DITEC
Data Information Technology & Expert Consulting

Profil XAdES_ZEPbp v1.0

formát zaručeného elektronického podpisu na báze XAdES Baseline profile

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Profil XAdES_ZEPbp v1.0		
Podnázov	formát zaručeného elektronického podpisu na báze XAdES Baseline profile		
Ref. číslo	GOV_ZEP.192	Verzia	8

Vypracoval		Podpis	Dátum
Preveril		Podpis	Dátum
Schválil		Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum

Akceptované dňa : <Dátum akceptácie>

Za <Objednávateľa>: Za <Dodávateľa>.:

<Meno zodpovednej osoby> < Meno zodpovednej osoby >

Projekt	GOV_ZEP		A3019_002
Dokument	Profil XAdES_ZEPbp v1.0		
Referencia	GOV_ZEP.192	Verzia	8

Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia
M.Mikuš	Dátový kontajner je ASiC, topológia podpisu je výhradne detached, dátové objekty sú bez verifikačných objektov (pre XML je definovaný osobitný kontajner), xades:DataObjectFormat je povinný pre ds:KeyInfo aj ds:SignatureProperties, element xadesv141: TimeStampValidationData už nie je zakázaný.	19.3.2015	
M.Mikuš	Špecifikované podmienky na dátové objekty	11.12.2015	5
M.Mikuš	Podpora troch kanonikalizácií, DataObjectFormat element má povinne vyplnené ObjectIdentifier a Description, SignaturePolicy je voliteľný. Zmena názvu profilu na XAdES_ZEPbp v1.0	18.12.2015	6
M.Mikuš	Pridanie Rozhodnutia 2015/1506/EU	1.3.2016	6

Pripomienkovanie a kontrola

Autor	Stanovisko	Dátum	Verzia

Rozdeľovník

	Priezvisko Meno	Firma, Funkcia
Originál		
Kópia		
Kópia		
Kópia		

Obsah

1. Zoznam použitých skratiek

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

2. Referencie

[1] W3C/IETF Recommendation: "XML Signature Syntax and Processing v1.1" v2013-04-11 (XMLDSIG)

[2] ETSI TS 101 733 – CMS Advanced Electronic Signatures (CAdES) v1.6.3

[3] ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES) v1.4.2

[4] ETSI TS 103 171 – XAdES Baseline Profile v2.1.1 (2012-03)

[5] ETSI TS 102 918 v.1.3.1 (2013-06). Electronic Signatures and Infrastructures (ESI);. Associated Signature Containers (ASiC).

[6] ETSI TS 103 174 v.2.2.1 (2013-06). Electronic Signatures and Infrastructures (ESI);. ASiC Baseline Profile.

[7] OASIS: "Open Document Format for Office Applications (OpenDocument) Version 1.2; Part 3: Packages" 29 September 2011. OASIS Standard.

[8] RFC 3125 – Electronic Signature Policies

[9] RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol

[10] RFC 3279 – Algorithms and Identifiers for the Internet X.509 PKI

[11] RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[12] RFC 3548 – The Base16, Base32, and Base64 Data Encodings

[13] RFC 3852 – Cryptographic Message Syntax (CMS)

[14] RFC 4051 – Additional XML Security Uniform Resource Identifiers

[15] Nariadenie Európskeho Parlamentu a Rady EÚ č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES

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

[17] Vyhláška NBÚ č. 131/2009 Z.z., o certifikátoch a kvalifikovaných certifikátoch v znení neskorších predpisov

[18] Vyhláška NBÚ č. 134/2009 Z.z., o produktoch elektronického podpisu v znení neskorších predpisov

[19] Vyhláška NBÚ č. 135/2009 Z.z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky v znení neskorších predpisov

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

[21] NBÚ Formáty certifikátov a kvalifikovaných certifikátov, v4.0

[22] NBÚ Formáty zoznamu zrušených kvalifikovaných certifikátov, v3.0

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

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

[25] Výnos MF SR č. 55/2014 o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov

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

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

[28] XMLENC – XML Encryption Syntax and Processing", J. Reagle, D. Eastlake, December 2002.

[29] Rozhodnutie komisie 2011/130/EU, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu

[30] Rozhodnutie komisie 2014/148/EU, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu

[31] PDF Reference, Sixth Edition, version 1.7, Adobe Incorporated

[32] Document management – Electronic document file format for long-term preservation – Use of PDF 1.4 (PDF/A 1), ISO 19005 1:2005(E)

[33] Document management – Electronic document file format for long-term preservation – Use of PDF 1.4 (PDF/A 1), TECHNICAL CORRIGENDUM 1, ISO 19005 1:2005/Cor.1:2007(E)

[34] Information technology – Computer graphics and image processing – Portable Network Graphics (PNG): Functional specification, ISO/IEC 15948:2004

[35] Rozhodnutie komisie 2015/1506/EU, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať

3. Úvod

Cieľom tohto dokumentu je návrh profilu XAdES_ZEPbp – formátu zaručeného elektronického podpisu na báze špecifikácie XAdES [3] a základného profilu XAdES [4] (XAdES BP) pre vytváranie a overovanie elektronického podpisu nad množinou rôznych formátov (resp. typov) dát:

- XML dokumenty,
- HTML stránky,
- PDF súbory,
- PNG dokumenty, ap.,

ktoré sú definované v rámci dokumentu [20].

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 [15] a obsahujú ďalšie užitočné informácie pre bežné prípady použitia elektronických podpisov.

Špecifikácia XAdES BP [4] definuje užšiu množinu štyroch formátov XAdES, ktoré sú v súlade s [3]. Tieto štyri základné formáty neponechávajú toľko voľnosti pri implementácii, takže umožňujú jednotný prístup a väčšiu interoperabilitu. Spracovanie základného profilu elektronického podpisu (okrem LTA formy) vo formáte XAdES je navyše povinné vo všetkých členských štátoch EU na základe Rozhodnutia 2015/1506/EU [35].

Táto špecifikácia profilu XAdES_ZEPbp zároveň nevylučuje 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 pre vytvorenie elektronického podpisu (SCA) bude môcť pomocou samostatných komponentov (pre jednotlivé formáty, resp. typy dát) pripraviť na podpis a zobraziť používateľovi pred vytvorením podpisu všetky podpisované dátové objekty. Aplikácia pre overenie elektronického podpisu (SVA) 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,
- 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.

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],
- XAdES BP – XAdES Baseline Profile [4],
- ASiC – Associated Signature Containers [5],
- ASiC BP – ASiC Baseline Profile [6],
- Smernica Európskej únie o rámci spoločenstva pre elektronické podpisy [15],
- zákon Slovenskej republiky o elektronickom podpise a príslušné vyhlášky a usmernenia NBÚ SR [16] – [24],
- Výnos MF SR o štandardoch pre IS VS [25],
- Rozhodnutie komisie 2014/148/EU [30] (ktoré nahrádza rozhodnutie [29]) a
- Rozhodnutie komisie 2015/1506/EU [35].

V rámci tejto koncepcie návrhu formátu ZEP je definovaný profil XAdES_ZEPbp 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 nenahradzuje špecifikácie XML Signature [1] a XAdES [3], [4] 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.

4. Špecifikácia profilu XAdES_ZEPbp

V tejto kapitole je popísaný profil XAdES_ZEPbp formátu zaručeného elektronického podpisu na báze špecifikácií: XML Signature [1], XAdES [3] a XAdES Baseline profile [4]. V nasledujúcom texte je stručný prehľad týchto špecifikácií.

Formát pokročilého elektronického podpisu XAdES vychádza zo všeobecnej špecifikácie XML-Signature Syntax and Processing [1], ktorá poskytuje základnú funkcionalitu 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 (topológia) 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 dátovým objektami, ktoré obaľujú 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, susedné XML štruktúry).

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

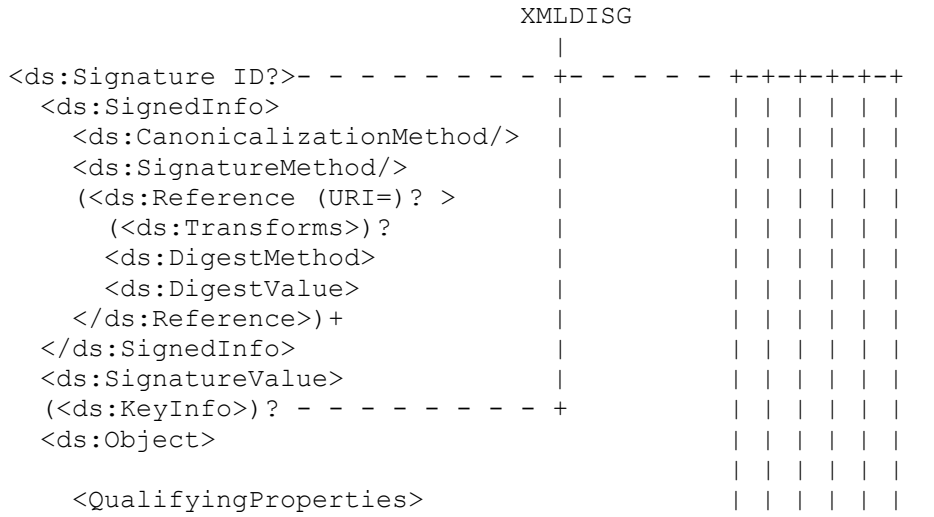
Špecifikácia pokročilého elektronického podpisu XAdES [3] je rozšírením XML Signature, pričom:

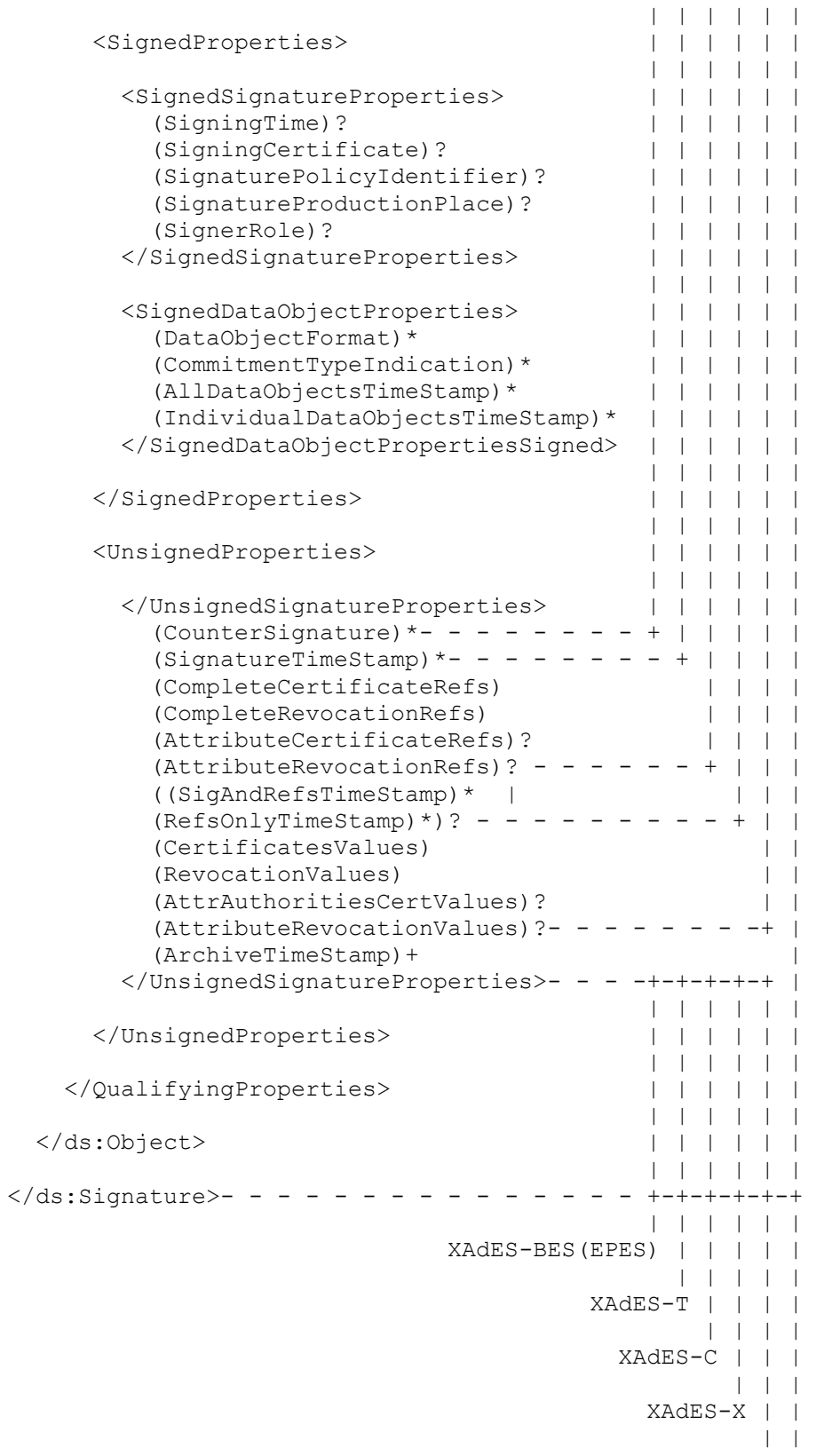
- špecifikuje XML schémy pre definíciu ďalších XML elementov, ktoré dopĺňajú základnú XMLDSIG štruktúru o ďalšie (kvalifikujúce) informácie, potrebné pre naplnenie požiadaviek, ako napr. zabezpečenie dlhotrvajúcej overiteľnosti podpisu,
- definuje mechanizmy pre zahrnutie uvedených informácií do podpisu,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

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:




<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>
</ds:Object>
</ds:Signature>
XAdES-BES(EPES)
XAdES-T
XAdES-C
XAdES-X

```
                                        XAdES-X-L |
                                                  |
                                            XAdES-A
```

Špecifikácia XAdES opäť obsahuje povinné časti, zároveň však poskytuje pre implementátorov niekoľko stupňov voľnosti.

Základný profil (XAdES baseline profile [4]) formátu XAdES definuje štyri základné formáty (B, T, LT a LTA), ktoré by mali pokryť väčšinu scenárov. Výrazne znižujú počet možností pri implementácii, no stále ponechávajú niekoľko voliteľných elementov a atribútov na splnenie rôznych aplikačných a procesných požiadaviek.

4.1. Podporované pokročilé formy XAdES

V rámci profilu XAdES_ZEPbp sú podporované všetky štyri pokročilé formy XML elektronických podpisov zo základného profilu [4]:

XAdES-B – rozširuje základnú štruktúru XML Signature o informáciu o čase vzniku ZEP, referenciu podpisového certifikátu a (voliteľne) o explicitnú podpísanú referenciu podpisovej politiky a podpísané informácie o typoch a formátoch podpísaných dátových objektov,

XAdES-T – rozširuje XAdES-T o časovú pečiatku, ktorá je zviazaná s hodnotou elektronického podpisu a takto poskytuje dôveryhodný čas existencie elektronického podpisu,

XAdES-LT – rozširuje XAdES-T množinu validačných dát umožňujúcich overenie elektronického podpisu, certifikáty z certifikačnej cesty pre podpisový certifikát a príslušné informácie o revokácii certifikátov (CRL alebo OCSP odpoveď),

XAdES-LTA – rozširuje XAdES-LT o archívnu pečiatku a umožňuje tak vytvoriť archívny elektronický podpis a zabezpečiť jeho ochranu pred hrozbou oslabenia použitých kryptografických funkcií, prípadne pred hrozbou exspirácie alebo zneplatnenia niektorého certifikátu z certifikačnej cesty.

4.2. Štruktúra podpisu

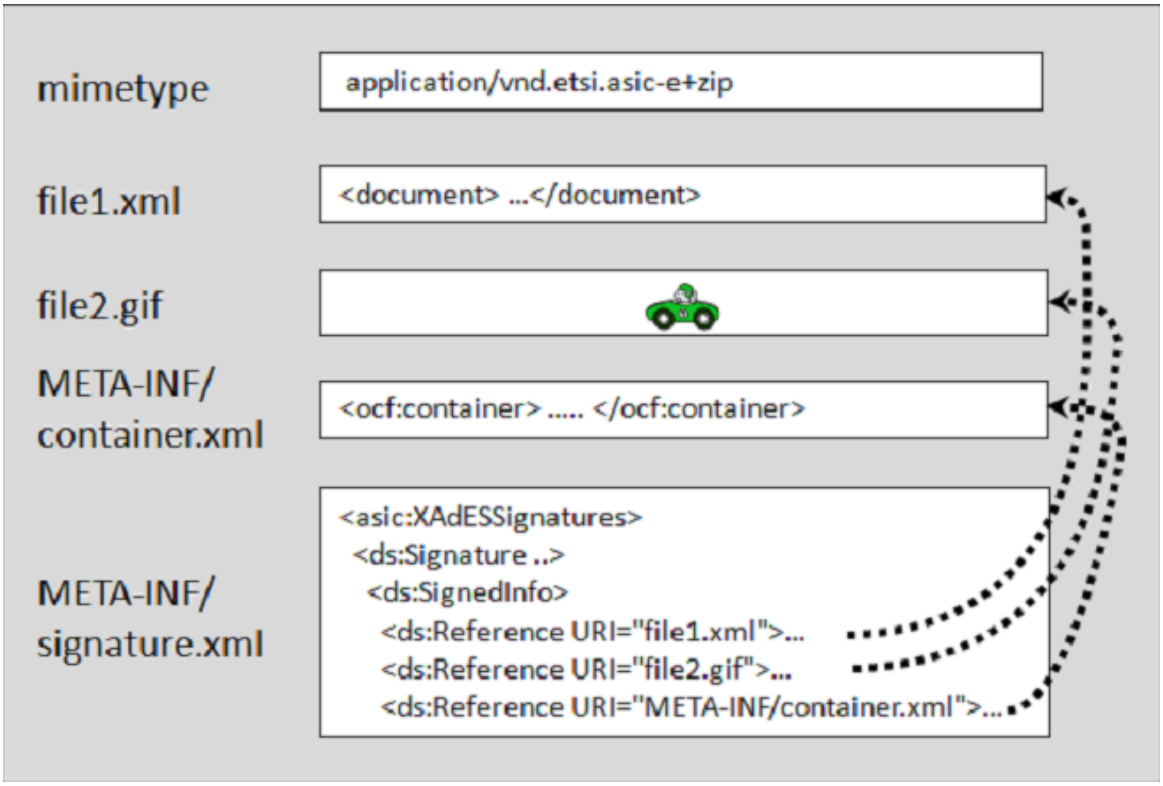
V tejto časti je popísaný spôsob spojenia podpísaných objektov s digitálnym podpisom v rámci profilu XAdES_ZEPbp, bližšie upresnené použitie kontajnera na elektronické podpisy (ASiC) a základná štruktúra podpisu, t.j. ds:Signature element a ds:SignatureProperties element.

4.2.1. Topológia podpisu

Podporovaný typ štruktúry podpisu v rámci profilu XAdES_ZEPbp je

- **detached** – podpisované dátové objekty sú uložené mimo samotnej štruktúry XML Signature (ako samostatné súbory v rámci nadradeného ASiC – tzv. obaľujúci kontajner, viac v kapitole 4.2.2), a

Topológia elektronického podpisu detached je ilustrovaná na nasledujúcom obrázku.



Obr. 1 [5] Príklad obsahu ASiC, ktorý vystihuje detached štruktúru podpisu. Pozn. príklad je iba informatívneho charakteru, presný obsah kontajnera (súbory „signature.xml" a „container.xml") nie je v súlade so špecifikáciou [5] a [6].

4.2.2. Dátový kontajner

V rámci jedného elektronického podpisu môžu byť podpísané komplexné dátové štruktúry, pozostávajúce z dátových objektov rôznych typov:

- XML dokumentov,
- PDF dokumentov,
- TXT dokumentov,
- grafických súborov PNG,
- iných dátových objektov (profil XAdES_ZEPbp sa však v súlade s Výnosom o štandardoch [25] obmedzuje len na vyššie uvedené štyri typy).

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

Pre dátový kontajner elektronického podpisu boli identifikované nasledujúce požiadavky:

- potreba definovať spôsob pre spojenie elektronického podpisu/podpisov (s topológiou detached) s množinou dátových objektov rôznych formátov,
- potreba identifikovať profil a obsah kontajnera pre elektronické podpisy na aplikačnej úrovni,
- efektívne uloženie podpísaných dátových objektov (dokumentov) v rámci dátového kontajnera,
- možnosť pripojiť k obálke elektronického podpisu ďalšie sprievodné dáta (XML štruktúry) pre potreby aplikačnej úrovne.

Tieto požiadavky sú vyriešené v rámci špecifikácie tzv. Associated Signature Container [5] a [6], kde bol definovaný spôsob prepojenia digitálneho podpisu (formátu XAdES alebo CAdES) s externými údajmi tak, aby boli splnené vyššieuvedené požiadavky a údaje boli navyše ľahko prístupné.

Tento kontajner (ASiC) je založený na ZIP formáte, ktorý je navyše natívne spracovávaný vo väčšine operačných systémov. Ďalšou výhodou je, že takto definovaný kontajner je kompatibilný s ďalšími štandardami EPUB Open Container Format a OASIS Open Document Format.

Žiadne ďalšie požiadavky na štruktúru alebo obsah dátovej obálky nie sú v rámci tohto profilu XAdES_ZEPbp stanovené.

4.2.2.1. Associated Signature Container

Použitie kontajnera sa riadi technickou špecifikáciou [5] a jej základným profilom [6]. V tejto časti sú špecifikované len také postupy, ktorým bola v uvedených špecifikáciách ponechaná voľnosť. ASiC v súlade s XAdES_ZEPbp musí spĺňať nasledovné:

- mimetype kontajnera je špecifikovaný v súbore s názvom „mimetype“, ktorý leží priamo v koreňovom adresári a jeho obsahom je reťazec „application/vnd.etsi.asic-e+zip“,
- jednotlivé elektronické podpisy sú uložené v súboroch „/META-INF/signatures*.xml“, kde za znak * sa doplní číselný reťazec tak, aby mali súbory jednoznačný názov,
- každý súbor „signatures*.xml“ obsahuje koreňový element asic:xadesSignatures, ktorý obsahuje jeden alebo viac elementov ds:Signature,

- dátové súbory sú uložené v koreňovom adresári (nie v META-INF), bez dodatočných požiadaviek na ich adresárovú štruktúru,
- adresár META-INF obsahuje navyše súbor „manifest.xml“, ktorý obsahuje v položkách <file-entry> len zoznam podpísaných objektov. Elementy <file-entry> obsahujú len povinné atribúty špecifikované v [7] a tie sa vyplnia v súlade s elementom xades:DataObjectFormat (viac v 4.4.4.1, nižšie) z podpisu.

4.2.3. XML namespaces

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

Element asic:xadesSignatures musí mať špecifikovaný namespace:

- xmlns:asic="http://uri.etsi.org/02918/v1.2.1#"

ds:SignatureProperties element musí mať špecifikovaný namespace:

- xmlns:xzep="http://www.ditec.sk/ep/signature_formats/xades_zepbp/v1.0/"

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.

xadesv141:ArchiveTimeStamp element musí mať špecifikovaný namespace:

- xmlns:xadesv141="http://uri.etsi.org/01903/v1.4.1#"

Podpísané dátové objekty (a podpísané objekty s verifikačnými dátami pre dátové objekty) musia mať takisto definovaný atribút namespace (pozri kapitolu 4.2.7), pričom nepovinné prefixovanie názvov elementov zabezpečuje v tomto prípade aplikačná úroveň.

4.2.4. Id atribúty

Id pre jednotlivé elementy v rámci štruktúry elektronického podpisu musia byť jedinečné nielen pre danú inštanciu štruktúry zaručeného elektronického podpisu podľa profilu XAdES_ZEPbp ale aj pre celý ASiC. 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.

4.2.5. Kódovanie XML

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

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

4.2.6. ds:Signature element

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

Element ds:Signature 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.

4.2.7. Dátové objekty

Podpísaný dátový objekt je akákoľvek informácia, ktorá je podpisom chránená. V zmysle tejto definície sem patria aj všetky časti podpisu, ktoré sú referencované v elemente ds:SignedInfo (viac v časti 4.3.1.3).

Každý užívateľom zvolený podpísaný dátový objekt však predstavuje samostatný súbor, ktorý sa nachádza v príslušnom ASiC a je referencovaný z elementu ds:SignedInfo podľa pravidiel uvedených v [5].

Dátový objekt nesmie obsahovať vnorenú štruktúru elektronického podpisu.

4.2.7.1. Externé dátové objekty

Pre niektoré typy dátových objektov sú definované bezpečnostné požiadavky, ktoré nie je možné naplniť pomocou štruktúr definovaných v rámci špecifikácií XML Signature alebo XAdES.

Keďže všetky dátové objekty chránené digitálnym podpisom sú iba postupnosťou núl a jednotiek, je dôležité, aby boli užívateľovi správne zobrazené a aby boli vždy zobrazované rovnako. Elektronický podpis vytvorený v súlade s týmto

profilom síce zabezpečí integritu podpísaných údajov, no je potrebné zabezpečiť, aby bol podpisom chránený aj spôsob interpretácie týchto údajov.

Tento problém je zahrnutý aj v požiadavkách CWA 14170 [26] a označuje sa aj slovným spojením WYSIWYS (What You See Is What You Sign).

V rámci tohto profilu XAdES_ZEPbp je teda definovaná požiadavka, aby z údajov dátového objektu bolo možné vždy jednoznačne určiť, akým spôsobom bol tento objekt prezentovaný užívateľovi pri podpise. Z tohto dôvodu je množina dátových objektov, ktoré možno podpísať, obmedzená na tieto štyri typy: XML, PDF, PNG a TXT, pričom na tieto typy sa kladú dodatočné podmienky popísané v nasledujúcich častiach.

Súčasná legislatíva – Výnos MF SR o štandardoch [25] – stanovuje rovnaké typy dokumentov pre zaručený elektronický podpis v administratívnom styku, spolu s dodatočnými podmienkami na tieto dokumenty. Podmienky, ktoré kladieme na dátové objekty v tomto profile sú nadmnožinou podmienok uvedených vo Výnose [25].

4.2.7.1.1. Objekty typu XML

Formát XML v súčasnosti predstavuje rozšírený a podporovaný štandard pre elektronickú komunikáciu a výmenu dát medzi rôznymi systémami v heterogénnych prostrediach, pričom umožňuje jednoznačnú definíciu štruktúry, jednoznačnú interpretáciu obsiahnutých údajov, ako aj ich jednoduché automatické spracovanie.

Požiadavka WYSIWYS v tomto prípade implikuje, aby podpis zároveň chránil aj schémy použité na validáciu (XSD) a prezentáciu (XSLT) týchto XML údajov, resp. aspoň referencie týchto schém.

Podpísané dáta, ktoré sú vo formáte XML, musia byť vložené v kontajneri pre XML dáta v súlade s [25] a podpísané ako celok spolu so schémami (resp. s referenciami na schémy), ktoré sú použité na validáciu a zobrazenie týchto XML dát. Tento kontajner spája pôvodné XML dáta s ich validačnou a prezentačnou schémou a predstavuje jeden samostatný súbor, ktorý je podľa bežných pravidiel z [5] vložený do kontajnera a referencovaný z príslušného podpisu.

Podmienky na dátový objekt typu XML:

- XML objekt musí byť vložený do štruktúry XMLDataContainer, do elementu XMLData, pričom:
  - XML údaje vložené do XMLData, už nesmú obsahovať XML Declaration
  - schémy vložené do elementov UsedXSDEmbedded a UsedPresentationSchemaEmbedded tiež nesmú obsahovať XML Declaration,

- obsah elementu XMLData musí byť validný vzhľadom na priloženú (príp. referencovanú) XSD schému,

- štruktúra XMLDataContainer musí byť validná vzhľadom na aktuálnu XSD schému kontajnera,
- element XMLDataContainer musí obsahovať atribút xmlns:xdc="http://data.gov.sk/def/container/xmldatacontainer+xml/1.0" a všetky jeho elementy musia byť uvedené s prefixom,
- podpisované XML údaje a rovnako aj výsledný XMLDataContainer musia byť kódované v UTF-8,
- výsledok priloženej (resp. referencovanej) XSLT transformácie na údaje v elemente XMLData musí spĺňať:
  - ⇒ pre vizualizáciu do plain text (TXT) – výsledný text nesmie obsahovať nepovolené znaky (viď povolené znaky pre entitu Char – http://www.w3.org/TR/2008/REC-xml-20081126/#charsets),
  - ⇒ pre vizualizáciu do HTML – výsledný HTML kód nesmie obsahovať nepovolené HTML tagy: applet, script, iframe, link, object.

SignedDataObjectProperties:

Pre XML dokument musí mať zodpovedajúci element xades:DataObjectFormat vyplnené nasledovné hodnoty:

- Description – povinný string, obsahuje popis, ktorý bližšie definuje typ podpísaného dátového objektu (napr. "DPPO 2007"),
- ObjectIdentifier – URI, povinný, obsahuje identifikátor, ktorý bližšie definuje typ podpísaného dátového objektu (napr. URI pre daný typ XML dokumentov; definuje správca daného typu dokumentov),
- MimeType – hodnota „application/vnd.gov.sk.xmldatacontainer+xml; charset=UTF-8”, povinný string,
- Encoding – nevypĺňa sa.

4.2.7.1.2. Objekty typu PNG

PNG ponúka podporu 24-bitovej farebnej hĺbky, nemá teda ako GIF obmedzenie na maximálny počet 256 farieb súčasne. PNG teda do istej miery nahradzuje GIF, ponúka viac farieb a lepšiu kompresiu. Navyše obsahuje osembitovú priehľadnosť (tzv. alfa kanál), to znamená, že obrázok môže byť v rôznych častiach rôzne priehľadný (tzv. RGBA farebný model). PNG však neumožňuje jednoduché animácie, ktoré naopak umožňuje formát GIF.

Obrázky vo formáte PNG sa používajú aj na dlhodobú archiváciu. Medzi ich základné výhody patrí široká podpora na úrovni operačných systémov a grafických programov, nakoľko pre jeho použitie nie je potrebná licencia. Primárne je tento formát určený na prenos obrázkov na internete. Patrí k najmladším grafickým formátom.

Podmienky na dátový objekt typu PNG:

- dátový objekt musí mať formát PNG obrázka ([34]),

SignedDataObjectProperties:

Pre PNG dokument musí mať zodpovedajúci element xades:DataObjectFormat vyplnené nasledovné hodnoty:

- Description – povinný string, obsahuje popis, ktorý bližšie definuje typ podpísaného dátového objektu (napr. "Fotografia na pas"),
- ObjectIdentifier – URI, povinný, obsahuje identifikátor, ktorý bližšie definuje typ podpísaného dátového objektu (napr. URI pre daný typ PNG dokumentov; definuje správca daného typu dokumentov),
- MimeType – string, povinný, hodnota "image/png",
- Encoding – nevypĺňa sa.

4.2.7.1.3. Objekty typu PDF

Formát PDF bol vytvorený v roku 1993 firmou Adobe Systems a v súčasnosti je aktuálna verzia 1.7 špecifikácie formátu PDF [31].

Dokumenty vo formáte PDF je možné podľa CWA 14170 [26] (kapitola 8.2) zaradiť do skupiny Presentation Sensitive SDs, pretože ich sémantika je závislá na presnosti prezentácie dokumentu podpisovateľovi, resp. overovateľovi.

Naplnenie požiadaviek WYSIWYS pre PDF dokumenty verzie 1.4 realizuje špecifikácia PDF/A-1 [32][33], ktorá poskytuje mechanizmus pre takú reprezentáciu elektronických dokumentov vo formáte PDF, ktorá umožňuje zabezpečenie ich vizualizácie a čitateľnosti (teda reprodukovateľnosti) v rámci dlhého časového obdobia a bez ohľadu na použitú technológiu ich reprodukcie.

Podmienky na dátový objekt typu PDF:

- verzia formátu PDF je 1.4,
- súlad s normou PDF/A.

SignedDataObjectProperties:

Pre PDF dokument musí mať zodpovedajúci element xades:DataObjectFormat vyplnené nasledovné hodnoty:

- Description – povinný string, obsahuje popis, ktorý bližšie definuje typ podpísaného dátového objektu (napr. "Všeobecné zmluvné podmienky"),
- ObjectIdentifier – URI, povinný, obsahuje identifikátor, ktorý bližšie definuje typ podpísaného dátového objektu (napr. URI pre daný typ PDF dokumentov; definuje správca daného typu dokumentov),
- MimeType – string, povinný, hodnota "application/pdf",
- Encoding – nevypĺňa sa.

4.2.7.1.4. Objekty typu TXT

Vzhľadom k ich jednoduchosti, sú textové súbory bežne používané na ukladanie informácií. Jednoduchý textový súbor nevyžaduje žiadne ďalšie metadáta na interpretáciu svojho obsahu a z tohto dôvodu sú textové súbory považované za univerzálne (alebo nezávislé na platforme). TXT súbory však môžu mať na rôznych platformách rôzne kódovania – ASCII, Unicode, UTF-8, až po zastaralé platformovo závislé kódovania (napr. Windows code pages). Takisto sa na rôznych platformách môžu líšiť preferovanou konvenciou pre ukončenie riadku (napr. LF na Unix systémoch vs. CR+LF na DOS a Windows). Niektoré kódovania textových súborov môžu vyžadovať na začiatku súboru značku BOM (Byte Order Mark), ktorá indikuje typ kódovania a usporiadanie bytov.

Podmienky na dátový objekt typu TXT:

- kódovanie UTF-8,
- kontrola na nepovolené znaky (viď povolené znaky pre entitu Char – http://www.w3.org/TR/2008/REC-xml-20081126/#charsets).

SignedDataObjectProperties:

Pre TXT dokument musí mať zodpovedajúci element xades:DataObjectFormat vyplnené nasledovné hodnoty:

- Description – povinný string, obsahuje popis, ktorý bližšie definuje typ podpísaného dátového objektu (napr. "Všeobecné podanie"),
- ObjectIdentifier – URI, povinný, obsahuje identifikátor, ktorý bližšie definuje typ podpísaného dátového objektu (napr. URI pre daný typ TXT dokumentov; definuje správca daného typu dokumentov),
- MimeType – string, povinný, hodnota "text/plain; charset=UTF-8",
- Encoding – nevypĺňa sa.

4.2.8. ds:SignatureProperties element

Element ds:SignatureProperties môže podľa špecifikácie XML Signature [1] obsahovať doplňujúce informácie, týkajúce sa vytvoreného elektronického podpisu, napr. informácie o použitom kryptografickom hardvéri, 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_ZEPbp 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_ZEPbp,
- xzep:ProductInfos – obsahuje identifikáciu produktu (a všetkých jeho komponentov), pomocou ktorého bola vytvorená daná štruktúra elektronického podpisu.

Každý ds:SignatureProperty element musí obsahovať atribút:

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

Časť XML schémy profilu XAdES_ZEPbp pre element xzep:SignatureVersion je nasledujúca:

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

Časť XML schémy profilu XAdES_ZEPbp 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>
```

4.3. Profil časti XML Signature

4.3.1. ds:SignedInfo element

Element ds:SignedInfo zahŕňa:

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

Informácie uložené v rámci všetkých referencovaných elementov z elementu ds:SignedInfo budú zahrnuté do elektronického podpisu. Všetky podpisované informácie by mala SCA aplikácia pred vytvorením podpisu zobraziť používateľovi a SVA aplikácia overiť voči referenčným údajom evidovaným v rámci IS spracovateľa elektronického podpisu.

4.3.1.1. ds:CanonicalizationMethod element

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

V rámci tohto profilu XAdES_ZEPbp sú povolené všetky tri kanonikalizačné algoritmy špecifikované v XAdES Baseline Profile:

- c14n – http://www.w3.org/TR/2001/REC-xml-c14n-20010315,
- c14n11 – http://www.w3.org/2006/12/xml-c14n11,
- exc_c14n11 – http://www.w3.org/2001/10/xml-exc-c14n.

ds:CanonicalizationMethod element musí obsahovať atribút s hodnotou použitého kanonikalizačného algoritmu, odporúčaná hodnota je c14n:

- 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/2001/04/xmldsig-more#rsa-sha256"/>
```

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 podpisovaného objektu.

V rámci tohto profilu XAdES_ZEPbp sú povinne referencované tieto tri časti podpisu: ds:KeyInfo, ds:SignatureProperties a xades:SignedProperties.

Referencia elementu ds:KeyInfo musí mať hodnotu atribútu Type:

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

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".

Pozn. Referencia elementu xades:SignedProperties je predpísaná špecifikáciou XAdES [3], ostatné dve sú požadované profilom XAdES_ZEPbp.

Všetky ostatné podpísané objekty, ktoré ukazujú na externý súbor v ASiC kontajneri, nemusia mať hodnotu atribútu Type definovanú.

4.3.1.3.1. ds:Transforms element

Element ds:Transforms obsahuje zoznam transformácií, ktoré je potrebné aplikovať na referencovaný objekt 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_ZEPbp sú ako transformácie podporované len kanonikalizačné algoritmy uvedené v 4.3.1.1. URI daného algoritmu sa uvedie ako hodnota atribútu Algorithm v príslušnom ds:Transforms elemente.

4.3.1.3.2. ds:DigestMethod element

Povinný element ds:DigestMethod 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

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

4.3.2. ds:SignatureValue element

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

Element ds:SignatureValue musí obsahovať nasledujúce atribúty:

- Id – umožňuje v prípade potreby referencovať tento element z iných elementov XML dokumentu.

4.3.3. ds:KeyInfo element

Element ds:KeyInfo obsahuje podpisový certifikát a jeho referenciu, teda verejný kľúč, ktorý má byť použitý pre overenie ZEP. V rámci tohto profilu XAdES_ZEPbp je ds:KeyInfo element povinný.

Implementovaný mechanizmus pre získanie verejného kľúča pre overenie ZEP v rámci ds:KeyInfo je element ds:X509Data[1], ktorý obsahuje elementy:

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

ds:KeyInfo element obsahuje len informácie o podpisovom certifikáte, nesmú sa v ňom nachádzať žiadne ďalšie certifikáty, CRL alebo ich referencie.

ds:KeyInfo element musí obsahovať atribút:

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

4.4. Profil xades:QualifyingProperties

Podľa všeobecnej špecifikácie XAdES [3] je základná štruktúra objektu pre xades:QualifyingProperties element nasledujúca, pričom SCVA aplikácie môžu vytvárať pridávaním jednotlivých špecifikovaných elementov postupne pokročilejšie (advanced) formy elektronického podpisu:

[1] 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, profil XAdES_ZEPbp vyžaduje len zahrnutie elementu ds:X509Data.

```
<ds:Object>
  <QualifyingProperties>
    <SignedProperties>

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

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

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

- 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_ZEPbp 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:SignedSignatureProperties
    - ♦ xades:SigningTime,
    - ♦ xades:SigningCertificate,
    - ♦ xades:SignaturePolicyIdentifier (voliteľný),
  - ⇒ xades:SignedDataObjectProperties
    - ♦ xades:DataObjectFormat elementy,
- nasledujúce xades:UnsignedProperties elementy, ktoré sa vzťahujú k samotnému podpisu:
  - ⇒ xades:UnsignedSignatureProperties
    - ♦ xades:SignatureTimeStamp,
    - ♦ xadesv141:TimeStampValidationData
    - ♦ xades:CertificatesValues,
    - ♦ xades:RevocationValues,
    - ♦ xadesv141:ArchiveTimeStamp.

V nasledujúcej tabuľke je uvedený prehľad, ktoré z uvedených elementov sú v danej podporovanej pokročilej forme XAdES v rámci profilu XAdES_ZEPbp povinné (P) a ktoré sú voliteľné (V).

	SignedProperties	SignedSignatureProperties	SigningTime	SigningCertificate	SignaturePolicyIdentifier	SignedDataObjectProperties	DataObjectFormat	UnsignedProperties	UnsignedSignatureProperties	SignatureTimeStamp	TimeStampVAlidationData	CertificatesValues	RevocationValues	ArchiveTimeStamp
Level-B	P	P	P	P	V	P	P							
Level-T	P	P	P	P	V	P	P	P	P	P	V			
Level-LT	P	P	P	P	V	P	P	P	P	P	V	V	V	
Level-LTA	P	P	P	P	V	P	P	P	P	P	V	V	V	P

Ostatné elementy špecifikácie XAdES, ktoré nie sú v tabuľke pre danú pokročilú formu profilu XAdES_ZEPbp uvedené ako povinné alebo voliteľné, sú pre danú formu profilu XAdES_ZEPbp zakázané.

Element xades:QualifyingProperties musí mať nasledujúce atribúty:

- xmlns:xades = "http://uri.etsi.org/01903/v1.3.2#"
- xmlns:xadesv141 = "http://uri.etsi.org/01903/v1.4.1#"
- 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.

Všetky podpisované vlastnosti elektronického podpisu a podpisovaných dátových objektov by mala SCA aplikácia pred vytvorením podpisu zobraziť používateľovi a SVA aplikácia overiť voči referenčným údajom evidovaným v rámci IS spracovateľa elektronického podpisu.

4.4.2. xades:UnsignedProperties element

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

- samotný elektronický podpis, resp. podpisovateľa – xades:UnsignedSignatureProperties element (pozri kapitolu 4.4.5),
- 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_ZEPbp 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_ZEPbp povinné.

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_ZEPbp nevyžaduje zahrnutie explicitnej referencie podpisovej politiky do štruktúry elektronického podpisu prostredníctvom xades:SignaturePolicyIdentifier elementu.

Ak je zahrnutý, tak element xades:SignaturePolicyIdentifier musí obsahovať:

- 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_ZEPbp musí existovať príslušný xades:DataObjectFormat element **pre každý** element ds:Reference, okrem referencie na xades:SignedProperties element. Element xades:DataObjectFormat obsahuje 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,[2]

⇒ MimeType – povinný string, definuje MIME type podpísaného dátového objektu (napr. "application/xml", "application/pdf"),

⇒ Encoding – nepovinné URI, definuje kódovanie podpísaného dátového objektu.

- atribúty:

⇒ ObjectReference – povinná referencia na príslušnú ds:Reference v rámci ds:SignedInfo, ktorá korešponduje s dátovým objektom, určeným týmto xades:DataObjectFormat elementom.

Pozn. Pre “triviálne referencie” na elementy ds:KeyInfo, príp. ds:SignatureProperties sa vyplní len s povinným MimeType “application/xml” a atribútom ObjectReference.

4.4.5. xades:UnsignedSignatureProperties element

4.4.5.1. xades:SignatureTimeStamp element

Element xades:SignatureTimeStamp rozširuje podpis 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). V rámci tohto profilu je podporovaný **viacnásobný** výskyt elementu xades:SignatureTimeStamp v štruktúre podpisu.

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

Element xades:SignatureTimeStamp je typu xades:XAdESTimeStampType. V rámci profilu XAdES_ZEPbp musí tento element obsahovať:

- xades:EncapsulatedTimeStamp typu xades:EncapsulatedPKIDataType, ktorý obsahuje base64 kódovaný Time Stamp Token z časovej pečiatky,
- element ds:CanonicalizationMethod, v ktorom je uvedený algoritmus kanonikalizácie použitý pri vutvorení oktet streamu daného tokenu,
- atribút Id – umožňuje v prípade potreby referencovať tento element z iných elementov XML dokumentu.

Pravidlá pre generovanie oktet 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.

[2] Odporúčame definovať jednotlivé URI tak, aby obsahovali aj informáciu o verzii (formátu) pre daný typ podpísaných dát.

4.4.5.2. xades:CertificatesValues element

Element xades:CertificatesValues musí obsahovať celú certifikačnú cestu okrem podpisového certifikátu, ktorého obsah sa nachádza v ds:KeyInfo elemente.

Tento element musí obsahovať atribút:

- Id – umožňuje v prípade potreby referencovať tento element z iných elementov XML dokumentu.

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

4.4.5.3. xades:RevocationValues element

Element xades:RevocationValues obsahuje množinu CRL a OCSP odpovedí, ktoré sú potrebné pre overenie podpisového certifikátu.

Tento element musí obsahovať atribút:

- Id – umožňuje v prípade potreby referencovať tento element z iných elementov XML dokumentu.

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

Každý z EncapsulatedOCSPValue elementov musí obsahovať base64 kódovanú reprezentáciu OCSP odpovede.

4.4.5.4. xadesv141:ArchiveTimeStamp element

Element xadesv141:ArchiveTimeStamp slúži na pripojenie archívnej časovej pečiatky k štruktúre elektronického podpisu, ktorá je zviazaná:

- s hodnotou elektronického podpisu,
- podpísanými dátovými objektami,
- obsahom 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, pričom nová archívna pečiatka už je vytvorená pomocou algoritmov, ktorých platnosť presahuje tie pôvodné.

Element xadesv141:ArchiveTimeStamp je typu xades:XAdESTimeStampType. V rámci profilu XAdES_ZEPbp musí tento element obsahovať:

- element xades:EncapsulatedTimeStamp typu xades: EncapsulatedPKIDataType, ktorý obsahuje base64 kódovaný Time Stamp Token z časovej pečiatky,
- element ds:CanonicalizationMethod, v ktorom je uvedený algoritmus kanonikalizácie použitý pri vytvorení oktet streamu daného tokenu,
- atribút Id – umožňuje v prípade potreby referencovať tento element z iných elementov XML dokumentu.

Pravidlá pre generovanie oktet 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 8.2.

4.4.5.5. xadesv141:TimeStampValidationData

Tento element je v rámci profilu XAdES_ZEPbp podporovaný. Profil XAdES_ZEPbp podporuje ukladanie validačných údajov ku časovým pečiatkam do elementu xadesv141:TimeStampValidationData podľa pravidiel špecifikovaných v [3].

4.4.6. xades:UnsignedDataObjectProperties element

Tento element nie je v rámci profilu XAdES_ZEPbp podporovaný.

4.5. Podporované kryptografické algoritmy

V rámci profilu XAdES_ZEPbp sú podporované nasledujúce podpisové schémy:

Názov	Identifikátor	Poznámka
RSA-SHA256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	voliteľná, RFC4051 [14] odporúčaná v rámci profilu XAdES_ZEPbp
RSA-SHA384	http://www.w3.org/2001/04/xmldsig-more#rsa-sha384	voliteľná, RFC4051 [14] voliteľná v rámci profilu XAdES_ZEPbp
RSA-SHA512	http://www.w3.org/2001/04/xmldsig-more#rsa-sha512	voliteľná, RFC4051 [14] voliteľná v rámci profilu XAdES_ZEPbp

V rámci profilu XAdES_ZEPbp sú podporované nasledujúce algoritmy pre výpočet digitálneho odtlačku:

Názov	Identifikátor	Poznámka

Názov	Identifikátor	Poznámka
SHA-256	http://www.w3.org/2001/04/xmlenc#sha256	odporúčaný, XMLENC [28] odporúčaný v rámci profilu XAdES_ZEPbp
SHA-384	http://www.w3.org/2001/04/xmldsig-more#sha384	voliteľný, RFC4051 [14] voliteľný v rámci profilu XAdES_ZEPbp
SHA-512	http://www.w3.org/2001/04/xmlenc#sha512	voliteľný, XMLENC [28] voliteľný v rámci profilu XAdES_ZEPbp