



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

**Verzia 3.0**

## **Formáty podpisových politík**

**19.4.2021**

---

**NÁRODNÝ BEZPEČNOSTNÝ ÚRAD**

odbor bezpečnostných politík sekcie regulácie a dohľadu

Budatínska č. 30, 851 06 Bratislava

<http://www.nbu.gov.sk/>

e-mail: [podatelna@nbu.gov.sk](mailto:podatelna@nbu.gov.sk)

## Obsah

<b>1</b>	<b>ÚVOD.....</b>	<b>4</b>
<b>2</b>	<b>PREDMET DOKUMENTU.....</b>	<b>4</b>
<b>3</b>	<b>ODKAZY .....</b>	<b>5</b>
<b>4</b>	<b>SKRATKY .....</b>	<b>6</b>
<b>5</b>	<b>PODPISOVÉ POLITIKY.....</b>	<b>7</b>
5.1	ZVEREJNENIE PODPISOVEJ POLITIKY .....	7
5.2	VÝBER PODPISOVEJ POLITIKY VO VALIDAČNEJ APLIKÁCII.....	8
5.3	PROCES POUŽITIA PODPISOVEJ POLITIKY .....	9
	<b>PRÍLOHA A (NORMALITVNA) ASN.1 PRE PODPISOVÚ POLITIKU.....</b>	<b>11</b>
	<b>PRÍLOHA B (INFORMATÍVNA) ZOZNAM POUŽITEJ LITERATÚRY .....</b>	<b>27</b>
	<b>PRÍLOHA C HISTÓRIA.....</b>	<b>28</b>

## 1 Úvod

Členské štáty v súlade s podmienkami podľa vnútroštátneho práva na základe článku 17 ods. 5 nariadenia (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „nariadenie (EÚ) č. 910/2014“ alebo „nariadenie eIDAS“), vydajú pre dôveryhodnú infraštruktúru implementačné štandardy, ktoré mapujú požiadavky vnútroštátneho práva a EÚ legislatív do technických postupov pre jej vykonateľnosť. Splnenie tejto požiadavky je realizované na viacerých úrovniach:

- Na základe požiadaviek podľa kapitoly II prílohy I [vykonávacieho rozhodnutia Komisie \(EÚ\) 2015/1505 z 8. septembra 2015, ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa čl. 22 ods. 5 nariadenia Európskeho parlamentu a Rady \(EÚ\) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu](#) a vnútroštátneho práva, je orgánom dohľadu (NBÚ) vydaná [schéma dohľadu](#).
- Na základe § 11 písm. k) [zákona č. 272/2016 Z. z.](#) o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) (ďalej len „zákon č. 272/2016 Z. z.“) vydáva NBÚ štandardy pre oblasť dôveryhodných služieb.

## 2 Predmet dokumentu

Tento implementačný štandard je vydaný na základe § 11 písm. m) [zákona č. 272/2016 Z. z.](#) podľa ktorého NBÚ vydáva, spravuje a zverejňuje podpisové politiky, ktoré obsahujú najmä zoznam algoritmov a ich minimálne parametre pre elektronický podpis od úrovne bezpečnosti zdokonalený elektronický podpis a pre elektronickú pečať od úrovne bezpečnosti zdokonalená elektronická pečať, ktoré sa od ich zverejnenia NBÚ musia dodržiavať v styku s orgánmi verejnej moci a so subjektom verejného sektora definovaného v článku 3 ods. 7 nariadenia (EU) č. 910/2014.

### 3 Odkazy

Odkazy na dokumenty, ktoré definujú použité typy a postupy.

- [1] ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8
- [2] RFC 5280 X.509 PKI Certificate and Certificate Revocation List 5-2008
- [3] Schéma dohľadu - orgánu dohľadu NBÚ  
(pozri <https://www.nbu.gov.sk/doveryhodne-sluzby/dohlad/>  
<https://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/docs/SchemaDohladu.pdf>)
- [4] ETSI TS 101 733 V1.4.0 (2002-09) Electronic Signatures and Infrastructures (ESI);  
Electronic Signature Formats (pozri štruktúru ASN.1 podpisovej politiky  
v kapitolách 6 a 11)  
[https://www.etsi.org/deliver/etsi\\_ts/101700\\_101799/101733/01.04.00\\_60/ts\\_101\\_733v010400p.pdf](https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.04.00_60/ts_101_733v010400p.pdf)
- [5] ETSI TS 119 612 Trusted Lists
- [6] NBU Dokumentácia TL X.509 XML schémy pre dôveryhodný zoznam  
(Pozri <http://ep.nbu.gov.sk/kca/tsl/tlx509XMLSchemaDocumentation.pdf>)
- [7] RFC 5652 Cryptographic Message Syntax 9-2009  
(Pozri <https://tools.ietf.org/html/rfc5652>)
- [8] Vykonávacie rozhodnutie Komisie (EÚ) 2015/1506 z 8. septembra 2015, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať, podľa článkov 27 ods. 5 a 37 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.
- [9] Vykonávacie rozhodnutie Komisie (EÚ) 2015/1505 z 8. septembra 2015, ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa článku 22 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.
- [10] ISO 14533-4 Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes)  
(Pozri <https://www.iso.org/obp/ui/#iso:std:iso:14533:-4:ed-1:v1:en>)

## 4 Skratky

ASN.1	Abstract Syntax Notation 1
CMS	Cryptographic Message Syntax
DER	Distinguished Encoding Rules (for ASN.1)
eIDAS	Nariadenie Európskeho parlamentu a Rady o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
ISO	International Organization for Standardization
NBÚ	Národný bezpečnostný úrad
OID	Object Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XER	XML encoding rules (for ASN.1)

## 5 Podpisové politiky

### 5.1 Zverejnenie podpisovej politiky

Podpisové politiky sú dostupné na webovom sídle NBÚ:

<http://www.nbu.gov.sk/doveryhodne-sluzby/doveryhodna-infrastruktura/podpisove-politiky/>

Podpisové politiky sú dôveryhodne zverejňované prostredníctvom zapečateného textového dokumentu, ktorý obsahuje sekvenciu http odkazu, hash hodnoty z odkazovaného dokumentu podpisovej politiky alebo dôveryhodného certifikátu a údaj o čase konca platnosti, keďže v podpisovej politike nemusí byť koniec obdobia platnosti uvedený alebo je potrebné ho skrátiť.

Zapečatený zoznam odkazov pre automatické spracovanie je zverejnený na webovom sídle NBÚ <https://www.nbu.gov.sk/doveryhodne-sluzby/doveryhodne-zoznamy/> a odkaz je uvedený aj v dôveryhodnom zozname v službe typu:

<http://uri.etsi.org/TrstSvc/Svctype/SignaturePolicyAuthority>

Vo formáte interného CMS podpisu TXT dokumentu, definovaného v tejto kapitole, s rozšírením súboru (\*.p7m). [TrustedList.p7m](#) [TrustedList.p7m](#) [TrustedList.p7m](#)

Vo formáte interného CMS podpisu TXT dokumentu, definovaného v kapitole 4.7 v ISO 14533-4, s rozšírením súboru (\*.p7m). [preservation-integrity-list.p7m](#) [preservation-integrity-list.p7m](#) [preservation-integrity-list.p7m](#)

NBÚ vydáva, spravuje a zverejňuje podpisové politiky, ktoré obsahujú najmä zoznam algoritmov a ich minimálne parametre pre elektronický podpis od úrovne bezpečnosti zdokonalený elektronický podpis a pre elektronickú pečať od úrovne bezpečnosti zdokonalená elektronická pečať, ktoré sa od ich zverejnenia NBÚ musia dodržiavať v styku s orgánmi verejnej moci.

Podpisová politika je zverejnená v dvoch formátoch:

- v záväznom DER kódovaní podpisovej politiky, ktorej štruktúra v ASN.1 jazyku je uvedená v prílohe A,
- v informatívnom XER kódovaní, ako transformácia z DER kódovania, s textovými komentárimi popisujúcimi položky.

Podpisové politiky a dôveryhodné certifikáty sú zverejnené prostredníctvom http odkazov uvedených v textovom dokumente, ktorý je v UTF-8 kódovaní a obsahuje postupnosti riadkov začínajúcich s reťazcami "FILE=", "HASH(SHA256:2 16 840 1 101 3 4 2 1)=" a "NOTICE=", kde v riadku označenom FILE je http adresa na dokument, v HASH riadku je hash odtlačok z DER dokumentu podpisovej politiky alebo z dôveryhodného certifikátu a v riadku "NOTICE=" je ako prvá hodnota čas konca platnosti podpisovej politiky alebo dôveryhodného certifikátu alebo čas predčasného ukončenia platnosti vo formáte *GeneralizedTime* a medzerou sú oddelené ďalšie nepovinné informácie.

TXT dokument definovaný v kapitole 4.7 v ISO 14533-4, preservation-integrity-list, obsahuje rovnaké hodnoty ako sú uvedené vyššie a má nasledovnú štruktúru:

The text of the preservation-integrity-list shall consist of 3 types of subsequent text lines: mandatory "FILE=x", mandatory "HASH=x" and

optional "NOTICE=x" followed by a single EOL marker, where 'x' shall be as follows:

- If the line is "FILE=x", the x shall be a URL of the object. See IETF RFC 7230, Section 2.7, where URI is used throughout HTTP as the means for identifying resources.
- If the line is "HASH=x", the x shall be a Base64 (IETF RFC 4648) encoded DID of the object whose location is in the previous line "FILE=x". The subsequent line may be repeated more than once with the line "HASH=x", e.g. with a different hash algorithm and hash value for the same object referenced by URL in previous line "FILE=x".
- If the line is "NOTICE=x", the x shall be any additional information of the object whose location and hash are in the previous lines "FILE=x" and "HASH=x".

The subsequent text lines "FILE=x", "HASH=x" and optional "NOTICE=x" may be repeated more than once, e.g. with a different object referenced by URL in the "FILE=x" line.

Textový dokument odkazov na podpisové politiky a dôveryhodné certifikáty je zapečatený zdokonalenou elektronickou pečaťou vo formáte interného CMS podpisu.

## 5.2 Výber podpisovej politiky vo validačnej aplikácii

Od 1.7.2016, kedy nadobudlo účinnosť nariadenie eIDAS, sa **neodporúča explicitne uviesť** odkaz na **podpisovú politiku** v kvalifikovanom elektronickej podpise alebo kvalifikovanej elektronickej pečati (postup pre explicitnú podpisovú politiku je uvedený vo verzii č. 2 tohto štandardu, ktorý opravil chybne definované položky prílohy A, napr. položku *cautionPeriod*, ktorú ETSI vo verzii z roku 2019 úplne odstránilo, pozri [ETSI TS 119 172-3 V1.1.1 \(2019-12\) ASN.1 format for signature policies](#)), ale používať implicitné podpisové politiky, ktoré zverejňuje NBÚ na základe § 11 písm. m) [zákona č. 272/2016 Z. z..](#)

Pri vyhotovovaní podpisov a validovaní algoritmov je potrebné vychádzať aj z iných odporúčaní, napríklad pre hardvérové zariadenia, keďže formát podpisovej politiky neumožňuje uviesť detailné požiadavky, napr. koniec používania RSA-PKCS#1v1.5, ktorý je potrebné postupne nahradíť napr. s RSA-PSS, ako je uvedené v [SOG-IS Crypto Working Group](#): "SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms" Version 1.2.

**Note 27-LegacyRSA.** The acceptability deadline for the legacy use of modulus of size above 1900 bits, but less than 3000 bits, is set to December 31, 2025.

In case a padding oracle is available, the RSA-PKCS#1v1.5 scheme is vulnerable to efficient attacks.

Proces kontroly:

- Validujúca aplikácia načíta a overí podpis / pečať podľa kapitoly 5.1 [preservation-integrity-list.p7m](#) alebo [TrustedList.p7m](#) pomocou certifikátu vydaného KCA NBÚ na validovanie dôveryhodného zoznamu. V dôveryhodnom zozname je certifikát na overenie podpisu / pečate uvedený v službe typu *ServiceTypeIdentifier* "<http://uri.etsi.org/TrstSvc/Svctype/SignaturePolicyAuthority>". Po overení získa TXT dokument obsahujúci zoznam http adries a mien súborov na podpisové politiky, ich hash hodnôt a časov konca platnosti, dokedy sú podpisové politiky platné.
- Podpis / pečať zoznamu odkazov na podpisové politiky sa overuje certifikátom, v ktorom je uvedený OID 1.3.158.36061701.0.0.1.10.5.0.1 certifikačnej politiky.

- Získaný zoznam odkazov, hash hodnôt na podpisové politiky a časov konca platnosti podpisovej politiky aplikácia neskôr použije pri overovaní, či validovaný podpis / pečiatka a ostatné objekty obsahujú bezpečné algoritmy.

### 5.3 Proces použitia podpisovej politiky

Podpisová politika vybraná zo zoznamu podľa kapitoly 5.1 a 5.2 slúži podľa § 11 písm. m) [zákona č. 272/2016 Z. z.](#) na preverenie dodržiavania algoritmov a ich minimálnych parametrov v styku s orgánmi verejnej moci.

Položky podpisovej politiky definuje príloha A. Položky podpisovej politiky v prílohe A boli definované pred nadobudnutím účinnosti nariadenia eIDAS, ktoré vyžaduje použiť dôveryhodný zoznam, keďže dôveryhodný zoznam **má konštitutívny charakter**. Aplikácia, ktorá pri validácii nepoužíva dôveryhodný zoznam, nie je v súlade s nariadením eIDAS a minimálne **subjekt verejného sektora ju nesmie používať na validáciu** kvalifikovaného elektronického podpisu alebo kvalifikovanej elektronickej pečiate.

Ak je použitý dôveryhodný zoznam, položka *cautionPeriod* definovaná napr. v kapitole 11.8 a 6.5.3 v ETSI ETSI TS 101 733 V1.4.0 je použitá s nulovou hodnotou, keďže položka *TimestampTrustCondition* definovaná napr. v kapitole 11.8 v ETSI ETSI TS 101 733 V1.4.0 je nahradená údajmi z dôveryhodného zoznamu. (Napr. ETSI validačná politika pri použití dôveryhodného zoznamu požaduje: The *RevocationFreshnessConstraints* defined in ETSI TS 119 172-1, clause A.4.2.1, table A.2 rows (m)2.2 shall be used with a maximum value of 0, ensuring that the revocation information is only accepted if it has been issued after the best signature time.)

Ak sa nevaliduje podľa dôveryhodného zoznamu (podľa nariadenia eIDAS), hodnota položky *cautionPeriod* slúži pre overenie v hierarchii niekoľkých CA vytvárajúcich certifikačnú cestu, kedy napr.

- pre CRLs na overenie certifikátu podpisovateľa je potrebné čakať dokiaľ položka *thisUpdate* z CRLs nie je po čase časovej pečiatky zahrňujúcej podpis,
- následne na overenie podpisu CRLs je potrebné čakať dokiaľ položka *thisUpdate* z *CRLca1* nie je po čase z *thisUpdate* z CRLs,
- následne na overenie podpisu *CRLca1* je potrebné čakať dokiaľ položka *thisUpdate* z *CRLca2* nie je po čase z *thisUpdate* z *CRLca1* a
- predchádzajúci krok sa opakuje až dokiaľ nie je overená celá certifikačná cesta.

Pre splnenie § 11 písm. m) [zákona č. 272/2016 Z. z.](#) sa použijú len nasledovné položky podpisovej politiky:

- a) *SignaturePolicy.signPolicyInfo.signatureValidationPolicy.signingPeriod.notBefore*,
- b) *SignaturePolicy.signPolicyInfo.signatureValidationPolicy.signingPeriod.notAfter*,
- c) *SignaturePolicy.signPolicyInfo.signatureValidationPolicy.commonRules.algorithmConstraintSet*.

Obdobie *signingPeriod* podľa písmen a) a b) označuje dátum a čas, pred ktorým by sa podpisová politika nemala používať na vyhotovenie podpisu a voliteľný dátum, po ktorom by sa nemala používať na vyhotovenie podpisov, ak toto obdobie nie je skrátené v položke "NOTICE=", v ktorej sa nachádza čas konca platnosti identický s písmenom b) alebo kratší pre potrebu skrátenia v súlade s kapitolou 5.1. NBÚ zverejňuje podpisové politiky na fixné obdobia a ak nedošlo k oslabeniu algoritmov, zverejní v novej podpisovej politike rovnaké požiadavky na tie isté algoritmy na ďalšie obdobie v zapečatenom zozname odkazov, čo umožní validujúcej aplikácii správne vyhodnotiť platnosť použitého algoritmu.

Položky podľa písmena c) obsahujú zoznam algoritmov a ich parametrov, ktoré sa pri validácii overia a musia byť splnené pre automatizované rozhodnutie. Ak sa odhalí nezhoda, automatická validácia nie je možná a postupuje sa na základe iného overenia, kedy sa rozhodne napríklad o akceptovaní, ak krajina, v ktorej bol algoritmus použitý na komunikáciu so subjektom verejného sektora, akceptuje takýto algoritmus a jeho parametre v danom konaní.

Pred validovaním kvalifikovaného elektronického podpisu / pečate a iného objektu, v ktorom bol použitý hash algoritmus alebo asymetrický algoritmus, je potrebné dôveryhodne získať **čas, kedy bol algoritmus použitý** vo vyhotovenom objekte. Postup určenia času vyhotovenia objektu, v ktorom je použitý algoritmus, definuje schéma dohľadu [3] v kapitole 5.3.2 s názvom "SD čl. 32 a 40 nariadenia (EÚ) č. 910/2014". Pre kvalifikovanú elektronickú časovú pečiatku, ktorá je vydaná podľa aktuálneho dôveryhodného zoznamu aktuálne kvalifikovanou dôveryhodnou službou, **je to čas uvedený v tejto časovej pečiatke**. Rovnako to platí aj pre CRL a OCSP odpovede, ktoré v sebe obsahujú čas ich vyhotovenia, ak sú vydané dôveryhodnou treťou stranou, ktorej dôveryhodná služba má v aktuálnom dôveryhodnom zozname udelený kvalifikovaný štatút.

Aj keď štandard uvedený v prílohe A umožňuje rôzne účely použitia podpisovej politiky, tento dokument, od účinnosti nariadenia eIDAS, definuje použitie formátu podpisovej politiky, zverejnenej NBÚ, na vedenie zoznamu algoritmov bezpečných v časovom intervale uvedenom v podpisovej politike, ktorý v prípade potreby skráti pomocou údajov v zozname odkazov na podpisové politiky.

Na základe dôveryhodného času vyhotovenia objektu *given-time*, podľa schémy dohľadu a odporúčania ITU-T X.509, sa vyberie zo zoznamu podpisová politika platná v čase *given-time* a podľa nej sa overí algoritmus. Tento postup platí pre všetky typy objektov obsahujúcich použitý algoritmus, napríklad časovú pečiatku, OCSP odpoved', certifikát X.509, CRL alebo len hash hodnotu.

Jednotlivé podpisové politiky zverejňované NBÚ podľa § 11 písm. m) [zákona č. 272/2016 Z. z.](#) sa v intervaloch svojej platnosti prekrývajú tak, aby tvorili súvislú postupnosť bez konfliktných situácií platnosti algoritmov v čase.

NBÚ musí zabezpečiť, aby dve aktuálne platné podpisové politiky neobsahovali rozdielne požiadavky. Ak by bolo potrebné napr. zrušiť algoritmus, skráta sa v aktuálnych podpisových politikách platnosti do času xz a od času xz bude platiť nová podpisová politika, pričom čas xz bude minimálne 5 dní po čase zverejnenia zmeny v zapečatenom zozname odkazov na podpisové politiky, ak to z hľadiska akútnosti zmeny bude možné.

## Príloha A (normatívna) ASN.1 pre podpisovú politiku

Vzhľadom na chybne zapísané niektoré štruktúry ASN.1 podpisovej politiky v kapitolách 6 a 11 v [ETSI TS 101 733](#) V1.4.0, sú v tejto prílohe uvedené kompletne ASN.1 moduly pre ASN.1 podpisovú politiku a jej prevod z DER do XER kódovania.

Právny odbor ETSI organizácie povolil uviest' kompletnej opravený text ASN.1 PP z ETSI štandardu v NBÚ štandarde na webovom sídle NBÚ.

PP v ASN.1:

```
ETS-ElectronicSignaturePolicies-88syntax { iso(1) member-body(2) us(840)
                                             rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-mod(0) 7 }
DEFINITIONS EXPLICIT TAGS ::=
BEGIN

SignaturePolicy ::= SEQUENCE {
    signPolicyHashAlg      AlgorithmIdentifier,
    signPolicyInfo         SignPolicyInfo,
    signPolicyHash         SignPolicyHash OPTIONAL
}

SignPolicyHash ::= OCTET STRING

SignPolicyInfo ::= SEQUENCE {
    signPolicyIdentifier   SignPolicyId,
    dateOfIssue            GeneralizedTime,
    policyIssuerName       PolicyIssuerName,
    fieldOfApplication     FieldOfApplication,
    signatureValidationPolicy SignatureValidationPolicy,
    signPolExtensions      SignPolExtensions OPTIONAL
}

SignPolicyId ::= OBJECT IDENTIFIER

PolicyIssuerName ::= GeneralNames

FieldOfApplication ::= DirectoryString

SignatureValidationPolicy ::= SEQUENCE {
    signingPeriod          SigningPeriod,
    commonRules             CommonRules,
    commitmentRules         CommitmentRules,
    signPolExtensions       SignPolExtensions OPTIONAL
}

SigningPeriod ::= SEQUENCE {
    notBefore               GeneralizedTime,
    notAfter                GeneralizedTime OPTIONAL
}

CommonRules ::= SEQUENCE {
    signerAndVerifierRules [0] SignerAndVerifierRules OPTIONAL,
    signingCertTrustCondition [1] SigningCertTrustCondition OPTIONAL,
    timeStampTrustCondition [2] TimestampTrustCondition OPTIONAL,
    attributeTrustCondition [3] AttributeTrustCondition OPTIONAL,
    algorithmConstraintSet [4] AlgorithmConstraintSet OPTIONAL,
    signPolExtensions       [5] SignPolExtensions OPTIONAL
}

CommitmentRules ::= SEQUENCE OF CommitmentRule
```

```
CommitmentRule ::= SEQUENCE {
    selCommitmentTypes SelectedCommitmentTypes,
    signerAndVerifierRules [0] SignerAndVerifierRules OPTIONAL,
    signingCertTrustCondition [1] SigningCertTrustCondition OPTIONAL,
    timeStampTrustCondition [2] TimestampTrustCondition OPTIONAL,
    attributeTrustCondition [3] AttributeTrustCondition OPTIONAL,
    algorithmConstraintSet [4] AlgorithmConstraintSet OPTIONAL,
    signPolExtensions [5] SignPolExtensions OPTIONAL
}

SelectedCommitmentTypes ::= SEQUENCE OF SelectedCommitmentType

SelectedCommitmentType ::= CHOICE {
    empty NULL,
    recognizedCommitmentType CommitmentType
}

CommitmentType ::= SEQUENCE {
    identifier CommitmentTypeIdentifier,
    fieldOfApplication [0] FieldOfApplication OPTIONAL,
    semantics [1] DirectoryString OPTIONAL
}

CommitmentTypeIdentifier ::= OBJECT IDENTIFIER

SignerAndVerifierRules ::= SEQUENCE {
    signerRules SignerRules,
    verifierRules VerifierRules
}

SignerRules ::= SEQUENCE {
    externalSignedData BOOLEAN OPTIONAL,
    mandatedSignedAttr CMSAttrs,
    mandatedUnsignedAttr CMSAttrs,
    mandatedCertificateRef [0] CertRefReq DEFAULT signerOnly,
    mandatedCertificateInfo [1] CertInfoReq DEFAULT none,
    signPolExtensions [2] SignPolExtensions OPTIONAL
}

CMSAttrs ::= SEQUENCE OF OBJECT IDENTIFIER

CertRefReq ::= ENUMERATED {
    signerOnly(1),
    fullPath(2)
}

CertInfoReq ::= ENUMERATED {
    none(0),
    signerOnly(1),
    fullPath(2)
}

VerifierRules ::= SEQUENCE {
    mandatedUnsignedAttr MandatedUnsignedAttr,
    signPolExtensions SignPolExtensions OPTIONAL
}

MandatedUnsignedAttr ::= CMSAttrs

CertificateTrustTrees ::= SEQUENCE OF CertificateTrustPoint

CertificateTrustPoint ::= SEQUENCE {
    trustpoint Certificate,
```

```

pathLenConstraint      [0] PathLenConstraint OPTIONAL,
acceptablePolicySet   [1] AcceptablePolicySet OPTIONAL,
nameConstraints       [2] NameConstraints OPTIONAL,
policyConstraints     [3] PolicyConstraints OPTIONAL
}

PathLenConstraint ::= INTEGER (0 .. MAX)

AcceptablePolicySet ::= SEQUENCE OF CertPolicyId

CertRevReq ::= SEQUENCE {
    endCertRevReq  RevReq,
    caCerts        [0] RevReq
}

RevReq ::= SEQUENCE {
    enuRevReq      EnuRevReq,
    exRevReq       SignPolExtensions OPTIONAL
}

EnuRevReq ::= ENUMERATED {
    clrCheck(0),
    ocspCheck(1),
    bothCheck(2),
    eitherCheck(3),
    noCheck(4),
    other(5)
}

SigningCertTrustCondition ::= SEQUENCE {
    signerTrustTrees  CertificateTrustTrees,
    signerRevReq     CertRevReq
}

TimestampTrustCondition ::= SEQUENCE {
    ttsCertificateTrustTrees [0] CertificateTrustTrees OPTIONAL,
    ttsRevReq         [1] CertRevReq OPTIONAL,
    ttsNameConstraints [2] NameConstraints OPTIONAL,
    cautionPeriod    [3] DeltaTime OPTIONAL,
    signatureTimestampDelay [4] DeltaTime OPTIONAL
}

DeltaTime ::= SEQUENCE {
    deltaSeconds    INTEGER,
    deltaMinutes   INTEGER,
    deltaHours     INTEGER,
    deltaDays      INTEGER
}

AttributeTrustCondition ::= SEQUENCE {
    attributeMandated BOOLEAN,
    howCertAttribute HowCertAttribute,
    attrCertificateTrustTrees [0] CertificateTrustTrees OPTIONAL,
    attrRevReq       [1] CertRevReq OPTIONAL,
    attributeConstraints [2] AttributeConstraints OPTIONAL
}

HowCertAttribute ::= ENUMERATED {
    claimedAttribute(0),
    certifiedAttribtes(1),
    either(2)
}

AttributeConstraints ::= SEQUENCE {

```

```

attributeTypeConstraints [0] AttributeTypeConstraints OPTIONAL,
attributeValueConstraints [1] AttributeValueConstraints OPTIONAL
}

AttributeTypeConstraints ::= SEQUENCE OF AttributeType

AttributeValueConstraints ::= SEQUENCE OF AttributeTypeAndValue

AlgorithmConstraintSet ::= SEQUENCE {
    signerAlgorithmConstraints [0] AlgorithmConstraints OPTIONAL,
    eeCertAlgorithmConstraints [1] AlgorithmConstraints OPTIONAL,
    caCertAlgorithmConstraints [2] AlgorithmConstraints OPTIONAL,
    aaCertAlgorithmConstraints [3] AlgorithmConstraints OPTIONAL,
    tsaCertAlgorithmConstraints [4] AlgorithmConstraints OPTIONAL
}

AlgorithmConstraints ::= SEQUENCE OF AlgAndLength

AlgAndLength ::= SEQUENCE {
    algID OBJECT IDENTIFIER,
    minKeyLength INTEGER OPTIONAL,
    other SignPolExtensions OPTIONAL
}

SignPolExtensions ::= SEQUENCE OF SignPolExtn

SignPolExtn ::= SEQUENCE {
    extnID OBJECT IDENTIFIER,
    extnValue OCTET STRING
}

END

PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-explicit(18) }
DEFINITIONS EXPLICIT TAGS :=

BEGIN

id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6)
internet(1)
    security(5) mechanisms(5) pkix(7) }

id-pe OBJECT IDENTIFIER ::= { id-pkix 1 }

id-qt OBJECT IDENTIFIER ::= { id-pkix 2 }

id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }

id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }

id-qt-cps OBJECT IDENTIFIER ::= { id-qt 1 }

id-qt-unotice OBJECT IDENTIFIER ::= { id-qt 2 }

id-ad-ocsp OBJECT IDENTIFIER ::= { id-ad 1 }

id-ad-caIssuers OBJECT IDENTIFIER ::= { id-ad 2 }

id-ad-timeStamping OBJECT IDENTIFIER ::= { id-ad 3 }

id-ad-caRepository OBJECT IDENTIFIER ::= { id-ad 5 }

Attribute ::= SEQUENCE {
    type AttributeType,

```

```
values      SET OF AttributeValue
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY

AttributeTypeAndValue ::= SEQUENCE {
    type      AttributeType,
    value     AttributeValue
}

id-at OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 4 }

id-at-name AttributeType ::= { id-at 41 }

id-at-surname AttributeType ::= { id-at 4 }

id-at-givenName AttributeType ::= { id-at 42 }

id-at-initials AttributeType ::= { id-at 43 }

id-at-generationQualifier AttributeType ::= { id-at 44 }

X520name ::= CHOICE {
    teletexString TeletexString (SIZE(1..ub-name)),
    printableString PrintableString (SIZE(1..ub-name)),
    universalString UniversalString (SIZE(1..ub-name)),
    utf8String    UTF8String (SIZE(1..ub-name)),
    bmpString     BMPString (SIZE(1..ub-name))
}

id-at-commonName AttributeType ::= { id-at 3 }

X520CommonName ::= CHOICE {
    teletexString TeletexString (SIZE(1..ub-common-name)),
    printableString PrintableString (SIZE(1..ub-common-name)),
    universalString UniversalString (SIZE(1..ub-common-name)),
    utf8String    UTF8String (SIZE(1..ub-common-name)),
    bmpString     BMPString (SIZE(1..ub-common-name))
}

id-at-localityName AttributeType ::= { id-at 7 }

X520LocalityName ::= CHOICE {
    teletexString TeletexString (SIZE(1..ub-locality-name)),
    printableString PrintableString (SIZE(1..ub-locality-name)),
    universalString UniversalString (SIZE(1..ub-locality-name)),
    utf8String    UTF8String (SIZE(1..ub-locality-name)),
    bmpString     BMPString (SIZE(1..ub-locality-name))
}

id-at-stateOrProvinceName AttributeType ::= { id-at 8 }

X520StateOrProvinceName ::= CHOICE {
    teletexString TeletexString (SIZE(1..ub-state-name)),
    printableString PrintableString (SIZE(1..ub-state-name)),
    universalString UniversalString (SIZE(1..ub-state-name)),
    utf8String    UTF8String (SIZE(1..ub-state-name)),
    bmpString     BMPString (SIZE(1..ub-state-name))
}

id-at-organizationName AttributeType ::= { id-at 10 }
```

```

X520OrganizationName ::= CHOICE {
    teletexString TeletexString (SIZE(1..ub-organization-name)),
    printableString PrintableString (SIZE(1..ub-organization-name)),
    universalString UniversalString (SIZE(1..ub-organization-name)),
    utf8String UTF8String (SIZE(1..ub-organization-name)),
    bmpString BMPString (SIZE(1..ub-organization-name))
}

id-at-organizationalUnitName AttributeType ::= { id-at 11 }

X520OrganizationalUnitName ::= CHOICE {
    teletexString TeletexString (SIZE(1..ub-organizational-unit-name)),
    printableString PrintableString (SIZE(1..ub-organizational-unit-name)),
    universalString UniversalString (SIZE(1..ub-organizational-unit-name)),
    utf8String UTF8String (SIZE(1..ub-organizational-unit-name)),
    bmpString BMPString (SIZE(1..ub-organizational-unit-name))
}

id-at-title AttributeType ::= { id-at 12 }

X520Title ::= CHOICE {
    teletexString TeletexString (SIZE(1..ub-title)),
    printableString PrintableString (SIZE(1..ub-title)),
    universalString UniversalString (SIZE(1..ub-title)),
    utf8String UTF8String (SIZE(1..ub-title)),
    bmpString BMPString (SIZE(1..ub-title))
}

id-at-dnQualifier AttributeType ::= { id-at 46 }

X520dnQualifier ::= PrintableString

id-at-countryName AttributeType ::= { id-at 6 }

X520countryName ::= PrintableString (SIZE(2))

id-at-serialNumber AttributeType ::= { id-at 5 }

X520SerialNumber ::= PrintableString (SIZE(1..ub-serial-number))

id-at-pseudonym AttributeType ::= { id-at 65 }

X520Pseudonym ::= CHOICE {
    teletexString TeletexString (SIZE(1..ub-pseudonym)),
    printableString PrintableString (SIZE(1..ub-pseudonym)),
    universalString UniversalString (SIZE(1..ub-pseudonym)),
    utf8String UTF8String (SIZE(1..ub-pseudonym)),
    bmpString BMPString (SIZE(1..ub-pseudonym))
}

id-domainComponent AttributeType ::= { 0 9 2342 19200300 100 1 25 }

DomainComponent ::= IA5String

pkcs-9 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549)
pkcs(1) 9 }

id-emailAddress AttributeType ::= { pkcs-9 1 }

EmailAddress ::= IA5String (SIZE(1..ub-emailaddress-length))

Name ::= CHOICE {
    rdnSequence RDNSequence
}

```

```
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
DistinguishedName ::= RDNSequence
RelativeDistinguishedName ::= SET SIZE(1..MAX) OF AttributeTypeAndValue
DirectoryString ::= CHOICE {
    teletexString TeletexString (SIZE(1..MAX)),
    printableString PrintableString (SIZE(1..MAX)),
    universalString UniversalString (SIZE(1..MAX)),
    utf8String UTF8String (SIZE(1..MAX)),
    bmpString BMPString (SIZE(1..MAX))
}
Certificate ::= SEQUENCE {
    tbsCertificate          TBSCertificate,
    signatureAlgorithm      AlgorithmIdentifier,
    signature                BIT STRING
}
TBSCertificate ::= SEQUENCE {
    version [0] Version DEFAULT v1,
    serialNumber   CertificateSerialNumber,
    signature      AlgorithmIdentifier,
    issuer        Name,
    validity       Validity,
    subject        Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,
    subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,
    extensions     [3] Extensions OPTIONAL
}
Version ::= INTEGER {
    v1(0),
    v2(1),
    v3(2)
}
CertificateSerialNumber ::= INTEGER
Validity ::= SEQUENCE {
    notBefore    Time,
    notAfter     Time
}
Time ::= CHOICE {
    utcTime     UTCTime,
    generalTime GeneralizedTime
}
UniqueIdentifier ::= BIT STRING
SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm      AlgorithmIdentifier,
    subjectPublicKey BIT STRING
}
Extensions ::= SEQUENCE SIZE(1..MAX) OF Extension
Extension ::= SEQUENCE {
    extnID   OBJECT IDENTIFIER,
    critical BOOLEAN DEFAULT FALSE,
```

```

        extnValue      OCTET STRING
    }

CertificateList ::= SEQUENCE {
    tbsCertList    TBSCertList,
    signatureAlgorithm AlgorithmIdentifier,
    signature      BIT STRING
}

TBSCertList ::= SEQUENCE {
    version Version OPTIONAL,
    signature AlgorithmIdentifier,
    issuer   Name,
    thisUpdate Time,
    nextUpdate Time OPTIONAL,
    revokedCertificates SEQUENCE OF SEQUENCE {
        userCertificate CertificateSerialNumber,
        revocationDate Time,
        crlEntryExtensions Extensions OPTIONAL
    } OPTIONAL,
    crlExtensions [0] Extensions OPTIONAL
}

AlgorithmIdentifier ::= SEQUENCE {
    algorithm OBJECT IDENTIFIER,
    parameters ANY algorithm OPTIONAL
}

ORAddress ::= SEQUENCE {
    built-in-standard-attributes BuiltInStandardAttributes,
    built-in-domain-defined-attributes BuiltInDomainDefinedAttributes
OPTIONAL,
    extension-attributes ExtensionAttributes OPTIONAL
}

BuiltInStandardAttributes ::= SEQUENCE {
    country-name CountryName OPTIONAL,
    administration-domain-name AdministrationDomainName OPTIONAL,
    network-address [0] IMPLICIT NetworkAddress OPTIONAL,
    terminal-identifier [1] IMPLICIT TerminalIdentifier OPTIONAL,
    private-domain-name [2] PrivateDomainName OPTIONAL,
    organization-name [3] IMPLICIT OrganizationName OPTIONAL,
    numeric-user-identifier [4] IMPLICIT NumericUserIdentifer OPTIONAL,
    personal-name [5] IMPLICIT PersonalName OPTIONAL,
    organizational-unit-names [6] IMPLICIT OrganizationalUnitNames OPTIONAL
}

CountryName ::= [APPLICATION 1] CHOICE {
    x121-dcc-code NumericString (SIZE(ub-country-name-numeric-length)),
    iso-3166-alpha2-code PrintableString (SIZE(ub-country-name-alpha-length))
}

AdministrationDomainName ::= [APPLICATION 2] CHOICE {
    numeric NumericString (SIZE(0..ub-domain-name-length)),
    printable PrintableString (SIZE(0..ub-domain-name-length))
}

NetworkAddress ::= X121Address

X121Address ::= NumericString (SIZE(1..ub-x121-address-length))

TerminalIdentifier ::= PrintableString (SIZE(1..ub-terminal-id-length))

```

```
PrivateDomainName ::= CHOICE {
    numeric NumericString (SIZE(1..ub-domain-name-length)),
    printable     PrintableString (SIZE(1..ub-domain-name-length))
}

OrganizationName ::= PrintableString (SIZE(1..ub-organization-name-length))

NumericUserIdentifer ::= NumericString (SIZE(1..ub-numeric-user-id-length))

PersonalName ::= SET {
    surname [0] IMPLICIT PrintableString (SIZE(1..ub-surname-length)),
    given-name [1] IMPLICIT PrintableString (SIZE(1..ub-given-name-length))
} OPTIONAL,
initials [2] IMPLICIT PrintableString (SIZE(1..ub-initials-length)) OPTIONAL,
generation-qualifier [3] IMPLICIT PrintableString (SIZE(1..ub-generation-qualifier-length)) OPTIONAL
}

OrganizationalUnitNames ::= SEQUENCE SIZE(1..ub-organizational-units) OF
OrganizationalUnitName

OrganizationalUnitName ::= PrintableString (SIZE(1..ub-organizational-unit-name-length))

BuiltInDomainDefinedAttributes ::= SEQUENCE SIZE(1..ub-domain-defined-attributes) OF BuiltInDomainDefinedAttribute

BuiltInDomainDefinedAttribute ::= SEQUENCE {
    type     PrintableString (SIZE(1..ub-domain-defined-attribute-type-length)),
    value     PrintableString (SIZE(1..ub-domain-defined-attribute-value-length))
} 

ExtensionAttributes ::= SET SIZE(1..ub-extension-attributes) OF
ExtensionAttribute

ExtensionAttribute ::= SEQUENCE {
    extension-attribute-type [0] IMPLICIT INTEGER (0..ub-extension-attributes),
    extension-attribute-value [1] ANY extension-attribute-type
}

common-name INTEGER ::= 1

CommonName ::= PrintableString (SIZE(1..ub-common-name-length))

teletex-common-name INTEGER ::= 2

TeletexCommonName ::= TeletexString (SIZE(1..ub-common-name-length))

teletex-organization-name INTEGER ::= 3

TeletexOrganizationName ::= TeletexString (SIZE(1..ub-organization-name-length))

teletex-personal-name INTEGER ::= 4

TeletexPersonalName ::= SET {
    surname [0] IMPLICIT TeletexString (SIZE(1..ub-surname-length)),
    given-name [1] IMPLICIT TeletexString (SIZE(1..ub-given-name-length))
} OPTIONAL,
initials [2] IMPLICIT TeletexString (SIZE(1..ub-initials-length)) OPTIONAL,
generation-qualifier [3] IMPLICIT TeletexString (SIZE(1..ub-generation-qualifier-length)) OPTIONAL
```

```
}

teletex-organizational-unit-names INTEGER ::= 5

TeletexOrganizationalUnitNames ::= SEQUENCE SIZE(1..ub-organizational-units) OF
TeletexOrganizationalUnitName

TeletexOrganizationalUnitName ::= TeletexString (SIZE(1..ub-organizational-unit-
name-length))

pds-name INTEGER ::= 7

PDSName ::= PrintableString (SIZE(1..ub-pds-name-length))

physical-delivery-country-name INTEGER ::= 8

PhysicalDeliveryCountryName ::= CHOICE {
    x121-dcc-code NumericString (SIZE(ub-country-name-numeric-length)),
    iso-3166-alpha2-code      PrintableString (SIZE(ub-country-name-alpha-
length))
}

postal-code INTEGER ::= 9

PostalCode ::= CHOICE {
    numeric-code   NumericString (SIZE(1..ub-postal-code-length)),
    printable-code   PrintableString (SIZE(1..ub-postal-code-length))
}

physical-delivery-office-name INTEGER ::= 10

PhysicalDeliveryOfficeName ::= PDSPparameter

physical-delivery-office-number INTEGER ::= 11

PhysicalDeliveryOfficeNumber ::= PDSPparameter

extension-OR-address-components INTEGER ::= 12

ExtensionORAddressComponents ::= PDSPparameter

physical-delivery-personal-name INTEGER ::= 13

PhysicalDeliveryPersonalName ::= PDSPparameter

physical-delivery-organization-name INTEGER ::= 14

PhysicalDeliveryOrganizationName ::= PDSPparameter

extension-physical-delivery-address-components INTEGER ::= 15

ExtensionPhysicalDeliveryAddressComponents ::= PDSPparameter

unformatted-postal-address INTEGER ::= 16

UnformattedPostalAddress ::= SET {
    printable-address   SEQUENCE SIZE(1..ub-pds-physical-address-lines) OF
PrintableString (SIZE(1..ub-pds-parameter-length)) OPTIONAL,
    teletex-string      TeletexString (SIZE(1..ub-unformatted-address-length)) 
OPTIONAL
}

street-address INTEGER ::= 17
```

```
StreetAddress ::= PDSPparameter

post-office-box-address INTEGER ::= 18

PostOfficeBoxAddress ::= PDSPparameter

poste-restante-address INTEGER ::= 19

PosteRestanteAddress ::= PDSPparameter

unique-postal-name INTEGER ::= 20

UniquePostalName ::= PDSPparameter

local-postal-attributes INTEGER ::= 21

LocalPostalAttributes ::= PDSPparameter

PDSPparameter ::= SET {
    printable-string      PrintableString (SIZE(1..ub-pds-parameter-length))
OPTIONAL,
    teletex-string        TeletexString (SIZE(1..ub-pds-parameter-length))
OPTIONAL
}

extended-network-address INTEGER ::= 22

ExtendedNetworkAddress ::= CHOICE {
    e163-4-address       SEQUENCE {
        number          [0] IMPLICIT NumericString (SIZE(1..ub-e163-4-number-
length)),
        sub-address     [1] IMPLICIT NumericString (SIZE(1..ub-e163-4-sub-
address-length)) OPTIONAL
    },
    psap-address         [0] IMPLICIT PresentationAddress
}

PresentationAddress ::= SEQUENCE {
    pSelector            [0] EXPLICIT OCTET STRING OPTIONAL,
    sSelector            [1] EXPLICIT OCTET STRING OPTIONAL,
    tSelector            [2] EXPLICIT OCTET STRING OPTIONAL,
    nAddresses          [3] EXPLICIT SET SIZE(1..MAX) OF OCTET STRING
}

terminal-type INTEGER ::= 23

TerminalType ::= INTEGER {
    telex(3),
    teletex(4),
    g3-facsimile(5),
    g4-facsimile(6),
    ia5-terminal(7),
    videotex(8)
} (0..ub-integer-options)

teletex-domain-defined-attributes INTEGER ::= 6

TeletexDomainDefinedAttributes ::= SEQUENCE SIZE(1..ub-domain-defined-
attributes) OF TeletexDomainDefinedAttribute

TeletexDomainDefinedAttribute ::= SEQUENCE {
    type    TeletexString (SIZE(1..ub-domain-defined-attribute-type-length)),
    value   TeletexString (SIZE(1..ub-domain-defined-attribute-value-length))
}
```

ub-name INTEGER ::= 32768  
ub-common-name INTEGER ::= 64  
ub-locality-name INTEGER ::= 128  
ub-state-name INTEGER ::= 128  
ub-organization-name INTEGER ::= 64  
ub-organizational-unit-name INTEGER ::= 64  
ub-title INTEGER ::= 64  
ub-serial-number INTEGER ::= 64  
ub-match INTEGER ::= 128  
ub-emailaddress-length INTEGER ::= 128  
ub-common-name-length INTEGER ::= 64  
ub-country-name-alpha-length INTEGER ::= 2  
ub-country-name-numeric-length INTEGER ::= 3  
ub-domain-defined-attributes INTEGER ::= 4  
ub-domain-defined-attribute-type-length INTEGER ::= 8  
ub-domain-defined-attribute-value-length INTEGER ::= 128  
ub-domain-name-length INTEGER ::= 16  
ub-extension-attributes INTEGER ::= 256  
ub-e163-4-number-length INTEGER ::= 15  
ub-e163-4-sub-address-length INTEGER ::= 40  
ub-generation-qualifier-length INTEGER ::= 3  
ub-given-name-length INTEGER ::= 16  
ub-initials-length INTEGER ::= 5  
ub-integer-options INTEGER ::= 256  
ub-numeric-user-id-length INTEGER ::= 32  
ub-organization-name-length INTEGER ::= 64  
ub-organizational-unit-name-length INTEGER ::= 32  
ub-organizational-units INTEGER ::= 4  
ub-pds-name-length INTEGER ::= 16  
ub-pds-parameter-length INTEGER ::= 30  
ub-pds-physical-address-lines INTEGER ::= 6  
ub-postal-code-length INTEGER ::= 16

```
ub-pseudonym INTEGER ::= 128
ub-surname-length INTEGER ::= 40
ub-terminal-id-length INTEGER ::= 24
ub-unformatted-address-length INTEGER ::= 180
ub-x121-address-length INTEGER ::= 16
END

PKIX1Implicit88 { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-implicit(19) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN

id-ce OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 29}

id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 35 }

AuthorityKeyIdentifier ::= SEQUENCE {
    keyIdentifier [0] KeyIdentifier OPTIONAL,
    authorityCertIssuer [1] GeneralNames OPTIONAL,
    authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL
}

KeyIdentifier ::= OCTET STRING

id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 14 }

SubjectKeyIdentifier ::= KeyIdentifier

id-ce-keyUsage OBJECT IDENTIFIER ::= { id-ce 15 }

KeyUsage ::= BIT STRING {
    digitalSignature(0),
    nonRepudiation(1),
    keyEncipherment(2),
    dataEncipherment(3),
    keyAgreement(4),
    keyCertSign(5),
    cRLSign(6),
    encipherOnly(7),
    decipherOnly(8)
}

id-ce-privateKeyUsagePeriod OBJECT IDENTIFIER ::= { id-ce 16 }

PrivateKeyUsagePeriod ::= SEQUENCE {
    notBefore [0] GeneralizedTime OPTIONAL,
    notAfter [1] GeneralizedTime OPTIONAL
}

id-ce-certificatePolicies OBJECT IDENTIFIER ::= { id-ce 32 }

anyPolicy OBJECT IDENTIFIER ::= { id-ce-certificatePolicies 0 }

CertificatePolicies ::= SEQUENCE SIZE(1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
    policyIdentifier CertPolicyId,
    policyQualifiers SEQUENCE SIZE(1..MAX) OF PolicyQualifierInfo OPTIONAL
```

```
}

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
    policyQualifierId   PolicyQualifierId,
    qualifier          ANY policyQualifierId
}

PolicyQualifierId ::= OBJECT IDENTIFIER (id-qt-cps | id-qt-unotice)

CPSuri ::= IA5String

UserNotice ::= SEQUENCE {
    noticeRef        NoticeReference OPTIONAL,
    explicitText     DisplayText OPTIONAL
}

NoticeReference ::= SEQUENCE {
    organization     DisplayText,
    noticeNumbers   SEQUENCE OF INTEGER
}

DisplayText ::= CHOICE {
    ia5String        IA5String (SIZE(1..200)),
    visibleString    VisibleString (SIZE(1..200)),
    bmpString        BMPString (SIZE(1..200)),
    utf8String       UTF8String (SIZE(1..200))
}

id-ce-policyMappings OBJECT IDENTIFIER ::= { id-ce 33 }

PolicyMappings ::= SEQUENCE SIZE(1..MAX) OF SEQUENCE {
    issuerDomainPolicy   CertPolicyId,
    subjectDomainPolicy  CertPolicyId
}

id-ce-subjectAltName OBJECT IDENTIFIER ::= { id-ce 17 }

SubjectAltName ::= GeneralNames

GeneralNames ::= SEQUENCE SIZE(1..MAX) OF GeneralName

GeneralName ::= CHOICE {
    otherName      [0] AnotherName,
    rfc822Name    [1] IA5String,
    dNSName       [2] IA5String,
    x400Address   [3] ORAddress,
    directoryName [4] Name,
    ediPartyName  [5] EDIPartyName,
    uniformResourceIdentifier [6] IA5String,
    ipAddress     [7] OCTET STRING,
    registeredID  [8] OBJECT IDENTIFIER
}

AnotherName ::= SEQUENCE {
    type-id  OBJECT IDENTIFIER,
    value    [0] EXPLICIT ANY type-id
}

EDIPartyName ::= SEQUENCE {
    nameAssigner [0] DirectoryString OPTIONAL,
    partyName   [1] DirectoryString
}
```

```
id-ce-issuerAltName OBJECT IDENTIFIER ::= { id-ce 18 }

IssuerAltName ::= GeneralNames

id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::= { id-ce 9 }

SubjectDirectoryAttributes ::= SEQUENCE SIZE(1..MAX) OF Attribute

id-ce-basicConstraints OBJECT IDENTIFIER ::= { id-ce 19 }

BasicConstraints ::= SEQUENCE {
    cA          BOOLEAN DEFAULT FALSE,
    pathLenConstraint   INTEGER (0..MAX) OPTIONAL
}

id-ce-nameConstraints OBJECT IDENTIFIER ::= { id-ce 30 }

NameConstraints ::= SEQUENCE {
    permittedSubtrees [0] GeneralSubtrees OPTIONAL,
    excludedSubtrees [1] GeneralSubtrees OPTIONAL
}

GeneralSubtrees ::= SEQUENCE SIZE(1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
    base      GeneralName,
    minimum   [0] BaseDistance DEFAULT 0,
    maximum   [1] BaseDistance OPTIONAL
}

BaseDistance ::= INTEGER (0..MAX)

id-ce-policyConstraints OBJECT IDENTIFIER ::= { id-ce 36 }

PolicyConstraints ::= SEQUENCE {
    requireExplicitPolicy [0] SkipCerts OPTIONAL,
    inhibitPolicyMapping [1] SkipCerts OPTIONAL
}

SkipCerts ::= INTEGER (0..MAX)

id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::= { id-ce 31 }

CRLDistributionPoints ::= SEQUENCE SIZE(1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
    distributionPoint [0] DistributionPointName OPTIONAL,
    reasons [1] ReasonFlags OPTIONAL,
    cRLIssuer [2] GeneralNames OPTIONAL
}

DistributionPointName ::= CHOICE {
    fullName [0] GeneralNames,
    nameRelativeToCRLIssuer [1] RelativeDistinguishedName
}

ReasonFlags ::= BIT STRING {
    unused(0),
    keyCompromise(1),
    cACompromise(2),
    affiliationChanged(3),
    superseded(4),
    cessationOfOperation(5),
```

```
certificateHold(6),
privilegeWithdrawn(7),
aACompromise(8)
}

id-ce-extKeyUsage OBJECT IDENTIFIER ::= { id-ce 37 }

ExtKeyUsageSyntax ::= SEQUENCE SIZE(1..MAX) OF KeyPurposeId

KeyPurposeId ::= OBJECT IDENTIFIER

anyExtendedKeyUsage OBJECT IDENTIFIER ::= { id-ce-extKeyUsage 0 }

id-kp-serverAuth OBJECT IDENTIFIER ::= { id-kp 1 }

id-kp-clientAuth OBJECT IDENTIFIER ::= { id-kp 2 }

id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }

id-kp-emailProtection OBJECT IDENTIFIER ::= { id-kp 4 }

id-kp-timeStamping OBJECT IDENTIFIER ::= { id-kp 8 }

id-kp-OCSPSigning OBJECT IDENTIFIER ::= { id-kp 9 }

id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::= { id-ce 54 }

InhibitAnyPolicy ::= SkipCerts

id-ce-freshestCRL OBJECT IDENTIFIER ::= { id-ce 46 }

FreshestCRL ::= CRLDistributionPoints

id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }

AuthorityInfoAccessSyntax ::= SEQUENCE SIZE(1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE {
    accessMethod   OBJECT IDENTIFIER,
    accessLocation   GeneralName
}

id-pe-subjectInfoAccess OBJECT IDENTIFIER ::= { id-pe 11 }

SubjectInfoAccessSyntax ::= SEQUENCE SIZE(1..MAX) OF AccessDescription

id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }

CRLNumber ::= INTEGER (0..MAX)

id-ce-issuingDistributionPoint OBJECT IDENTIFIER ::= { id-ce 28 }

IssuingDistributionPoint ::= SEQUENCE {
    distributionPoint [0] DistributionPointName OPTIONAL,
    onlyContainsUserCerts [1] BOOLEAN DEFAULT FALSE,
    onlyContainsCACerts [2] BOOLEAN DEFAULT FALSE,
    onlySomeReasons [3] ReasonFlags OPTIONAL,
    indirectCRL [4] BOOLEAN DEFAULT FALSE,
    onlyContainsAttributeCerts [5] BOOLEAN DEFAULT FALSE
}

id-ce-deltaCRLIndicator OBJECT IDENTIFIER ::= { id-ce 27 }

BaseCRLNumber ::= CRLNumber
```

```
id-ce-cRLReasons OBJECT IDENTIFIER ::= { id-ce 21 }

CRLReason ::= ENUMERATED {
    unspecified(0),
    keyCompromise(1),
    cACompromise(2),
    affiliationChanged(3),
    superseded(4),
    cessationOfOperation(5),
    certificateHold(6),
    removeFromCRL(8),
    privilegeWithdrawn(9),
    aACompromise(10)
}

id-ce-certificateIssuer OBJECT IDENTIFIER ::= { id-ce 29 }

CertificateIssuer ::= GeneralNames

id-ce-holdInstructionCode OBJECT IDENTIFIER ::= { id-ce 23 }

HoldInstructionCode ::= OBJECT IDENTIFIER

holdInstruction OBJECT IDENTIFIER ::= {joint-iso-itut(2) member-body(2) us(840) x9cm(10040) 2}

id-holdinstruction-none OBJECT IDENTIFIER ::= {holdInstruction 1}

id-holdinstruction-callissuer OBJECT IDENTIFIER ::= {holdInstruction 2}

id-holdinstruction-reject OBJECT IDENTIFIER ::= {holdInstruction 3}

id-ce-invalidityDate OBJECT IDENTIFIER ::= { id-ce 24 }

InvalidityDate ::= GeneralizedTime

END
```

## Príloha B (informatívna) Zoznam použitej literatúry

Základná legislatíva Slovenskej republiky a EÚ pre elektronický podpis:

<http://www.nbu.gov.sk/urad/pravne-predpisy/doveryhodne-sluzby/index.html>

Štandardy NBÚ:

<http://www.nbu.gov.sk/doveryhodne-sluzby/standardy/index.html>

Zostavenie certifikačnej cesty a overenie platnosti certifikátov:

<http://www.nbu.gov.sk/doveryhodne-sluzby/dohlad/index.html>

## Príloha C História

Verzia	Dátum	Poznámka	Vypracoval
V 1.0	24.8.2005	Prvé vydanie	Ing. Peter Rybár, NBÚ RNDr. Július Šiška, PhD., KPMG
Verzia 1.1	6.11.2005	Jednotný formát NBÚ dokumentov	Ing. Peter Rybár, NBÚ
Verzia 2.0 7561/2016/IBEP/OA-001	19.12.2016	Zmena podľa <a href="#">zákona č. 272/2016 Z. z.</a>	Ing. Peter Rybár, NBÚ
Verzia 3.0 04323/2021/ SRD/OBPI-002	19.4.2021	Len podľa § 11 písm. m) <a href="#">zákona č. 272/2016 Z. z.</a>	Ing. Peter Rybár, NBÚ