NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verzia 3.0

Formáty zoznamu zrušených certifikátov a potvrdzovania stavu a platnosti certifikátov.

17.1.2010

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

Pri overovaní zaručených elektronických podpisov (ďalej len ZEP) je základným predpokladom správne overenie platnosti kvalifikovaného certifikátu a certifikátov na správu kvalifikovaných certifikátov (ďalej ako "certifikáty na správu", ktoré sú použité na overenie zaručeného elektronického podpisu). Aby bolo možné jednoznačne overiť stav certifikátu, je potrebné definovať jednoznačné pravidlá pre obsah údajov uvedených v CRL a OCSP. Podľa zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, najmä v znení zákona č. 214/2008 Z. z.:

- CA a ACA podľa § 14 ods. 1 písm. i) bod 4 zverejňuje zoznam zrušených certifikátov, podľa § 15 ods. 4 Certifikačná autorita poskytuje informácie o stave certifikátu poskytnutím zoznamu zrušených certifikátov (CRL) podľa § 8 obsahujúceho všetky certifikáty, ktorých platnosť bola predčasne zrušená, pričom certifikát, ktorého platnosť bola predčasne zrušená, musí byť minimálne jedenkrát uvedený v zozname podľa § 8 a podľa § 15 ods. 5. Ak má certifikačná autorita vytvorené technické podmienky, poskytuje informácie o stave certifikátu aj vo forme potvrdenia existencie a platnosti kvalifikovaného certifikátu (OCSP).
- Je povinnosťou akreditovanej certifikačnej autority (ďalej len ACA) pri poskytovaní akreditovaných certifikačných služieb podľa § 14 ods. 3 písm. e) zasielať úradu zoznamy vydaných kvalifikovaných certifikátov a zoznamy zrušených kvalifikovaných certifikátov; formát, spôsob a periodicitu zasielania týchto zoznamov ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.
- Úrad podľa § 10 bodu m) vedie zoznam všetkých vydaných kvalifikovaných certifikátov spolu s informáciami o ich platnosti zaslaných podľa § 14 ods. 3 písm. e) a poskytuje z neho informácie.

2 Predmet dokumentu

Úrad vydáva tento štandard podľa § 3 ods. 1, § 4 ods. 2 a § 8 ods. 7 vyhlášky č. 131/2009 Z. z. o formáte, obsahu a správe certifikátov a kvalifikovaných certifikátov a formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o certifikátoch a kvalifikovaných certifikátoch) a zákona č. 215/2002 Z. z. podľa § 10 ods. 2 písm. j). Štandard je vydaný pre účely zabezpečenia jednoznačného určenia stavu kvalifikovaných certifikátov a certifikátov na správu, ďalej na účely spracovania údajov zasielaných úradu a jednotného spôsobu poskytovania informácií zo získaných údajov úradom pre verejnosť. Dokument technicky špecifikuje požadované vlastnosti a množiny použitých protokolov, aby bolo možné vytvorenie jednotného prostredia pre poskytovanie požadovaných služieb pre verejnosť.

Potrebu dlhodobej overiteľnosti platnosti zaručených elektronických podpisov rieši zákon č. 214/2008 Z. z. novelou zákona o EP, ktorá požaduje od ACA zasielanie vydaných kvalifikovaných certifikátov a certifikátov na správu do úradu a od úradu požaduje dlhodobé poskytovanie informácií o platnosti týchto certifikátov. Dokument špecifikuje, akým spôsobom ACA zasiela tieto údaje úradu a akým spôsobom úrad tieto informácie poskytuje verejnosti.

Úrad poskytuje okrem ním vydaných certifikátov aj informácie o platnosti exspirovaných kvalifikovaných certifikátov a exspirovaných certifikátov na správu vydaných ním akreditovanými CA vo forme OCSP odpovede s možnými troma stavmi:

1. **platný**,
2. **neplatný** od času a dátumu a poprípade aj s uvedeným dôvodom neplatnosti, ak tento dôvod poskytla ACA,
3. **neznámy,** ak ACA neposkytla informácie o certifikáte úradu alebo certifikát vydaný ACA nie je exspirovaný.

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 zaručených elektronických podpisov

[10] ITU-T RECOMMENDATION X.509 (08/2005) | ISO/IEC 9594-8:2005

[11] ETSI TS 102 280 X.509 V.3 Cert. Profile for Cert. Issued to Natural Persons

[12] Common PKI COMMON PKI SPECIFICATIONS FOR INTEROPERABLE APPLICATIONS FROM T7 & TELETRUST

[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

[16] RFC 2560 X.509 PKI Online Certificate Status Protocol 6-1999

[17] ISO/IEC 7064 Data processing - Check character systems 2003

[18] RFC 3548 The Base16, Base32, and Base64 Data Encodings 7-2003

[19] ISO/IEC 3166 Codes for the representation of countries

[20] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[21] RFC 2822 Internet Message Format 4-2001

[22] RFC 2046 MIME Part Two- Media Types 11-1996

[23] RFC 3629 UTF-8, a transformation format of ISO 10646 11- 2003

[24] RFC 2585 Operational Protocols: FTP and HTTP 5- 1999

[25] Vyhláška NBÚ č. 131/2009 Z. z. o formáte, obsahu a správe certifikátov a kvalifikovaných certifikátov …

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

[27] NBÚ Formáty certifikátov a kvalifikovaných certifikátov

4 Definície a skratky

ACA	Akreditovaná certifikačná autorita
AdES	Advanced Electronic Signature
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
BASE64	Typ kódovanie obsahu v MIME
CA	Certification Authority
CBC	Cipher-block chaining
CMS	Cryptographic Message Syntax
CAdES	CMS Advanced Electronic Signature
CRL	Certificate Revocation List – zoznam zrušených certifikátov
DER	Distinguished Encoding Rules (for ASN.1)
ESS	Enhanced Security Services (enhances CMS)
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
ISO	International Organization for Standardization
Common PKI	COMMON PKI SPECIFICATIONS FOR INTEROPERABLE APPLICATIONS
MIME	Multipurpose Internet Mail Extensions
NBÚ	Národný bezpečnostný úrad
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKIX	Internet X.509 Public Key Infrastructure
SMTP	Simple Mail Transfer Protocol
TSP	Time Stamp Protocol
URL	Uniform Resource Locator
UTF-8	Transformation format of ISO 10646
Úrad	Národný bezpečnostný úrad
Zákon o EP	Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
ZEP	Zaručený elektronický podpis (Qualified Electronic Signature)

5 Formát CRL

Certifikačné autority akreditované na Slovensku musia podľa zákona o EP vydávať CRL, v ktorom uvádzajú stav vydaných kvalifikovaných certifikátov a certifikátov na správu. CRL musí obsahovať v správnom tvare minimálne položky, ktorých obsah tento profil upresňuje.

Tabuľka 1. Základný formát zoznamu zrušených kvalifikovaných certifikátov - CRL

	Zápis v ASN.1	Stručný popis
1.	`CertificateList ::= SEQUENCE {`	
2.	`tbsCertList TBSCertList,`	DER kódované údaje, podpísané CA.
3.	`signatureAlgorithm AlgorithmIdentifier,`	Identifikátor podpisového algoritmu a jeho parametre, ak podpisový algoritmus vyžaduje parametre. Algoritmus je použitý certifikačnou autoritou na podpísanie *tbsCertList*.
4.	`signatureValue BIT STRING }`	Podpis CRL.

Tabuľka 2. TBSCertList - podpísaný blok

	Zápis v ASN.1	Stručný popis
1.	`TBSCertList ::= SEQUENCE {`	
2.	`version Version OPTIONAL, -- if present, MUST be v2`	Verzia CRL musí byť v2 (hodnota 1), lebo CRL pre kvalifikované certifikáty musí obsahovať *crlExtensions* a môže obsahovať *crlEntryExtensions*.
3.	`signature AlgorithmIdentifier,`	Presne rovnaký obsah ako v tabuľke 1, riadok 3.
4.	`issuer Name,`	Meno vydavateľa CRL (CA). Požiadavky na meno *issuer* sú rovnaké ako v dokumente NBÚ „Formáty certifikátov a kvalifikovaných certifikátov“ tabuľka 2, riadok 5.
5.	`thisUpdate Time,`	Dátum a čas, kedy bolo CRL vydané. Formát je rovnaký ako v dokumente NBÚ „Formáty certifikátov a kvalifikovaných certifikátov“ tabuľka 2, riadok 6.
6.	`nextUpdate Time OPTIONAL,`	Dátum a čas ďalšieho vydania CRL. Každé CRL **musí obsahovať** túto položku. CRL môže byť vydané aj pred časom v *nextUpdate*, ale nesmie byť vydané po tomto čase. CA vydáva CRL s časom v *nextUpdate* rovnakým alebo väčším než je vo vydaných CRL. Formát je rovnaký ako v tabuľke 2, riadok 5.
7.	`revokedCertificates SEQUENCE OF SEQUENCE {`	Zoznam zrušených certifikátov. Táto položka je vynechaná, ak nie je zrušený žiadny certifikát.
8.	`userCertificate CertificateSerialNumber,`	Sériové číslo zrušeného certifikátu.
9.	`revocationDate Time,`	Dátum a čas zrušenia certifikátu. Formát je rovnaký ako v tabuľke 2, riadok 5.
10.	`crlEntryExtensions Extensions OPTIONAL --if present, MUST be v2 } OPTIONAL,`	Neprázdny zoznam rozšírení, ktoré presnejšie špecifikujú zrušenie certifikátu.
11.	`crlExtensions [0] EXPLICIT Extensions OPTIONAL -- if present, MUST be v2 }`	Neprázdny zoznam rozšírení CRL.

Tabuľka 3. Typy CRL podľa CA, ktorá zrušuje certifikáty

	Typ	Stručný popis
1.	Priame CRL "*direct*"	Priame CRL je také, pri ktorom položka *DName* vydavateľa CRL je zhodná s položkou *DName* vydavateľa zrušených certifikátov.
2.	Nepriame CRL "*indirect*"	Nepriame CRL je také, v ktorom *DName* vydavateľa CRL je iné ako *DName* vydavateľa zrušených certifikátov. Toto CRL obsahuje rozšírenie *issuingDistributionPoint* s položkou *indirectCRL* = TRUE. Certifikát môže odkazovať na nepriame CRL, ak obsahuje rozšírenie certifikátu *CRLDistributionPoints* s položkou *distributionPoint* obsahujúcou položku *cRLIssuer.* Položka *cRLIssuer* obsahuje *DName*, ktoré je rozdielne od mena *subject v* CA certifikáte, ktorý patrí certifikátu vydavateľa.

Certifikáty v podstrome NBÚ koreňového certifikátu musia obsahovať prvé rozšírenie certifikátu *CRLDistributionPoints* na priame CRL.

Vydávanie **nepriamych** CRL je **zakázané** kvôli nejednoznačnému vytvoreniu certifikačnej cesty na overenie podpisu CRL a možným podvodom (kedy falošná CA môže zmeniť stav platnosti certifikátu, ktorý vydala iná CA), okrem výnimky:

a. Povolené sú len nepriame CRL vydávané NBÚ alebo nepriame CRL overované certifikátom vydaným CA, ktorá vydala certifikáty, ktorých platnosť sa pomocou nepriameho CRL overuje.

b. Podobný problém nastáva aj pri OCSP odpovedi (RFC 2560), ktorá zvyčajne nie je priamo overovaná CA certifikátom na overenie vydaných certifikátov, ktoré OCSP overuje a tak aj pri vydávaní OCSP odpovedi platia rovnaké pravidlá ako pri vydávaní nepriamych CRL v bode 1.

Tabuľka 4. crlExtensions – rozšírenia CRL

	Rozšírenia CRL	OID a nutnosť položky v CRL	Stručný popis	Kritické
1.	`IssuerAltNames`	`{2 5 29 18}` `Iba ak ho obsahuje CA certifikát`	Alternatívne (technické) meno vydavateľa certifikátu: napríklad OtherName, e-mail, DNS meno, IP adresa, URI alebo iné.	Nemalo by byť
2.	`CRLNumber`	`{2 5 29 20}` `Musí byť v CRL`	Kladné sekvenčné číslo CRL, ktoré sa zväčšuje o jedna pri vydaní. Max. veľkosti 20 BYTE. $1 \leq \text{CRLNumber} \leq 2^{159}$	Nesmie
3.	`DeltaCRLIndicator`	`{2 5 29 27}` `Neodporúča sa`	Indikuje, že sa jedná o delta-CRL. Vydávanie delta-CRL sa neodporúča.	Musí
4.	`IssuingDistributionPoint`	`{2 5 29 28}` `Musí byť v CRL`	Určuje pre koho (User/CA), dôvod, či je indirectCRL, alebo akým spôsobom a odkiaľ je možné získať CRL. Musí obsahovať HTTP adresu a môže obsahovať LDAP, ale v tom prípade musí obsahovať aj internetovú adresu LDAP servera. Pre overenie platnosti	Musí

			kvalifikovaných certifikátov a certifikátov na správu musí CA vydávať jedno úplné nesegmentované CRL (obsahujúce všetky zrušené používateľské a CA certifikáty vydané CA).	
5.	AuthorityKeyIdentifier	{2 5 29 35} Musí byť v CRL	Identifikátor verejného kľúča *keyIdentifier* certifikačnej autority CA, ktorá vydala CRL. Odporúča sa vyplniť aj *authorityCertSerialNumber*.	Nesmie

Tabuľka 5. crlEntryExtensions – rozšírenia zrušených certifikátov v CRL

	Rozšírenia zoznamu certifikátov v CRL	**OID a nutnosť položky v CRL**	**Stručný popis**	**Kritické**
1.	ReasonCode	{2 5 29 21} Iba ak je známy dôvod.	Dôvod zrušenia certifikátu.	Nesmie
2.	HoldInstructionCode	{2 5 29 23} Nesmie sa používať.	Identifikátor, ktorý indikuje, prečo bol certifikát v stave *Hold*. (Len pri delta CRL. Delta nie sú povolené).	Nesmie
3.	InvalidityDate	{2 5 29 24} Môže sa nachádzať.	Indikuje čas, kedy došlo k podozreniu zo skompromitovania súkromného kľúča.	Nesmie
4.	CertificateIssuer	{2 5 29 29} Indirect CRL musí obsahovať. Direct CRL nesmie obsahovať.	Používa sa len pri nepriamych CRL na určenie mena vydavateľa zrušeného certifikátu, ak je meno vydavateľa iné, než je meno vydavateľa CRL. Hodnota *GeneralNames* musí obsahovať iba jedno *directoryName* zo *subject* DName certifikátu vydavateľa zrušeného certifikátu. Ak prvá položka *crlEntryExtensions* neobsahuje *CertificateIssuer*, tak vydavateľom zrušeného certifikátu je vydavateľ CRL, dokiaľ sa v postupnosti neobjaví položka s prvým *CertificateIssuer*, potom nasledujúce položky budú mať predchádzajúceho vydavateľa, dokiaľ sa v postupnosti neobjaví ďalšia položka s *CertificateIssuer*. Teda zoznam je utriedený podľa *CertificateIssuer* a v certifikátoch vydaných s rovnakým vydavateľom sa *CertificateIssuer* nachádza iba v prvom zázname zrušeného certifikátu.	Musí

6 Formát OCSP

Certifikačné autority akreditované na Slovensku môžu podľa zákona o EP vydávať OCSP, v ktorom uvádzajú stav vydaných kvalifikovaných certifikátov a certifikátov na správu. OCSP musí obsahovať minimálne položky, ktoré sú uvedené v tomto profile a ktorých obsah tento profil upresňuje.

6.1 Formát žiadosti o získanie stavu certifikátu

Tabuľka 6. OCSP žiadosť

	Zápis v ASN.1	Požiadavky rozširujúce RFC 2560
1.	`OCSPRequest ::= SEQUENCE {`	
2.	`tbsRequest TBSRequest,`	
3.	`optionalSignature [0] EXPLICIT Signature OPTIONAL }`	Položka `optionalSignature` nesmie byť požadovaná pre získanie OCSP odpovede.
4.	`TBSRequest ::= SEQUENCE {`	
5.	`Version [0] EXPLICIT Version DEFAULT v1,`	
6.	`requestorName [1] EXPLICIT GeneralName OPTIONAL,`	Položka `requestorName` nesmie byť požadovaná pre získanie OCSP odpovede.
7.	`requestList SEQUENCE OF Request,`	
8.	`requestExtensions [2] EXPLICIT Extensions OPTIONAL }`	
9.	`Signature ::= SEQUENCE { signatureAlgorithm AlgorithmIdentifier, signature BIT STRING, certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL}`	
10.	`Version ::= INTEGER { v1(0) }`	
11.	`Request ::= SEQUENCE {`	
12.	`reqCert CertID,`	
13.	`singleRequestExtensions [0] EXPLICIT Extensions OPTIONAL }`	
14.	`CertID ::= SEQUENCE {`	
15.	`hashAlgorithm AlgorithmIdentifier,`	Algoritmus musí byť len z množiny algoritmov, ktoré sú v danom období považované za bezpečné. Táto množina algoritmov je zverejnená vyhláškou a automaticky overiteľná pomocou podpisovej politiky zverejnenej úradom, platnej v období, kedy bola žiadosť zaslaná.
16.	`issuerNameHash OCTET STRING, -- Hash of Issuer's DN`	
17.	`issuerKeyHash OCTET STRING, -- Hash of Issuers public key`	
18.	`serialNumber CertificateSerialNumber}`	

Pre komunikáciu s úradom, OCSP žiadosť musí byť v DER kódovaní a zaslaná len cez HTTP a SMTP protokoly na adresu, ktorú zverejní úrad na internetovej stránke úradu. Formát a typ MIME pre OCSP žiadosť je uvedená v prílohe C v tabuľke 10 na riadku 6.

6.2 Formát OCSP odpovede

Tabuľka 7. OCSP odpoveď

	Zápis v ASN.1	Požiadavky rozširujúce RFC 2560

1.	`BasicOCSPResponse ::= SEQUENCE {`
	` tbsResponseData ResponseData,`
	` signatureAlgorithm AlgorithmIdentifier,`
	` signature BIT STRING,`	

2.	` certs [0] EXPLICIT SEQUENCE OF` ` Certificate OPTIONAL }`	Odpoveď musí obsahovať certifikát, ktorým je podpis OCSP overovaný.
3.	`ResponseData ::= SEQUENCE {`	
4.	` version [0] EXPLICIT Version DEFAULT v1,`	
5.	` responderID ResponderID,`	
6.	` producedAt GeneralizedTime,`	Čas a dátum podpísania OCSP odpovede.
7.	` responses SEQUENCE OF SingleResponse,`	
8.	` responseExtensions [1] EXPLICIT` ` Extensions OPTIONAL }`	

9.	`ResponderID ::= CHOICE {`
	` byName [1] Name,`
	` byKey [2] KeyHash }`
		V OCSP odpovedi sa musí uvádzať položka `byName`.

10.	`SingleResponse ::= SEQUENCE {`	
11.	` certID CertID,`	
12.	` certStatus CertStatus,`	
13.	` thisUpdate GeneralizedTime,`	Pri exspirovaných certifikátoch musí položka obsahovať čas a dátum, kedy certifikát exspiroval alebo väčšiu hodnotu, ale nesmie byť väčšia ako `thisUpdate` z posledného CRL, ktoré sériové číslo overovaného certifikátu mohlo obsahovať. Ak posledné CRL, ktoré môže obsahovať stav certifikátu, má hodnotu v `thisUpdate` menšiu ako je čas exspirovania overovaného certifikátu, `v OCSP-SingleResponse-thisUpdate musí byť hodnota CRL-thisUpdate`. OCSP poskytované úradom pre stav certifikátov vydaných akreditovanými CA musí vrátiť stav v `certStatus` **`unknown`**, ak certifikát ešte neexspiroval.
14.	` nextUpdate [0]EXPLICIT GeneralizedTime` ` OPTIONAL,`	Pri stave exspirovaného certifikátu nie je táto položka uvedená.
15.	` singleExtensions [1]EXPLICIT Extensions` ` OPTIONAL }`	Musí obsahovať [12] `CertHash` z certifikátu, ktorého stav obsahuje.

16.	`CertStatus ::= CHOICE {`
	`  good [0] IMPLICIT NULL,`
	`  revoked [1] IMPLICIT RevokedInfo,`
	`  unknown [2] IMPLICIT UnknownInfo }`	

17.	`RevokedInfo ::= SEQUENCE {`
	` revocationTime GeneralizedTime,`
	` revocationReason [0] EXPLICIT CRLReason`
	` OPTIONAL }`	

18.	`UnknownInfo ::= NULL` `--this can be replaced with an enumeration`	

CertHash (pozitívne prehlásenie) - rozšírenie definované pre typ SingleResponse v singleExtensions:

```
Definícia rozšírenia CertHash prebraná z Common PKI [12] Optional SigG-Profile:

Common PKI Object Identifiers
      id-commonpki OBJECT IDENTIFIER ::= {1 3 36 8 }
      id-commonpki-at OBJECT IDENTIFIER ::= {id-commonpki 3}
      id-commonpki-at-certHash OBJECT IDENTIFIER ::= {id-commonpki-at 13}

Common PKI PRIVATE EXTENSIONS
CertHash ::= SEQUENCE {
      hashAlgorithm AlgorithmIdentifier,
            -- The identifier of the algorithm that has been used the
            -- hash value below.
      certificateHash OCTET STRING
            -- The hash over DER-encoding of the entire PKC
      }     -- or AC (i.e. NOT a hash over tbsCertificate).
```

Odpoveď OCSP musí byť vo formáte BasicOCSPResponse v DER kódovaní a každá SingleResponse v singleExtensions musí obsahovať rozšírenie CertHash (pozitívne prehlásenie).

7 Formát a spôsob poskytovania údajov z ACA pre úrad

7.1 Formát poskytovaných kvalifikovaných certifikátov a certifikátov na správu

ACA vydáva kvalifikované certifikáty vo formáte X.509 [11] a pre verejnosť poskytuje informácie o platnosti vo forme CRL [11] a môže aj vo forme OCSP [8]. ACA musí podľa zákona č. 215/2002 Z. z. zasielať úradu zoznamy vydaných a zrušených kvalifikovaných certifikátov (§ 14 ods.3 písm.e), pričom úrad stanovuje formát, spôsob a periodicitu ich zasielania. Prijaté kvalifikované certifikáty úrad nesmie zverejňovať, ale len poskytovať informácie o ich platnosti. ACA zasiela vydané kvalifikované certifikáty úradu vo formáte *Certificate* v DER kódovaní.

Formát podľa X.509:

```
Certificate  ::=  SEQUENCE  {
        tbsCertificate       TBSCertificate,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }
```

ACA zasiela do 8 dní od vydania certifikátu zašifrované zoznamy vydaných kvalifikovaných certifikátov na elektronickú adresu úradu, ktorú úrad zverejňuje na svojej internetovej stránke pre tento účel. Pred odoslaním uloží ACA vydané kvalifikované certifikáty v DER kódovaní podľa ASN.1 pre X.509 do prílohy elektronickej pošty podľa MIME [21] v BASE64 kódovaní [18] a vytvorí tak `multipart/mixed` podpísanú S/MIME správu. Túto zašifruje verejným kľúčom z certifikátu úradu, ktorý je zverejnený na stránke úradu pre účely šifrovania zasielanej elektronickej pošty obsahujúcej kvalifikované certifikáty a certifikáty na správu. Šifrovaná správa bude vo formáte CMS [6] a na šifrovanie budú použité algoritmy AES 256bit v CBC móde. Šifrovaná správa sa zakóduje do MIME elektronickej pošty a odošle na elektronickú adresu úradu.

Úrad po prijatí elektronickej správy túto odšifruje a postupne overí integritu prijatých kvalifikovaných certifikátov a certifikátov na správu pomocou certifikátov vydaných úradom pre ACA. Platnosť certifikátov nebude úrad overovať.
Úrad na základe overenia integrity a obsahu zaslaných kvalifikovaných certifikátov a certifikátov na správu uloží do svojej databázy len kvalifikované certifikáty a certifikáty na správu, ktoré sú vydané akreditovanou certifikačnou autoritou v súlade so štandardom NBÚ o formáte certifikátov a kvalifikovaných certifikátov [27]. Iné typy certifikátov nebudú do databázy uložené.
Úrad na základe overenia podpisu a obsahu doručených certifikátov vytvorí **integritný podpis**, ktorý bude obsahovať všetky prijaté certifikáty a v položke NOTICE uvedie stav:

- OK - overený, zaradený do databázy NBÚ;
- NO - neoverený, nezaradený do databázy NBÚ – dôvod, napr. chybný formát, nepovolený algoritmus, nepovolená krátka dĺžka kľúča, nevydaný akreditovanou CA;
- DP – duplicitný, už zaradený do databázy NBÚ.

Úrad odošle integritný podpis elektronickou poštou do ACA ako potvrdenku o prijatí certifikátov. Ak ACA do 5 dní od odoslania zoznamu nedostane potvrdenie o prijatí, zopakuje odoslanie certifikátov a ak opätovne nezíska potvrdenie o prijatí od úradu elektronickou poštou, kontaktuje úrad cez podateľňu úradu.

7.2 Formát poskytovania zmeny platnosti certifikátov

ACA zasiela zoznamy zrušených kvalifikovaných certifikátov a certifikátov na správu na elektronickú adresu úradu, ktorú úrad zverejňuje na svojej internetovej stránke pre tento účel. Ak ACA zruší ňou vydané kvalifikované certifikáty alebo ňou vydané certifikáty na správu, potom je povinná úradu zaslať CRL, ktoré obsahuje toto zrušenie, do 8 dní od zverejnenia tejto zmeny, a to v prílohe elektronickej pošty. Správa elektronickej pošty obsahuje DER kódované CRL podľa ASN.1 definovaného v X.509 v prílohe podľa MIME [21] v BASE64 kódovaní [18] a vytvorí tak `multipart/mixed` podpísanú S/MIME správu.

Úrad odošle do ACA elektronickou poštou integritný podpis z prijatých CRL ako potvrdenku o prijatí CRL, ktorý bude obsahovať všetky prijaté CRL a v položke NOTICE uvedie stav overenia zoznamu:

- OK – overený, zaradený do databázy NBÚ;
- NO – neoverený, nezaradený do databázy NBÚ – dôvod napr. chybný formát, nepovolený algoritmus, nepovolená krátka dĺžka kľúča, nevydaný akreditovanou CA;
- DP – duplicitný, už zaradený do databázy NBÚ.

Ak ACA do 5 dní od odoslania zoznamu nedostane potvrdenie o prijatí, zopakuje odoslanie CRL a ak opätovne nezíska potvrdenie o prijatí od úradu elektronickou poštou, kontaktuje úrad cez podateľňu úradu.

Formát podľa X.509:

```
CertificateList  ::=  SEQUENCE  {
     tbsCertList          TBSCertList,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING
}
TBSCertList  ::=  SEQUENCE  {
     version  Version OPTIONAL,    -- if present, MUST be v2
     signature               AlgorithmIdentifier,
     issuer                  Name,
     thisUpdate              Time,
     nextUpdate              Time OPTIONAL,
     revokedCertificates     SEQUENCE OF SEQUENCE  {
          userCertificate         CertificateSerialNumber,
          revocationDate          Time,
          crlEntryExtensions      Extensions OPTIONAL
                                   -- if present, version MUST be v2
                             }  OPTIONAL,
     crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                   -- if present, version MUST be v2
}
```

8 Formát a spôsob poskytovania informácií o stave certifikátu úradom pre verejnosť pomocou OCSP

Úrad poskytuje informácie iba o platnosti exspirovaných certifikátov, ktoré boli vydané úradom akreditovanými CA, a to kvalifikovaných certifikátov a certifikátov na správu vo formáte X.509 [10]. Úrad poskytuje informácie vo formáte nepriameho OCSP [8] obsahujúceho Common PKI rozšírenie CertHash (Positive Statement) a môže ich poskytovať aj v nepriamom CRL [10].
Úrad uchováva nasledujúce informácie pre poskytovanie platnosti exspirovaného certifikátu:

- certifikáty a CRL podľa X.509 [10] chránené zreťazenými integritnými podpismi s časovou pečiatkou podpisu,
- čas a dátum zrušenia certifikátu vo formáte GeneralizedTime a CRL, ktoré informáciu o zrušení certifikátu obsahuje,
- dôvod zrušenia certifikátu v type CRLReason.

```
CRLReason ::= ENUMERATED {
        unspecified             (0),
        keyCompromise           (1),
        cACompromise            (2),
        affiliationChanged      (3),
        superseded              (4),
        cessationOfOperation    (5),
        certificateHold         (6),    -- value 7 is not used
        removeFromCRL           (8),
        privilegeWithdrawn      (9),
        aACompromise           (10) }
```

Úrad na základe týchto údajov poskytuje overovateľovi informáciu, či exspirované kvalifikované certifikáty alebo certifikáty na správu (ne)boli zrušené počas svojej platnosti. Žiadosť o poskytnutie informácie o platnosti certifikátu možno zasielať na e-mailovú adresu alebo na URL adresu zverejnenú na internetovej stránke úradu pre tieto účely.
Profil OCSP žiadosti a odpovede je uvedený v kapitole 6. Príklad MIME kódovania OCSP žiadosti a odpovede je uvedený v prílohe C. Formát žiadosti je definovaný v RFC 2560 v kapitole 4 článok 1 a odpoveď je definovaná v kapitole 4 článok 2, kde rozšírenie odpovede `SingleResponse` musí obsahovať Common PKI pozitívne prehlásenie certHash. Pozitívne prehlásenie certHash rozširuje OCSP odpoveď podľa RFC 2560 o stave certifikátu o hash hodnotu z certifikátu, ktorého stav odpoveď obsahuje, teda overovateľ si je istý, že OCSP pozná certifikát a aj jeho stav. Stav platnosti exspirovaného certifikátu je možné overiť pomocou OCSP odpovede, ktorej podpis je overovaný certifikačnou cestou. Prvý certifikát certifikačnej cesty je overovaný aktuálnym platným dôveryhodným koreňovým certifikátom a všetky použité algoritmy sú podľa aktuálne platnej podpisovej politiky považované za bezpečné. OCSP sa teda overuje k aktuálne platnému koreňovému certifikátu, aj keď stavy certifikátov, ktoré OCSP vracia, sú už dávno spolu s celou certifikačnou cestou exspirované. Rozšírenie *certHash* zabezpečuje pozitívnu odpoveď, že systém, ktorý vydáva OCSP odpoveď, pozná certifikát, ktorého stav vracia (bol vydaný a je v databáze).
OCSP žiadosť a OCSP odpoveď je poskytovaná vo forme prílohy e-mailovej správy a môže byť poskytnutá aj vo forme uvedenej podľa RFC 2560 v prílohe A.1 OCSP over HTTP (OCSP cez HTTP protokol). Pri e-mailovej správe je odpoveď uvedená v type BasicOCSPResponse podľa kapitoly 4 článok 2.1 z RFC 2560.

Príloha A (normatívna) Výsledný stav platnosti certifikátu

ITU-T X.509 (08/2005) | ISO/IEC 9594-8:2005, IETF RFC 5280 a IETF RFC 2560 definujú formáty certifikátov, CRL a OCSP a definujú pravidlá pre overenie platnosti certifikátov v čase použitia certifikátov, čo je využívané pri systémoch, ktoré neumožňujú čakanie a teda získanie skutočného stavu platnosti certifikátu. Tieto systémy akceptujú potenciálne riziko, že v čase, kedy sa použil súkromný kľúč k nemu priradený, certifikát bol už zrušený, ale táto informácia o zrušení nebola v čase použitia certifikátu a súkromného kľúča dostupná. Pri overovaní platnosti zaručených elektronických podpisov, ktoré prebieha k času v minulosti, kedy sa podpis zrealizoval, je takéto riziko s neistým stavom platnosti certifikátu neakceptovateľné. Z toho dôvodu sa pri overovaní kvalifikovaných certifikátov a certifikátov na správu musí použiť podmienka zabezpečujúca jednoznačný a nemenný stav overenia platnosti certifikátov.

A.1 Zistenie stavu platnosti certifikátu pomocou CRL

Podmienka pre overenie stavu platnosti certifikátu pomocou CRL vracia stav k času ControlTime. V prípade, že sa overuje platnosť exspirovaných certifikátov, CRL musí obsahovať rozšírenie *expiredCertsOnCRL* s hodnotou, ktorá je menšia, než je hodnota v overovanom certifikáte certificate.*notAfter*.

Tabuľka 8. Stav podľa CRL

1. **if** (certificate.*notBefore* **<** *CRL.thisUpdate*) **and**
   (((CRL.*expiredCertsOnCRL* **<=** certificate.*notAfter*) **and** (0 < CRL.*expiredCertsOnCRL*)) **or**
   ((*CRL.thisUpdate* **<=** certificate.*notAfter*) **and** (0 = CRL.*expiredCertsOnCRL*))) **then**
2. **if** certificate **is not in** *CRL* **then**
3. **if** (ControlTime **+** *cautionPeriod*) <= *CRL.thisUpdate* **then**
   VALID
4. **else**
   INCOMPLETE VERIFICATION: čakanie na nové CRL
5. **else**
   if ControlTime < *CRL*[certificate].*revocationDate* **then**
   VALID
6. **else**
   INVALID
7. **else**
   INCOMPLETE AUTOMATIC VERIFICATION: požiadavka na CA o CRL, ktoré môže obsahovať stav overovaného certifikátu.

Kde:

- Ak CRL.*expiredCertsOnCRL* nie je uvedené v rozšírení CRL, tak premenná má hodnotu 0, inak má hodnotu podľa definície v ITU-T X.509 (08/2005).
- *CRL.thisUpdate* je čas, pred ktorým a vrátane ktorého je informácia o stave certifikátu už stabilná a nemenná.
- Certificate.*notBefore* je čas, od kedy je možné certifikát použiť a jeho stav sa môže v CRL uvádzať.
- Certificate.*notAfter* je čas, po ktorom sa stav certifikátu v CRL už nemôže meniť, ale môže sa uvádzať.
- *CRL*[certificate].*revocationDate* je čas zrušenia certifikátu, ktorý je uvedený v CRL.

Vysvetlenia blokov podmienky:.

- CRL je vydané v čase, kedy môže obsahovať informácie o stave certifikátu.
- Sériové číslo certifikátu nie je v CRL, teda certifikát nie je zrušený.
- CRL bolo vydané po čase použitia kľúča v minulosti, kedy CRL už musí obsahovať informáciu o zrušení, ak k nej došlo.
- CRL nie je vydané v čase po použití kľúča, kedy CRL už musí obsahovať stabilnú informáciu o stave certifikátu.

- Certifikát bol zrušený po čase použitia kľúča, a teda certifikát je platný.
- Certifikát bol zrušený pred a vrátane času použitia kľúča, preto je certifikát neplatný.
- Je potrebné použiť také CRL, ktoré je vydané v čase, kedy CRL môže obsahovať informáciu o zrušení: v čase z periódy použiteľnosti certifikátu, alebo ak CRL obsahuje aj exspirované certifikáty, tak z periódy, v ktorej CRL môže obsahovať stav overovaného certifikátu.

A.2 Zistenie stavu platnosti certifikátu pomocou OCSP

Podmienka pre overenie stavu platnosti certifikátu pomocou OCSP odpovede vracia stav k času ControlTime. OCSP odpoveď musí byť vydaná :
- v intervale, v ktorom je certifikát použiteľný <certificate.*notBefore,* certificate.*notAfter*>,
- alebo v čase, v ktorom OCSP odpoveď môže obsahovať informáciu o platnosti exspirovaného certifikátu, ktorá je určená hodnotou *ArchiveCutoff* s hodnotu menšou, než je čas exspirovania overovaného certifikátu certificate.*notAfter,*
- alebo OCSP odpoveď pre exspirovaný certifikát obsahuje pozitívne prehlásenie *CertHash* v rozšírení OCSP odpovede s haš hodnotou overovaného certifikátu, čím sa potvrdzuje nielen vedomosť o stave, ale aj integrita certifikátu s aktuálne bezpečným haš algoritmom.

Tabuľka 9. Stav podľa OCSP odpovede

```
1.  if ( certificate.notBefore < OCSP[certificate].thisUpdate ) and
       ( (( OCSP.ArchiveCutoff <= certificate.notAfter ) and ( 0 < OCSP.ArchiveCutoff )) or
        (( OCSP[certificate].thisUpdate <= certificate.notAfter) and (0 = OCSP.ArchiveCutoff )) or
        (OCSP[certificate].CertHash = certificate.CertHash) ) then
2.          if OCSP[certificate].CertStatus = good then
3.                  if (ControlTime + cautionPeriod ) <= OCSP[certificate].thisUpdate then
                            VALID
4.                  else
                            INCOMPLETE VERIFICATION: je potrebné získanie novšej OCSP odpovede
5.          else
                    if OCSP[certificate].CertStatus = revoked then
                            if Control Time < OCSP[certificate].revocationTime then
                                    VALID
6.                          else
                                    INVALID
7.                  else
                            INCOMPLETE AUTOMATIC VERIFICATION: OCSP nepozná aktuálny stav
                            platnosti certifikátu, lebo OCSP[certificate].CertStatus = unknown
                            Overenie je možné pomocou iného OCSP alebo CRL.
8.  else
          INCOMPLETE AUTOMATIC VERIFICATION: požiadavka na CA o OCSP odpoveď alebo CRL, ktoré
          môže obsahovať stav overovaného certifikátu.
```

Kde:

- OCSP.ArchiveCutoff - ak ArchiveCutoff sa nenachádza v OCSP odpovedi, potom je hodnota 0, inak hodnota uložená v ArchiveCutoff je podľa RFC 2560.
- OCSP[certificate].*CertHash* je haš hodnota certifikátu, ktorého stav OCSP odpoveď vracia (Common PKI private extensions). Ak OCSP odpoveď obsahuje toto rozšírenie, tak stav certifikátu je pre OCSP známy a haš hodnota zabezpečuje integritu aktuálne bezpečným haš algoritmom.
- Certificate.*CertHash* je haš hodnota certifikátu, ktorého stav chceme overiť.
- OCSP.*producedAt* je čas vydania OCSP odpovede.
- *OCSP*[certificate].*thisUpdate* je čas, pred ktorým a vrátane ktorého je informácia o stave certifikátu už stabilná a nemenná. Hodnota musí byť menšia alebo rovná OCSP.*producedAt.*
- *OCSP*[certificate].*nextUpdate* je pomocný čas oznamujúci, kedy najneskôr bude dostupná novšia informácia o stave. OCSP odpoveď nesmie obsahovať položku *nextUpdate*, ak certifikát, ktorého stav vracia, je expirovaný.
- Certificate.*notBefore* je čas, od kedy je možné certifikát použiť a jeho stav sa môže v CRL(OCSP) uvádzať.

- Certificate.*notAfter* je čas, po ktorom sa stav certifikátu v CRL(OCSP) už nemôže meniť, ale môže sa uvádzať.
- OCSP[certificate].*revocationTime* je čas, kedy došlo k zrušeniu certifikátu.
- OCSP[certificate].*CertStatus* je status overovaného certifikátu s hodnotami: *good, revoked* a *unknown*.

Vysvetlenia blokov podmienky:

1) OCSP je vydané v čase, kedy môže obsahovať informácie o stave certifikátu.

- Sériové číslo certifikátu nie je v OCSP (CRL), teda certifikát nie je zrušený.
- OCSP bolo vydané po čase použitia kľúča v minulosti, kedy OCSP už musí obsahovať informáciu o zrušení, ak k nemu došlo.
- OCSP nie je vydané v čase po použití kľúča, kedy OCSP už musí obsahovať stabilnú informáciu o stave certifikátu.
- Certifikát bol zrušený po čase použitia kľúča, a teda certifikát je platný.
- Certifikát bol zrušený pred a vrátane času použitia kľúča, preto je certifikát neplatný.
- OCSP nieje schopné určiť stav platnosti certifikátu, preto je potrebné získať iné OCSP alebo CRL.
- Je potrebné použiť také CRL(OCSP), ktoré je vydané v čase, kedy CRL(OCSP) môže obsahovať informáciu o zrušení: v čase z periódy použiteľnosti certifikátu, alebo ak CRL(OCSP) obsahuje aj exspirované certifikáty, tak z periódy, v ktorej CRL(OCSP) môže obsahovať stav overovaného certifikátu.

A.3 Zistenie stavu certifikátu pomocou TSL vydávaného podľa rozhodnutia Komisie EÚ (2009/767/ES)

Na základe Rozhodnutia Komisie zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu [oznámené pod číslom K(2009) 7806] (Text s významom pre EHP) (2009/767/ES) a Korigenda k rozhodnutiu Komisie 2009/767/ES zo 16. októbra 2009, ktorým sa ustanovujú opatrenia na uľahčenie postupov elektronickými spôsobmi prostredníctvom „miest jednotného kontaktu“ podľa smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:SK:PDF úrad vydáva TSL vo forme podpísaného PDF a voliteľne podpísaného TSL vo formáte XML.

Úrad zverejňuje certifikát na podpísanie TSL vo formáte XML v Dôveryhodnom zozname (koreňových certifikátov a podpisových politík) na stránke úradu.

Overovateľ v zahraničí pri overovaní slovenských kvalifikovaných certifikátov a slovenských certifikátov na správu používa údaje uložené v Dôveryhodnom zozname na stránke úradu a dôveru odvádza od dôvery v koreňový certifikát NBÚ. Certifikát NBÚ bol zverejnený okrem stránky úradu aj v tlači (Verejná správa, číslo vydania 25-26/2009 a Hospodárske noviny zo dňa 19.11.2009), čo je tiež zverejnené na internetovej stránke úradu, aby sa zabezpečila dôveryhodná možnosť overenia koreňového certifikátu inou cestou než elektronickou. Ak nemá možnosť zistiť, ktorý koreňový certifikát je dôveryhodný, postupuje podľa pravidiel pre TSL, vydávané podľa rozhodnutia EK č. 2009/767/ES, definovaných vo vlastnej krajine.

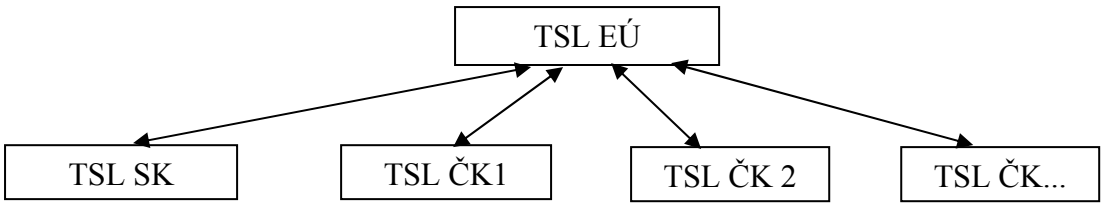
Overovateľ v SR pri overovaní zahraničných kvalifikovaných certifikátov alebo certifikátov na správu, overovanie začína overením dôvery v koreňový certifikát NBÚ, následne z Dôveryhodného zoznamu NBÚ získa certifikát na overenie podpísania slovenského TSL. Slovenský TSL je

zverejnený na internetovej stránke úradu a obsahuje URL odkaz na TSL EÚ. TSL EÚ obsahuje zoznam odkazov URL na národné TSL členských krajín. URL odkaz na TSL inej krajiny EÚ môže ukazovať na TSL vo formáte PDF alebo XML alebo TSL v podpísanej forme alebo URL na prístup k TSL cez zabezpečený kanál SSL/TLS a pri URL môže byť uvedený aj certifikát, ktorý overovateľ použije na overenie podpisu národného TSL alebo overenie vytvorenia bezpečného kanála SSL/TLS pre získanie národného TSL.

Spoliehajúca sa strana použije národné TSL na zistenie, či certifikát je kvalifikovaný, ak priamo v sebe tieto údaje neobsahuje, a či certifikát bol vydaný akreditovaným poskytovateľom certifikačných služieb alebo poskytovateľom, ktorý je pod dohľadom danej krajiny v čase vydania overovaného certifikátu (k času thisUpdate).

Pri overovaní pomocou TSL spoliehajúca sa strana postupuje nasledovne:

- Overovateľ, na základe údajov uvedených v elektronickom podpise, overí platnosť certifikátu podpisovateľa a certifikátov na správu podľa pravidiel pre overenie X.509 certifikátu profilovaných postupmi danej krajiny EÚ.
- Výsledkom overenia je informácia o tom, či certifikát podpisovateľa a certifikačná cesta a certifikáty na overenie časových pečiatok a iné certifikáty na správu, je platný alebo bol zrušený.
- Na základe certifikátu vydavateľa kvalifikovaného certifikátu alebo certifikátu na správu koncovej entity, overovateľ vyberie cez odkaz URL zo slovenského TSL odkaz na TSL EÚ, z ktorého získa odkaz na TSL inej členskej krajiny, v ktorej TSL obsahuje certifikát vydavateľa v položke *Service Digital Identity* alebo je certifikát vydavateľa zahrnutý v podstrome poskytovateľa certifikačných služieb, ak má poskytovateľ služby vo svojej internej hierarchii X.509.
- Na základe času vydania certifikátu podpisovateľa (thisUpdate) overovateľ overí, či vydavateľ certifikátu bol akreditovaný alebo pod dohľadom a na základe rozšírení uvedených v TSL overí, či sa jedná o kvalifikovaný certifikát podpisovateľa alebo kvalifikovaný certifikát podpisovateľa vydaný pre SSCD, ak túto informáciu certifikát podpisovateľa priamo v sebe neobsahuje.
- Ak v TSL v aktuálne platných službách podľa času vydania certifikátu podpisovateľa (thisUpdate) overovateľ nenájde požadovaného poskytovateľa certifikačných služieb, prehľadá históriu TSL a ak ani tam nenájde požadovaného poskytovateľa, ktorý bol k danému času thisUpdate akreditovaný alebo pod dohľadom, prehlási certifikát za certifikát, ktorý nespĺňa požiadavky pre kvalifikované certifikáty alebo certifikáty na správu vydávané na základe smernice o elektronickom podpise, inak sa certifikát považuje za kvalifikovaný alebo certifikát na správu.
- Nasleduje overenie, či v čase podpisu, napríklad k času z časovej pečiatky podpisu, bol stav platnosti certifikátu poskytnutý poskytovateľmi certifikačných služieb, ktorí boli k času *thisUpdate* poskytnutia CRL alebo OCSP akreditovaní alebo pod dohľadom.
- Overovateľ rovnako postupuje aj pri overovaní certifikátov časových pečiatok alebo certifikátov na podpísanie OCSP či CRL, teda pri overovaní certifikátov na správu, či boli vydané poskytovateľmi certifikačných služieb, ktorí boli v čase vydania daného certifikátu akreditovaní alebo pod dohľadom dozorného orgánu príslušného štátu EÚ.



Príloha B (informatívna) Príklady CRL

Poznámka: Použité údaje v príklade zoznamu zrušených kvalifikovaných certifikátov sú len informatívne a nie sú reálne dostupné.

```
SEQUENCE {
  SEQUENCE {
    INTEGER 1
    SEQUENCE {
      OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
      NULL
      }
    SEQUENCE {
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER countryName (2 5 4 6)
          PrintableString 'SK'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER localityName (2 5 4 7)
          UTF8String 'Bratislava'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER organizationName (2 5 4 10)
          UTF8String 'Narodny bezpecnostny urad'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER commonName (2 5 4 3)
          UTF8String 'CA NBU'
          }
        }
      }
    UTCTime 05/08/2010 12:58:57 GMT
    UTCTime 08/08/2010 20:14:39 GMT
    SEQUENCE {
      SEQUENCE {
        INTEGER 5061
        UTCTime 12/10/2009 20:01:17 GMT
        SEQUENCE {
          SEQUENCE {
            OBJECT IDENTIFIER cRLReason (2 5 29 21)
            OCTET STRING, encapsulates {
              ENUMERATED 5
              }
            }
          }
        }
      SEQUENCE {
        INTEGER 5101
        UTCTime 12/07/2005 13:02:00 GMT
        SEQUENCE {
          SEQUENCE {
            OBJECT IDENTIFIER cRLReason (2 5 29 21)
            OCTET STRING, encapsulates {
              ENUMERATED 1
```

```
            }
          }
        }
      }
    SEQUENCE {
      INTEGER 715
      UTCTime 13/07/2005 18:42:12 GMT
      }
    }
  [0] {
    SEQUENCE {
      SEQUENCE {
        OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
        OCTET STRING, encapsulates {
          SEQUENCE {
            [0]
              DF AF AD 80 AA 83 A1 2A 1D BB DF 5C 33 4A 1D 8E
              11 82 5E 71
            }
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER cRLNumber (2 5 29 20)
        OCTET STRING, encapsulates {
          INTEGER 81
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER issuingDistributionPoint (2 5 29 28)
        OCTET STRING, encapsulates {
          SEQUENCE {
            [0] {
              [0] {
                [6]
                ' http://ep.nbusr.sk/kca/RootCaNBU3.crl'
                }
              }
            }
          }
        }
      }
    }
SEQUENCE {
  OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
  NULL
  }
BIT STRING
  93 FA 85 6E 57 60 B8 E2 08 D0 E1 1B A3 A9 ED 51
  D6 99 66 C3 CD ED B7 6B 95 25 41 F3 EC 7C BB ED
  7C 35 8D 16 01 13 3C 7A 32 66 E5 7D B6 9D D6 D0
  4A 9A 39 53 29 11 40 F9 59 F5 1C 0F D1 CA BD 04
  2C 4B 97 54 35 21 0E D7 71 FA 93 F3 52 3E 59 A0
  9C 27 E7 6A E1 EF B8 20 4E 92 E7 F8 5F AD A3 80
  9F 98 A7 FC D0 54 05 27 F8 8F 4F C4 14 DE 35 6F
  47 42 F5 6D F6 49 DF 44 64 9E 07 6F 9B 50 7F 0C
          [ Another 128 bytes skipped ]
}
```

Príloha C (informatívna) Príklady zasielaných údajov v MIME

Údaje zasielané úradu musia obsahovať minimálne MIME atribúty a parametre typov uvedených v nasledujúcich príkladoch, ale môžu obsahovať aj MIME atribúty a parametre iných typov.

Tabuľka 10. Základné MIME typy pre e-mail a HTTP protokol

	Registrovaný MIME Content-Type	Stručný popis
1.	`message/rfc822`	Všeobecné označenie obálky MIME správy obsahujúcej nižšie špecifikované MIME typy.
2.	`multipart/mixed; boundary="oddeľovač-dokumentov"`	Definuje postupnosť podpísaných dokumentov, ktorých MIME kódovania oddeľuje oddeľovač uvedený v atribúte *boundary*.
3.	`text/plain; charset=UTF-8`	ASCII textový dokument v UTF-8 kódovaní.
4.	`application/pkix-cert`	DER kódovaný certifikát v base64 a koncovka súboru je ".cer"
5.	`application/pkix-crl`	DER kódované CRL v base64 a koncovka súboru je ".crl"
6.	`application/ocsp-reques`	DER kódovaný OCSPRequest v base64 a koncovka súboru je ".ORQ"
7.	`application/ocsp-response`	DER kódovaný BasicOCSPResponse v base64 a koncovka súboru je ".ORS"
8.	`application/pkcs7-mime`	Obsahuje DER kódovaný CMS v base64, ktorý obsahuje objekty typu EnvelopedData alebo SignedData. MIME hlavička musí obsahovať parameter smime-type=enveloped-data a koncovka súboru je ".p7m"
9.	`application/pkcs7-signature`	Obsahuje jeden DER kódovaný CMS objekt v base64, ktorý obsahuje objekty typu SignedData. Koncovka súboru application/pkcs7-signature je ".p7m" a ".p7s" pri externom podpise.

Tabuľka 11. Základné MIME typy kódovania

	MIME Content-Transfer-Encoding	Stručný popis
1.	`8bit`	Kódovanie znaku do 8 bitov.
2.	`base64`	Kódovanie dokumentu pomocou Base64.

C.1 Príklad formátu šifrovanej správy

```
MIME-Version: 1.0
Content-Type: application/pkcs7-mime;
       smime-type=enveloped-data;
       name="smime.p7m";
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename="smime.p7m"

MIKGHwYJKoZIhvcNAQcDoIKGEDCChgwCAQAxggFDMIIBPwIBADAnMBsxCzAJBgNVBAYTAlJVMQww
CgYDVQQDEwN3d3cCCF24n57g9O/YMA0GCSqGSIb3DQEBAQUABIIBAE5PWSZksLBHA7h2gS6xCLhq
n4ZwYP7WU9iKZIHJ846ZYmcy2gwPZY8geNatGFa+nQKJNGkPgmRfD90Nf0Sy4JPYNkuZDp+nMYLP
...
p4nP+cFreMIEAiFS9SwfwzUN/EX//cfQ6A==
```

C.2 Príklad formátu podpísanej správy

```
MIME-Version: 1.0
Content-Type: application/pkcs7-mime;
       smime-type=signed-data;
       name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename=smime.p7m

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB9HG4VQbnj7
...
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8HHGghyHh
6YT64V0GhIGfHfQbnj75
```

C.3 Príklad formátu zaslaných certifikátov v jednom multipart MIME kódovaní

```
Content-Type: multipart/mixed;
       boundary="----=_NextPart_000_"

This is a multi-part message in MIME format.

------=_NextPart_000_
Content-type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

Zasielame zoznam vydaných kvalifikovaných certifikátov
a certifikátov na správu kvalifikovaných certifikátov.

------=_NextPart_000_
Content-Type: application/pkix-cert
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename="cert1.cer"

e1xydGYxXGFuc2lcYW5zaWNwZzEyNTBcZGVmZjBcZGVmbGFuZzEwNTF7XGZvbnR0Ymx7XGYwXGZz
d2lzc1xmY2hhcnNldDIzOHtcKlxmbmFtZSBBcmlhbDt9QXJpYWwgQ0U7fXtcZjFcZm5pbFxmY2hh
...
YmVcJ2ZhXCdlOGEgXCc5ZVwnZWRcJzllbGlcJ2U4a3UgbVwnZTRzYSBuXCdmYVwnOWQgYSBtXCdm
ZGxcJ2U4aVwnZThrYSBrXCdmNFwnZjIgXGxhbmcxMDMzXGYxXHBhcg0KfQ0KAA==

------=_NextPart_000_
Content-Type: application/pkix-cert
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename="cert2.cer"

JVBERi0xLjQKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFIvRmlsdGVyIC9GbGF0ZURlY29k
ZT4+CnN0cmVhbQp4nIVSPU8DMQwVLZRyoEJL+doyJsOFON9ekRASG9VtlKmITkVq+f8STu+uOemQ
...
dCAxIDAgUiAvSW5mbyAyIDAgUgovSUQgWzw1QzIyNUI0RkIxQzU2RTVFMEUxOTAyQzgyNTdDOUI4
Nj48NUMyMjVCNEZCMUM1NkU1RTBFMTkwMkM4MjU3QzlCODY+XQo+PgpzdGFydHhyZWYKMTQ5MjIK
JSVFT0YK

------=_NextPart_000_--
```

C.4 Príklad formátu zaslaných CRL v jednom multipart MIME kódovaní

```
Content-Type: multipart/mixed;
       boundary="----=_NextPart_000_"

This is a multi-part message in MIME format.

------=_NextPart_000_
Content-type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

Zasielame zoznam CRL zrušených kvalifikovaných certifikátov
a certifikátov na správu kvalifikovaných certifikátov.
ACA

------=_NextPart_000_
Content-Type: application/pkix-crl
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename="crl1.crl"

e1xydGYxXGFuc2lcYW5zaWNwZzEyNTBcZGVmZjBcZGVmbGFuZzEwNTF7XGZvbnR0Ymx7XGYwXGZz
d2lzc1xmY2hhcnNldDIzOHtcK1xmbmFtZSBBcmlhbDt9QXJpYWwgQ0U7fXtcZjFcZm5pbFxmY2hh
...
NFx1YzFccGFyZFxmMFxmczIwXCdjOGlzdG8gdGVzdCBcJ2U4byBcJzlhXCdlOGlqIFwnOWRhIFwn
YmVcJ2ZhXCdlOGEgXCc5ZVwnZWRcJzllbGlcJ2U4a3UgbVwnZTRzYSBuXCdmYVwnOWQgYSBtXCdm
ZGxcJ2U4aVwnZThrYSBrXCdmNFwnZjIgXGxhbmcxMDMzXGYxXHBhcg0KfQ0KAA==

------=_NextPart_000_
Content-Type: application/pkix-crl
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename="crl2.crl"

JVBERi0xLjQKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFIvRmlsdGVyIC9GbGF0ZURlY29k
ZT4+CnN0cmVhbQp4nIVSPU8DMQwVLZRyoEJL+doyJsOFON9ekRASG9VtlKmITkVq+f8STu+uOemQ
...
dCAxIDAgUiAvSW5mbyAyIDAgUgovSUQgWzw1QzIyNUI0RkIxQzU2RTVFMEUxOTAyQzgyNTdDOUI4
Nj48NUMyMjVCNEZCMUM1NkU1RTBFMTkwMkM4MjU3QzlCODY+XQo+PgpzdGFydHhyZWYKMTQ5MjIK
JSVFT0YK

------=_NextPart_000_--
```

C.5 Príklad potvrdenia z úradu vo formáte integritného podpisu

```
MIME-Version: 1.0
Content-Type: multipart/signed;
      protocol="application/pkcs7-signature";
      micalg=SHA256;
      boundary="--=_NextPart16x10x2008at11x57x17x4CB5"

This is a multi-part message in MIME format.

----=_NextPart16x10x2008at11x57x17x4CB5
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

FILE=selesp.cer
```

```
HASH(SHA256:2 16 840 1 101 3 4 2 1)=
3ACF7A60B3F1219AE46E8E0F83D1B1C2C44249FD9578520EC19BDF6D39693B50
NOTICE=NO - Neoverený - nezaradený do databázy NBÚ
FILE=aca_disig.cer
HASH(SHA256:2 16 840 1 101 3 4 2 1)=
5872456739B61BFEB55D8715567A2E815FA09147AF0AC998685CA27B5B969547
NOTICE=OK - Overený - zaradený do databázy NBÚ
FILE=Korenova_CA_pre_kvalifikovane_certifikaty_1.cer
HASH(SHA256:2 16 840 1 101 3 4 2 1)=
6FBF021174831BE8B5889C9077F7BD6C385B5541B759E2F096D7D3BDBF774CDB
NOTICE=OK - Overený - zaradený do databázy NBÚ

----=_NextPart16x10x2008at11x57x17x4CB5
Content-Type: application/pkcs7-signature;
      name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="smime.p7s"

MIIFvgYJKoZIhvcNAQcCoIIFrzCCBasCAQExDzANBglghkgBZQMEAgEFADALBgkqhkiG9w0BBwGg
ggNsMIIDaDCCAlCgAwIBAgIIWzP7mMqijPwwDQYJKoZIhvcNAQEFBQAwGjELMAkGA1UEBhMCU0sx
CzAJBgNVBAMTAmphMB4XDTA4MDkxNTEwNDg0NloXDTA5MDkxNTEwNDg0NlowGjELMAkGA1UEBhMC
...
nWueKbh/pGtMXsotpc4OQrmdxtJEwB0ADY2pnWxgT/z3CoA4ZFO0nbrLpw3IzlWgEckXJAfG4VlX
V1XnLKS+c+itA2y8Z1gye2e1sMw0aSomyIsRUBM7TExP0jGb0rygCF3g6u3VpSlwSg==

----=_NextPart16x10x2008at11x57x17x4CB5--
```

C.6 Príklad formátu žiadosti o stav certifikátu

```
MIME-Version: 1.0
Content-Type: application/ocsp-reques;
       name="ocsp.orq";
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename="ocsp.orq"

MIKGHwYJKoZIhvcNAQcDoIKGEDCCChgwCAQAxggFDMIIBPwIBADAnMBsxCzAJBgNVBAYTAlJVMQww
CgYDVQQDEwN3d3cCCF24n57g9O/YMA0GCSqGSIb3DQEBAQUABIIBAE5PWSZksLBHA7h2gS6xCLhq
...
p4nP+cFreMIEAiFS9SwfwzUN/EX//cfQ6A==
```

C.7 Príklad formátu odpovede na žiadosť o stav certifikátu

```
MIME-Version: 1.0
Content-Type: application/ocsp-response;
       name="ocsp.ors";
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
       filename="ocsp.ors"

MIKGHwYJKoZIhvcNAQcDoIKGEDCCChgwCAQAxggFDMIIBPwIBADAnMBsxCzAJBgNVBAYTAlJVMQww
CgYDVQQDEwN3d3cCCF24n57g9O/YMA0GCSqGSIb3DQEBAQUABIIBAE5PWSZksLBHA7h2gS6xCLhq
n4ZwYP7WU9iKZIHJ846ZYmcy2gwPZY8geNatGFa+nQKJNGkPgmRfD90Nf0Sy4JPYNkuZDp+nMYLP
...
p4nP+cFreMIEAiFS9SwfwzUN/EX//cfQ6A==
```

Príloha D (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 PKI specification: "COMMON PKI SPECIFICATIONS FOR INTEROPERABLE APPLICATIONS FROM T7 & TELETRUST - SPECIFICATION PART 4:OPERATIONAL PROTOCOLS, http://www.common-pki.org/uploads/media/Common-PKI_v2.0.pdf"

- 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/

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

NOTE: Available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett

- 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 E História

Verzia:	Dátum vydania:	Poznámka:	Vypracoval:
V 1.0	30.9.2004	Prvé vydanie (zrušené)	Ing. Peter Rybár
V 1.1	14.8.2005	Druhé vydanie	Ing. Peter Rybár, NBÚ
V 1.2	6.11.2005	Jednotný formát NBÚ	Ing. Peter Rybár, NBÚ
V 3.0 Č.: 535/2009/IBEP/OEP-001	17.1.2010	Pridanie OCSP, zasielanie informácií pre NBÚ OCSP a implementácia TSL na základe rozhodnutia Komisie EÚ 2009/767/ES.	Ing. Peter Rybár, NBÚ