nie sú podporované z nasledujúcich dôvodov:

- XPath Filtering – primárny význam tejto transformácie je umožniť vynechanie určitých elementov vstupného XML dokumentu pred výpočtom príslušnej referencie, pre ktoré sú možné špecifické zmeny aj po vytvorení elektronického podpisu. Vzhľadom na požiadavky zákona [12] stanovené pre vytváranie a overovanie ZEP (najmä par. 24, odsek 5, písmeno c) nemá podpora tejto transformácie praktický význam,
- Enveloped Signature Transform – enveloped typ podpisu nie je v rámci tohto profilu XAdES\_ZEP podporovaný,
- XSLT – môže dochádzať k sémantickej zmene, navyše na rôznych platformách poskytuje odlišné výstupy (napr. odriadkovanie CRLF vs. LF).

Vzhľadom k tomu, že v rámci jadra formátu podpisu (XML Signature) nie je vhodné riešiť špecifiká jednotlivých podporovaných dátových typov, žiadne ďalšie *user-specific* algoritmy pre transformácie nie sú podporované.

#### 4.3.4.2. ds:DigestMethod element

ds:DigestMethod je požadovaný element, ktorý identifikuje algoritmus výpočtu odtlačku, ktorý má byť aplikovaný na podpisovaný objekt po aplikovaní poslednej transformácie.

Podporované algoritmy pre digest sú špecifikované v kapitole 4.5.

#### 4.3.4.3. ds:DigestValue element

ds:DigestValue element obsahuje base64 kódovanú hodnotu odtlačku referencovaného objektu.

### 4.4. Profil xades:QualifyingProperties

Základná štruktúra objektu pre xades:QualifyingProperties element v rámci špecifikácie XAdES je nasledujúca, pričom SCVA aplikácie môžu vytvárať pridávaním jednotlivých špecifikovaných elementov postupne pokročilejšie (advanced) formy elektronického podpisu:

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

```

<ds:Object>
  <QualifyingProperties>

    <SignedProperties>

      <SignedSignatureProperties>
        (SigningTime)?
        (SigningCertificate)?
        (SignaturePolicyIdentifier)?
        (SignatureProductionPlace)?
        (SignerRole)?
      </SignedSignatureProperties>

      <SignedDataObjectProperties>
        (DataObjectFormat)*
        (CommitmentTypeIndication)*
        (AllDataObjectsTimeStamp)*
        (IndividualDataObjectsTimeStamp)*
      </SignedDataObjectPropertiesSigned>

    </SignedProperties>

    <UnsignedProperties>

      </UnsignedSignatureProperties>
        (CounterSignature)*
        (SignatureTimeStamp)*
        (CompleteCertificateRefs)?
        (CompleteRevocationRefs)?
        (AttributeCertificateRefs)?
        (AttributeRevocationRefs)?
        ((SigAndRefsTimeStamp)*
        (RefsOnlyTimeStamp)*)?
        (CertificatesValues)
        (RevocationValues)
        (AttrAuthoritiesCertValues)?
        (AttributeRevocationValues)?
        (ArchiveTimeStamp)+
      </UnsignedSignatureProperties>

    </UnsignedProperties>

  </QualifyingProperties>

  (QualifyingPropertiesReference)*
</ds:Object>

```

XAdES teda umožňuje vo všeobecnosti rozdeliť vlastnosti, bližšie určujúce elektronický podpis, podpisovateľa a podpísané dátové objekty do viacerých xades:QualifyingProperties elementov, pričom však

- musia byť splnené obmedzenia stanovené v špecifikácii XAdES [3], kapitola 6.3,

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

- všetky xades:QualifyingProperties elementy (aj tie, ktoré obsahujú len xades:UnsignedProperties) musia cez Target atribút referencovať ds:Signature element príslušného elektronického podpisu.

V rámci elektronického podpisu podľa profilu XAdES\_ZEP musí dátový objekt ds:Object obsahovať práve jeden xades:QualifyingProperties element, ktorý v závislosti od príslušnej pokročilej formy elektronického podpisu musí obsahovať:

- nasledujúce xades:SignedProperties elementy, ktoré sa vzťahujú k samotnému podpisu, podpísaným dátovým objektom alebo objektom s verifikačnými dátami pre podpísané objekty:
  - ⇒ xades:SigningCertificate,
  - ⇒ xades:SignaturePolicyIdentifier,
  - ⇒ xades:DataObjectFormat elementy,
- nasledujúce xades:UnsignedProperties elementy, ktoré sa vzťahujú k samotnému podpisu:
  - ⇒ xades:SignatureTimeStamp,
  - ⇒ xades:CompleteCertificateRefs,
  - ⇒ xades:CompleteRevocationRefs,
  - ⇒ xades:SigAndRefsTimeStamp elementy,
  - ⇒ xades:CertificatesValues,
  - ⇒ xades:RevocationValues,
  - ⇒ xades:ArchiveTimeStamp elementy.

V nasledujúcej tabuľke je uvedený prehľad, ktoré xades:QualifyingProperties elementy musia existovať v danej podporovanej pokročilej forme XAdES v rámci profilu XAdES\_ZEP.

|            | SigningCertificate | SignaturePolicyIdentifier | DataObjectFormat | SignatureTimeStamp | CompleteCertificateRefs | CompleteRevocationRefs | SigAndRefsTimeStamp | CertificatesValues | RevocationValues | ArchiveTimeStamp |
|------------|--------------------|---------------------------|------------------|--------------------|-------------------------|------------------------|---------------------|--------------------|------------------|------------------|
| XAdES-EPES | ✓                  | ✓                         | ✓                |                    |                         |                        |                     |                    |                  |                  |
| XAdES-T    | ✓                  | ✓                         | ✓                | ✓                  |                         |                        |                     |                    |                  |                  |

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

|               | SigningCertificate | SignaturePolicyIdentifier | DataObjectFormat | SignatureTimeStamp | CompleteCertificateRefs | CompleteRevocationRefs | SigAndRefsTimeStamp | CertificatesValues | RevocationValues | ArchiveTimeStamp |
|---------------|--------------------|---------------------------|------------------|--------------------|-------------------------|------------------------|---------------------|--------------------|------------------|------------------|
| XAdES-X type1 | ✓                  | ✓                         | ✓                | ✓                  | ✓                       | ✓                      | ✓                   |                    |                  |                  |
| XAdES-A       | ✓                  | ✓                         | ✓                | ✓                  |                         |                        |                     | ✓                  | ✓                | ✓                |

V prípade, že forma XAdES-A je vytváraná z formy XAdES-T, tak elementy `xades:CompleteCertificateRefs`, `xades:CompleteRevocationRefs` a `xades:SigAndRefsTimeStamp` nemusia byť do XAdES-A doplnené.

`xades:QualifyingProperties` element musí mať nasledujúce atribúty:

- `xmlns:xades = "http://uri.etsi.org/01903/v1.3.2#"`
- `xmlns:ds = "http://www.w3.org/2000/09/xmldsig#"`
- Target – referencia na Id atribút príslušného `ds:Signature` elementu.

#### 4.4.1. `xades:SignedProperties` element

`xades:SignedProperties` element obsahuje tie vlastnosti charakterizujúce elektronický podpis alebo dáta, ktoré sú zahrnuté do vytvárania elektronického podpisu a bližšie určujú:

- samotný elektronický podpis, resp. podpisovateľa – `xades:SignedSignatureProperties` element (pozri kapitolu 4.4.3),
- podpísané dátové objekty – `xades:SignedDataObjectProperties` element (pozri kapitolu 4.4.4).

`xades:SignedProperties` element musí mať atribút:

- Id – `xades:SignedProperties` element je referencovaný z elementu `ds:Reference` v rámci elementu `ds:SignedInfo`.

#### 4.4.2. `xades:UnsignedProperties` element

`xades:UnsignedProperties` element obsahuje tie vlastnosti charakterizujúce elektronický podpis alebo dáta, ktoré NIE sú zahrnuté do vytvárania elektronického podpisu a bližšie určujú:

- samotný elektronický podpis, resp. podpisovateľa – `xades:UnsignedSignatureProperties` element (pozri kapitolu 0),

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

- podpísané dátové objekty – xades:UnsignedDataObjectProperties element (pozri kapitolu 4.4.6).

### 4.4.3. xades:SignedSignatureProperties element

Tento element obsahuje vlastnosti, ktoré bližšie určujú elektronický podpis, ktorý je referencovaný z Target atribútu elementu xades:QualifyingProperties.

V rámci profilu XAdES\_ZEP sú podporované nasledujúce elementy:

- xades:SigningTime,
- xades:SigningCertificate,
- xades:SignaturePolicyIdentifier.

#### 4.4.3.1. xades:SigningTime element

Element xades:SigningTime špecifikuje čas, kedy podpisovateľ údajne vytvoril ZEP. Použitie tohto elementu je v rámci profilu XAdES\_ZEP voliteľné.

#### 4.4.3.2. xades:SigningCertificate element

Element xades:SigningCertificate musí obsahovať jednoznačnú referenciu podpisového certifikátu (pozri [3], kapitolu 7.2.2). Podpisový certifikát musí byť navyše uložený v elemente ds:KeyInfo (pozri 4.3.3).

#### 4.4.3.3. xades:SignaturePolicyIdentifier element

Podpisová politika predstavuje množinu pravidiel pre vytváranie a overovanie elektronického podpisu a vzhľadom ku ktorej môže byť elektronický podpis vyhodnotený ako platný, resp. neplatný. Požiadavky na obsah podpisovej politiky sú dané právnym alebo obchodným kontextom, v rámci ktorého je potrebné implementovať elektronický podpis.

Podpisová politika musí byť pre účely vyhodnotenia naplnenia požiadaviek, (daných uvedeným právnym, resp. obchodným kontextom) k dispozícii v čitateľnej forme.

Pre účely automatického spracovania elektronických podpisov, tie časti podpisovej politiky, ktoré špecifikujú elektronické pravidlá pre vytváranie a overovanie elektronického podpisu, musia byť k dispozícii v počítačovo spracovateľnej forme.

Podpisová politika môže byť jednoznačne určená implicitne národnou legislatívou alebo zmluvou (ktorá uvádza, aká podpisová politika musí byť v danom kontexte použitá) alebo môže byť definovaná explicitne v rámci elektronického podpisu. V takom prípade musí mať podpisová politika jedinečný identifikátor, ktorý musí byť zviazaný s vytvoreným elektronickým podpisom. V takom prípade musí tiež pre danú explicitnú podpisovú politiku existovať práve jedna definitívna forma s jedinečnou binárne kódovanou reprezentáciou.

Profil XAdES\_ZEP vyžaduje zahrnutie explicitnej referencie podpisovej politiky do štruktúry elektronického podpisu prostredníctvom xades:SignaturePolicyIdentifier elementu.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

xades:SignaturePolicyIdentifier element musí obsahovať nasledujúci element:

- SignaturePolicyId – obsahuje elementy
  - ⇒ SigPolicyId – obsahuje OID použitej podpisovej politiky,
  - ⇒ SigPolicyHash – obsahuje špecifikáciu algoritmu pre výpočet hodnoty digitálneho odtlačku a hodnotu digitálneho odtlačku danej podpisovej politiky.

#### 4.4.4. xades:SignedDataObjectProperties element

Tento element obsahuje podpísané vlastnosti, ktoré bližšie určujú podpísané dátové objekty, prípadne objekty obsahujúce verifikačné údaje pre jednotlivé podpísané dátové objekty.

V rámci xades:SignedDataObjectProperties je podporovaný len element xades:DataObjectFormat.

##### 4.4.4.1. xades:DataObjectFormat element

xades:DataObjectFormat element poskytuje možnosť bližšie určiť formát dát podpísaného dátového objektu. V rámci profilu XAdES\_ZEP musí existovať pre každý podpísaný dátový objekt, prípadne pre každý objekt s verifikačnými údajmi pre niektorý podpísaný dátový objekt príslušný xades:DataObjectFormat element, ktorý musí obsahovať nasledujúce:

- elementy:
  - ⇒ 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,<sup>8</sup>
  - ⇒ MimeType – string, definuje MIME type podpísaného dátového objektu (napr. "application/xml", "application/pdf"),
- atribúty:
  - ⇒ ObjectReference – referencia na príslušnú ds:Reference v rámci ds:SignedInfo, ktorá korešponduje s dátovým objektom, určeným týmto xades:DataObjectFormat elementom.

V prípade potreby môže xades:DataObjectFormat element obsahovať aj element:

- Encoding – URI, definuje kódovanie podpísaného dátového objektu.<sup>9</sup>

<sup>8</sup> Odporúčame definovať jednotlivé URI tak, aby obsahovali aj informáciu o verzii (formátu) pre daný typ podpísaných dát.

<sup>9</sup> Aké kódovanie?, pozri <http://www.w3.org/Submission/2003/01/Comment>, kapitola 4.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

## 4.4.5. xades:UnsignedSignatureProperties element

### 4.4.5.1. xades:SignatureTimeStamp element

xades:SignatureTimeStamp element rozširuje XAdES-EPES formát o časovú pečiatku, ktorá je zviazaná s hodnotou elektronického podpisu ds:SignatureValue a takto poskytuje dôveryhodný čas existencie elektronického podpisu a ochranu proti jeho odmietnutiu alebo neuznaniu (repudiation).

Toto rozšírenie používa implicitný mechanizmus pre vybudovanie vstupu pre výpočet odtlačku (pozri [3], kapitola 7.3).

Pripojením xades:SignatureTimeStamp elementu k štruktúre elektronického podpisu vznikne forma XAdES-T elektronického podpisu.

xades:SignatureTimeStamp element je typu xades:XAdESTimeStampType. V rámci profilu XAdES\_ZEP musí tento element obsahovať:

- xades:EncapsulatedTimeStamp typu xades:EncapsulatedPKIDataType, ktorý obsahuje base64 kódovaný Time Stamp Token z časovej pečiatky,
- atribút Id – je referencovaný z elementu xades:ArchiveTimeStamp.

Pravidlá pre generovanie octet streamu pre výpočet digitálneho odtlačku pre ktorý bude vystavená časová pečiatka a pre overenie hodnoty odtlačku v rámci časovej pečiatky sú stanovené v [3], kapitola 7.3.

### 4.4.5.2. xades:CompleteCertificateRefs element

xades:CompleteCertificateRefs element obsahuje sekvenciu referencií na úplnú množinu CA certifikátov, ktoré boli použité na overenie platnosti elektronického podpisu, vrátane trusted root certifikátu (neobsahuje podpisový certifikát).

Jednotlivé Cert elementy v sekvencii CertRefs nemusia obsahovať URI atribúty.

xades:CompleteCertificateRefs element musí obsahovať atribút:

- Id – xades:CompleteCertificateRefs element je referencovaný z xades:ArchiveTimeStamp.

### 4.4.5.3. xades:CompleteRevocationRefs element

xades:CompleteRevocationRefs element obsahuje sekvenciu referencií na úplnú množinu CRL, ktoré boli použité na overenie platnosti elektronického podpisu, vrátane CRL pre podpisový certifikát.

Jednotlivé CRLRef elementy v sekvencii CRLRefs musia obsahovať elementy:

- DigestAlgAndValue,
- CRLIdentifierType, ktorý musí obsahovať elementy:
  - ⇒ Issuer,
  - ⇒ IssueTime,
  - ⇒ Number,

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

a nemusia obsahovať URI atribút.

xades:CompleteRevocationRefs element musí obsahovať atribút::

- Id – xades:CompleteRevocationRefs element je referencovaný z elementu xades:ArchiveTimeStamp.

#### 4.4.5.4. xades:SigAndRefsTimeStamp element

Element xades:SigAndRefsTimeStamp obsahuje časovú pečiatku, ktorá chráni integritu ZEP, časovej pečiatky pre ZEP a referencií na množinu validačných dát, ktoré boli použité na overenie platnosti elektronického podpisu. Zároveň poskytuje dôveryhodný čas existencie elektronického podpisu, pripojenej časovej pečiatky a validačných dát pre prípad kompromitácie privátneho kľúča niektorej z CA.

xades:SigAndRefsTimeStamp element je typu xades:XAdESTimeStampType. V rámci profilu XAdES\_ZEP musí tento element obsahovať:

- Include element pre xades:SignatureTimeStamp s atribútmi:
  - ⇒ URI – referencia xades:SignatureTimeStamp elementu,
  - ⇒ referencedData = "false",
- Include element pre xades:CompleteCertificateRefs s atribútmi:
  - ⇒ URI – referencia xades:CompleteCertificateRefs elementu,
  - ⇒ referencedData = "false",
- Include element pre xades:CompleteRevocationRefs s atribútmi:
  - ⇒ URI – referencia xades:CompleteRevocationRefs elementu,
  - ⇒ referencedData = "false",
- element xades:EncapsulatedTimeStamp typu xades:EncapsulatedPKIDataType, ktorý obsahuje base64 kódovaný Time Stamp Token z časovej pečiatky,
- atribút Id – je referencovaný z elementu xades:ArchiveTimeStamp.

Pravidlá pre generovanie octet streamu pre výpočet digitálneho odtlačku pre ktorý bude vystavená časová pečiatka a pre overenie hodnoty odtlačku v rámci časovej pečiatky sú stanovené v [3], kapitola 7.5.1.

#### 4.4.5.5. xades:CertificatesValues element

xades:CertificatesValues element musí obsahovať množinu všetkých certifikátov, ktorých referencie sa nachádzajú v xades:CompleteCertificateRefs elemente (t.j. celú certifikačnú cestu okrem podpisového certifikátu, ktorého obsah sa nachádza v ds:KeyInfo elemente).

xades:CertificatesValues element musí obsahovať atribút:

- Id – je referencovaný z elementu xades:ArchiveTimeStamp.

Každý xades:EncapsulatedX509Certificate element obsahuje base64 kódovanú reprezentáciu jedného z X.509 certifikátov v DER kódovaní.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

#### 4.4.5.6. xades:RevocationValues element

xades:RevocationValues element musí obsahovať množinu všetkých CRL, ktorých referencie sa nachádzajú v xades:CompleteRevocationRefs elemente.

xades:RevocationValues element musí obsahovať atribút:

- Id – je referencovaný z elementu xades:ArchiveTimeStamp.

Každý z EncapsulatedCRLValue elementov musí obsahovať base64 kódovanú reprezentáciu jedného z X.509 CRL v DER kódovaní.

#### 4.4.5.7. xades:ArchiveTimeStamp element

xades:ArchiveTimeStamp element slúži na pripojenie archívnej časovej pečiatky k štruktúre elektronického podpisu, ktorá je zviazaná:

- s hodnotou elektronického podpisu,
  - podpísanými dátovými objektami,
  - referenciami všetkých validačných údajov
  - a obsahom týchto validačných údajov,
- pričom takto poskytuje ochranu týchto dát proti:

- odmietnutiu alebo neuznaniu (repudiation),
- zneplatneniu (revokácii) niektorého z použitých privátnych kľúčov,
- oslabeniu použitých kryptografických algoritmov.

Archívne pečiatky môžu byť opakovane pridávané do štruktúry elektronického podpisu. Nová časová pečiatka vždy zahrnie spolu s vyššie uvedenými dátami aj predchádzajúcu časovú pečiatku, čím vytvárajú vnorenú štruktúru. Tento proces musí byť iterovaný vždy predtým, ako použité kryptografické algoritmy pre predchádzajúcu pečiatku prestanú byť považované za bezpečné.

Pripojením xades:ArchiveTimeStamp elementu k štruktúre elektronického podpisu vznikne forma XAdES-A – archívny elektronický podpis.

xades:ArchiveTimeStamp element je typu xades:XAdESTimeStampType. V rámci profilu XAdES\_ZEP musí tento element obsahovať:

- Include element pre xades:SignatureTimeStamp s atribútmi:
  - ⇒ URI – referencia xades:SignatureTimeStamp elementu,
  - ⇒ referencedData = "false",
- Include element pre xades:CompleteCertificateRefs<sup>10</sup> s atribútmi:
  - ⇒ URI – referencia xades:CompleteCertificateRefs elementu,
  - ⇒ referencedData = "false",
- Include element pre xades:CompleteRevocationRefs<sup>11</sup> s atribútmi:
  - ⇒ URI – referencia xades:CompleteRevocationRefs elementu,

<sup>10</sup> Len ak je tento element prítomný.

<sup>11</sup> Len ak je tento element prítomný.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

- ⇒ referencedData = "false",
- Include element pre xades:SigAndRefsTimeStamp<sup>12</sup> s atribútmi:
  - ⇒ URI – referencia xades:SigAndRefsTimeStamp elementu,
  - ⇒ referencedData = "false",
- Include element pre xades:CertificateValues s atribútmi:
  - ⇒ URI – referencia xades:CertificateValues elementu,
  - ⇒ referencedData = "false",
- Include element pre xades:RevocationValues s atribútmi:
  - ⇒ URI – referencia xades:RevocationValues elementu,
  - ⇒ referencedData = "false",
- Include element pre ľubovoľný existujúci xades:ArchiveTimeStamp element s atribútmi:
  - ⇒ URI – referencia xades:ArchiveTimeStamp elementu,
  - ⇒ referencedData = "false",
- element xades:EncapsulatedTimeStamp typu xades:EncapsulatedPKIDataType, ktorý obsahuje base64 kódovaný Time Stamp Token z časovej pečiatky,
- atribút Id – xades:ArchiveTimeStamp element bude referencovaný z nasledujúcej xades:ArchiveTimeStamp.

Pravidlá pre generovanie octet streamu pre výpočet digitálneho odtlačku pre ktorý bude vystavená časová pečiatka a pre overenie hodnoty odtlačku v rámci časovej pečiatky sú stanovené v [3], kapitola 7.7.

#### 4.4.5.7.1. Zaradenie referencovaných dátových objektov pod ds:Signature pre XAdES-A

V rámci profilu XAdES\_ZEP musia byť pred vytvorením formy XAdES-A zahrnuté pod ds:Signature element nasledujúce objekty:

- 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 (napr. obsahujúceho referencie verifikačných údajov pre XML, t.j. referenciu XML schémy a XML transformácie).

Jednotlivé dátové objekty ds:Object musia byť zaradené pod ds:Signature element v takom poradí, v akom sú referencované v rámci ds:SignedInfo príslušné ds:Manifest elementy.

Každý externý objekt, referencovaný pomocou ds:Reference elementu z niektorého z podpísaných dátových objektov musí byť zaradený do

<sup>12</sup> Len ak je tento element prítomný.

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

samostatného ds:Object elementu. Referencované externé objekty musia byť zaradené za príslušný dátový objekt, z ktorého sú referencované, v takom poradí, v akom sú referencované.

#### 4.4.6. xades:UnsignedDataObjectProperties element

Tento element nie je v rámci profilu XAdES\_ZEP podporovaný.

### 4.5. Podporované kryptografické algoritmy

V rámci profilu XAdES\_ZEP sú podporované nasledujúce podpisové schémy:

| Názov             | Identifikátor   | Poznámka   |
|-------------------|---|--|
| DSA-SHA1<br>(DSS) | <a href="http://www.w3.org/2000/09/xmldsig#g#dsa-sha1">http://www.w3.org/2000/09/xmldsig#g#dsa-sha1</a>               | povinná v rámci XML Signature [1]<br>povinná v rámci profilu XAdES_ZEP       |
| RSA-SHA1          | <a href="http://www.w3.org/2000/09/xmldsig#g#rsa-sha1">http://www.w3.org/2000/09/xmldsig#g#rsa-sha1</a>               | odporúčaná v rámci XML Signature [1]<br>odporúčaná v rámci profilu XAdES_ZEP |
| RSA-SHA256        | <a href="http://www.w3.org/2001/04/xmldsig-g-more#rsa-sha256">http://www.w3.org/2001/04/xmldsig-g-more#rsa-sha256</a> | voliteľná, RFC4051 [10]<br>voliteľná v rámci profilu XAdES_ZEP               |
| RSA-SHA384        | <a href="http://www.w3.org/2001/04/xmldsig-g-more#rsa-sha384">http://www.w3.org/2001/04/xmldsig-g-more#rsa-sha384</a> | voliteľná, RFC4051 [10]<br>voliteľná v rámci profilu XAdES_ZEP               |
| RSA-SHA512        | <a href="http://www.w3.org/2001/04/xmldsig-g-more#rsa-sha512">http://www.w3.org/2001/04/xmldsig-g-more#rsa-sha512</a> | voliteľná, RFC4051 [10]<br>voliteľná v rámci profilu XAdES_ZEP               |

V rámci profilu XAdES\_ZEP sú podporované nasledujúce algoritmy pre výpočet digitálneho odtlačku:

| Názov   | Identifikátor   | Poznámka   |
|---------|---|--|
| SHA-1   | <a href="http://www.w3.org/2000/09/xmldsig#sha1">http://www.w3.org/2000/09/xmldsig#sha1</a>               | povinný v rámci XML Signature [1]<br>povinný v rámci profilu XAdES_ZEP |
| SHA-224 | <a href="http://www.w3.org/2001/04/xmldsig-more#sha224">http://www.w3.org/2001/04/xmldsig-more#sha224</a> | voliteľný, RFC4051 [10]  |

|            |                       |           |
|------------|-----------------------|-----------|
| Projekt    | GOV_ZEP               | A3019_002 |
| Dokument   | Profil XAdES_ZEP v1.1 |           |
| Referencia | GOV_ZEP.2             | Verzia 6  |

| Názov   | Identifikátor   | Poznámka  |
|---------|---|---|
|         |   | voliteľný v rámci profilu XAdES_ZEP                             |
| SHA-256 | <a href="http://www.w3.org/2001/04/xmlenc#sha256">http://www.w3.org/2001/04/xmlenc#sha256</a>             | odporúčaný, XMLENC [23]<br>odporúčaný v rámci profilu XAdES_ZEP |
| SHA-384 | <a href="http://www.w3.org/2001/04/xmldsig-more#sha384">http://www.w3.org/2001/04/xmldsig-more#sha384</a> | voliteľný, RFC4051 [10]<br>voliteľný v rámci profilu XAdES_ZEP  |
| SHA-512 | <a href="http://www.w3.org/2001/04/xmlenc#sha512">http://www.w3.org/2001/04/xmlenc#sha512</a>             | voliteľný, XMLENC [23]<br>voliteľný v rámci profilu XAdES_ZEP   |