NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verzia 3.0

Formáty zaručených elektronických podpisov

12.8.2009

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Sekcia informačnej bezpečnosti a elektronického podpisu

Budatínska č. 30, 850 07 Bratislava 57

http://www.nbusr.sk/

e-mail: info@nbusr.sk

Obsah

1 Úvod 5

2 Predmet dokumentu 5

3 Odkazy 6

4 Skratky 7

5 Pravidlá pre štruktúry ZEP nad AdES 8

5.1 Podpis v ASN.1 formáte 8
Tabuľka 1. CMS obálka elektronického podpisu 8
Tabuľka 2. CMS typ - podpísané údaje SignedData 8
Tabuľka 3. EncapsulatedContentInfo – vložené podpisované údaje 8
Tabuľka 4. SignerInfo – údaje podpisovateľa s jeho podpisom 9
Tabuľka 5. CMS podpisované a nepodpisované atribúty 10
Tabuľka 6. Other signing certificate 10
Tabuľka 7. CertificateRefs 11
Tabuľka 8. RevocationRefs 11
Tabuľka 9. SignatureTimeStampToken 12
Tabuľka 10. EscTimeStamp 13
Tabuľka 11. CertCRLTimestamp 13
Tabuľka 12. ArchiveTimestamp 14
Tabuľka 13. SigningCertificate 14
Tabuľka 14. CertValues 15
Tabuľka 15. RevocationValues 15
Tabuľka 16. SignerLocation 15
Tabuľka 17. SigPolicyId 16
Tabuľka 18. ContentTimestamp 17
Tabuľka 19. Signer attribute - atribúty podpisovateľa (rola) 17
Tabuľka 20. ESS signing certificate v2 18
5.2 Podpis v XML formáte 19
Tabuľka 21. Atribúty ASN.1 a XML elementy ZEP s rovnakým významom obsahu 19
5.3 Ostatné formáty podpisov a PAdES 20

Príloha A (normatívna) Formáty zaručených elektronických podpisov 21

A.1 Zaručený elektronický podpis bez časovej pečiatky 21
A.2 Zaručený elektronický podpis s časovou pečiatkou 21
A.3 Zaručený elektronický podpis s úplnou informáciou na overenie platnosti 22
A.4 Archívny zaručený elektronický podpis 22
A.5 Viacnásobný podpis 23

Príloha B (normatívna) Postup uchovania a formát podpisu pre dlhodobé uchovanie elektronických dokumentov podpísaných ZEP 24

B.1 Postup pri vytvorení a kontrole integritného podpisu súborov 24
B.2 Integritný elektronický podpis 24
B.3 Formát textového dokumentu 25
B.4 Príklad postupnosti atribútov súborov 25

Príloha C (normatívna) Uloženie certifikačných ciest vo všetkých formátoch ZEP 25

Príloha D (normatívna) Výpočet časovej pečiatky 26

Tabuľka 22. Identifikácia atribútov podpisu, z ktorých sa počíta haš 26

Tabuľka 23. CAdES podpis v ASN.1 26
Tabuľka 24. Úplné SignedData v ASN.1 26

Príloha E (informatívna) Formáty spojenia elektronických dokumentov s elektronickým podpisom alebo ZEP 27

E.1 S/MIME formát súboru 27
E.1.1 Príklad podpísaných údajov CMS (*.p7s) zakódovaných do S/MIME 28
E.2 ZIP formát súboru (ZEPf) 29
Tabuľka 25. Názvy základnej množiny súborov v ZIP formáte 29
E.2.1 Príklad položiek v ZIP formáte (ZEPf) a názvy štandardných adresárov 30
E.3 DITEC XML formát súboru 30

Príloha F (informatívna) Revízie vykonané od predošlého vydania 31

F.1 Pridané požiadavky 31
F.2 Upravené požiadavky 31
F.3 Vysvetlenia 31
F.4 Publikačné zmeny 31

Príloha G (informatívna) Zoznam použitej literatúry 32

Príloha H História 34

1 Úvod

Pri vytváraní a overení zaručeného elektronického podpisu (ďalej len ZEP) je vyžadovaná splnenie radu požiadaviek, z ktorých nezanedbateľná je jednoznačná vizualizácia podpisovaného a overovaného elektronického dokumentu. Zásadná požiadavka je, aby podpis tohto dokumentu bol vytvorený so súkromným kľúčom uloženým na SSCD, ku ktorému patriaci verejný kľúč bol uložený do kvalifikovaného certifikátu vydaného akreditovanou certifikačnou autoritu. Aby bolo možné jednoznačne overiť ZEP, je potrebné definovať jednoznačné pravidlá pre formát a obsah podpisu a identifikáciu typu podpisovaného elektronického dokumentu s ohľadom na potrebu jeho jednoznačnej vizualizácie.

2 Predmet dokumentu

Štandard „Formáty zaručených elektronických podpisov“ je vydaný na základe § 3 ods. 6 vyhlášky Národného bezpečnostného úradu (ďalej len NBÚ) č. 135/2009 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, podmienkach platnosti pre zaručený elektronický podpis, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky).

Účelom tohto štandardu je vymedziť technické požiadavky na jednotlivé typy zaručených elektronických podpisov pre zabezpečenie kompatibility a jednotného prostredia elektronického podpisu v SR s ohľadom na prostredie elektronického podpisu v rámci EÚ, keďže členské štáty sú povinné zaistiť, aby zaručený elektronický podpis (Qualified Electronic Signature – CWA 14170) definovaný na základe článku 5, odsek 1 Smernice 1999/93/ES [26] spĺňal nasledovné:

Právne účinky elektronických podpisov
Členské štáty zabezpečia, aby zdokonalené elektronické podpisy, ktoré sú založené na kvalifikovanom certifikáte a ktoré sú vytvorené bezpečným zariadením na vytvorenie podpisu:

a) spĺňali zákonné požiadavky na podpis vo vzťahu k údajom v elektronickej forme rovnakým spôsobom, ako vlastnoručný podpis spĺňa takéto požiadavky vo vzťahu k údajom na papieri, a
b) boli prípustné ako dôkaz v konaní pred súdmi.

3 Odkazy

Odkazy na dokumenty, ktoré definujú použité typy a postupy.

[1] ETSI	TS 101 733 Electronic Signature Formats (CAdES)	
[2] ETSI	TR 102 272 ASN.1 format for signature policies	
[3] RFC 5280	X.509 PKI Certificate and Certificate Revocation List	5-2008
[4] RFC 3739	Qualified Certificates Profile	3-2004
[5] ETSI	TS 101 862 Qualified Certificate Profile	
[6] RFC 5652	Cryptographic Message Syntax	9-2009
[7] RFC 3161	Time-Stamp Protocol (TSP)	8-2001
[8] RFC 2560	X.509 PKI Online Certificate Status Protocol	8-1999
[9] NBÚ	Formáty kvalifikovaných certifikátov	
[10] Vyhláška	č. 135/2009 Z. z., o formáte a spôsobe vyhotovenia ZEP	
[11] ETSI	TS 102 280 X.509 V.3 Cert. Profile for Cert. Issued to Natural Persons	
[12] ETSI	TR 102 437 Guidance on TS 101 456	
[13] ETSI	TS 101 456 Policy requirements for cert. authorities issuing qualified cert.	
[14] ETSI	TS 102 042 Policy requirements for cert. authorities issuing public key cert.	
[15] ETSI	TS 102 231 Provision of harmonized Trust-service status information	3-2006
[16] ETSI	TS 101 903 XML Advanced Electronic Signatures (XAdES)	
[17] RFC 5035	Enhanced Security Services (ESS) Update	8-2007
[18] ITU-T	RECOMMENDATION X.509 (08/2005) | ISO/IEC 9594-8:2005	
[19] RFC 3548	The Base16, Base32, and Base64 Data Encodings	7-2003
[20] ISO/IEC	3166 Codes for the representation of countries	
[21] NBÚ	Upresnenia obsahu a formálne špecifikácie formátov dokumentov pre ZEP	
[22] CEN/CWA	14170 Security Requirements for Signature Creation Applications	
[23] NBÚ	Kontrola certifikačnej cesty	
[24] RFC 2046	MIME Part Two: Media Types	11-1996
[25] CEN/CWA	14171 General guidelines for electronic signature verification	

[26] SMERNICA EURÓPSKEHO PARLAMENTU A RADY 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy

Poznámka 1: Aktuálne znenie smernice 1999/93/ES je dostupné na adrese: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&model=guicheti&numdoc=31999L0093

4 Skratky

ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
DTD	Document Type Definition
EPES	Explicit Policy-based Electronic Signature
ES-A	Electronic Signature with Archive validation
ES-C	Electronic Signature with Complete validation data
ES-T	Electronic Signature with Time-stamp data
ESS	Enhanced Security Services (enhances CMS)
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
ISO	International Organization for Standardization
MIME	Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PKCS	Public Key Cryptographic Standards, Standards published by RSA, Labs.
RIPEMD-160	Race Integrity Primitives Evaluation Message Digest 160
PKIX	internet X.509 Public Key Infrastructure
QC	Qualified Certificate
RSA	Rivest, Shamir and Adleman Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Algorithm 1
SSCD	Secure-Signature-Creation Device
TSA	Time-Stamping Authorities
TSP	Time Stamp Protocol
TST	Time-Stamp Token
URL	Uniform Resource Locator
XAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language
ZEP	Zaručený elektronický podpis (Qualified Electronic Signature)

5 Pravidlá pre štruktúry ZEP nad AdES

5.1 Podpis v ASN.1 formáte

Tabuľka 1. CMS obálka elektronického podpisu

	Zápis v ASN.1	Stručný popis
1.	`ContentInfo ::= SEQUENCE {`	Obálka CMS, v našom prípade podpisu.
2.	`contentType ContentType,`	OID typu údajov, ktoré obsahuje *content.*
3.	`content [0] EXPLICIT ANY DEFINED BY contentType }`	Údaje identifikované pomocou OID.
4.	`ContentType ::= OBJECT IDENTIFIER`	OID identifikujúci typ.
5.	`id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }`	OID identifikujúci typ podpísané údaje *SignedData*.

Tabuľka 2. CMS typ - podpísané údaje SignedData

	Zápis v ASN.1	Stručný popis
1.	`SignedData ::= SEQUENCE {`	Podpísané údaje identifikované s *id-signedData.*
2.	`version CMSVersion,`	Verzia CMS syntaxe.
3.	`digestAlgorithms DigestAlgorithmIdentifiers,`	Množina identifikátorov algoritmov, ktoré sa použijú na výpočet hašu z podpisovaného dokumentu.
4.	`encapContentInfo EncapsulatedContentInfo,`	Údaje, z ktorých sa vypočíta haš. • interný podpis: OID údajov a samotné údaje • externý podpis: obsahuje iba OID údajov
5.	`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	Množina certifikátov. Musí obsahovať aspoň certifikát(y) podpisovateľa(ov). Ak celé cesty nie sú uložené v atribúte (Tabuľka 14), tak obsahuje aj celé certifikačné cesty v prípade ak sa má použiť podpis pre dlhodobé overenie..
6.	`crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,`	Množina CRL. Nemusí sa použiťak je zoznam CRL uložený v atribúte (Tabuľka 15), inak sa musí použiť.
7.	`signerInfos SignerInfos }`	Množina blokov s podpismi jednotlivých podpisovateľov.
8.	`DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier`	Množina hašovacích algoritmov s ich parametrami definovaná pomocou OID.
9.	`SignerInfos ::= SET OF SignerInfo`	Množina podpisov.

Tabuľka 3. EncapsulatedContentInfo – vložené podpisované údaje

	Zápis v ASN.1	Stručný popis
1.	`EncapsulatedContentInfo ::= SEQUENCE`	Obsahuje údaje, ktoré sa podpisujú.
2.	`{ eContentType ContentType,`	OID typu údajov, ktoré podpisujeme. Typ *id-data* (OID 1.2.840.113549.1.7.1 pre binárne neinterpretovateľné údaje). Pre údaje sa odporúča použiť MIME obálku.
3.	`eContent [0] EXPLICIT OCTET STRING OPTIONAL }`	Ak je *eContent* vynechaný, tak sa haš počíta z externých údajov. Ak obsahuje *eContent,* tak sa haš počíta z obsahu *OCTET STRING* bez tagu a veľkosti *OCTET STRINGu*.

Tabuľka 4. SignerInfo – údaje podpisovateľa s jeho podpisom

	Zápis v ASN.1	Stručný popis
1.	`SignerInfo ::= SEQUENCE {`	Údaje podpisovateľa.
2.	`  version  CMSVersion,`	Verzia syntaxe je podľa RFC 3852.
3.	`  sid  SignerIdentifier,`	Pomocná identifikácia certifikátu podpisovateľa - informatívna. Kvôli kompatibilite s CAdES a podpisu ZEP sa musí použiť identifikátor *IssuerAndSerialNumber*. Skutočný identifikátor je priamo v podpisovaných atribútoch (signingCertificate/V2), na zabránenie substitučnému útoku.
4.	`  digestAlgorithm DigestAlgorithmIdentifier,`	Identifikátor podpisovateľovho hašovacieho algoritmu, ktorým sa vypočíta haš do podpisu. Jeden z algoritmov z Tabuľky 2. riadok 3.
5.	`  signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,`	Množina podpisovaných atribútov. Musí byť.
6.	`  signatureAlgorithm SignatureAlgorithmIdentifier,`	Identifikátor algoritmu, ktorého súkromný kľúč vlastní podpisovateľ. Napr. *RsaEncryption (1.2.840.113549.1.1.1)*
7.	`  signature SignatureValue,`	Digitálny podpis.
8.	`  unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }`	Množina nepodpisovaných atribútov. Obsahuje napríklad časovú pečiatku, ETSI atribúty a iné.
9.	`SignerIdentifier ::= CHOICE {`	Identifikátor certifikátu podpisovateľa.
10.	`  issuerAndSerialNumber IssuerAndSerialNumber,`	Meno vydavateľa certifikátu a sériové číslo certifikátu podpisovateľa.
11.	`  subjectKeyIdentifier [0] IMPLICIT SubjectKeyIdentifier }`	Identifikátor podpisovateľovho verejného kľúča z jeho certifikátu.
12.	`SignedAttributes ::= SET SIZE (1..MAX) OF Attribute`	Množina podpisovaných atribútov. Musia byť v DER kódovaní.
13.	`UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute`	Množina nepodpisovaných atribútov. Odporúča sa DER kódovanie pre všetky položky podpisu.
14.	`Attribute ::= SEQUENCE {`	Atribút sa skladá z:
15.	`  attrType OBJECT IDENTIFIER,`	OID identifikátora,
16.	`  attrValues SET OF AttributeValue }`	a hodnoty podľa OID.
17.	`AttributeValue ::= ANY`	Definované v nasledujúcich tabuľkách.
18.	`SignatureValue ::= OCTET STRING`	Podpis.

Tabuľka 5. CMS podpisované a nepodpisované atribúty

	Zápis v ASN.1	Stručný popis
1.	`id-contentType OBJECT IDENTIFIER ::= {1 2 840 113549 1 9 3}` `contentType ::= OBJECT IDENTIFIER`	Použitie: podpisovaný atribút použitý v atribútoch iba raz. OID typu údajov. Je rovnaký ako v *eContentType* a v atribútoch sa musí nachádzať iba raz. napríklad: *id-data* (1 2 840 113549 1 7 1)
2.	`id-messageDigest OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 4 }` `MessageDigest ::= OCTET STRING`	Použitie: podpisovaný atribút použitý v atribútoch iba raz. Haš sa vypočíta z údajov podľa postupu v tabuľke 3. riadok 3.

3.	`id-signingTime OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 5 }`
	`SigningTime ::= Time`
	`Time ::= CHOICE {`
	`utcTime UTCTime,`
	`generalizedTime GeneralizedTime }`
		Použitie: podpisovaný atribút použitý v atribútoch iba raz.
		Podpisovateľom deklarovaný čas.
		Od 1. januára 1950 a do 31. decembra 2049 musí byť kódovaný v *UTCTime,* potom v *GeneralizedTime* a v časovom pásme Greenwich Mean Time (Zulu) a musí obsahovať sekundy. Aplikácie by mali vedieť spracovať oba typy.
		Formát *UTCTime:* YYMMDDHHMMSSZ,
		GeneralizedTime (ETSI odporúča): YYYYMMDDHHMMSSZ.

4.	`id-countersignature OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 6 }` `Countersignature ::= SignerInfo`	Použitie: iba v nepodpísaných atribútoch. Podpisuje v zreťazení jeden alebo viac podpisov z DER kódovaného atribútu *signature* typu *signatureValue* zo *SignerInfo*. Nie je určený pre ZEP, lebo nepodpisuje údaje, ale len nadradený digitálny podpis, v ktorého nepodpísaných atribútoch sa nachádza. Nie je definovaný pre archívny typ podpisu. Neodporúča sa používať.

Tabuľka 6. Other signing certificate

	Zápis v ASN.1	Stručný popis
1.	`id-aa-ets-otherSigCert OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 19 }`	Použitie: podpisovaný atribút použitý v atribútoch iba raz. Neodporúča sa používať, lebo ho nahradil *ESS signing certificate v2*. OID identifikujúci atribút, s postupnosťou identifikátorov certifikátov od certifikátu podpisovateľa až po koreňový certifikát. Musí obsahovať minimálne identifikátor certifikátu podpisovateľa.

2.	`OtherSigningCertificate ::= SEQUENCE { certs SEQUENCE OF OtherCertID,`
	`policies SEQUENCE OF PolicyInformation OPTIONAL`
	`-- NOT USED IN THE PRESENT DOCUMENT }`
		Certs - postupnosť identifikátorov certifikátov od certifikátu podpisovateľa.
		Policies sa nepoužíva.

3.	`OtherCertID ::= SEQUENCE { otherCertHash OtherHash, issuerSerial IssuerSerial OPTIONAL }`	*OtherCertHash* haš certifikátu. Ak je zadané *issuerSerial,* tak sa musí zadať *directoryName* kvôli jednoduchosti pri vyhľadávaní.

	Zápis v ASN.1	Stručný popis

4.	OtherHash ::= CHOICE {
	  sha1Hash OtherHashValue,
	  -- This contains a SHA-1 hash
	  otherHash OtherHashAlgAndValue}
	OtherHashValue ::= OCTET STRING
	OtherHashAlgAndValue ::= SEQUENCE {
	  hashAlgorithm AlgorithmIdentifier,
	  hashValue OtherHashValue }
		Kvôli kompatibilite sa odporúča používať *haš sha1,* ak nie je potrebné použiť iný hašovací algoritmus.

Tabuľka 7. CertificateRefs

	A.1.1.1 Zápis v ASN.1	Stručný popis
1.	id-aa-ets-certificateRefs OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 21}	Použitie: nepodpisovaný atribút použitý v atribútoch iba raz. OID identifikujúci kompletný zoznam identifikátorov certifikátov celej certifikačnej cesty bez certifikátu podpisovateľa. - položka má iba informatívny význam
2.	CompleteCertificateRefs ::= SEQUENCE OF OtherCertID	Úplný zoznam identifikátorov certifikátov *OtherCertID* celej certifikačnej cesty, ktorá slúži na overenie podpisu certifikátu podpisovateľa. Cesta je bez certifikátu podpisovateľa. *OtherCertID* je definovaný v tabuľke 6 r. 3.

Tabuľka 8. RevocationRefs

	Zápis v ASN.1	Stručný popis
1.	id-aa-ets-revocationRefs OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 22}	Použitie: nepodpisovaný atribút použitý v atribútoch iba raz. OID identifikujúci úplný zoznam identifikátorov CRL alebo OCSP slúžiacich na overenie platnosti certifikátu podpisovateľa a celej certifikačnej cesty, tabuľka 7. - položka má iba informatívny význam

2.	CompleteRevocationRefs ::= SEQUENCE OF CrlOcspRef
	CrlOcspRef ::= SEQUENCE {
	  crlids [0] CRLListID OPTIONAL,
	  ocspids [1] OcspListID OPTIONAL,
	  otherRev [2] OtherRevRefs OPTIONAL
	}
		Úplný zoznam odkazov na CRL alebo OCSP, ktorý začína informáciou na overenie certifikátu podpisovateľa a končí u dôveryhodnej koreňovej CA, presne podľa cesty v tabuľke 7. Pre certifikát identifikovaný pomocou *OtherCertID.*

3.	CRLListID ::= SEQUENCE {
	  crls SEQUENCE OF CrlValidatedID
	}
	CrlValidatedID ::= SEQUENCE {
	  crlHash OtherHash,
	  crlIdentifier CrlIdentifier OPTIONAL }
	CrlIdentifier ::= SEQUENCE {
	  crlissuer Name,
	  crlIssuedTime UTCTime,
	  crlNumber INTEGER OPTIONAL }
	OcspListID ::= SEQUENCE {
	  ocspResponses SEQUENCE OF OcspResponsesID }
	OcspResponsesID ::= SEQUENCE {
		Minimálne jeden *CRLListID* alebo *OcspListID* musí byť definovaný pre každý certifikát z certifikačnej cesty z tabuľky 7.
		V identifikátoroch CRL musí byť zadaný *crlIdentifier.* V *crlIdentifier* nemusí byť zadané *crlNumber*.
		
		V identifikátoroch *OcspResponsesID* musí byť zadaný *ocspRepHash*.

	Zápis v ASN.1	Stručný popis
	ocspIdentifier OcspIdentifier, ocspRepHash OtherHash OPTIONAL } OcspIdentifier ::= SEQUENCE { ocspResponderID ResponderID, -- As in OCSP response data producedAt GeneralizedTime -- As in OCSP response data }	
4.	OtherRevRefs ::= SEQUENCE { otherRevRefType OtherRevRefType, otherRevRefs ANY DEFINED BY otherRevRefType} OtherRevRefType ::= OBJECT IDENTIFIER	Nepoužíva sa.

Tabuľka 9. SignatureTimeStampToken

	Zápis v ASN.1	Stručný popis
1.	id-aa-signatureTimeStampToken OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 14 }	Použitie: nepodpisovaný atribút, ktorý sa môže použiť v atribútoch aj viackrát s rôznymi TSA. OID identifikujúci časovú pečiatku, ktorá opečiatkuje hodnotu podpisu podpisovateľa tabuľka 4 riadok 7.

2.	TimeStampToken ::= ContentInfo
	-- contentType is id-signedData
	-- content is SignedData
	-- eContentType within SignedData
	-- is id-ct-TSTInfo
	-- eContent within SignedData is
	-- TSTInfo
	
	TSTInfo ::= SEQUENCE {
	version INTEGER { v1(1) },
	policy TSAPolicyId,
	messageImprint MessageImprint,
	-- MUST have the same value as the
	-- similar field in TimeStampReq
	serialNumber INTEGER,
	-- Time-Stamping users MUST be
	-- ready to accommodate integers
	-- up to 160 bits.
	genTime GeneralizedTime,
	accuracy Accuracy OPTIONAL,
	ordering BOOLEAN DEFAULT FALSE,
	nonce INTEGER OPTIONAL,
	-- MUST be present if the similar
	-- field was present in
	-- TimeStampReq. In that case it
	-- MUST have the same value.
	tsa [0] GeneralName OPTIONAL,
	extensions [1] IMPLICIT Extensions
	OPTIONAL
	}
	Accuracy ::= SEQUENCE {
	seconds INTEGER OPTIONAL,
	millis [0] INTEGER (1..999)
	OPTIONAL,
	micros [1] INTEGER (1..999)
	OPTIONAL }
		Hodnota v položke *messageImprint* vo vnútri *TimeStampToken* je haš vypočítaný z podpisu podpisovateľa *signature* tabuľka 4 riadok 7, ktorý je vo vnútri SignerInfo v CMS type signedData, ktorá sa časovo opečiatkuje. Časová pečiatka je jediný údaj o čase uložený priamo v podpise, ktorému môžeme pri podpise dôverovať. Neslúži len na získanie informácie o čase, ale aj na zabezpečenie podpisu, ak dôjde ku kompromitovaniu podpisovateľovho kľúča. Ak je podpis opečiatkovaný pred časom, kedy došlo ku skompromitovaniu kľúča, tak sa považuje za platný, lebo časová pečiatka dokazuje, že bol použitý platný kľúč pred skompromitovaním.
		
		CRL alebo OCSP na overenie platnosti časovej pečiatky sa pridávajú do časovej pečiatky a nie do podpisu, ktorého komponenty časová pečiatka opečiatkovala.
		
		Časovo opečiatkovať je možné aj ľubovoľný elektronický dokument a tak dokázať jeho neporušenú existenciu ešte pred časom jeho samotného podpisovania. Pri podpisovaní sa potom táto časová pečiatka vloží do podpisovaného atribútu *id-aa-ets-contentTimestamp*.
		Podrobnejší popis poskytuje Príloha D.

Tabuľka 10. EscTimeStamp

	Zápis v ASN.1	Stručný popis
1.	`id-aa-ets-escTimeStamp OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 25}`	Použitie: nepodpisovaný atribút, ktorý sa môže použiť v atribútoch aj viackrát s rôznymi TSA. OID identifikujúci časovú pečiatku, ktorej účelom je ochrániť platnosť elektronického podpisu, ak dôjde k skompromitovaniu kľúča CA a zrušeniu CA certifikátu.
2.	`ESCTimeStampToken ::= TimeStampToken`	Časová pečiatka opečiatkuje haš, ktorý uloží do *messageImprint* položky v *TimeStampToken.* Haš sa vypočíta zo spojených hodnôt položiek (V DER bez typu a veľkosti zakódovanej hodnoty) z nasledujúcich atribútov: • *OCTETSTRING* zo *SignatureValue* položky z vnútra SignerInfo; • signature-time-stamp tabuľka 9; • complete-certificate-references tabuľka 7; • complete-revocation-references tabuľka 8.

Tabuľka 11. CertCRLTimestamp

	Zápis v ASN.1	Stručný popis
1.	`id-aa-ets-certCRLTimestamp OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 26}`	Použitie: nepodpisovaný atribút, ktorý sa môže použiť v atribútoch aj viackrát s rôznymi TSA. OID identifikujúci časovú pečiatku, ktorej účelom je ochrániť platnosť elektronického podpisu, ak dôjde k skompromitovaniu CA kľúča a zrušeniu platnosti CA certifikátu, opečiatkovaním iba odkazov na CA certifikáty a zoznamov zrušených certifikátov.
2.	`TimestampedCertsCRLs ::= TimeStampToken`	Časová pečiatka opečiatkuje haš, ktorý uloží do *messageImprint* položky v *TimeStampToken.* Haš sa vypočíta zo spojených hodnôt položiek (v DER bez typu a veľkosti zakódovanej hodnoty) z nasledujúcich atribútov: • complete-certificate-references tabuľka 7; • complete-revocation-references tabuľka 8. Umožní to zefektívnenie celej prevádzky TSA, ktorá vydáva časové pečiatky pre veľké organizácie. CA si pri vydaní nového CRL opečiatkuje kompletný zoznam certifikátov a CRL iba raz. Potom tento opečiatkovaný zoznam zverejní a jednotliví podpisovatelia ho do podpisu pridajú bez nutnosti ďalšieho pečiatkovania.

Tabuľka 12. ArchiveTimestamp

	Zápis v ASN.1	Stručný popis
1.	`id-aa-ets-archiveTimestamp OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 48}`	Použitie: nepodpisovaný atribút, ktorý sa môže použiť v atribútoch aj viackrát s rôznymi TSA. OID identifikujúci časovú pečiatku, ktorej účelom je dlhodobé archivovanie elektronického podpisu s kompletnými certifikátmi a údajmi na overenie platnosti, aby bolo možné elektronický podpis overiť, aj keď dôjde po časovom opečiatkovaní k skompromitovaniu CA kľúča a zrušeniu platnosti CA certifikátu, nedostupnosti CA alebo iným dôvodom, ako napríklad, ak sa stane podpisový algoritmus po čase menej bezpečný. Pred exspirovaním alebo zrušením archívneho TSA certifikátu, ak je potrebné dlhodobé overenie, je potrebné opätovné pridanie novej *archiveTimestamp.*
2.	`ArchiveTimeStampToken ::= TimeStampToken`	Časová autorita TSA opečiatkuje (podpíše) haš s algoritmom s väčším kľúčom, aby ochránila podpis na dlhšiu dobu, ktorý uloží do *messageImprint* položky v *TimeStampToken.* Haš sa vypočíta zo spojených hodnôt z položiek v takom poradí, v akom sú uvedené v podpise, pričom položky *Attribute* sa použijú v takom poradí, v akom sa nachádzajú v nepodpísaných atribútoch podpisu. Príloha D. Pri overovaní sa používa schválená podpisová politika platná k času vydania overovanej časovej pečiatky.

Tabuľka 13. SigningCertificate

	Zápis v ASN.1	Stručný popis
1.	`id-aa-signingCertificate OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 12 }`	Použitie: podpisovaný atribút, ktorý sa môže použiť v atribútoch iba raz. Namiesto neho sa odporúča použiť *ESS signing certificate v2* tabuľka 20 [17]. OID identifikujúci atribút s postupnosťou identifikátorov certifikátov od certifikátu podpisovateľa až po koreňový (NBÚ) certifikát. Musí obsahovať minimálne identifikátor certifikátu podpisovateľa.
2.	`SigningCertificate ::= SEQUENCE { certs SEQUENCE OF ESSCertID, policies SEQUENCE OF PolicyInformation OPTIONAL }`	*Certs* - postupnosť identifikátorov certifikátov od certifikátu podpisovateľa. *Policies* sa nepoužíva.
3.	`ESSCertID ::= SEQUENCE { certHash Hash, issuerSerial IssuerSerial OPTIONAL }`	*CertHash* haš SHA-1 certifikátu. Ak je zadané *issuerSerial,* tak sa musí zadať *directoryName* kvôli jednoduchosti pri vyhľadávaní.
4.	`Hash ::= OCTET STRING -- SHA1 hash` `IssuerSerial ::= SEQUENCE { issuer GeneralNames, serialNumber CertificateSerialNumber}`	Používa sa iba haš *sha1* z celého certifikátu.

Tabuľka 14. CertValues

	Zápis v ASN.1	Stručný popis
1.	id-aa-ets-certValues OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 23}	Použitie: nepodpisovaný atribút, ktorý sa môže použiť v atribútoch iba raz. OID identifikujúci zoznam certifikátov minimálne celej certifikačnej cesty bez certifikátu podpisovateľa, podľa odkazov z tabuľky 7. Môže obsahovať aj iné certifikáty, napríklad krížové, alebo pre overenie nepriamych CRL či OCSP odpovede.
2.	CertificateValues ::= SEQUENCE OF Certificate	Zoznam certifikátov X.509

Tabuľka 15. RevocationValues

	Zápis v ASN.1	Stručný popis
1.	id-aa-ets-revocationValues OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 24}	Použitie: nepodpisovaný atribút, ktorý sa môže použiť v atribútoch iba raz. OID identifikujúci zoznam CRL a OCSP minimálne celej certifikačnej cesty, podľa odkazov z tabuľky 8. Môže obsahovať aj iné CRL a OCSP, napríklad slúžiace na overenie krížových certifikátov či CRL alebo OCSP.

2.	RevocationValues ::= SEQUENCE {
	crlVals [0] EXPLICIT SEQUENCE OF CertificateList OPTIONAL,
	ocspVals [1] EXPLICIT SEQUENCE OF BasicOCSPResponse OPTIONAL,
	otherRevVals [2] EXPLICIT OtherRevVals OPTIONAL }
	OtherRevVals ::= SEQUENCE {
	otherRevValType OtherRevValType,
	otherRevVals ANY DEFINED BY OtherRevValType }
	OtherRevValType ::= OBJECT IDENTIFIER
		Zoznam CRL a OCSP informácií o zrušení platnosti certifikátov podľa odkazov z tabuľky 8.

Tabuľka 16. SignerLocation

	Zápis v ASN.1	Stručný popis
1.	id-aa-ets-signerLocation OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 17}	Použitie: podpisovaný atribút, ktorý sa môže použiť v atribútoch iba raz. OID identifikujúci pomocnú informáciu o adrese miesta (poštovej ITU-T), kde podpisovateľ vykonal elektronické podpísanie
2.	SignerLocation ::= SEQUENCE { -- at least one of the following -- shall be present countryName [0] DirectoryString OPTIONAL, localityName [1] DirectoryString OPTIONAL, -- As used to name a locality in X.500 postalAdddress [2] PostalAddress OPTIONAL } PostalAddress ::= SEQUENCE SIZE(1..6) OF DirectoryString	Adresa miesta podpisu, napríklad mesta, kde podpisovateľ vykonal elektronické podpísanie. Text v položkách *DirectoryString* je neprázdny a musí sa použiť *UTF8String* kódovanie. Formát *PostalAddress* je 6 riadkov x 30 znakov 1. Ulica Číslo 2. Smerové číslo Lokalita 3. Štát

Tabuľka 17. SigPolicyId

	Zápis v ASN.1	Stručný popis
1.	`id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 15 }`	Použitie: podpisovaný atribút, ktorý sa môže použiť v atribútoch iba raz. OID identifikujúci podpisovú politiku, ktorá bola použitá. Podpisová politika určuje minimálne technické bezpečnostné pravidlá, ktoré musí podpisovateľ a overovateľ dodržať, aby sa certifikát a elektronický podpis mohol považovať za platný a v súlade s obsahom položky *FieldOfApplication* z podpisovej politiky. Definuje napr. množinu bezpečných algoritmov pre výpočet haš a minimálne veľkosti kľúčov pre asymetrické algoritmy použité v certifikátoch a elektronických podpisoch.

2.	`SignaturePolicyIdentifier ::=CHOICE{`
	`SignaturePolicyId SignaturePolicyId,`
	`SignaturePolicyImplied`
	`SignaturePolicyImplied`
	`-- not used in this version }`
	`SignaturePolicyId ::= SEQUENCE {`
	`sigPolicyId SigPolicyId,`
	`sigPolicyHash SigPolicyHash,`
	`sigPolicyQualifiers SEQUENCE SIZE`
	`(1..MAX) OF`
	`SigPolicyQualifierInfo OPTIONAL }`
	`SignaturePolicyImplied ::= NULL`
	`SigPolicyId ::= OBJECT IDENTIFIER`
		Používa sa len *SigPolicyId* - OID identifikátor, ktorý jednoznačne identifikuje podpisovú politiku, ktorá je pri podpisovaní a overovaní použitá.

3.	`SigPolicyHash ::=OtherHashAlgAndValue`	Obsahuje identifikátor hašovacieho algoritmu a hašu z podpisovej politiky. Ak podpisová politika je v ASN.1 v DER kódovaní, tak zo `signPolicyHashAlg` a `signPolicyInfo` sa vypočíta haš.

4.	`SigPolicyQualifierInfo ::= SEQUENCE {`
	`sigPolicyQualifierId`
	`SigPolicyQualifierId,`
	`sigQualifier ANY DEFINED BY`
	`sigPolicyQualifierId }`
		Tu je definovaná adresa, z ktorej je možné podpisovú politiku získať.

5.	`-- sigpolicyQualifierIds defined`
	`-- in the present document`
	`SigPolicyQualifierId ::= OBJECT`
	`IDENTIFIER`
	`id-spq-ets-uri OBJECT IDENTIFIER ::=`
	`{ 1 2 840 113549 1 9 16 5 1 }`
	`SPuri ::= IA5String`
	`id-spq-ets-unotice OBJECT IDENTIFIER`
	`::= { 1 2 840 113549 1 9 16 5 2}`
	`SPUserNotice ::= SEQUENCE {`
	`noticeRef NoticeReference OPTIONAL,`
	`explicitText DisplayText OPTIONAL }`
	`NoticeReference ::= SEQUENCE {`
	`organization DisplayText,`
	`noticeNumbers SEQUENCE OF INTEGER }`
	`DisplayText ::= CHOICE {`
	`visibleString VisibleString (SIZE`
		V *SPuri* je informatívna internetová adresa na získanie podpisovej politiky napríklad v kódovaní ASN.1 DER.
		
		V *SPUserNotice* je zobrazená informácia o podpisovej politiky, jej type a možnom použití.
		
		Pri overovaní podpisu sa vždy musí zobraziť overovateľovi OID politiky, haš z politiky a obsah *SPUserNotice* v čitateľnej podobe.

	Zápis v ASN.1	Stručný popis
	(1..200)), bmpString BMPString (SIZE (1..200)), utf8String UTF8String(SIZE(1..200))}	

Tabuľka 18. ContentTimestamp

	Zápis v ASN.1	Stručný popis
1.	id-aa-ets-contentTimestamp OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 20}	Použitie: podpisovaný atribút, ktorý sa môže použiť v atribútoch aj viackrát s rôznymi TSA. OID identifikujúci časovú pečiatku, ktorej účelom je potvrdiť, že forma podpisovaných údajov existovala už v čase vydania časovej pečiatky a teda pred samotným podpisom. C*ontentTimestamp,* vypočítaný z podpisovaných údajov, je možné vložiť alebo vytvoriť v procese podpisovania.
2.	ContentTimestamp ::= TimeStampToken	Časová pečiatka opečiatkuje haš, ktorý uloží do *messageImprint* položky v *TimeStampToken.* Haš sa vypočíta z údajov podľa postupu v tabuľke 3 riadok 3. Alebo podľa postupu, ktorý definuje Príloha D.

Tabuľka 19. Signer attribute - atribúty podpisovateľa (rola)

	Zápis v ASN.1	Stručný popis
1.	id-aa-ets-signerAttr OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 18}	Použitie: podpisovaný atribút, ktorý sa môže použiť v atribútoch iba raz. OID identifikujúci atribúty podpisovateľa, ktorých účelom je potvrdiť, že podpisované údaje boli podpisované podpisovateľom v role, ktorú prehlasuje alebo preukazuje prostredníctvom atribútového certifikátu.

2.	SignerAttribute ::= SEQUENCE OF
	CHOICE {
	claimedAttributes
	[0] ClaimedAttributes,
	certifiedAttributes
	[1] CertifiedAttributes
	}
	ClaimedAttributes ::= SEQUENCE OF
	Attribute
	CertifiedAttributes ::=
	AttributeCertificate -- as defined
	-- in RFC 3281: see clause 4.1.
		Roly, ktoré podpisovateľ len prehlasuje, sa uvádzajú do atribútu `claimedAttributes`.
		Certifikované roly pomocou atribútových certifikátov sa uvádzajú do `CertifiedAttributes`.

Tabuľka 20. ESS signing certificate v2

	Zápis v ASN.1	Stručný popis
1.	`id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= { 1 2 840 113549 1 9 16 2 47}`	Použitie: podpisovaný atribút použitý v atribútoch iba raz. OID identifikujúci atribút s postupnosťou identifikátorov certifikátov od certifikátu podpisovateľa až po koreňový (NBÚ) certifikát. Musí obsahovať minimálne identifikátor certifikátu podpisovateľa. [17]
2.	`SigningCertificateV2 ::= SEQUENCE { certs SEQUENCE OF ESSCertIDv2, policies SEQUENCE OF PolicyInformation OPTIONAL }`	*Certs* - postupnosť identifikátorov certifikátov od certifikátu podpisovateľa. *Policies* sa nepoužíva.
3.	`ESSCertIDv2 ::= SEQUENCE { hashAlgorithm AlgorithmIdentifier DEFAULT {algorithm id-sha256 }, certHash Hash, issuerSerial IssuerSerial OPTIONAL }`	*certHash* haš certifikátu. Ak je zadané *issuerSerial,* tak sa musí zadať *directoryName* kvôli jednoduchosti pri vyhľadávaní.
4.	`Hash ::= OCTET STRING` `IssuerSerial ::= SEQUENCE { issuer GeneralNames, serialNumber CertificateSerialNumber }`	Kvôli kompatibilite sa odporúča používať haš *sha1,* ale iba ak nie je požadovaný iný bezpečnejší hašovací algoritmus.

5.2 Podpis v XML formáte

Pravidlá pre obsah atribútov v ASN.1 CMS podpise definované v kapitole 5.1 platia rovnako pre obsah elementov v XML podpise , ktorý je špecifikovaný v dokumente XAdES ETSI TS 101 903. Kvôli jednoznačnosti pri definovaní povinných atribútov zaručeného elektronického podpisu je uvedená tabuľka, ktorá atribútu z ASN.1 podpisu priraďuje XML element z XML podpisu.

Tabuľka 21. Atribúty ASN.1 a XML elementy ZEP s rovnakým významom obsahu

	ASN.1 atribút	XML element
1.	(id-contentType)	*(DataObjectFormat)*+ pri MIME obálke je typ MimeType = "message/rfc822" a Encoding = "base64" a ak nie je použitá MIME obálka, tak typ uvedený v MimeType musí byť v súlade s dokumentom [21].
2.	(id-messageDigest)	Nemá ekvivalent v XML podpise. V XML podpise je haš počítaný na základe pravidiel definovaných v dokumente XAdES a je obsiahnutý v elemente *DigestValue* .
3.	(id-signingTime)	*(SigningTime)*
4.	(id-aa-ets-signingCertificateV2) alebo (id-aa-signingCertificate)	*(SigningCertificate)*
5.	(id-aa-ets-sigPolicyId)	*(SignaturePolicyIdentifier)*
6.	(id-aa-ets-contentTimestamp)*	*(AllDataObjectsTimeStamp)** alebo *(IndividualDataObjectsTimeStamp)**
7.	(id-aa-ets-signerLocation)?	*(SignatureProductionPlace)?*
8.	(id-aa-ets-certificateRefs)	*(CompleteCertificateRefs)*
9.	(id-aa-ets-revocationRefs)	*(CompleteRevocationRefs)*
10.	(id-aa-signatureTimeStampToken)+	*(SignatureTimeStamp)*+
11.	((id-aa-ets-escTimeStamp)* (id-aa-ets-certCRLTimestam)*)+	*((SigAndRefsTimeStamp)** *(RefsOnlyTimeStamp)*)*+
12.	(id-aa-ets-archiveTimestamp)+	*(ArchiveTimeStamp)*+
13.	(id-aa-ets-certValues)	*(CertificatesValues)*
14.	(id-aa-ets-revocationValues)	*(RevocationValues)*
15.	(id-aa-ets-signerAttr)	*(SignerRole)*

Výskyt ASN.1 atribútu v CMS podpise a XML elementu v XML podpise:

( ) - iba jeden raz
( )* - nemusí, ale môže byť aj viackrát
( )? - nemusí, ale môže byť jedenkrát
( )+ - musí byť minimálne jedenkrát

Pri implementácii XML podpisu sa musí použiť namespace URI http://uri.etsi.org/01903/v1.3.2#

Pri XML schéme sa musia použiť nasledujúce deklarácie namespace XML

```
<?xml version="1.0"?>
<schema
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns="http://uri.etsi.org/01903/v1.3.2#"
```

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

Detailnejšie informácie o profiloch XAdES podpisov používaných v administratívnom styku na výmenu XML podpísaných údajov a upresnenia použitia jednotlivých XAdES elementov definujú profily uvedené v dokumente: Profil XAdES_ZEP - formát zaručeného elektronického podpisu na báze XAdES[1].

Poznámka 1: V prípade nejednoznačnosti požiadaviek z odkazovaného dokumentu Profil XAdES_ZEP s požiadavkami uvedenými v tomto NBÚ štandarde, sú záväzné požiadavky tohoto štandardu.

5.3 Ostatné formáty podpisov a PAdES

Smernica Európskeho parlamentu a Rady 1999/93/ES [26] ako aj vyhláška NBÚ č. 135/2009 Z. z. neobmedzujú formát zdokonaleného elektronického podpisu len na CMS či XML formát podpisu, ale umožňujú implementáciu podpisu aj v iných formátoch, ktoré zabezpečujú nimi stanovené požiadavky. Príkladom je PDF AdES či PGP AdES, alebo aj iné formáty podpisu používané v rôznych typoch dokumentov. V súčasnosti tieto formáty neumožňujú uloženie všetkých potrebných údajov na overenie platnosti kvalifikovaného certifikátu, ktorý musí byť vydaný na verejný kľúč prislúchajúci k súkromnému kľúču uloženému na SSCD podpisovateľa. Aby sa zabezpečila krátkodobá ale aj dlhodobá overiteľnosť týchto formátov podpisov, je potrebné definovanie jednotného miesta uloženia údajov na krátkodobé a dlhodobé overenie platnosti týchto podpisov.

Údaje na overenie krátkodobej a dlhodobej platnosti podpisov pozostávajú minimálne z:

- časovej pečiatky, ktorej haš hodnota pri výpočte zahŕňa minimálne digitálny podpis podpisovateľa,
- údajov na overenie platnosti vo forme CRL alebo OCSP pre certifikáty: podpisovateľa, časovej pečiatky, CA a certifikátov na overenie údajov o zrušení platnosti certifikátov (nepriame CRL alebo OCSP),
- podpisových certifikátov pre overenie podpisu časovej pečiatky, CRL, OCSP a podpisu dokumentu,
- krížových a CA certifikátov,
- použitých podpisových politík.

Pre zabezpečenie kompatibility a možnosti dlhodobého overovania je definovaný jednotný formát pre uloženie týchto údajov v prílohe E.2 a pre zabezpečenie časového opečiatkovania aj pre formáty, ktoré neumožňujú pridanie časovej pečiatky pre dlhodobú overiteľnosť, je definovaný Integritný typ podpisu v prílohe B.2, ktorý sa musí v tomto prípade doplniť o časovú pečiatku podpisu. Všetky typy podpisov je možné dlhodobo archivovať aj pomocou postupu, ktorý popisuje Príloha B.

[1] XAdES_ZEP v1.0 - http://www.ditec.sk/ep/signature_formats/xades_zep/v1.0
XAdES_ZEP v1.0 - http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1
Formát zloženého podpisu v1.0 - http://www.ditec.sk/ep/signature_formats/xades_zep_data_signatures/v1.0
Formát zloženého podpisu v1.1 - http://www.ditec.sk/ep/signature_formats/xades_zep_data_signatures/v1.1

Príloha A (normatívna) Formáty zaručených elektronických podpisov

Zaručené elektronické podpisy slúžiace na komunikáciu s orgánmi verejnej moci v Slovenskej republike vytvorené od 1.1.2008 musia byť typu CAdES [1] alebo XAdES [16], iné typy než CAdES a XAdES sa nesmú použiť. CAdES alebo XAdES podpisy musia obsahovať všetky povinné atribúty, ktoré sú pre jednotlivé formáty ZEP požadované, ale môžu obsahovať aj iné, nižšie nešpecifikované voliteľné atribúty.

Vzhľadom na potrebu interoperability je pre komunikáciu s orgánmi verejnej moci v Slovenskej republike odporúčané podpisovať MIME obálku obsahujúcu elektronické dokumenty podľa pravidiel dokumentu [21] vydaného NBÚ na základe § 3 ods. 5 vyhlášky NBÚ č. 136/2009 Z. z.

Poznámka 2: MIME obálka umožňuje jednoznačne priradiť MIME typ a kódovanie k elektronickému dokumentu, taktiež zabezpečí jednotnú binárnu formu podpisovaného dokumentu, čo umožní kompatibilitu podpisov typu XAdES a CAdES, ktoré podpisujú rovnaký haš, vďaka čomu nevzniká nejednoznačnosť pri viacnásobnom podpise.

Poznámka 3: Pri priamom podpise elektronického dokumentu v XAdES podpise bez použitia MIME obálky je možné použiť rôzne kanonikalizačné funkcie, a teda podpisovať rôzne haš hodnoty z rovnakého dokumentu, čo pri viacnásobných podpisoch môže spôsobiť nejednoznačnosť; jej riešením je podpisovanie MIME obálky aj pri XAdES.

Poznámka 4: Ak atribút *id-aa-ets-sigPolicyId* nie je súčasťou podpisovaných atribútov alebo nie je použitý OID a hash publikovaný v dôveryhodnom zozname úradu, potom aplikácia pre ZEP musí zabezpečiť preverenie, že pri podpisovaní a overovaní ZEP boli splnené všetky požiadavky aspoň jednej podpisovej politiky platnej a schválenej NBÚ v čase vytvorenia podpisu. (Požiadavka pre zabezpečenie interoperability v EU, pri splnení národných minimálnych požiadaviek napríklad na veľkosti kľúčov a typy algoritmov.)

A.1 Zaručený elektronický podpis bez časovej pečiatky

Povinné atribúty:

```
id-contentType
id-messageDigest
id-aa-ets-signingCertificateV2 alebo id-aa-signingCertificate
id-aa-ets-sigPolicyId
```

Voliteľné atribúty:

```
id-signingTime
id-aa-ets-contentTimestamp
id-aa-ets-signerLocation
id-aa-ets-certificateRefs
id-aa-ets-revocationRefs
id-aa-signatureTimeStampToken
id-aa-ets-escTimeStamp alebo id-aa-ets-certCRLTimestamp
id-aa-ets-archiveTimestamp
id-aa-ets-certValues
id-aa-ets-revocationValues
id-aa-ets-signerAttr
```

A.2 Zaručený elektronický podpis s časovou pečiatkou

Povinné atribúty:

```
id-contentType
id-messageDigest
id-aa-ets-signingCertificateV2 alebo id-aa-signingCertificate
id-aa-ets-sigPolicyId
id-aa-signatureTimeStampToken
```

Voliteľné atribúty:

```
id-signingTime
id-aa-ets-contentTimestamp
id-aa-ets-signerLocation
id-aa-ets-certificateRefs
id-aa-ets-revocationRefs
id-aa-ets-escTimeStamp alebo id-aa-ets-certCRLTimestamp
id-aa-ets-archiveTimestamp
id-aa-ets-certValues
id-aa-ets-revocationValues
id-aa-ets-signerAttr
```

A.3 Zaručený elektronický podpis s úplnou informáciou na overenie platnosti

Povinné atribúty:

```
id-contentType
id-messageDigest
id-aa-ets-signingCertificateV2 alebo id-aa-signingCertificate
id-aa-ets-sigPolicyId
id-aa-signatureTimeStampToken
id-aa-ets-certificateRefs
id-aa-ets-revocationRefs
id-aa-ets-certValues alebo v SignedData.certificates musia byť všetky certifikáty na overenie podpisového certifikátu až po Trust Anchor (koreňový certifikát)
```

Voliteľné atribúty:

```
id-signingTime
id-aa-ets-escTimeStamp alebo id-aa-ets-certCRLTimestamp
id-aa-ets-contentTimestamp
id-aa-ets-signerLocation
id-aa-ets-archiveTimestamp
id-aa-ets-revocationValues
id-aa-ets-signerAttr
```

Poznámka 5: Tento typ podpisu vzhľadom na zistené nedostatky pri uvádzaní nepriamych CRL a OCSP sa neodporúča používať.

A.4 Archívny zaručený elektronický podpis

Povinné atribúty:

```
id-contentType
id-messageDigest
id-aa-ets-signingCertificateV2 alebo id-aa-signingCertificate
id-aa-ets-sigPolicyId
id-aa-signatureTimeStampToken
id-aa-ets-certValues
id-aa-ets-revocationValues
id-aa-ets-archiveTimestamp
```

Voliteľné atribúty:

```
id-signingTime
id-aa-ets-certificateRefs
id-aa-ets-revocationRefs
```

```
id-aa-ets-escTimeStamp alebo id-aa-ets-certCRLTimestamp
id-aa-ets-contentTimestamp
id-aa-ets-signerLocation
id-aa-ets-signerAttr
```

Poznámka 6: Archívny podpis slúži hlavne na ochranu podpisu podpisovateľa z dlhodobého hľadiska, aby bolo možné podpis overiť a považovať ho za platný aj v prípadoch, ak dôjde ku kompromitácii CA alebo znemožneniu prístupu k informáciám o CRL, OCSP alebo, ak algoritmy použité na vytvorenie podpisu sa po dlhšej dobe stanú menej bezpečnými. V takýchto prípadoch bude možné podpis overiť a považovať za platný vďaka tomu, že archívny podpis zabezpečí podpisom časovej pečiatky dlhodobejšie dôveryhodné uzavretie obsahu všetkých potrebných informácií na overenie podpisu.

Poznámka 7: Archivovanie elektronického podpisu pomocou archívneho zaručeného podpisu vyžaduje samostatné archívne opečiatkovanie každého podpisu so silnejším kľúčom a v dostatočne dlhých časových intervaloch, čo so všetkými certifikátmi a údajmi potrebnými na overenie platnosti certifikátov je neefektívne pri väčších počtoch podpisov a preto sa odporúča, pri systémoch archivujúcich veľké množstvo elektronických podpisov, použitie integritného podpisu podľa postupu v Príloha B.

A.5 Viacnásobný podpis

Ak je použitý viacnásobný podpis, tak pri overovaní elektronického podpisu sa platnosť podpisov jednotlivých podpisovateľov overuje samostatne. Neplatnosť podpisu jedného podpisovateľa nespôsobí neplatnosť podpisu iného podpisovateľa, ktorý bol predtým platný a ktorý podpísal rovnaký dokument. Zreťazené podpisy (countersignature) sa pri ZEP neodporúča používať.

Viacnásobný podpis XAdES alebo súčasne XAdES s CAdES nie je možné zrealizovať pomocou jedného ETSI formátu a tak je definované uloženie ETSI formátov do „ZEPf (ZIP) formátu“, ktorý umožňuje zrealizovanie viacnásobného podpisu nad binárne rovnakým podpísaným dokumentom uložením v MIME obálke podľa [21].

Príloha B (normatívna) Postup uchovania a formát podpisu pre dlhodobé uchovanie elektronických dokumentov podpísaných ZEP

Pre účel dlhodobého uchovania elektronických dokumentov a podpísaných elektronických dokumentov podpisom ZEP alebo dokumentov podpísaných inými typmi podpisu sa použije integritný typ podpisu definovaný v kapitole B.2 spôsobom definovaným v B.1, ak nie je použitý iný postup zabezpečujúci integritu archivovaných údajov, ktorý umožňuje overenie k dôveryhodnému času, ku ktorému použité kľúče, algoritmy, archivované údaje boli overené ako platné, nepoškodené a po tomto čase je ich akákoľvek zmena odhaliteľná.

B.1 Postup pri vytvorení a kontrole integritného podpisu súborov

Zo súborov dokumentov a súborov podpisov, ktoré je potrebné integritne zabezpečiť napríklad pri archivovaní sa podľa B.2 vytvorí postupnosť odkazov na integritne zabezpečené dokumenty, ktorá sa podpíše, čím sa vytvorí prvý integritný podpis.
Pred skončením platnosti certifikátu podpisovateľa prvého integritného podpisu, alebo certifikátu časovej pečiatky tohto digitálneho podpisu, ak bola na integritný podpis pridaná časová pečiatka, sa vypočíta nová postupnosť zo všetkých súborov z predchádzajúceho integritného podpisu použitím aktuálne bezpečného haš algoritmu. Predchádzajúci integritný podpis a aj jeho časová pečiatka sa doplnia o všetky certifikáty potrebné na ich overenie spolu aj s údajmi na overenie platnosti (CRL, OCSP) týchto certifikátov až po dôveryhodný koreňový certifikát. Na koniec novej postupnosti sa pridá záznam na súbor s predchádzajúcim integritným podpisom. Nová postupnosť sa podpíše novým kľúčom, ku ktorému bol vydaný certifikát s platnosťou dlhšou než bol predchádzajúci integritný podpis.

Pri overovaní [25] sa postupuje v opačnom poradí. Najprv sa overí najnovší inegritný podpis, potom sa prekontrolujú haš hodnoty z textového dokumentu a takto sa postupuje až po prvý integritný podpis. Overovanie každého podpisu prebieha k času z časovej pečiatky podpisu, alebo ak podpis neobsahuje časovú pečiatku, tak k času z nasledujúceho integritného podpisu, ktorý môže obsahovať CRL alebo OCSP na overenie predchádzajúceho integritného podpisu. Pri overovaní sa môžu overiť aj haše jednotlivých súborov uvedených v podpísanom textovom dokumente, kde ale chybný haš nespôsobí chybu overenia integritného podpisu, ale výsledkom bude len informácia, že integritne archivovaný súbor bol od poslednej integritnej archivácie zmenený.

Výstupom overenia dlhodobého uchovania elektronických dokumentov bude:

- stav overenia,
- overovaný elektronický súbor,
- postupnosť integritných podpisov od prvého až po aktuálny integritný podpis, čo umožní spätné overenie integrity a platnosti elektronického dokumentu ľubovoľnému overovateľovi, pričom neumožní získať obsah ostatných integritne archivovaných elektronických dokumentoch iba ich názov, haš a poznámku.

B.2 Integritný elektronický podpis

Integritný elektronický podpis je interný CMS podpis podľa A.1 s nepovinnou časovou pečiatkou, ktorý podpisuje textový dokument kódovaný v UTF8, ktorého vnútorná štruktúra pozostáva z postupnosti riadkov ktorých formát je definovaný v B.3, pričom riadok s návestím NOTICE je nepovinný a riadok s návestím FILE s nasledujúcim riadkom s návestím HASH s haš hodnotou sú povinné. Integritný elektronický podpis sa ukladá do súboru s koncovkou „.P7M“. Textový dokument je uložený do položky *encapContentInfo v SignedData* (tabuľka 2 riadok 4.).

B.3 Formát textového dokumentu

Oddeľovač riadkov:
CRLF znak (13) + znak (10)

Textový dokument v UTF8 kódovaní pozostáva s neprázdnej opakujúcej sa postupnosti trojice riadkov, ktoré začínajú návestím **FILE, HASH** a nepovinným riadkom s návestím **NOTICE.**

FILE =<[URL]|[názov súboru]>CRLF
HASH (< algoritmus >**:**<OID algoritmu >**) =**< haš súboru - veľké písmená >CRLF
NOTICE=< poznámka, napríklad meno archívneho CD/DVD disku >CRLF

B.4 Príklad postupnosti atribútov súborov

FILE=odmeny.eml
HASH(SHA1:1 3 14 3 2 26) = F15BF971C276AC7173065A741DF998C00DF44F31
NOTICE= Podpisovaný súbor.
FILE=http://www.example.sk/other/rules.doc
HASH(SHA1:1 3 14 3 2 26) = 8A01657D752FEFF5A7F3E7910C2C5D45D708D7EB
NOTICE= Originálny súbor, ktorý nespĺňa požiadavky na formát dokumentu povoleného pre ZEP.

Integritný podpis je možné použiť aj na archivovanie súborov, napríklad publikovaných na webe alebo v archívnych CD/DVD alebo súborových serveroch. Položka FILE môže obsahovať iba meno súboru, alebo URL na súbor, alebo kompletnú cestu s názvom súboru v súborovom systéme, na ktorom sa integritná archivácia zrealizovala. V poznámke k menu súboru sa môže uviesť napríklad meno CD/DVD média alebo fyzické umiestnenie v sklade – archíve, či iné potrebné poznámky ku integritne archivovanému súboru. Integritný podpis neslúži na dlhodobú archiváciu, ale iba na zabezpečenie integrity dokumentov počas doby použiteľnosti hašovacích a podpisových algoritmov, ktoré sú použité v podpisovanom TXT dokumente a podpise. Predpokladaná overiteľnosť integritného podpisu je maximálne do času, dokedy sú hašovacie algoritmy použité v TXT dokumente považované za bezpečné a maximálne do času, do kedy je možné získať dôveryhodný stav platnosti o použitých certifikátoch v integritnom podpise.

Príloha C (normatívna) Uloženie certifikačných ciest vo všetkých formátoch ZEP

Atribúty, ktoré v zaručených elektronických podpisoch jednoznačne identifikujú certifikačnú cestu, ktorú vložil podpisovateľ a ktorú musí použiť overovateľ:

CAdES: id-aa-ets-signingCertificateV2 alebo id-aa-signingCertificate
XAdES: SigningCertificate

Tieto atribúty sa naplnia odkazmi na certifikáty podľa zostavenej certifikačnej cesty. Certifikačná cesta sa zostaví a overuje na základe pravidiel definovaných v dokumente NBÚ [23], ktorý upresňuje hlavne profil RFC 5280 z ITU-T X.509, kde nie sú definované pravidlá pre kvalifikované certifikáty.

Príloha D (normatívna) Výpočet časovej pečiatky

Nasledujúca tabuľka popisuje atribúty, ktoré sú zahrnuté pri výpočte haš hodnoty, ktorá je uložená v položke *messageImprint* vo vnútri v *TimeStampToken*.

Tabuľka 22. Identifikácia atribútov podpisu, z ktorých sa počíta haš

Typ časovej pečiatky	Identifikácia
id-aa-ets-contentTimestamp	D
id-aa-signatureTimeStampToken	S
id-aa-ets-archiveTimestamp	A

ASN.1 údajové elementy, ktoré sú zahrnuté ako súčasť nadradeného objektu pri počítaní haš hodnoty, sú označované pomocou ‘" ‘.

Tabuľka 23. CAdES podpis v ASN.1

ASN.1
ContentInfo ::= SEQUENCE {
contentType ContentType, -- id-signedData
content [0] EXPLICIT ANY DEFINED BY contentType }

Tabuľka 24. Úplné SignedData v ASN.1

	ASN.1	**Tag**	**Len**	**Value**
1.	SignedData ::= SEQUENCE {			
2.	version CMSVersion,			
3.	digestAlgorithms DigestAlgorithmIdentifiers,			
4.	encapContentInfo SEQUENCE {	A	A	A
5.	eContentType ContentType,	"	"	"
6.	eContent [0] EXPLICIT	"	"	"
7.	OCTET STRING OPTIONAL -- not present if signature is detached },	"	"	", D
8.	-- External Data (if signature detached)*			A, D
9.	certificates [0] IMPLICIT CertificateSet OPTIONAL,	A	A	A
10.	crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,	A	A	A
11.	signerInfos SET OF			
12.	SEQUENCE { -- SignerInfo			
13.	version CMSVersion,	A	A	A
14.	sid SignerIdentifier,	A	A	A
15.	digestAlgorithm DigestAlgorithmIdentifier,	A	A	A
16.	signedAttrs [0] IMPLICIT SET SIZE (1..MAX) OF	A	A	A
17.	SEQUENCE { -- Attribute	"	"	"
18.	attrType OBJECT IDENTIFIER,	"	"	"
19.	attrValues SET OF AttributeValue } OPTIONAL,	"	"	"
20.	signatureAlgorithm SignatureAlgorithmIdentifier,	A	A	A
21.	signature OCTET STRING, -- SignatureValue	A	A	A, S
22.	unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF			

23.	SEQUENCE {	A	A	A
24.	attrType OBJECT IDENTIFIER,	"	"	"
25.	attrValues SET OF AttributeValue } OPTIONAL } }	"	"	"

* *External data* znamená údaje chránené externým podpisom (detached signature), kde tieto údaje nie sú súčasťou *eContent* položky podpisu CAdES. Výpočet haš hodnoty pre *contentTimestamp* a *archiveTimestamp* zahrňuje výpočet hašu cez externé údaje. Algoritmus použitý pri externom podpise sa môže v budúcnosti stať nedôveryhodným (z dôvodu nájdenia spôsobov jeho prelomenia) a preto je potrebné zabezpečovať integritu externých podpísaných údajov pomocou pridania nových *archiveTimestamp* alebo integritným podpisom.

Príloha E (informatívna) Formáty spojenia elektronických dokumentov s elektronickým podpisom alebo ZEP

E.1 S/MIME formát súboru

Pri overovaní a zobrazovaní zaručených elektronických podpisov uložených v S/MIME, ktoré v *ContentType* obsahujú OID *id-data* (1 2 840 113549 1 7 1), ktorý nešpecifikuje presne typ podpísaných údajov, sa musia kvôli jednoznačnosti spracovania obmedziť jednotlivé MIME typy a kódovania na základnú množinu pre podpisované dokumenty podľa [21] a pre samotný podpis S/MIME nasledovne:

1. Text v US ASCII znakovej sade a 7 bitové kódovanie

   Ak v S/MIME nie je uvedený typ a kódovanie, tak sa predpokladá tento typ a kódovanie, pričom výhodou je, že je podmnožinou UTF-8.

   Content-Type: text/plain; charset=us-ascii
   Content-Transfer-Encoding: 7bit

2. Text v UTF-8 znakovej sade a 8 bitové kódovanie

   Content-Type: text/plain; charset=UTF-8
   Content-Transfer-Encoding: 8bit

3. Dokument v povolenom formáte [21] a v Base64 kódovaní

   Ak je potrebné podpísať dokumenty nespĺňajúce požiadavky pre Content-Type: text/plain, tieto dokumenty musia byť len vo formátoch, ktoré povoľujú vyhlášky NBÚ vydané k zákonu č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov a podľa [21]. Dokumenty musia byť kódované v Base64 (`Content-Transfer-Encoding`). Aplikácia, ktorá podpisuje alebo overuje zaručený elektronický podpis, musí vedieť na základe `Content-Type` zobraziť dokument, inak prehlási, že podpis nie je možné overiť, lebo dokument nie je možné podpisovateľovi alebo overovateľovi zobraziť.

4. Typy, ktoré rozdeľujú MIME na jednotlivé časti

   Content-Type: multipart/signed

   Content-Type: multipart/mixed

Pri ZEP uloženom v internom podpise CMS v (*.p7m) S/MIME sa predpokladá textový dokument v UTF-8 alebo dokument s MIME hlavičkou podľa [21].

Formát šifrovanej správy (*.p7m) v S/MIME nie je v tomto dokumente podrobnejšie rozoberaný, lebo **kvalifikovaný certifikát sa nesmie použiť na šifrovanie,** ale iba na overovanie platnosti a pravosti zaručeného elektronického podpisu a na overovanie identity podpisovateľa.

E.1.1 Príklad podpísaných údajov CMS (*.p7s) zakódovaných do S/MIME

Podpísaná správa vo formáte S/MIME je doplnená o nepovinnú hlavičku (prvých 6 riadkov v príklade), ktorá umožňuje overenie podpisu aj v bežne dostupných e-mail klientoch.
Správa je uložená do súboru, ktorého koncovka je ***.eml** (e-mail). Podpísané správy sa odporúča posielať ako prílohy iného e-mailu, lebo ak by v procese odosielania, prenosu alebo spracovania e-mail správy došlo k jej modifikácii, podpis by sa nenávratne poškodil a nebolo by možné jeho overenie. Jednoduchým príkladom môžu byť S/MIME nekompatibilné programy, ktoré preformátujú správu a tiež rôzne antivírusové hlásenia o kontrole správy alebo reklamné informácie dopĺňané počas prenosu správy, ktoré úplne znehodnotia podpisované údaje.

```
Message-ID: <27x5x2004at09x30x57x3B90>
From: <peter.rybar@infolooks.sk>
To: <info@nbusr.sk>
Subject: Podpis v S/MIME subore (*.EML)
Date: Thu, 27 May 2004 09:30:57 +0200
MIME-Version: 1.0
Content-Type: multipart/signed;
       protocol="application/x-pkcs7-signature";
       micalg=SHA1;
       boundary="--=_NextPart27x5x2004at09x30x57x3B90"

This is a multi-part message in MIME format.

----=_NextPart27x5x2004at09x30x57x3B90
Content-Type: multipart/mixed;
       boundary="--=_NextPart2X8X2005at11X20X05-E97E"

----=_NextPart2X8X2005at11X20X05-E97E

To to je podpisana sprava.
Vo formate SMIME.

----=_NextPart2X8X2005at11X20X05-E97E
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: base64

77u/dGVzdCBzIENQDQrEvsWhxI3FpcWlxb7FpcO9w73DocOtw63DqcOpw6nDqT3DusOkxYjDtMKn
w7TCp8Knw7TDtC4tLQ0KLS4tLQ0KwqfDusKnw7rFiMO6cMWIw7pww6TDusOkPcK0w6nDrW8NCnl1
...
xL4rxL7EjSvEvg0KxL7EvsWhxaHEjcSNxaXFpcW+xb7DvcO9w6HDocOtw63DqcOpPT3CtMK0w7rD
usOkw6TDtMO0wqfCp8WIxYgNCktPTklFQw0K

----=_NextPart2X8X2005at11X20X05-E97E--

----=_NextPart27x5x2004at09x30x57x3B90
Content-Type: application/x-pkcs7-signature;
       name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename="smime.p7s"

MIIGQQYJKoZIhvcNAQcCoIIGMjCCBi4CAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCA9gw
...
F9Q5jHSMaByoXE2wkZ365srlimkKXO97p+NiEpZwzI9tIi37Z4IrRbppjz3BjbMqHYdpkP06jWzm
KYbhjscDhpoL

----=_NextPart27x5x2004at09x30x57x3B90—
```

E.2 ZIP formát súboru (ZEPf)

Podpisovaný dokument, jeho podpisy, informácie potrebné na overenie podpisu dokumentu a ďalšie dokumenty súvisiace s podpisovaným dokumentom je potrebné spojiť do formátu, ktorého spracovanie je jednoduché a bežne dostupné. Medzi takéto bežne dostupné formáty patrí aj ZIP. Pre jednoduchšie spracovanie a zabezpečenie kompatibility aplikácií, ktoré využívajú alebo chcú využívať uvedený formát, je potrebné stanoviť pravidlá o pomenovaní jednotlivých položiek v ZIP súbore. Jednou z dôležitých informácií pri práci s podpismi je čas, kedy sa určitá činnosť udiala. Túto skutočnosť využijeme pri pomenovaní jednotlivých položiek. Mená jednotlivých položiek v adresárovej štruktúre budú obsahovať čas vloženia do ZIP súboru, vo formáte GeneralizedTime "YYYYMMDDhhmmssZ". Prvé písmená položiek v adresárovej štruktúre naznačujú typ položky. Za písmenom „Z" môže nasledovať poradové číslo, ktoré rozlišuje v rámci ZIP adresára súbory s rovnakým typom a časom. Súbory v ZIP môžu byť uložené v jednom hlavnom adresáre „DYYYYMMDDhhmmssZ", ktorý vždy obsahuje podpísaný dokument a jeho podpisy, pričom pomocné údaje môžu byť roztriedené do podadresárov: Certificate (zoznam certifikátov), Revocation (zoznam CRL a OCSP, nielen pre overenie použitých podpisov v ZIP súbore, ale aj pre overenie iných podpisov, ktoré sú integritne archivované s integritným podpisom umiestneným v ZIP súbore), Policy (zoznam použitých politík), Other (nešpecifikovaný zoznam priložených súborov).

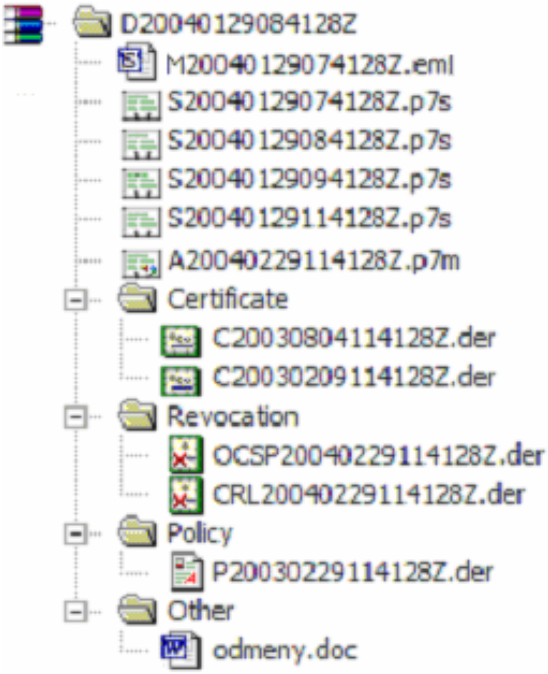
Tabuľka 25. Názvy základnej množiny súborov v ZIP formáte.

	Typ položky	Popis	Príklad
1.	D	Directory – hlavný adresár podpisu. Nie je povinný, ale sprehľadňuje používanie pri vykopírovaní podpisu mimo ZEPf (ZIP) súboru.	D20040129084128Z
2.	S	Sign – externý podpis: jednoduchý, s časovou pečiatkou, s úplnou informáciou na overenie, archívny alebo viacnásobný podpis.	S20040129084128Z.p7s S20040129084128Z.xml
3.	M	MIME obálka podpísaných súborov uložených do súboru „.EML" podľa [21].	M20040129084128Z.eml
4.	A	Integrity - integritný (archivačný) podpis súborov podpisuje súbory *.p7s, *.p7m, *.XML, všetky certifikáty, CRL alebo OCSP, podpisovú politiku a môže podpísať aj iné súbory. Podpisy, ktoré sa integritne archivujú prvý raz, sa musia doplniť na formát Zaručený elektronický podpis archívny. Integritný podpis neslúži na dlhodobú archiváciu, ale iba na zabezpečenie integrity dokumentov počas doby použiteľnosti hašovacích algoritmov, ktoré sú použité v archivačnom TXT dokumente. Definovaný je v kapitole B.2	A20040229114128Z.p7m A20040229114128Z.xml
5.	P	Policy – Podpisová politika	P20030229114128Z.der
6.	C	Certifikát	C20030209114128Z.der
7.	CRL	Zoznam zrušených certifikátov	CRL20040229114128Z.der
8.	OCSP	Stav platnosti certifikátu	OCSP20040229114128Z.der

Predchádzajúca tabuľka špecifikuje minimálnu množinu typov súborov, ktorú musí vedieť spracovať každá ZEP aplikácie pre administratívny styk. Podpisované elektronické dokumenty pre administratívny styk sa odporúča uložiť v MIME kódovaní do súboru s koncovkou (*.EML).

E.2.1 Príklad položiek v ZIP formáte (ZEPf) a názvy štandardných adresárov

Súbor odmeny.eml môže obsahovať len samotné dokumenty, ktoré sú v jednej MIME obálke pospájané pomocou MIME kódovania profilovaného dokumente [21] vydaného NBÚ na základe § 3 ods. 5 vyhlášky NBÚ č. 136/2009 Z. z.. Súbor odmeny.eml môže predstavovať aj SMIME formát spojenia podpísaného dokumentu a samotného podpisu, ktorý možno kedykoľvek osamostatniť na samotný podpísaný súbor s koncovkou „.EML“ a súbor s podpisom, ktorý obsahuje CMS podpis s koncovkou súboru „.P7S“. Súbor s koncovkou „.P7M“ predstavuje interný CMS podpis, ktorý môže obsahovať podpísaný textový dokument vo formáte definovanom v prílohe B.2.



E.3 DITEC XML formát súboru

DITEC XML formát pre spájanie prevažne XML dokumentov a XAdES podpisov používaných v administratívnom styku na výmenu XML podpísaných údajov medzi systémami štátnej správy definujú profily uvedené v dokumente:

Profil XAdES_ZEP - formát zaručeného elektronického podpisu na báze XAdES. – príloha Formát zloženého elektronického podpisu.[2]

Poznámka 8: V prípade nejednoznačnosti požiadaviek z odkazovaného dokumentu s požiadavkami uvedenými v tomto NBÚ štandarde, sú záväzné požiadavky tohoto NBÚ štandardu.

[2] XAdES_ZEP v1.0 - http://www.ditec.sk/ep/signature_formats/xades_zep/v1.0
XAdES_ZEP v1.0 - http://www.ditec.sk/ep/signature_formats/xades_zep/v1.1
Formát zloženého podpisu v1.0 - http://www.ditec.sk/ep/signature_formats/xades_zep_data_signatures/v1.0
Formát zloženého podpisu v1.1 - http://www.ditec.sk/ep/signature_formats/xades_zep_data_signatures/v1.1

Príloha F (informatívna) Revízie vykonané od predošlého vydania

F.1 Pridané požiadavky

Pridané položky, ktoré významne zmenili význam predchádzajúcich požiadaviek:

Kapitoly 5.2 a E.3 špecifikujú profil ZEP XML AdES podpisu.
Kapitola 5.3 špecifikuje postupy pre dlhodobé overenie elektronických podpisov pomocou integritného podpisu a formátu ZEPf, ak formát podpisu neumožňuje uloženie všetkých potrebných údajov pre dlhodobé overenie.
Príloha A bola upravená podľa nových vykonávacích predpisov k zákonu č.215/2002 Z.z., vydaných v roku 2009.
Príloha A.4 už neobsahuje medzi povinnými položkami *id-aa-ets-certificateRefs* alebo *id-aa-ets-revocationRefs*, aby bolo možné priamo archivovať aj ZEP s časovou pečiatkou podpisu.
Bola pridaná príloha B, ktorá obsahuje definície postupov a formáty podpisov pre zabezpečenie požiadaviek novely zákona o EP definujúcej novú akreditovanú službu „dlhodobé uchovávanie elektronických dokumentov podpísaných zaručeným elektronickým podpisom“.
V kapitole E.2 bola nadefinovaná minimálna množina typov súborov pre formát ZEPf.

F.2 Upravené požiadavky

Položky, ktoré upravujú predchádzajúce požiadavky:

Obsah dokumentu je zmenený najmä na základe vyhlášky NBÚ č. 135/2009 Z. z. a ostatných vyhlášok k novelizovanému zákonu o EP.
Príloha C obsahuje už len položky zabezpečené podpisovateľovým podpisom a nechránené položky boli odstránené, lebo ich obsah nemôže byť povinný, ak nie je chránený pred modifikáciou.
V kapitole E.2 bol odstránený uzatvárací podpis “F“, tento podpis bol odstránený aj z vyhlášky definujúcej dva spôsoby vytvárania viacnásobných podpisov.
Kapitola E.2 obsahuje definíciu mien adresárov a povinných mien súborov a aj nového mena pre MIME obálku obsahujúcu podpisované súbory.

F.3 Vysvetlenia

Položky, ktoré boli zmenené pre vysvetlenie predchádzajúcich požiadaviek:

Novela zákona a vyhlášok k zákonu o EP spresnila a nadefinovala nové pravidlá, ktorých splnenie nebolo v predchádzajúcich verziách formátov ZEP a tak predchádzajúce dokumenty definujúce formáty ZEP boli zrušené, ako aj predošlé vyhlášky.

F.4 Publikačné zmeny

Zmeny, ktoré neovplyvňujú technický význam dokumentu:

Dokument bol preformátovaný a rozdelený do príloh. Archivačný podpis bol premenovaný na Integritný podpis, aby nedochádzalo k zámene s Archívnym formátom ZEP.
V prílohe A dokumentu 584/2009/IBEP-012 bola odstránená duplicita id-signingTime a atribút bol presunutý medzi voliteľné.

Príloha G (informatívna) Zoznam použitej literatúry

Základné dokumenty legislatívy Slovenskej republiky pre elektronický podpis
http://www.nbusr.sk/sk/elektronicky-podpis/legislativa/index.html

Formáty zaručených elektronických podpisov
http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html

Zostavenie certifikačnej cesty a overenie platnosti certifikátov
http://www.nbusr.sk/sk/elektronicky-podpis/overovanie/index.html

- IETF RFC 4158 "Internet X.509 Public Key Infrastructure: Certification Path Building"

NOTE: Available at http://www.rfc-archive.org/getrfc.php?rfc=4158

- IETF RFC 5217 "Multi-Domain PKI Interoperability" July 2008

NOTE: Available at http://www.rfc-archive.org/getrfc.php?rfc=5217

- IETF RFC 4853 (2007): "Cryptographic Message Syntax (CMS) Multiple Signer Clarification"
- IETF RFC 3447 (2003): "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"
- ISO/IEC 8825-1:1998, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- ISO/IEC 19794-2:2005, Biometrics — Biometric Data Interchange Formats — Part 2: Finger Minutiae
- IETF RFC 3279 (2002): "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- IETF RFC 4055 (2005): "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile"
- IETF RFC 3281 (2002): "An Internet Attribute Certificate profile for Authorization"
- IETF RFC 3370 (2002): "Cryptographic Message Syntax (CMS) Algorithms"
- ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies"
- ETSI TS 101 861: "Time stamping profile"
- EN 14890-2:2008: "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services"
- ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates"
- ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"
- CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements"
- CWA 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic module for CSP Signing Operations with Backup - Protection Profile"
- CWA 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)"

- CWA 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP"
- W3C Recommendation (10 June 2008): "XML Signature Syntax and Processing (Second Edition)"

NOTE: Available at http://www.w3.org/TR/xmldsig-core/

- W3C Recommendation (10 December 2002): "XML Encryption Syntax and Processing"

NOTE: Available at http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

- CWA 14169: "Secure Signature-Creation Devices "EAL 4+"
- IETF RFC 4949 "Internet Security Glossary, Version 2" August 2007

NOTE: Available at http://www.rfc-archive.org/getrfc.php?rfc=4949

- NIST X.509 path validation test suite

NOTE: Available at http://csrc.nist.gov/pki/testing/x509paths.html http://csrc.nist.gov/pki/testing/pathdiscovery.html

- Object Identifier (OID) Repository: ITU-T X.660 & X.670 Recommendation series (or ISO/IEC 9834 series of International Standards)

NOTE: Available at http://www.oid-info.com/

- FESA – Forum of European Supervisory Authorities,

NOTE: Available at http://www.fesa.rtr.at

- OID tree structure,

NOTE: Available at http://www.darmstadt.gmd.de/secude/Doc/htm/oidgraph.htm

- Common ISIS-MTT Specification for interoperable PKI applications. Version 1.1. 16 March 2004
- Internet Draft "X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA"

NOTE: Available at http://tools.ietf.org/html/draft-ietf-pkix-sha2-dsa-ecdsa-05

- Internet Draft "X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) "

NOTE: Available at http://tools.ietf.org/html/draft-ietf-pkix-rfc3161bis-01

- TeleTrusT Deutschland e. V., "OID-Liste",

NOTE: Available at http://www.teletrust.de/index.php?id=171

- European Commission http://ec.europa.eu/
- IDABC stands for Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens. - eSignature Agenda & Presentations

NOTE: Available at http://ec.europa.eu/idabc/en/document/7312

- European Network and Information Security Agency (ENISA)

NOTE: Available at http://www.enisa.europa.eu/

- PKIX Status Pages http://tools.ietf.org/wg/pkix/

Príloha H História

Verzia	Dátum vydania	Poznámka	Vypracoval
V 1.0	30.9.2004	Prvé vydanie (zrušené)	Ing. Peter Rybár
Verzia 1.1	14.8.2005	Druhé vydanie	Ing. Peter Rybár, NBÚ
Verzia 1.2	6.11.2005	Pridanie multipart MIME	Ing. Peter Rybár, NBÚ
Verzia 2.0 Č.: 3198/2007/IBEP-009	22.7.2007	Spresnenie identifikácie podpisu XAdES v ZEPf(ZIP)	Ing. Peter Rybár, NBÚ
Verzia 3.0 Č.: 1223/2010/IBEP/OEP-001	12.8.2009	Štandardy formátov ZEP pred verziou 3.0 sú zrušené. Zmena podľa novely vyhlášky z roku 2009.	Ing. Peter Rybár, NBÚ