DITEC
Data Information Technology & Expert Consulting

Profil CAdES_ZEP v1.0

Formát zaručeného elektronického podpisu na báze CAdES

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Profil CAdES_ZEP v1.0		
Podnázov	Formát zaručeného elektronického podpisu na báze CAdES		
Ref. číslo	CAdES.2	Verzia	3

Vypracoval	Peter Obeda	Podpis	Dátum 4. 2. 2016
Preveril		Podpis	Dátum
Schválil		Podpis	Dátum

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 17.5.2005

Projekt	GOV_ZEP		A3019_002
Dokument	Profil CAdES_ZEP v1.0		
Referencia	CAdES.2	Verzia	3

Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia

Pripomienkovanie a kontrola

Autor	Stanovisko	Dátum	Verzia

Rozdeľovník

	Priezvisko Meno	Firma, Funkcia
Originál		
Kópia		
Kópia		
Kópia		

Obsah

1. Úvod

Tento dokument obsahuje definíciu syntaxe elektronického podpisu CAdES-BES/EPES v súlade s [1], [3], [5], [7] a [9] vo formáte ASN.1 aj so stručným vysvetľujúcim popisom jednotlivých častí. Obsahuje tiež popis rozšírení vyžadovaných formátmi CAdES-T, CAdES-C, CAdES-X Long (aj typy 1 a 2) a CAdES-A.

2. Zoznam použitých skratiek

ASN.1 - Abstract Syntax Notation One

BER - Basic Encoding Rules

CAdES - CMS Advanced Electronic Signatures

CMS - Cryptographic Message Syntax

CRL - Certificate Revocation List

DER - Distinguished Encoding Rules

MIME - Multipurpose Internet Mail Extensions

OCSP - Online Certificate Status Protocol

OID - Object Identifier

TLV - Type-Length-Value

UTC - Coordinated Universal Time

ZEP - Zaručený elektronický podpis alebo Zaručená elektronická pečať (podľa kontextu)

3. Referencie

[1] ETSI TS 101 733 v.2.2.1: CMS Advanced Electronic Signatures (CAdES), http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf

[2] ETSI TS 103 173 – CAdES Baseline Profile V2.1.1, http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.01.01_60/ts_103173v020101p.pdf

[3] 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF

[4] RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 1999, http://tools.ietf.org/html/rfc2560.

[5] RFC 2634, Enhanced Security Services for S/MIME, http://tools.ietf.org/html/rfc2634.

[6] RFC 3281, An Internet Attribute Certificate Profile for Authorization, April 2002, http://tools.ietf.org/html/rfc3281.

[7] RFC 5035, Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility, http://tools.ietf.org/html/rfc5035.

[8] RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, http://tools.ietf.org/html/rfc5280.

[9] RFC 5652, Cryptographic Message Syntax (CMS), http://tools.ietf.org/html/rfc5652.

[10] NBÚ, Formáty zaručených elektronických podpisov, verzia 3.0, http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/schvalene-formaty/formaty_zep.pdf

[11] Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; Part 2: ‘Secure channel protocols and algorithms for signature creation devices’.

[12] ECRYPT II Yearly Report on Algorithms and Keysizes (2009-2010), Revision 1.0, 30. March 2010, http://www.ecrypt.eu.org/documents/D.SPA.13.pdf.

4. Formát zaručeného elektronického podpisu na báze CAdES

Tam, kde syntaktická definícia označuje niektoré časti podpisu ako voliteľné (OPTIONAL, prípadne CHOICE) a je to vhodné, pre zvýšenie prehľadnosti špecifikujeme potrebnosť týchto častí pomocou jednej z nasledujúcich skratiek:

- P – povinné
- O – odporúčané
- V – voliteľné
- N - neodporúčané

4.1. Podpis CAdES-BES/EPES

4.1.1. ContentInfo

Štruktúra ContentInfo je definovaná v RFC 5652 a tvorí základnú obálku pre všetky CMS formáty, teda aj pre digitálny podpis.

	Zápis v ASN.1	Popis
1	`ContentInfo ::= SEQUENCE {`	Obálka CMS.
2	`contentType ContentType,`	OID údajov v `content`, v prípade podpisu nadobúda hodnotu `id-signedData`.
3	`content [0] EXPLICIT DEFINED BY contentType }`	Údaje typu určeného podľa `contentType`, v prípade podpisu sú typu `SignedData`.
4	`ContentType ::= OBJECT IDENTIFIER`	
5	`id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }`	OID identifikujúce podpis v CMS formáte.

4.1.2. SignedData

Celková štruktúra elektronického podpisu je určená typom `SignedData`, tak ako ho špecifikuje nasledujúca tabuľka.

	Zápis v ASN.1		Popis
1	`SignedData ::= SEQUENCE {`		
2	`version CMSVersion,`		Verzia určená algoritmom v [9] str. 10.
3	`digestAlgorithms DigestAlgorithmIdentifiers,`		Môže obsahovať ľubovoľne veľa hašovacích algoritmov (aj žiadne). Podpis využívajúci hašovací algoritmus neobsiahnutý v tejto množine nemusí byť akceptovaný. Odporúčania ohľadom algoritmov v [11] a [12]. Nesmie sa použiť MD5 [3].
4	`encapContentInfo EncapsulatedContentInfo,`		Podrobnosti v tabuľke nižšie.
5	`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	P	Musí obsahovať X509 v3 certifikát podpisovateľa. Odporúča sa pridať všetky certifikáty overovacej cesty [3].
6	`crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,`	V	
7	`signerInfos SignerInfos }`		Množina blokov s jednotlivými podpismi. Môže obsahovať ľubovoľne veľa blokov (aspoň jeden [1]). Implementácie spracúvajúce jednu z položiek signerInfo musia zvládnuť neznámu verziu alebo podpisový algoritmus niektorej z ostatných položiek signerInfo.
8	`DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier`		
9	`DigestAlgorithmIdentifier ::= AlgorithmIdentifier`		
10	`CertificateSet ::= SET OF CertificateChoices`		Podrobnosti v tabuľke nižšie.
11	`RevocationInfoChoices ::= SET OF RevocationInfoChoice`		Podrobnosti v tabuľke nižšie.
12	`SignerInfos ::= SET OF SignerInfo`		Podrobnosti v tabuľke nižšie.

4.1.3. CertificateChoices

Štruktúra `CertificateChoices` zachytáva rôzne možnosti reprezentácie certifikátu v rámci položky `certificates` v štruktúre `SignedData`.

	Zápis v ASN.1		Popis
1	`CertificateChoices ::= CHOICE {`		
2	`certificate Certificate,`	O	X.509 certifikát, definovaný v [8].
3	`extendedCertificate [0] IMPLICIT ExtendedCertificate,`	N	PKCS #6 extended certifikát. Uvedený len pre spätnú kompatibilitu, zastaralý a nemal by sa používať.
4	`v1AttrCert [1] IMPLICIT AttributeCertificateV1,`	N	Attribute certificate X.509 v1. Uvedený len pre spätnú kompatibilitu, zastaralý a nemal by sa používať.
5	`v2AttrCert [2] IMPLICIT AttributeCertificateV2,`	O	Attribute certificate X.509 v2, definovaný v [6].
6	`other [3] IMPLICIT OtherCertificateFormat }`	V	Iný formát certifikátu.
7	`OtherCertificateFormat ::= SEQUENCE {`		
8	`otherCertFormat OBJECT IDENTIFIER,`		OID popisujúci použitý formát certifikátu.
9	`otherCert ANY DEFINED BY otherCertFormat }`		Samotný certifikát.

4.1.4. RevocationInfoChoice

Štruktúra Revocation`Choice` zachytáva rôzne možnosti pre položku `crls` v štruktúre `SignedData`.

	Zápis v ASN.1		Popis
1	`RevocationInfoChoice ::= CHOICE {`		
2	`crl CertificateList,`	V	Zoznam revokovaných certifikátov (CRL).
3	`other [1] IMPLICIT OtherRevocationInfoFormat }`	V	Iný formát informácií o revokácii.
4	`OtherRevocationInfoFormat ::= SEQUENCE {`		
5	`otherRevInfoFormat OBJECT`		OID určujúci formát informácií o

	IDENTIFIER,		revokácii.
6	otherRevInfo ANY DEFINED BY otherRevInfoFormat }		Samotné revokačné info.

4.1.5. EncapsulatedContentInfo

Samotné podpisované dáta sú v `SignedData` uložené v položke `EncapsulatedContentInfo` spolu s identifikátorom ich typu.

	Zápis v ASN.1		Popis
1	EncapsulatedContentInfo ::= SEQUENCE {		
2	eContentType ContentType,		OID typu podpisovaných údajov. Použije sa typ `id-data`.
3	eContent [0] EXPLICIT OCTET STRING OPTIONAL }	V	Samotný podpisovaný obsah. Pre `eContentType id-data` sa odporúča použiť MIME kódovanie, pričom uvedený MIME typ určuje formu prezentovania dát (viď [1] Annex F). Pri externom podpise je `eContent` vynechaný.
	id-data OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 1 }		

4.1.6. SignerInfo

`SignedData` obsahuje pre každý jednotlivý podpis (a prípadné prislúchajúce protipodpisy) jednu položku `SignerInfo`, obsahujúcu samotný podpis spolu s jeho atribútmi, informáciami o podpisovateľovi a použitých algoritmoch.

	Zápis v ASN.1		Popis
1	SignerInfo ::= SEQUENCE {		
2	version CMSVersion,		Verzia určená algoritmom v [9] str. 14.
3	sid SignerIdentifier,		
4	digestAlgorithm DigestAlgorithmIdentifier,		Mal by byť uvedený aj v položke digestAlgorithms štruktúry signedData, inak podpis nemusí

			byť akceptovaný. Odporúčania ohľadom algoritmov v [11] a [12]. Nesmie sa použiť MD5 [3].
5	`signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,`	P	Musia byť prítomné[4].
6	`signatureAlgorithm SignatureAlgorithmIdentifier,`		Odporúčania ohľadom algoritmov v [11] a [12].
7	`signature SignatureValue,`		
8	`unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }`	V	
9	`SignerIdentifier ::= CHOICE {`		Implementácie musia podporovať overovanie oboch možnosti a vytváranie aspoň jednej.
10	`issuerAndSerialNumber IssuerAndSerialNumber,`	V	Definované v [9] časť 10.2.4.
11	`subjectKeyIdentifier [0] SubjectKeyIdentifier }`	V	Musí byť použité pre iný ako X.509 certifikát.
12	`SignedAttributes ::= SET SIZE (1..MAX) OF Attribute`		
13	`UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute`		
14	`Attribute ::= SEQUENCE {`		
15	`attrType OBJECT IDENTIFIER,`		
16	`attrValues SET OF AttributeValue }`		
17	`AttributeValue ::= ANY`		
18	`SignatureAlgorithmIdentifier ::= AlgorithmIdentifier`		
19	`SignatureValue ::= OCTET STRING`		

4.1.7. Podpisované atribúty

V tejto časti je uvedený zoznam atribútov základného podpisu CAdES-BES/EPES, ktoré sú obsiahnuté v položke `signedAttrs` a podpísané spolu s dátami. Delia sa na povinné a voliteľné.

	Zápis v ASN.1		Popis
1	`id-contentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)`	P	Povinný atribút [1], obsahuje OID typu podpisovaných údajov.

	pkcs9(9) 3 } ContentType ::= OBJECT IDENTIFIER		Musí sa rovnať eContentType v príslušnom encapContentInfo, teda typu id-data. Musí byť prítomný len raz a v AttrValues obsahovať len jednu hodnotu.
2	id-messageDigest OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 } MessageDigest ::= OCTET STRING	P	Povinný atribút [1]. Obsahuje odtlačok hodnoty eContent v encapContentInfo. Musí byť prítomný len raz a v AttrValues obsahovať len jednu hodnotu.
3	id-aa-signingCertificate OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 12 } SigningCertificate ::= SEQUENCE { certs SEQUENCE OF ESSCertID, policies SEQUENCE OF PolicyInformation OPTIONAL }	P	Prítomnosť práve jedného z atribútov typu SigningCertificate resp. SigningCertificateV2 je povinná [1]. Ak je použitá hashovacia funkcia SHA1, musí byť prítomný atribút typu SigningCertificate, inak typu SigningCertificateV2 [1]. Musí byť prítomný len raz a v AttrValues obsahovať len jednu hodnotu. certs obsahuje postupnosť certifikátov, prvý musí byť X.509 v3 certifikát podpisovateľa používaný pri overovaní podpisu. Ak obsahuje viac certifikátov, len tieto sú použité pri overovaní. Pole policies sa nepoužíva [4].
4	id-aa-signingCertificateV2 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 47 } SigningCertificateV2 ::= SEQUENCE { certs SEQUENCE OF ESSCertIDv2, policies SEQUENCE OF PolicyInformation OPTIONAL }		
5	ESSCertID ::= SEQUENCE { certHash Hash,		Pole issuerSerial je povinné a musí sa zhodovať s hodnotou

	issuerSerial IssuerSerial OPTIONAL }		issuerAndSerialNumber v sid v SignerInfo, ak je prítomná [1]. certHash musí obsahovať korektný hash (pomocou SHA1 resp. pomocou hashAlgorithm) certifikátu použitého na podpis, inak je podpis neplatný.
6	ESSCertIDv2 ::= SEQUENCE { hashAlgorithm AlgorithmIdentifier DEFAULT {algorithm id-sha256}, certHash Hash, issuerSerial IssuerSerial OPTIONAL }		
7	Hash ::= OCTET STRING		
8	IssuerSerial ::= SEQUENCE { issuer GeneralNames, serialNumber CertificateSerialNumber }	P	
9	id-aa-ets-otherSigCert OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 19 } OtherSigningCertificate ::= SEQUENCE { certs SEQUENCE OF OtherCertID, policies SEQUENCE OF PolicyInformation OPTIONAL }	N	Formát certifikátu uvedený v starších verziách [1], zastaralý, len pre spätnú kompatibilitu. Podrobnosti v [1] časť 5.7.3.3.
10	id-aa-ets-sigPolicyId OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) id-aa(2) 15 } SignaturePolicyIdentifier ::=CHOICE { signaturePolicyId SignaturePolicyId, signaturePolicyImplied SignaturePolicyImplied }	V	Povinný atribút [1] pre CAdES-EPES, explicitne identifikuje podpisovú politiku. SignaturePolicyImplied sa nepoužíva.
11	SignaturePolicyId ::= SEQUENCE { sigPolicyId SigPolicyId, sigPolicyHash SigPolicyHash, sigPolicyQualifiers SEQUENCE SIZE (1..MAX) OF SigPolicyQualifierInfo OPTIONAL }		

12	`SigPolicyId ::= OBJECT IDENTIFIER`		Jednoznačne identifikuje presnú verziu podpisovej politiky.
13	`SigPolicyHash ::= OtherHashAlgAndValue`		
14	`OtherHashAlgAndValue ::= SEQUENCE { hashAlgorithm AlgorithmIdentifier, hashValue OtherHashValue }`		Hodnota `hashValue` môže byť 0 ak je hash politiky neznámy, v tom prípade sa neoveruje.
15	`OtherHashValue ::= OCTET STRING`		
16	`SigPolicyQualifierInfo ::= SEQUENCE { sigPolicyQualifierId SigPolicyQualifierId, sigQualifier ANY DEFINED BY sigPolicyQualifierId }`	V	Doplnkové informácie o podpisovej politike. Rôzne možnosti pre `sigQualifier` sú popísané v [1], str.30.
17	`id-signingTime OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 5 } SigningTime ::= Time Time ::= CHOICE { utcTime UTCTime, generalizedTime GeneralizedTime }`	P	Povinný atribút [3]. Obsahuje čas podpisu podľa podpisovateľa. Musí byť prítomný práve raz a v `AttrValues` obsahovať len jednu hodnotu. Podrobnosti voľby formátu a reprezentácie v [9], časť 11.3, pričom musí byť použitý formát UTC [3].
18	`id-aa-contentReference OBJECT IDENTIFIER ::= { iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 10 } ContentReference ::= SEQUENCE { contentType ContentType, signedContentIdentifier ContentIdentifier, originatorSignatureValue OCTET STRING }`	V	Voliteľný atribút [9] slúžiaci na referencovanie jedného `SignedData` iným. Podrobnosti použitia v [5] str. 24.
19	`id-aa-contentIdentifier OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 7 } ContentIdentifier ::= OCTET STRING`	V	Voliteľný atribút [1] identifikujúci `SignedData`, napríklad pre účely referencovania pomocou `ContentReference`. Podrobnosti použitia v [5] str. 21.
20	`id-aa-contentHint OBJECT IDENTIFIER ::= { iso(1) member-`	V	Voliteľný atribút [1] prítomný vo

	body(2) us(840)rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 4} ContentHints ::= SEQUENCE { contentDescription UTF8String (SIZE (1..MAX)) OPTIONAL, contentType ContentType }		vonkajšej vrstve viacvrstvovej správy a určujúci typ dát vo vnútornej vrstve. Podrobnosti použitia v [1] časť 5.10.3.
21	id-aa-ets-commitmentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 16 } CommitmentTypeIndication ::= SEQUENCE { commitmentTypeId CommitmentTypeIdentifier, commitmentTypeQualifier SEQUENCE SIZE (1..MAX) OF CommitmentTypeQualifier OPTIONAL }	V	Voliteľný atribút [1] určujúci typ záväzku, vyjadreného podpisom. Typy záväzkov majú presný význam určený buď registráciou alebo podpisovou politikou. [1] definuje niekoľko generických typov v časti 5.11.1.
22	CommitmentTypeIdentifier ::= OBJECT IDENTIFIER		
23	CommitmentTypeQualifier ::= SEQUENCE { commitmentTypeIdentifier CommitmentTypeIdentifier, qualifier ANY DEFINED BY commitmentTypeIdentifier }		
24	id-aa-ets-signerLocation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 17} SignerLocation ::= SEQUENCE { countryName [0] DirectoryString OPTIONAL, localityName [1] DirectoryString OPTIONAL, postalAdddress [2] PostalAddress OPTIONAL }	V	Voliteľný atribút [1] obsahujúci adresu podpisovateľa. Aspoň jedno z OPTIONAL polí musí byť prítomné.
25	id-aa-ets-signerAttr OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 18} SignerAttribute ::= SEQUENCE OF CHOICE { claimedAttributes [0]ClaimedAttributes,	V	Voliteľný atribút [1] obsahujúci atribúty (napr. role) podpisovateľa. Atribúty môžu byť iba deklarované podpisovateľom, alebo potvrdené certifikátom. Môže byť prítomný najviac raz.

	certifiedAttributes [1]CertifiedAttributes }		
26	ClaimedAttributes ::= SEQUENCE OF Attribute		
27	CertifiedAttributes ::= AttributeCertificate		
28	id-aa-ets-contentTimestamp OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 20} ContentTimestamp::= TimeStampToken	V	Voliteľný atribút [1] obsahujúci časovú pečiatku podpísaných dát pred podpisom. Dokazuje, že dáta vznikli pred uvedeným časom. Pre obsah položky messageImprint v štruktúre TimeStampToken pozri [1], Annex K, tab. K.3.

4.1.8. Nepodpisované atribúty

V tejto časti je uvedený zoznam atribútov základného podpisu CAdES-BES/EPES, ktoré sú obsiahnuté v položke unsignedAttrs a nie sú chránené podpisom.

	Zápis v ASN.1		Popis
1	id-countersignature OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 6 } Countersignature ::= SignerInfo	N	Voliteľný atribút. Obsahuje podpis DER-kódovanej hodnoty signature zo SignerInfo, ktorého je súčasťou. UnsignedAttributes môže obsahovať nula alebo viac countersignature atribútov a každý musí obsahovať jednu alebo viac hodnôt (attrValue). Nie je určený pre ZEP/ZEPe, lebo nepodpisuje údaje, ale len nadradený digitálny podpis, v ktorého nepodpísaných atribútoch sa nachádza. Nie je definovaný pre archívny typ podpisu. Neodporúča sa používať.

4.2. Dodatočné atribúty v CAdES-T

V tejto časti sú uvedené dodatočné atribúty pre podpis s časovou pečiatkou CAdES-T. Typ atribútu (povinný/voliteľný) je určený vzhľadom na špecifikáciu CAdES-T, okrem tu uvedených atribútov musí platný CAdES-T podpis obsahovať aj všetky povinné náležitosti podpisu CAdES-BES/EPES. Všetky atribúty uvedené v tejto časti sú nepodpisované.

	Zápis v ASN.1		Popis
1	`id-aa-signatureTimeStampToken OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 14} SignatureTimeStampToken ::= TimeStampToken`	V	Voliteľný atribút, jeho pridaním vzniká CAdES-T [1]. Podrobnosti o formáte TimeStampToken sú v [1] časť 4.4. Položka `messageImprint` v rámci `TimeStampToken` bude obsahovať hash hodnoty `signature` v príslušnej štruktúre `SignerInfo` (pozri [1], Annex K, tab. K.3). V prípade viacerých podpisov (`SignerInfo`) môžu časovú pečiatku obsahovať iba niektoré z nich alebo aj všetky. V tom istom `SignerInfo` môžu byť prítomné viaceré časové pečiatky od rôznych autorít.

Poznámka: atribút `SignatureTimeStampToken` je v podpise CAdES-T voliteľný, pretože tento typ podpisu môže vzniknúť aj využitím časovej značky (time mark) od Time Marking Authority bez potreby časovej pečiatky.

4.3. Dodatočné atribúty v CAdES-C

V tejto časti sú uvedené dodatočné atribúty pre podpis s úplnými referenciami validačných dát CAdES-C. Typ atribútu (povinný/voliteľný) je určený vzhľadom na špecifikáciu CAdES-C, okrem tu uvedených atribútov musí platný CAdES-C podpis obsahovať aj všetky povinné náležitosti podpisu CAdES-T. Všetky atribúty uvedené v tejto časti sú nepodpisované.

	Zápis v ASN.1		Popis
1	`id-aa-ets-certificateRefs OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-`	P	Povinný atribút pre CAdES-C, musí byť prítomný práve raz. Obsahuje odkazy na všetky

	aa(2) 21} CompleteCertificateRefs ::= SEQUENCE OF OtherCertID		certifikáty CA potrebné na overenie podpisu, no neobsahuje certifikát podpisovateľa (ten sa nachádza v podpisovanom atribúte SigningCertificate alebo SigningCertificateV2).
2	OtherCertID ::= SEQUENCE { otherCertHash OtherHash, issuerSerial IssuerSerial OPTIONAL }		issuerSerial je tu povinný, otherCertHash musí obsahovať hash príslušného certifikátu.
3	OtherHash ::= CHOICE { sha1Hash OtherHashValue, otherHash OtherHashAlgAndValue}		V prípade hashovacej funkcie SHA1 sa použije sha1Hash, inak otherHash.
4	id-aa-ets-revocationRefs OBJECT IDENTIFIER ::= { iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id- aa(2) 22} CompleteRevocationRefs ::= SEQUENCE OF CrlOcspRef	P	Povinný atribút pre CAdES-C, musí byť prítomný práve raz. Obsahuje odkazy na všetky revokačné informácie, potrebné na overenie platnosti podpisu. CompleteRevocationRefs musí obsahovať CrlOcspRef pre certifikát podpisovateľa a za ním postupnosť jedného CrlOcspRef pre každý certifikát v CompleteCertificateRefs v rovnakom poradí, v akom sú uvedené certifikáty.

5	CrlOcspRef ::= SEQUENCE {
	crlids [0] CRLListID OPTIONAL,
	ocspids [1] OcspListID
	OPTIONAL,
	otherRev [2] OtherRevRefs
	OPTIONAL
	}
			Pre všetky certifikáty okrem koreňového by mal CrlOcspRef obsahovať aspoň jednu z uvedených troch možností.

6	CRLListID ::= SEQUENCE { crls SEQUENCE OF CrlValidatedID }		Ak sa jedná o Delta CRL, musia byť obsiahnuté referencie na kompletný CRL.
7	CrlValidatedID ::= SEQUENCE { crlHash OtherHash, crlIdentifier CrlIdentifier OPTIONAL }		crlHash sa počíta z DER-kódovaného CRL aj s jeho podpisom. crlIdentifier by mal byť prítomný, ak nie je

			odvoditeľný z iných údajov.
8	`CrlIdentifier ::= SEQUENCE { crlissuer Name, crlIssuedTime UTCTime, crlNumber INTEGER OPTIONAL }`		Identifikuje CRL pomocou mena a času vydania, ktorý musí zodpovedať položke `thisUpdate` v CRL.
9	`OcspListID ::= SEQUENCE { ocspResponses SEQUENCE OF OcspResponsesID }`		
10	`OcspResponsesID ::= SEQUENCE { ocspIdentifier OcspIdentifier, ocspRepHash OtherHash OPTIONAL }`		Položka `ocspRepHash` je nepovinná kvôli spätnej kompatibilite, ale jej prítomnosť je silne odporúčaná. Podpisy bez `ocspRepHash` môžu byť akceptované, ale sú náchylné na substitučný útok.
11	`OcspIdentifier ::= SEQUENCE { ocspResponderID ResponderID, producedAt GeneralizedTime }`		Položky `ocspResponderID` a `producedAt` musia mať rovnaké hodnoty ako tie obsiahnuté v OCSP odpovedi.
12	`OtherRevRefs ::= SEQUENCE { otherRevRefType OtherRevRefType, otherRevRefs ANY DEFINED BY otherRevRefType }`		Iný formát revokačných informácií.
13	`OtherRevRefType ::= OBJECT IDENTIFIER`		OID identifikujúce formát.
14	`id-aa-ets-attrCertificateRefs OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 44} AttributeCertificateRefs ::= SEQUENCE OF OtherCertID`	V	Voliteľný atribút pre CAdES-C, obsahuje referencie na všetky certifikáty atribútových autorít, potrebné na overenie atribútového certifikátu. Môže byť prítomný iba raz.
15	`id-aa-ets-attrRevocationRefs OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 45} AttributeRevocationRefs ::= SEQUENCE OF CrlOcspRef`	V	Voliteľný atribút pre CAdES-C, obsahuje referencie na všetky ACRL a OCSP odpovede potrebné na overenie atribútového certifikátu. Môže byť prítomný iba raz.

4.4. Dodatočné atribúty v CAdES-X Long

V tejto časti sú uvedené dodatočné atribúty pre rozšírený formát podpisu CAdES-X Long. Typ atribútu (povinný/voliteľný) je určený vzhľadom na špecifikáciu CAdES-X Long, okrem tu uvedených atribútov musí platný CAdES-X Long podpis obsahovať aj všetky povinné náležitosti podpisu CAdES-C. Všetky atribúty uvedené v tejto časti sú nepodpisované.

	Zápis v ASN.1		Popis
1	`id-aa-ets-certValues OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 23}` `CertificateValues ::= SEQUENCE OF Certificate`	P	Povinný atribút pre CAdES-X Long, môže byť prítomný iba raz. Obsahuje hodnoty všetkých certifikátov referencovaných v atribúte `complete-certificate-references`.

2	`id-aa-ets-revocationValues OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 24}`
	`RevocationValues ::= SEQUENCE {`
	`  crlVals [0] SEQUENCE OF CertificateList OPTIONAL,`
	`  ocspVals [1] SEQUENCE OF BasicOCSPResponse OPTIONAL,`
	`  otherRevVals [2] OtherRevVals OPTIONAL}`
		P	Povinný atribút pre CAdES-X Long, môže byť prítomný iba raz. Obsahuje hodnoty všetkých CRL a OCSP odpovedí referencovaných v atribúte `complete-revocation-references`. `CertificateList` je definovaný v [1] v časti 7.2, `BasicOCSPResponse` je definovaná v [4].

3	`OtherRevVals ::= SEQUENCE {`
	`  otherRevValType OtherRevValType,`
	`  otherRevVals ANY DEFINED BY OtherRevValType }`
			Iný formát revokačných informácií.

4	`OtherRevValType ::= OBJECT IDENTIFIER`		OID určujúce ich formát.

4.5. Dodatočné atribúty v CAdES-X Long Type 1

V tejto časti sú uvedené dodatočné atribúty pre rozšírený formát podpisu CAdES-X Long Type 1. Typ atribútu (povinný/voliteľný) je určený vzhľadom na špecifikáciu CAdES-X Long Type 1, okrem tu uvedených atribútov musí platný CAdES-X Long Type 1 podpis obsahovať aj všetky povinné náležitosti podpisu CAdES-X Long. Všetky atribúty uvedené v tejto časti sú nepodpisované.

	Zápis v ASN.1		Popis

1	id-aa-ets-escTimeStamp OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 25} ESCTimeStampToken ::= TimeStampToken	P	Povinný atribút pre CAdES-X Long Type 1, jeden podpis ich môže obsahovať viacero od rôznych autorít. Hodnota messageImprint v štruktúre TimeStampToken bude obsahovať hash zreťazenia nasledovných dát: • OCTET STRING z poľa SignatureValue v SignerInfo • atribút signature-time-stamp alebo príslušná časová značka. • atribút complete-certificate-references • atribút complete-revocation-references. Podrobnosti o formáte TimeStampToken sú v [1] časť 4.4.

Poznámka: Dáta určené na zhashovanie sú použité bez kódovania typu a dĺžky. V prípade atribútov sa použijú hodnoty attrType a attrValues spolu s kódovaním typu a dĺžky, ale bez kódovania typu a dĺžky vonkajšej štruktúry SEQUENCE (pozri **Error! Reference source not found.**, Annex K, tab. K.3).

4.6. Dodatočné atribúty v CAdES-X Long Type 2

V tejto časti sú uvedené dodatočné atribúty pre rozšírený formát podpisu CAdES-X Long Type 2. Typ atribútu (povinný/voliteľný) je určený vzhľadom na špecifikáciu CAdES-X Long Type 2, okrem tu uvedených atribútov musí platný CAdES-X Long Type 2 podpis obsahovať aj všetky povinné náležitosti podpisu CAdES-X Long. Všetky atribúty uvedené v tejto časti sú nepodpisované.

	Zápis v ASN.1		Popis
1	id-aa-ets-certCRLTimestamp OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 26} TimestampedCertsCRLs ::=	P	Povinný atribút pre CAdES-X Long Type 2. Hodnota messageImprint v štruktúre TimeStampToken bude obsahovať hash zreťazenia nasledovných

	TimeStampToken		dát: • atribút complete-certificate-references • atribút complete-revocation-references. Podrobnosti o formáte TimeStampToken sú v [1] časť 4.4.

Poznámka: Pri hashovaní oboch atribútov sa použijú hodnoty attrType a attrValues spolu s kódovaním typu a dĺžky, ale bez kódovania typu a dĺžky vonkajšej štruktúry SEQUENCE (pozri [1], Annex K, tab. K.3).

4.7. Dodatočné atribúty v CAdES-A

V tejto časti sú uvedené dodatočné atribúty pre archívny digitálny podpis CAdES-A. Typ atribútu (povinný/voliteľný) je určený vzhľadom na špecifikáciu CAdES-A, okrem tu uvedených atribútov musí platný CAdES-A podpis obsahovať aj všetky povinné náležitosti jedného z podpisov CAdES-X Long, CAdES-X Long Type 1 alebo CAdES-X Long Type 2. Všetky atribúty uvedené v tejto časti sú nepodpisované.

4.7.1. Archívna časová pečiatka verzie 2

Pre archívnu časovú pečiatku verzie 2 sa používajú atribúty v nasledujúcej tabuľke.

	Zápis v ASN.1		Popis
1	id-aa-ets-archiveTimestampV2 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 48} ArchiveTimeStampToken ::= TimeStampToken	P	Povinný atribút pre CAdES-A, jeden podpis ich môže obsahovať viacero od rôznych autorít a/alebo z rôznych časov. Hodnota messageImprint v štruktúre TimeStampToken bude obsahovať hash zreťazenia nasledovných dát: • encapContentInfo zo SignedData • ak je eContent vynechaný tak externé podpisované dáta

			• položka `certificates` zo `SignedData` • ak je prítomná tak položka crls zo `SignedData` • všetky položky `SignerInfo` vrátane všetkých podpisovaných aj nepodpisovaných atribútov Podrobnosti o formáte TimeStampToken sú v [1] časť 4.4.

Poznámka: Hashované hodnoty sú povinne DER-kódované [3], hash sa počíta zo zreťazenia uvedených hodnôt vrátane typu a dĺžky v TLV kódovaní. Do hashovaných dát nie sú zahrnuté hlavičky `signerInfos` a `unsignedAttrs`. (Pozri [1], Annex K, tab. K.3, hlavne riadky 11, 12, 22. Pre úplnosť uvádzame obsah tejto tabuľky pre archívny podpis nižšie, dáta na zahrnutie do hashovania sú označené značkou „A“.). Pri overovaní pečiatky sa do hashovaných dát nezahrnú neskôr pridané archívne časové pečiatky.

	Zápis v ASN.1	Tag	Len	Value
1	`SignedData ::= SEQUENCE {`			
2	`version CMSVersion,`			
3	`digestAlgorithms DigestAlgorithmIdentifiers,`			
4	`encapContentInfo SEQUENCE {`	A	A	A
5	`eContentType ContentType,`	A	A	A
6	`eContent [0] EXPLICIT`	A	A	A

7	`OCTET STRING OPTIONAL`
	`-- not present if signature is detached`
	`},`
		A	A	A

8	`-- External Data (if signature detached)`			A
9	`certificates [0] IMPLICIT CertificateSet OPTIONAL,`	A	A	A
10	`crls [1] IMPLICIT CertificateRevocationLists`	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`	A	A	A
18	`attrType OBJECT IDENTIFIER,`	A	A	A
19	`attrValues SET OF AttributeValue } OPTIONAL,`	A	A	A
20	`signatureAlgorithm SignatureAlgorithmIdentifier,`	A	A	A
21	`signature OCTET STRING, -- SignatureValue`	A	A	A
22	`unsignedAttrs [1] IMPLICIT SET SIZE (1..MAX) OF`			
23	`SEQUENCE { -- if attrType is id-aa-signatureTimeStampToken -- if attrType is id-aa-ets-certificateRefs -- if attrType is id-aa-ets-revocationRefs attrType OBJECT IDENTIFIER, attrValues SET OF AttributeValue } OPTIONAL } }`	A	A	A

Poznámka: Archívna časová pečiatka spolu s podpisom chráni aj všetky protipodpisy zahrnuté v atribúte `countersignature`.

Poznámka: Archívna časová pečiatka by mala byť vytvorená s použitím silnejších kryptografických nástrojov ako pôvodný podpis.

Poznámka: Certifikáty a revokačné informácie potrebné na overenie časovej pečiatky budú v nej obsiahnuté jedným z troch spôsobov uvedených v [1] časť 6.4.1, str. 43.

4.7.2. Archívna časová pečiatka verzie 3

Pre archívnu časovú pečiatku verzie 3 sa používajú atribúty v nasledujúcej tabuľke.

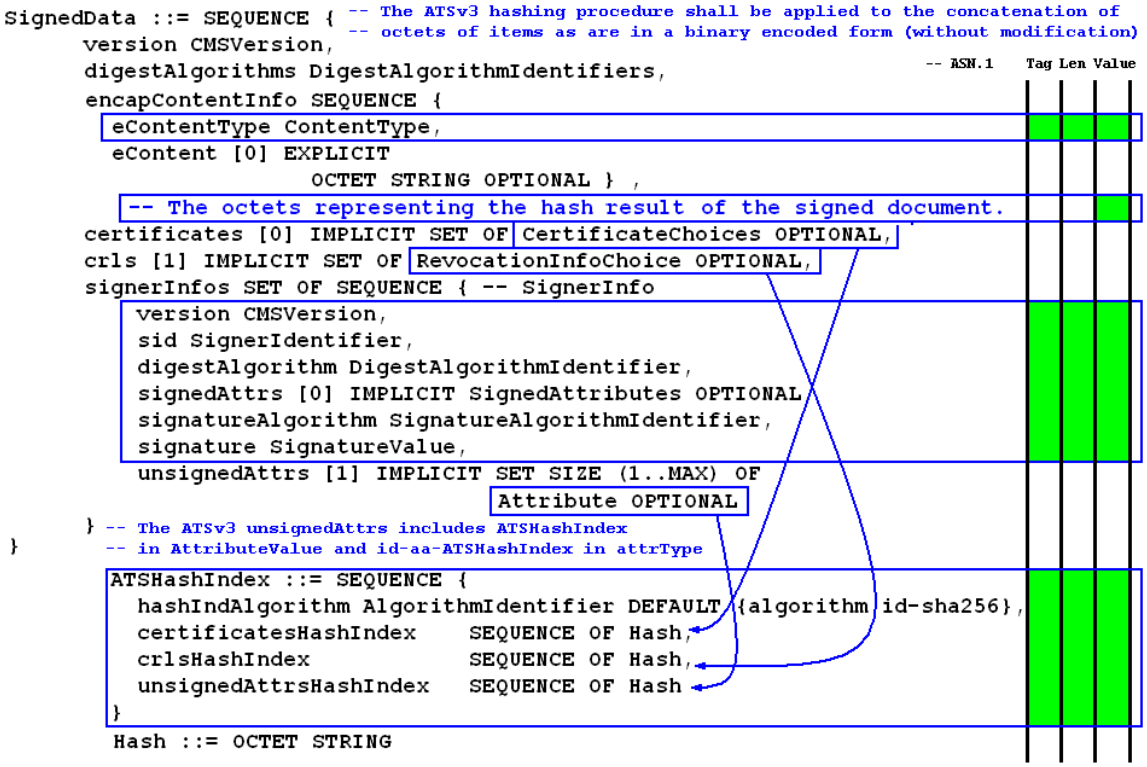
	Zápis v ASN.1		Popis
1	`id-aa-ATSHashIndex OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)`	P	Povinný atribút pre CAdES-A s ATS verzie 3 , môže byť prítomný iba raz. Atribút je vložený do nepodpísaných atribútov archívnej časovej pečiatky

	electronicsignature-standard(1733) attributes(2) 5 }
	ATSHashIndex ::= SEQUENCE {
	hashIndAlgorithm AlgorithmIdentifier DEFAULT {algorithm id-sha256},
	certificatesHashIndex SEQUENCE OF OCTET STRING,
	crlsHashIndex SEQUENCE OF OCTET STRING,
	unsignedAttrsHashIndex SEQUENCE OF OCTET STRING
	}
			verzie 3. Pole hashIndAlgorithm, ktoré obsahuje identifikátor algoritmu digitálneho odtlačku, ktorý je použitý na výpočet ostatných odtlačkov v atribúte. Algoritmus musí byť rovnaký ako je použitý na výpočet message-imprint v archívnej časovej pečiatke.
			Pole certificatesHashIndex je sekvencia odtlačkov všetkých položiek typu CertificateChoices v SignedData.certificates.
			Pole crlsHashIndex je sekvencia odtlačkov všetkých položiek typu RevocationInfoChoice v SignedData.crls.
			Pole unsignedAttrsHashIndex je sekvencia odtlačkov všetkých položiek typu Attribute v SignedData.signerInfo.unsignedAttrs zo signerInfo podpisu, do ktorého pridávame archívnu časovú pečiatku.

2	id-aa-ets-archiveTimestampV3 OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) electronic-signature-standard(1733) attributes(2) 4 } ArchiveTimeStampToken ::= TimeStampToken	P	Povinný atribút pre CAdES-A s ATS verzie 3, jeden podpis ich môže obsahovať viacero od rôznych autorít a/alebo z rôznych časov. Hodnota `messageImprint` v štruktúre `TimeStampToken` bude obsahovať hash zreťazenia nasledovných dát: • `SignedData.encapContentInfo.eContentType`. • Dáta reprezentujúce odtlačok podpísaných dát. Odtlačok je vypočítaný z rovnakých dát, ktoré boli použité na výpočet odtlačku v message-digest v podpísaných atribútoch podpisu pokrytého archívnou časovou pečiatkou. Algoritmus odtlačku musí byť rovnaký ako algoritmus použitý pre výpočet hodnoty message-imprint archívnej časovej pečiatky. • Polia `version`, `sid`, `digestAlgorithm`, `signedAttrs`, `signatureAlgorithm` a `signature` zo SignedData.signerInfo korešpondujúce podpisu, ktoré má byť rozšírený o archívnu časovú pečiatku. • jedna inštancia ATSHashIndex podľa definícia

			v bode 1 tabuľky.

Proces výpočtu hodnoty message-imprint archívnej časovej pečiatky verzie 3 názorne ilustruje nasledujúci obrázok.



4.8. Kódovanie

Všetky atribúty, zahrnuté do výpočtu hashu pre archívnu časovú pečiatku (pozri [1], Annex K, tab. K.3) musia byť kódované v DER, ostatné môžu byť kódované v BER kvôli zjednodušeniu jednoprechodového spracovania [3].

5. Formát ZEPfZIP obálky

Táto kapitola opisuje formát ZEPfZIP obálky, podľa dokumentu [10], kapitola 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 arcvhivované s integritným podpisom umiestneným v ZIP súbore), Policy (zoznam použitých politík), Other (nešpecifikovaný zoznam priložených súborov).

Nasledujúca tabuľka obsahuje názvy základnej množiny súborov v ZIP formáte.

	Typ položky	Popis	Príklad
1.	D	Directory – hlavný adresár podpisu. Nie je povinný, ale sprehľadňuje používanie pri kopírovaní 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	`M20040129084128Z.eml`

		uložených do súboru „.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.	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

Tabuľka špecifikuje minimálnu množinu typov súborov, ktorú musí vedieť spracovať každá ZEP aplikácia pre administratívny styk. Podpisované elektronické dokumenty pre administratívny styk sa odporúčajú uložiť v MIME kódovaní do súboru s koncovkou *.EML.

6. Podporované kryptografické algoritmy

V rámci profilu CAdES_ZEP sú podporované nasledujúce podpisové schémy:

Názov	Identifikátor (OID)
DSA-SHA1 (DSS)	1.3.14.3.2.27
RSA-SHA1	1.2.840.113549.1.1.5
RSA-SHA256	1.2.840.113549.1.1.5.11
RSA-SHA384	1.2.840.113549.1.1.5.12
RSA-SHA512	1.2.840.113549.1.1.5.13

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

Názov	Identifikátor (OID)
SHA-1	1.3.14.3.2.26
SHA-224	2.16.840.1.101.3.4.2.4
SHA-256	2.16.840.1.101.3.4.2.1
SHA-384	2.16.840.1.101.3.4.2.2
SHA-512	2.16.840.1.101.3.4.2.3