NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verzia 4.0

Formáty certifikátov a kvalifikovaných certifikátov

10.07.2014

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Sekcia informačnej bezpečnosti a elektronického podpisu

Budatínska č. 30, 850 07 Bratislava 57

http://www.nbusr.sk/

e-mail: podatelna@nbusr.sk

Obsah

1 Úvod

Pri overení zaručených elektronických pečatí a podpisov [1, 2, 6, 9, 10, 16, 18, 19] (ďalej len ZEP) je základným predpokladom správne overenie platnosti kvalifikovaného certifikátu [3, 4, 5, 11, 12, 13, 17, 22, 23]. Pre jednoznačné overenie kvalifikovaného certifikátu je potrebné definovať jednoznačné pravidlá pre obsah, identifikáciu a použitie kvalifikovaných certifikátov.

2 Predmet dokumentu

Štandard „Formáty certifikátov a kvalifikovaných certifikátov“ je vydaný na základe § 3 ods. 1 vyhlášky Národného bezpečnostného úradu 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) v znení neskorších predpisov (ďalej len „vyhláška NBÚ č. 131/2009 Z. z.“).

Účelom tohto dokumentu je stanovenie technických požiadaviek na jednotlivé typy kvalifikovaných certifikátov a certifikátov na správu, pre zabezpečenie kompatibility a jednotného prostredia elektronického podpisu v SR s ohľadom na prostredie elektronického podpisu najmä v krajinách EÚ.

Dokument definuje jednoznačný formát a obsah kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a certifikátu na správu, ďalej definuje spôsob identifikácie kvalifikovaných certifikátov podľa § 7 ods. 3 zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon“).

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 6960	X.509 PKI Online Certificate Status Protocol	6-2013
[9] NBÚ	Formáty zaručených elektronických pečatí a podpisov	
[10] ITU-T	RECOMMENDATION X.509 | ISO/IEC 9594-8	
[11] ETSI	TS 119 412-2 Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons	
[12] ETSI	TR 102 437 Guidance on TS 101 456	
[13] ETSI	EN 319 411-2 Policy and security requirements for TSP issuing certificates; Part 2: Policy requirements for CA issuing qualified certificates	
[14] ETSI	EN 319 411-3 Policy and security requirements for TSP issuing certificates; Part 3: Policy requirements for CA issuing public key certificates	
[15] ETSI	TS 119 612 Trusted Lists	
[16] ETSI	TS 101 903 XML Advanced Electronic Signatures (XAdES)	
[17] RFC 2560	X.509 PKI Online Certificate Status Protocol	6-1999

[18] 2014/148/EÚ VYKONÁVACIE ROZHODNUTIE KOMISIE zo 17. marca 2014, ktorým sa mení rozhodnutie 2011/130/EÚ, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu.

[19] ETSI	TS 102 778-3 Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles
[20] ISO/IEC	3166 Codes for the representation of countries
[21] RFC 3647	Internet X.509 PKI Certificate Policy and Certification Practices Framework

[22] 2013/662/EÚ VYKONÁVACIE ROZHODNUTIE KOMISIE zo 14. októbra 2013, ktorým sa mení rozhodnutie 2009/767/ES, pokiaľ ide o zostavovanie, vedenie a uverejňovanie zoznamov dôveryhodných informácií o poskytovateľoch certifikačných služieb, ktorí podliehajú dohľadu členského štátu alebo sú v ňom akreditovaní.

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

4 Skratky

ACA	Akreditovaná certifikačná autorita (Accredited Certification Authority)
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
CA	Certifikačná autorita (Certification Authority)
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
eIDAS	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
ESS	Enhanced Security Services (enhances CMS)
GMT	Greenwich Mean Time
HTTP	Hyper Text Transfer Protocol
ISO	International Organization for Standardization
ISIS - MTT	Industrial Signature Interoperability Standard - MailTrusT
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAdES	PDF Advanced Electronic Signature
PKCS	Public Key Cryptographic Standards, Standards published by RSA, Labs.
PKIX	Internet X.509 Public Key Infrastructure
QC	Qualified Certificate
QCP SK	Qualified Certificate Policy of Slovakia
SSCD	Secure-Signature-Creation Device
TSA	Time-Stamping Authorities
TSP	Time Stamp Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language
ZEP	Zaručený elektronický podpis alebo zaručená elektronická pečať (Qualified Electronic Signature or Qualified Electronic Seal)

5 Typ certifikátu a identita osoby v certifikáte

Na základe § 3 ods. 8 vyhlášky NBÚ č. 131/2009 Z. z. musí byť v kvalifikovaných certifikátoch a v certifikátoch na správu uvedený identifikátor certifikačného poriadku akreditovaných certifikačných služieb OID s hodnotou QCP SK '1 3 158 36061701 0 0 0 1 2 2'. Tento identifikátor musí byť uvedený v rozšírení certifikačnej politiky certifikátu a je aj identifikátorom certifikačnej politiky, ktorá sa smie uviesť len v kvalifikovaných certifikátoch a certifikátoch pre správu vydanými certifikačnými autoritami akreditovanými NBÚ. V certifikátoch koncového používateľa v rozšírení certifikačného poriadku, ktorého OID je '1 3 158 36061701 0 0 0 1 2 2', by mal byť uvedený v položke *userNotice-explicitText* (formát *utf8String*) text s informáciou o type certifikátu podľa slovenskej legislatívy uvádzaný v anglickom ako aj v slovenskom jazyku s úvodným textom „EN: “ a „SK: “, ktorý obsahuje najmä: "Certifikát je vydaný ako **kvalifikovaný** certifikát / kvalifikovaný **mandátny** certifikát / kvalifikovaný **systémový** certifikát / certifikát **na správu** podľa zákona č. 215/2002 Z. z. a vyhlášky NBÚ č. 131/2009 Z. z.". Obsah certifikačného poriadku je definovaný v prílohe č. 1 k vyhláške NBÚ č. 133/2009 Z. z. a odporúčanie pre obsah certifikačnej politiky je uvedené v RFC 3647.
Kvalifikovaný certifikát osoby spája identitu vlastníka súkromného kľúča s verejným kľúčom slúžiacim na overenie jeho pečatí alebo podpisov, pričom **všetky údaje obsiahnuté v kvalifikovanom certifikáte boli v čase jeho vydania poskytovateľom certifikačných služieb overené ako platné**. Tieto údaje sú uložené najmä v položkách mena subjektu *Certificate-tbsCertificate-subject-RelativeDistinguishedName*.

Obsah položky *commonName* je informatívny a pre overovateľa a podpisovateľa poskytuje stručnú informáciu o mene a prípadne type certifikátu. Položka *commonName* musí byť uvedená a musí sa nachádzať iba raz.

5.1 Typy kvalifikovaných certifikátov

Kvalifikovaný certifikát fyzickej osoby podľa § 3 ods. 4 vyhlášky NBÚ č. 131/2009 Z. z. musí obsahovať minimálne:

- krstné meno v *givenName*, priezvisko v *surname* alebo pseudonym v *pseudonym* a
- doplňujúci identifikátor zabezpečujúci jednoznačnosť identifikačných údajov držiteľa kvalifikovaného certifikátu v *serialNumber* vo forme „PNO“ (SK legislatíva) a môže obsahovať aj (legislatíva EÚ - eIDAS) „IDC“ a „PAS“.

Mandátny certifikát podľa § 3 ods. 5 vyhlášky NBÚ č. 131/2009 Z. z. musí obsahovať okrem položiek identifikujúcich mandatára v položkách podľa predchádzajúceho odseku aj:

- Identifikačné údaje osoby, za ktorú alebo v mene ktorej mandatár koná (ďalej len „mandant“), pričom v každej položke mandanta musí byť pred údajmi mandanta uvedený veľkými písmenami text „**MANDANT**“ (za úvodnými znakmi typu, napr. „PASSK-MANDANT“):
  - identifikačné údaje orgánu verejnej moci: meno v *organizationName* a minimálne v jednom *serialNumber* jeden identifikačný údaj typu „VAT“, „NTR“ alebo „SZ:“ alebo
  - identifikačné údaje osoby uvedené v položkách *givenName* krstné meno, *surname* priezvisko a minimálne v jednej položke *serialNumber* jeden údaj vo forme „PNO“, a môže obsahovať aj „IDC“ a „PAS“.
- Identifikačné údaje orgánu verejnej moci alebo osoby, u ktorej mandatár vykonáva činnosť podľa osobitného predpisu, alebo vykonáva funkciu podľa osobitného predpisu, sú uvedené v položke *organizationName* a minimálne v jednej položke *serialNumber* obsahujúcej jeden identifikačný údaj typu „VAT“, „NTR“ alebo „SZ:“ (podľa §7 ods. 3 písm. c) zákona).
- Označenie oprávnenia, podľa § 10a ods. 2 písm. a) v spojení s § 7 ods. 4 zákona, je uvedené ako posledné číslo OID (1.3.158.36061701.1.1.xyz) certifikačnej politiky v rozšírení certifikátu. V nepovinnej položke *userNotice-explicitText* ako *utf8String* je uvedených maximálne 200 znakov z oprávnenia zverejneného na webovom sídle NBÚ zo zoznamu oprávnení. V položke

userNotice-explicitText sa odporúča uviesť číslo a text oprávnenia v anglickom a slovenskom jazyku s úvodným textom „EN: “ a „SK: “. Manažment obsahu zoznamu oprávnení nie je predmetom tohto dokumentu a podrobnosti sa nachádzajú na webovom sídle NBÚ: http://www.nbusr.sk/sk/elektronicky-podpis/zoznam-opravneni.1.html V položke *cPSuri* je uvedený odkaz na „Pravidlá pre výkon certifikačných činností“ (CPS) obsahujúci informácie o postupoch pri overení oprávnenia identifikovaného pomocou OID podľa zoznamu dokladov, ktorými sa toto oprávnenie preukazuje a je uvedené v zozname oprávnení na webovom sídle NBÚ. ACA si môže pripraviť viacero dokumentov CPS, v ktorých bude uvedené, ako ACA postupuje pri vydaní certifikátu pre oprávnenie identifikované pomocou OID, pričom odkazuje na oprávnenia a požiadavky zverejnené v zozname NBÚ.

Kvalifikovaný systémový certifikát podľa § 3 ods. 6 vyhlášky NBÚ č. 131/2009 Z. z. musí obsahovať minimálne meno v položke *organizationName* a minimálne v jednej položke *serialNumber* jeden identifikačný údaj typu „VAT“, „NTR“ alebo „SZ:“. **Kvalifikovaný systémový certifikát nesmie obsahovať *givenName*, *surname* alebo *pseudonym*** (čím sa jednoznačne odlišuje od kvalifikovaných a mandátnych certifikátov vydaných fyzickej osobe).

Odkaz na identitu osoby v položke *serialNumber* musí byť uvedený vo formáte skladajúcom sa z **dvoch častí**, ktoré sú oddelené jednou medzerou (ASCII znak 0x20) alebo pomlčkou „-“ (ASCII znak 0x2D). Pomlčka „-“ namiesto znaku medzera sa musí uvádzať v položke *serialNumber* v certifikátoch vydaných minimálne od 1.9.2014, pričom v jednej položke *serialNumber* musí byť uvedený iba jeden odkaz na identitu osoby a kvalifikovaný certifikát musí obsahovať minimálne jednu položku *serialNumber* s odkazom na identitu osoby.

Prvá časť z položky *serialNumber* pozostáva z troch úvodných znakov určujúcich typ odkazu na identitu.
Tri úvodné znaky určujú typ odkazu na identitu:

1. „PAS“ pre identifikáciu na základe čísla pasu,
2. „IDC“ pre identifikáciu na základe čísla identifikačnej karty,
3. „PNO“ pre identifikáciu na základe osobného čísla, čo je rodné číslo u občanov SR alebo u cudzincov, ktorí majú pridelené rodné číslo podľa zákona č. 301/1995 Z. z. o rodnom čísle,
4. „SZ:“ pre identifikáciu na základe súboru znakov pridelených podľa § 27 ods. 4 zákona č. 540/2001 Z. z. o štátnej štatistike v znení zákona č. 55/2010 Z. z.,
5. „VAT“ pre identifikáciu na základe daňového identifikačného čísla,
6. „NTR“ pre identifikáciu na základe identifikačného čísla organizácie.

Nasledujúce dva znaky obsahujú kód krajiny podľa ISO 3166 (pre Slovensko „SK“), ktorá údaje uvedené v druhej časti vydala a poskytuje ich na základe legislatívnych požiadaviek definovaných vo svojej krajine.

Druhá časť z položky *serialNumber* pozostáva z údajov, ktorých typ určujú prvé tri úvodné znaky.

Príklady obsahu *serialNumber*: "PASSK-P3000180", "IDCSK-SP989783", "SZ:SK-MANDANT 123123" alebo "SZ:SK-123123".

Pri „PNO“ sa použije rodné číslo podľa § 5 ods. 2 zákona, ktoré bude pozostávať z číslic v desiatkovej sústave, bez uvedenia lomky medzi prvou a druhou časťou rodného čísla. Rodné číslo bude teda 10-miestne alebo 9-miestne (pri rodných číslach pridelených do 31.12.1953) podľa zákona č. 301/1995 Z. z. o rodnom čísle: príklad *serialNumber*: "PNOSK-9959199999" , "PNOSK-535919999", "PNOSK-MANDANT 535919999").

5.2 Odporúčania

Odporúčame akreditovaným poskytovateľom certifikačných služieb pri vydávaní kvalifikovaného certifikátu v súlade s legislatívou SR uvádzať minimálne jeden z vyššie uvedených odkazov na identitu osoby aj v prípade, že certifikát nebude použitý v komunikácii s orgánmi verejnej moci.

Každý kvalifikovaný certifikát fyzickej osoby by mal obsahovať aj **číslo identifikačného dokladu** alebo **pasu** použitého pri registračnom procese vydávania certifikátu (odporúčanie s ohľadom na prípravu sekundárnej legislatívy k Nariadeniu Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES).
Príklad čísla občianskeho preukazu:
IDCSK-P6553199999 - serialNumber(2.5.4.5)

Údaje v certifikáte by mali obsahovať len tie údaje, ktoré sú potrebné. Napríklad uvádzanie adresy trvalého bydliska by malo byť voliteľné.

V prípade ak SSCD alebo aplikácia na tvorbu podpisu/pečate obsahuje, alebo bude obsahovať viacero certifikátov rovnakého typu alebo iných typov certifikátov, používateľ sa môže rozhodnúť, ktorý použije na základe textu v položke *commonName*. Položka *commonName* je informatívna a mala by začínať nasledujúcou menovkou:
Menovku v tvare ZZZX, kde ZZZ sú 3 veľké písmená a X je rozlišovacie číslo, ak je na zariadení viacero rovnakých certifikátov, ako napríklad následný certifikát.

ZZZ nadobúda minimálne nasledovné hodnoty:

- pre kvalifikovaný „QES“ (Qualified Electronic Signature, Qualified Electronic Seal),
- pre šifrovací „ENC“ (encryption) a
- pre autentizačný „AUT“ (authentication).

Príklady:
QES J. C. Cruellas - *commonName*(2.5.4.3)
QES2 J. C. Cruellas - *commonName*(2.5.4.3)
ENC J. C. Cruellas - *commonName*(2.5.4.3)
AUT J. C. Cruellas - *commonName*(2.5.4.3)

Mandátny certifikát môže obsahovať menovku "MANDATÁR" nasledovanú skráteným menom mandatára a "OPRÁVNENIE" nasledované číslom oprávnenia a prípadne skráteným textom oprávnenia zo zoznamu oprávnení zverejnených na stránke úradu.
Príklad:
MANDATÁR J. C. Cruellas OPRÁVNENIE 346 Zákonný zástupca - commonName(2.5.4.3)

6 Formáty kvalifikovaných certifikátov a certifikátov na správu

Tabuľka 1. Základný formát kvalifikovaného certifikátu X.509

	Zápis v ASN.1	Stručný popis
1.	`Certificate ::= SEQUENCE {`	
2.	`tbsCertificate TBSCertificate,`	Údaje certifikátu podpísané v CA.
3.	`signatureAlgorithm AlgorithmIdentifier,`	Identifikátor podpisového algoritmu a parametre algoritmu, ak ich algoritmus vyžaduje. Algoritmus je použitý certifikačnou autoritou na podpísanie *tbsCertificate*.
4.	`signature BIT STRING }`	Podpis certifikátu.

Tabuľka 2. TBSCertificate

	Zápis v ASN.1	Stručný popis
1.	`TBSCertificate ::= SEQUENCE {`	
2.	`version [0] EXPLICIT Version DEFAULT v1,`	Verzia certifikátu musí byť v3 (hodnota 2).
3.	`serialNumber CertificateSerialNumber,`	Kladné sériové číslo certifikátu max. veľkosti 20 Byte. $1 \leq \text{serialNumber} < 2^{159}$
4.	`signature AlgorithmIdentifier,`	Presne rovnaký obsah ako v tabuľke 1 riadok 3.
5.	`issuer Name,`	Meno vydavateľa certifikátu (CA). *Issuer* spolu so *serialNumber* (riadok 3) musia **jednoznačne** identifikovať vydaný certifikát. Meno vydavateľa musí vždy obsahovať *countryName*, kde CA sídli, meno *organizationName.* V certifikátoch vydaných pre nový kľúčový pár vydavateľa najneskôr od 1.9.2014 musí byť aspoň v jedenej položke *serialNumber* jeden údaj typu „VAT“, „NTR“, „SZ:“, „PAS“, „PNO“ alebo„IDC“. Meno sa má skladať hlavne z atribútov *countryName*, *organizationName*, *organizationalUnitName*, *distinguishedNameQualifier*, *stateOrProvinceName*, *commonName*, *serialNumber* a *domainComponent*. Môže sa skladať aj z ďalších atribútov *localityName*, *title*, *surname*, *givenName*, *initials*, *pseudonym* a *generationQualifier*. Text v položkách *DirectoryString* je neprázdny a musí sa použiť *UTF8String* kódovanie.
6.	`validity Validity,`	Doba použiteľnosti certifikátu (od, do). Formát je v *UTCTime* a od roku 2050 musí byť *GeneralizedTime* (YYYYMMDDhhmmssZ). Formát musí obsahovať sekundy a je v časovom pásme Zulu (Universal Coordinated Time).
7.	`subject Name,`	Meno držiteľa certifikátu (DN pre koho je certifikát vydaný) musí byť v CA jednoznačné počas celej doby existencie CA. Rovnaké meno sa môže použiť aj v iných certifikátoch vydaných pre rovnakú osobu, ale nesmie sa

	Zápis v ASN.1	Stručný popis
		použiť v certifikátoch vydaných pre inú osobu. Odkaz na identitu osoby vlastníka súkromného kľúča, pre ktorého bol certifikát vydaný, sa nachádza v položke *serialNumber* a formát je definovaný v časti 5**.** *Name* musí obsahovať: *countryName, serialNumber, commonName,* pre fyzickú osobu *(surname a givenName)* alebo *pseudonym*, ak nie je pre fyzickú osobu *organizationName. Name* obsahuje hlavne položky: *countryName, commonName, surname, givenName, pseudonym, serialNumber, organizationName, organizational-UnitName, stateOrProvincename, localityName* a *title.* Ak je zadaný *pseudonym* v *Name*, potom *surname* a *givenName* nesmie byť zadané, a ak sa v *commonName* uvedie pseudonym, tak v položke musí byť doplnené slovo PSEUDONYM za alebo pred zadaným pseudonymom. V *Name* sa nemá používať *rfc822Name*, ale treba použiť atribút z rozšírenia certifikátu *subjectAltNames.* Text v položkách *DirectoryString* je neprázdny a musí sa použiť *UTF8String* kódovanie.
8.	`subjectPublicKeyInfo SubjectPublicKeyInfo,`	Verejný kľúč držiteľa certifikátu v DER kódovaní a identifikátor algoritmu, pre ktorý je tento kľúč určený.
9.	`issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,`	Nepoužíva sa.
10.	`subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,`	Nepoužíva sa.
11.	`extensions [3] EXPLICIT Extensions OPTIONAL }`	Rozšírenia certifikátu.

Tabuľka 3. Name

	Zápis v ASN.1	Stručný popis
1.	`Name ::= CHOICE { RDNSequence }`	Popis skladby poľa *Name*.
2.	`RDNSequence ::= SEQUENCE OF RelativeDistinguishedName`	
3.	`RelativeDistinguishedName ::= SET OF AttributeTypeAndValue`	
4.	`AttributeTypeAndValue ::= SEQUENCE { type AttributeType, value AttributeValue }`	
5.	`AttributeType ::= OBJECT IDENTIFIER`	
6.	`AttributeValue ::= ANY DEFINED BY AttributeType`	

Tabuľka 4. DirectoryString na ukladanie textu

	Zápis v ASN.1	Stručný popis
1.	`DirectoryString ::= CHOICE {`	Musí sa používať *UTF8String*.
2.	`teletexString TeletexString (SIZE (1..MAX)),`	

	Zápis v ASN.1	Stručný popis
3.	printableString PrintableString (SIZE (1..MAX)),	Je možné použiť v prípade, ak je potrebná spätná kompatibilita a reťazec je možné reprezentovať pomocou *PrintableString* kódovania v znakovej sade bez straty informácie (bez diakritiky), inak sa musí použiť *UTF8String* kódovanie textu.
4.	universalString UniversalString (SIZE (1..MAX)),	
5.	utf8String UTF8String (SIZE (1..MAX)),	Povinný formát, okrem výnimky uvedenej v riadku 3.
6.	bmpString BMPString (SIZE (1..MAX)) }	

Tabuľka 5. X.501 atribúty používané napr. v Name

	Meno	Oid	ASN.1 typ	Max veľkosť
1.	commonName	{id-at 3}	DirectoryString	64
2.	surName	{id-at 4}	DirectoryString	64
3.	givenName	{id-at 42}	DirectoryString	64
4.	serialNumber	{id-at 5}	PrintableString	64
5.	title	{id-at 12}	DirectoryString	64
6.	organizationName	{id-at 10}	DirectoryString	64
7.	organizationalUnitName	{id-at 11}	DirectoryString	64
8.	businessCategory	{id-at 15}	DirectoryString	128
9.	streetAddress	{id-at 9}	DirectoryString	128
10.	postalCode	{id-at 17}	DirectoryString	40
11.	localityName	{id-at 7}	DirectoryString	128
12.	stateOrProvinceName	{id-at 8}	DirectoryString	128
13.	countryName	{id-at 6}	PrintableString (SIZE(2))	2 ISO 3166 kód
14.	distinguishedNameQualifier	{id-at 46}	PrintableString	64
15.	initials	{id-at 43}	DirectoryString	64
16.	generationQualifier	{id-at 44}	DirectoryString	64
17.	emailAddress	{pkcs-9 1}	IA5String	128
18.	domainComponent	{0 9 2342 19200300100 1 25}	IA5String	Popis v [RFC2247]
19.	postalAddress	{id-at 16}	SEQUENCE SIZE(1..6) OF DirectoryString	6 x 30 v [RFC3739] 1. Ulica Číslo 2. Smerové číslo Lokalita 3. Štát
20.	pseudonym	{id-at 65}	DirectoryString	64
21.	dateOfBirth	{id-pda 1}	GeneralizedTime	YYYYMMDD000000Z
22.	placeOfBirth	{id-pda 2}	DirectoryString	128
23.	gender	{id-pda 3}	PrintableString (SIZE(1))	„M“ „F“
24.	countryOfCitizenship	{id-pda 4}	PrintableString (SIZE(2))	2 ISO 3166 kód
25.	countryOfResidence	{id-pda 5}	PrintableString (SIZE(2))	2 ISO 3166 kód
26.	nameAtBirth	{id-isismtt-at 14}	DirectoryString	64
27.	telephoneNumber	{id-at 20}	PrintableString (SIZE(32))	32 ITU-T Rec. E.123 "+44 582 10101"

Tabuľka 6. GeneralName

	Zápis v ASN.1	Stručný popis
1.	GeneralName ::= CHOICE {	

	Zápis v ASN.1	Stručný popis
2.	otherName [0] IMPLICIT OtherName,	Pre identifikáciu údajov iného typu, než sú použité nižšie.
3.	rfc822Name [1] IMPLICIT IA5String,	E-mail adresa podľa formátu "addr-spec" [RFC2822] bez „< >“ v tvare "local-part@domain".
4.	dNSName [2] IMPLICIT IA5String,	Internet domain name špecifikované v [RFC1034].
5.	x400Address [3] IMPLICIT ORAddress,	(nepoužíva sa) X400 adresa špecifikovaná v ITU-T X.411.
6.	directoryName [4] EXPLICIT Name,	X500 meno.
7.	ediPartyName [5] IMPLICIT EDIPartyName,	(nepoužíva sa) Meno z Electronic Data Exchange systému.
8.	uniformResourceIdentifier[6] IMPLICIT IA5String,	URI špecifikované v [RFC1630] obsahuje Uniform Resource Names (URNs) a tiež URLs. (http:// ...). Povolené URL formáty sú špecifikované v [RFC1738] a [RFC2255].
9.	iPAddress [7] IMPLICIT OCTET STRING,	IP adresa v IPv4 [RFC791] alebo IPv6 [RFC2460] formáte.
10.	registeredID [8] IMPLICIT OBJECT IDENTIFIER }	(nepoužíva sa) Registrovaný OBJECT IDENTIFIER (identifikujúci napríklad organizáciu).
11.	OtherName ::= SEQUENCE { type-id OBJECT IDENTIFIER, value [0] EXPLICIT ANY DEFINED BY type-id }	Uvedené vyššie.
12.	EDIPartyName ::= SEQUENCE { nameAssigner [0] EXPLICIT DirectoryString OPTIONAL, partyName [1] EXPLICIT DirectoryString }	Uvedené vyššie.

Tabuľka 7. Extension - rozšírenia certifikátu

	Zápis v ASN.1	Stručný popis
1.	Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension	Neprázdny zoznam rozšírení certifikátu.
2.	Extension ::= SEQUENCE {	
3.	extnID OBJECT IDENTIFIER,	OID špecifikujúci typ rozširujúcej informácie.
4.	critical BOOLEAN DEFAULT FALSE,	Ak je TRUE, rozšírenie je kritické a aplikácia musí vedieť informáciu spracovať, inak zamietne certifikát.
5.	extnValue OCTET STRING }	DER kódovaná hodnota rozširujúcej informácie.

Tabuľka 8. Rozšírenia certifikátu

	X.509 Základné rozšírenia	OID	Stručný popis	Kritické
1.	AuthorityKeyIdentifier	{2 5 29 35}	Identifikátor verejného kľúča certifikačnej autority, ktorá vydala tento certifikát.	nesmie
2.	SubjectKeyIdentifier	{2 5 29 14}	Identifikátor verejného kľúča držiteľa certifikátu.	nesmie

	X.509 Základné rozšírenia	OID	Stručný popis	Kritické
3.	KeyUsage	{2 5 29 15}	Definuje účel súkromného kľúča, ktorého verejný kľúč je súčasťou tohto certifikátu.	musí
4.	PrivateKeyUsagePeriod	{2 5 29 16}	Umožňuje určiť inú dobu použiteľnosti súkromného kľúča, než je použiteľnosť certifikátu.	nesmie
5.	CertificatePolicies	{2 5 29 32}	Identifikuje certifikačné politiky, pod ktorými bol certifikát vydaný. Kvalifikované certifikáty a certifikáty pre správu vydané úradom akreditovanými ACA musia obsahovať aj OID *QCP SK* (1 3 158 36061701 0 0 0 1 2 2).	môže, nemusí
6.	PolicyMappings	{2 5 29 33}	Potvrdzuje, že vydávajúca CA považuje svoju politiku za ekvivalentnú politike CA, pre ktorú je certifikát vydaný.	nesmie
7.	SubjectAltNames	{2 5 29 17}	Alternatívne (technické) meno držiteľa certifikátu: napríklad OtherName, e-mail, DNS meno, IP adresa, URI ...	nemalo by byť
8.	IssuerAltNames	{2 5 29 18}	Alternatívne (technické) meno vydavateľa certifikátu: napríklad OtherName, e-mail, DNS meno, IP adresa, URI alebo iné.	nemalo by byť
9.	SubjectDirectoryAttributes	{2 5 29 9}	Rozšírenie obsahuje detailnejšie X.500 atribúty držiteľa certifikátu.	nesmie
10.	BasicConstraints	{2 5 29 19}	Identifikuje CA certifikát. Pri CA certifikáte môže obmedziť certifikačnú cestu. Napríklad **nula** znamená, že CA vydáva len používateľské certifikáty.	musí pri CA certifikáte
11.	NameConstraints	{2 5 29 30}	CA určuje rozsah zmien v menách certifikátov, ktoré sa musia overiť vo všetkých menách subjektu (alebo alternatívne mená) v nasledujúcich certifikátoch v certifikačnej ceste.	musí
12.	PolicyConstraints	{2 5 29 36}	Môže byť použitý v CA certifikátoch na obmedzenie overovania certifikačnej cesty.	musí
13.	ExtendedKeyUsage	{2 5 29 37}	Označuje presnejšie účel, na ktorý je možné verejný kľúč v certifikáte použiť. Overuje sa nezávisle na *KeyUsage*	môže, nemusí, ale pri TSP

	X.509 Základné rozšírenia	OID	Stručný popis	Kritické
			rozšírení certifikátu.	certifikáte musí byť
14.	CRLDistributionPoints	{2 5 29 31}	Určuje, akým spôsobom a odkiaľ je možné získať CRL.	nemalo by byť
15.	AuthorityInfoAccess	{1 3 6 1 5 5 7 1 1}	Určuje (http:// … p7c, cer alebo aj ldap://...) adresu na získanie certifikátov vydaných pre vydavateľa tohto certifikátu a adresu na OCSP.	nesmie
16.	SubjectInfoAccess	{1 3 6 1 5 5 7 1 11}	Služby, ktoré poskytuje subjekt. Určuje (http:// … p7c, cer alebo aj ldap://...) adresu na získanie CA certifikátov vydaných subjektom tohto certifikátu a adresu na získanie časovej pečiatky.	nesmie
	RFC3739 QC rozšírenia			
17.	BiometricInfo	{1 3 6 1 5 5 7 1 2}	Obsahuje referencie na biometrické informácie za účelom preukázania / potvrdenia pravosti. Napríklad adresu na obrázok držiteľa certifikátu a haš (digitálny odtlačok) z obrázku.	nesmie
18.	QCStatements	{1 3 6 1 5 5 7 1 3}	Prehlásenie o tom, že certifikát je kvalifikovaný v súlade s konkrétnym technickým štandardom a obsahuje obmedzenia použitia kvalifikovaného certifikátu.	nemalo by byť

Tabuľka 9. Rozšírenia certifikátu koncovej entity

	Rozšírenie	Výskyt	Obsah hodnôt
1.	AuthorityKeyIdentifier	musí byť	Musí byť rovnaký, ako je v *subjectKeyIdentifier* vydavateľa certifikátu. *AuthorityKeyIdentifier.keyIdentifier* = *SubjectKeyIdentifier* a ak by mohlo dôjsť k nejednoznačnému vytvoreniu cesty, tak musí obsahovať aj authorityCertIssuer a authorityCertSerialNumber.
2.	*SubjectKeyIdentifier*	musí byť	Odporúča sa 20 byte haš SHA1 z *BIT STRING subjectPublicKeyInfo* (bez *tag, length* a nepoužitých bitov) (počítaný z generovaného verejného kľúča a slúži ako pomocný index (nejednoznačný – programu korektne pracuje aj ak nastane kolízia SHA-1))
3.	*KeyUsage*	musí byť	a) Používateľský: Pri kvalifikovaných certifikátoch musí byť iba *nonRepudiation* bit, a ak je certifikát určený aj pre iné účely (napríklad na overenie integrity alebo pre správu), tak sa môže nastaviť aj *digitalSignature* bit. Pre správu:

	Rozšírenie	Výskyt	Obsah hodnôt
			b) CRL: Ak je certifikát vydaný na podpisovanie nepriamych (*indirect*) CRL, tak potom obsahuje iba *crlSign* bit. c) OCSP: Ak je certifikát vydaný na podpisovanie OCSP, tak potom obsahuje iba *nonRepudiation* bit a v rozšírení *ExtendedKeyUsage* musí obsahovať iba *id-kp-OCSPSigning.* d) TSP: Ak je certifikát vydaný na podpisovanie TSP, tak potom obsahuje iba *nonRepudiation* bit a v rozšírení *ExtendedKeyUsage* musí obsahovať iba *id-kp-timeStamping.* V týchto prípadoch je kvôli jednoznačnosti BIT STRING DER kódovanie reprezentované ako jeden samostatný oktet (lebo *decipherOnly* nie je nastavené).
4.	*PrivateKeyUsagePeriod*	je voliteľné	Podľa RFC 5280.
5.	*CertificatePolicies*	musí byť	Pre koncového používateľa kvalifikovaného certifikátu určuje aj účel, na ktorý je certifikát vydaný, a ak obsahuje *UserNotice*, tak potom pri používaní certifikátu ho aplikácia musí vedieť zobraziť. Certifikáty pre správu a kvalifikované certifikáty vydané úradom akreditovanou ACA musia obsahovať minimálne certifikačnú politiku *QCP SK* (1 3 158 36061701 0 0 0 1 2 2). Ak dokumenty CPS a CP sú v PDF, mali by byť zabezpečené podľa ETSI TS 102 778-3 Part 3 [19].
6.	*PolicyMappings*	nesmie byť	Podľa RFC 5280.
7.	*SubjectAltNames*	je voliteľné	Podľa RFC 5280.
8.	*IssuerAltNames*	je voliteľné	Podľa RFC 5280.
9.	*SubjectDirectory-Attributes*	je voliteľné	Kvalifikované certifikáty MÔŽU v tomto rozšírení obsahovať štátom vydané identifikačné údaje (overené napríklad podľa občianskeho preukazu, pasu, ...) a údaje, ktoré sa nenachádzajú v položke *Subject*. Napríklad: *dateOfBirth, placeOfBirth,gender, countryOfCitizenship, countryOfResidence* definované v RFC 3739 a *nameAtBirth*.
10.	*BasicConstraints*	je voliteľné	Podľa RFC 5280.
11.	*NameConstraints*	nesmie byť	Podľa RFC 5280.
12.	*PolicyConstraints*	nesmie byť	Podľa RFC 5280.
13.	*ExtendedKeyUsage*	je voliteľné	Podľa RFC 5280. Pri TSP certifikáte musí obsahovať iba *id-kp-timeStamping.* Pri OCSP certifikáte musí obsahovať iba *id-kp-OCSPSigning.*
14.	*CRLDistributionPoints*	musí byť	Musí obsahovať HTTP adresu a môže obsahovať LDAP, ale v tom prípade musí obsahovať aj „host“ adresu LDAP servera aspoň v jednej LDAP adrese. Pre priame CRL “*direct*” a nepriame CRL “*indirect*” je vyplnenie položiek definované v NBÚ dokumente „Formáty zoznamu zrušených kvalifikovaných certifikátov“. V certifikátoch v NBÚ root podstrome musí byť zadané ako prvé priame CRL “*direct*” na vydavateľa certifikátu, a potom môže byť zadané nepriame CRL “*indirect*” na NBÚ certifikát, ktorý vydáva CRL pre certifikáty vydané akreditovanými CA.
15.	*AuthorityInfoAccess*	musí byť	Ak pri overovaní podpisu, podpis neobsahuje úplnú cestu, pre vytvorenie certifikačných ciest sú potrebné

	Rozšírenie	Výskyt	Obsah hodnôt
		(pri *self signed root* certifikátoch nemusí byť)	CA certifikáty na overenie podpisu certifikátu, uložené na HTTP adrese v „.p7c“ súbore alebo „.cer“. Súbor „.p7c“ je prázdny CMS podpis, ktorý obsahuje zoznam certifikátov, ktoré je možné použiť na overenie tohto certifikátu. Adresa na CA certifikáty musí obsahovať HTTP adresu a môže obsahovať LDAP, ale v tom prípade musí obsahovať aj internetovú adresu LDAP servera aspoň v jednej LDAP adrese. Môže obsahovať aj HTTP adresu na OCSP (on-line overovanie stavu certifikátu).
16.	*subjectInfoAccess*	je voliteľné	Informácie o subjekte. Zatiaľ má využitie iba pri CA certifikátoch.
17.	*BiometricInfo*	je voliteľné	Podľa RFC 3739.

18.	*QCStatements*	musí byť	Podľa RFC 3739 a hlavne podľa ETSI TS 101 862 je jednoznačná identifikácia typu kvalifikovaného certifikátu koncového používateľa pre vytváranie ZEP (Qualified Electronic Signatures) pomocou OID v *QCStatements.*
			
			Kvalifikovaný certifikát **musí** obsahovať OID identifikátor *id-etsi-qcs-QcCompliance,* a **ak** kvalifikovaný certifikát **obsahuje** certifikačnú politiku OID *QCP SK* (1 3 158 36061701 0 0 0 1 2 2), mal by obsahovať aj *id-etsi-qcs-QcSSCD.* OID *id-etsi-qcs-QcSSCD* je povinne vyžadovaný od 1.7.2010 dokiaľ ho nenahradí nový OID podľa nariadenia eIDAS, ktoré zruší smernicu o elektronickom podpise. Certifikát pre pečať môže obsahovať OID *id-etsi-qcs-QcSSCD.* Kvalifikovaný certifikát môže obsahovať obmedzenie výšky transakcie *etsi-qcs-QcLimitValue,* pre ktorú môže byť certifikát použitý.
			
			Význam OID identifikátorov:
			• *esi4-qcStatement-1(id-etsi-qcs-QcCompliance)* certifikát je kvalifikovaný
			• *esi4-qcStatement-4(id-etsi-qcs-QcSSCD)* kvalifikovaný certifikát obsahuje verejný kľúč patriaci k súkromnému kľúču uloženému v bezpečnom zariadení SSCD, pričom súkromný kľúč nie je možné z bezpečného zariadenia exportovať a je pod výhradnou kontrolou osoby, ktorej bol kvalifikovaný certifikát vydaný
			• *esi4-qcStatement-2 (etsi-qcs-QcLimitValue*) obmedzenie výšky transakcie
			`Príklad: SEQUENCE {`
			`PrintableString 'EUR'`
			`-- 978,` ISO 4217 Currency Code
			`INTEGER 1 --` amount
			`INTEGER 2 --` exponent `}`
			-- value = amount * 10^exponent

Príloha A (informatívna) Príklady kvalifikovaných certifikátov

A.1 Príklad užívateľského kvalifikovaného certifikátu

```
  0 1596: SEQUENCE {
  4 1316:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2    -- version
         :       }
 13    2:     INTEGER 3088   -- serialNumber
 17   13:     SEQUENCE {     -- signature
 19    9:       OBJECT IDENTIFIER
         :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 30    0:       NULL
         :       }
 32   83:     SEQUENCE {     -- issuer
 34   11:       SET {
 36    9:         SEQUENCE {
 38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43    2:           PrintableString 'EU'
         :           }
         :         }
 47   22:       SET {
 49   20:         SEQUENCE {
 51    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
 56   13:           UTF8String 'Test locality'
         :           }
         :         }
 71   26:       SET {
 73   24:         SEQUENCE {
 75    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 80   25:           UTF8String 'Narodny bezpecnostny urad'
         :           }
         :         }
 99   16:       SET {
101   14:         SEQUENCE {
103    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
108    7:           UTF8String 'Test CA'
         :           }
         :         }
258   21:       SET {
260   19:         SEQUENCE {
262    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
                              -- organisation unique identification data
267   14:           PrintableString 'NTRSK-36061701'
         :           }
         :         }
         :       }
117   30:     SEQUENCE {
119   13:       UTCTime 21/11/2006 15:21:16 GMT -- notBefore
134   13:       UTCTime 21/11/2007 15:21:16 GMT -- notAfter
         :       }
149  129:     SEQUENCE {     -- subject
152   11:       SET {
154    9:         SEQUENCE {
156    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
161    2:           PrintableString 'EU'
         :           }
         :         }
165   22:       SET {
167   20:         SEQUENCE {
```

```
169    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
174   13:           UTF8String 'Test locality'
        :           }
        :         }
189   20:       SET {
191   18:         SEQUENCE {
193    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
198   15:           UTF8String 'QES Peter Rybar'
        :           }
        :         }
211   14:       SET {
213   12:         SEQUENCE {
215    3:           OBJECT IDENTIFIER surname (2 5 4 4)
220    5:           UTF8String 'Rybar'
        :           }
        :         }
227   14:       SET {
229   12:         SEQUENCE {
231    3:           OBJECT IDENTIFIER givenName (2 5 4 42)
236    5:           UTF8String 'Peter'
        :           }
        :         }
243   13:       SET {
245   11:         SEQUENCE {
247    3:           OBJECT IDENTIFIER title (2 5 4 12)
252    4:           UTF8String 'Ing.'
        :           }
        :         }
258   21:       SET {
260   19:         SEQUENCE {
262    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
                              -- Personal unique identification data
267   16:           PrintableString 'PNOSK-1234567889'
        :           }
        :         }
        :       }
281  290:     SEQUENCE {     -- subjectPublicKeyInfo
285   13:       SEQUENCE {
287    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
298    0:         NULL
        :         }
300  271:       BIT STRING, encapsulates {
305  266:         SEQUENCE {
309  257:           INTEGER
        :             00 8A 32 3D 82 25 5D 31 DB CD 59 8B A2 8C 82 56
        :             0D F5 DE 0F 5A 3F 83 4F 88 41 62 7E 27 56 A6 88
        :             D8 8F CB D8 07 65 EE 32 3C C3 E8 46 15 3C F6 00
        :             C8 A8 67 43 1E CD 1D BF 32 DB 2B EC 33 BC 63 2D
        :             50 4E 1C 76 66 E7 88 C5 68 58 87 ED E1 DF 46 26
        :             BC 21 76 BF 91 33 54 0F BE 45 82 92 8D 41 31 1D
        :             A8 83 8E F1 EB 57 2A 5F 53 DA F9 FE 3A 28 CD FE
        :             25 CE E3 FA BD 0D 0E 9E DA 06 C6 93 CC 0D CF FF
        :                       [ Another 129 bytes skipped ]
570    3:           INTEGER 65537
        :           }
        :         }
        :       }
575  745:     [3] {          -- extensions
579  741:       SEQUENCE {
583   31:         SEQUENCE {
585    3:           OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
590   24:           OCTET STRING, encapsulates {
592   22:             SEQUENCE {
594   20:               [0]
```

```
        :                 38 B3 D9 00 A5 F6 81 B9 4B 0D 9B 2A DB 4D 65 67
        :                 B1 A5 1B CC
        :               }
        :             }
        :           }
 616   29:         SEQUENCE {
 618    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
 623   22:           OCTET STRING, encapsulates {
 625   20:             OCTET STRING
        :               38 94 23 FE 2B 7E 2C C8 5B 1E E3 D4 19 87 C6 54
        :               6A 93 BC B0
        :             }
        :           }
 647   14:         SEQUENCE {
 649    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
 654    1:           BOOLEAN TRUE   -- critical
 657    4:           OCTET STRING, encapsulates {
 659    2:             BIT STRING 6 unused bits
        :               '10'B (bit 1)   -- nonRepudiation
        :             }
        :           }
 663   36:         SEQUENCE {
 665    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 670   29:           OCTET STRING, encapsulates {
 672   27:             SEQUENCE {
 674    8:               SEQUENCE {      -- QCP public + SSCD
 676    6:                 OBJECT IDENTIFIER '0 4 0 1456 1 1'
        :                 }
 684   15:               SEQUENCE {      -- QCP SK
 686   13:                 OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
        :                 }
        :               }
        :             }
        :           }
 701    9:         SEQUENCE {
 703    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
 708    2:           OCTET STRING, encapsulates {
 710    0:             SEQUENCE {} -- end entity certificate
        :             }
        :           }
 712  265:         SEQUENCE {
 716    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
 721  256:           OCTET STRING, encapsulates {
 725  253:             SEQUENCE {
 728   40:               SEQUENCE {
 730   38:                 [0] {
 732   36:                   [0] {
 734   34:                     [6] 'http://qes.test.eu/test/testca.crl'
        :                     }
        :                   }
        :                 }
 770  109:               SEQUENCE {
 772  107:                 [0] {
 774  105:                   [0] {
 776  103:                     [6]
        :                     'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
        :                     'n,l=Test locality,c=EU?certificateRevocationList'
        :                     ';binary'
        :                     }
        :                   }
        :                 }
 881   98:               SEQUENCE {
 883   96:                 [0] {
 885   94:                   [0] {
```

```
 887   92:                     [6]
         :                   'ldap:///cn=Test CA,o=Test organization,l=Test lo'
         :                   'cality,c=EU?certificateRevocationList;binary'
         :                     }
         :                   }
         :                 }
         :               }
         :             }
         :           }
 981  303:         SEQUENCE {
 985    8:           OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
 995  289:           OCTET STRING, encapsulates {
 999  285:             SEQUENCE {
1003   36:               SEQUENCE {
1005    8:                 OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
1015   24:                 [6] 'http://ocsp.test.eu/ocsp'
         :                 }
                          -- certificate and cross-certificates
1041   46:               SEQUENCE {
1043    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1053   34:                 [6] 'http://qes.test.eu/test/testca.p7c'
         :                 }
1089  103:               SEQUENCE {
1091    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1101   91:                 [6]
         :                   'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
         :                   'n,l=Test locality,c=EU?caCertificate;binary'
         :                 }
1194   92:               SEQUENCE {
1196    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1206   80:                 [6]
         :                   'ldap:///cn=Test CA,o=Test organization,l=Test lo'
         :                   'cality,c=EU?caCertificate;binary'
         :                 }
         :               }
         :             }
         :           }
1288   34:         SEQUENCE {
1290    8:           OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
1300   22:           OCTET STRING, encapsulates {
1302   20:             SEQUENCE {
1304    8:               SEQUENCE {      -- etsi-qcs-QcCompliance
1306    6:                 OBJECT IDENTIFIER '0 4 0 1862 1 1'
         :                 }
1314    8:               SEQUENCE {      -- etsi-qcs-QcSSCD
1316    6:                 OBJECT IDENTIFIER '0 4 0 1862 1 4'
         :                 }
         :               }
         :             }
         :           }
         :         }
         :       }
         :     }
1324   13:   SEQUENCE {       -- signatureAlgorithm
1326    9:     OBJECT IDENTIFIER
         :       sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1337    0:     NULL
         :     }
1339  257:   BIT STRING       -- signatureValue
         :     A3 64 00 CC E5 ED 4A 20 5E D4 AD D9 E3 49 76 53
         :     3E 22 8D EB 5E B2 D3 53 B6 FB F2 58 21 4A 66 8C
         :     41 BC 6A D2 58 AC 1D 6A 09 F2 0C 1A 52 8E 67 15
         :     6B F0 4F AB 98 A9 C8 85 A4 19 1F 17 06 2D F1 45
         :     93 FC 7A 97 D3 1D 75 F3 3E E0 DA 5C 3D 50 02 4C
```

```
        :     68 7B AD 3B DB 92 6B 62 DC 65 64 50 98 F8 6B 55
        :     25 4B EC D6 6C 49 8E 7A 0A B8 C2 8E 2E 43 1D 52
        :     3F 37 A8 CC C6 FE D0 03 FC 55 87 A4 65 82 68 8E
        :             [ Another 128 bytes skipped ]
        :   }
```

A.2 Príklad mandátneho kvalifikovaného certifikátu

```
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER 2  -- version
      }
    INTEGER 30882      -- serialNumber
    SEQUENCE {   -- signature
      OBJECT IDENTIFIER
        sha256WithRSAEncryption (1 2 840 113549 1 1 11)
      NULL
      }
    SEQUENCE {   -- issuer
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER countryName (2 5 4 6)
          PrintableString 'EU'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER localityName (2 5 4 7)
          UTF8String 'Test locality'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER organizationName (2 5 4 10)
          UTF8String 'Narodny bezpecnostny urad'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER commonName (2 5 4 3)
          UTF8String 'Test CA'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER serialNumber (2 5 4 5)
                    -- organisation unique identification data
          PrintableString 'NTRSK-36061701'
          }
        }
      }
    SEQUENCE {
      UTCTime 21/11/2006 15:21:16 GMT -- notBefore
      UTCTime 21/11/2007 15:21:16 GMT -- notAfter
      }
    SEQUENCE {   -- subject
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER countryName (2 5 4 6)
          PrintableString 'EU'
          }
```

```
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER localityName (2 5 4 7)
      UTF8String 'Test locality'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER commonName (2 5 4 3)
      UTF8String 'MANDATÁR Peter Rybar OPRÁVNENIE 346 Zákonný zástupca'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER surname (2 5 4 4)
      UTF8String 'MANDANT Pekar'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER givenName (2 5 4 42)
      UTF8String 'MANDANT Jan'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER title (2 5 4 12)
      UTF8String 'MANDANT Ing.'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER surname (2 5 4 4)
      UTF8String 'Rybar'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER givenName (2 5 4 42)
      UTF8String 'Peter'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER title (2 5 4 12)
      UTF8String 'Ing.'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER serialNumber (2 5 4 5)
                -- personal unique identification data
      PrintableString 'PNOSK-1234567889'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER serialNumber (2 5 4 5)
                -- personal unique identification data
      PrintableString "PNOSK-MANDANT 535919999"'
      }
    }
  }
```

```
    SEQUENCE {   -- subjectPublicKeyInfo
      SEQUENCE {
        OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
        NULL
        }
      BIT STRING, encapsulates {
        SEQUENCE {
          INTEGER
            00 8A 32 3D 82 25 5D 31 DB CD 59 8B A2 8C 82 56
            0D F5 DE 0F 5A 3F 83 4F 88 41 62 7E 27 56 A6 88
            D8 8F CB D8 07 65 EE 32 3C C3 E8 46 15 3C F6 00
            C8 A8 67 43 1E CD 1D BF 32 DB 2B EC 33 BC 63 2D
            50 4E 1C 76 66 E7 88 C5 68 58 87 ED E1 DF 46 26
            BC 21 76 BF 91 33 54 0F BE 45 82 92 8D 41 31 1D
            A8 83 8E F1 EB 57 2A 5F 53 DA F9 FE 3A 28 CD FE
            25 CE E3 FA BD 0D 0E 9E DA 06 C6 93 CC 0D CF FF
                    [ Another 129 bytes skipped ]
          INTEGER 65537
          }
        }
      }
    [3] {        -- extensions
      SEQUENCE {
        SEQUENCE {
          OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
          OCTET STRING, encapsulates {
            SEQUENCE {
              [0]
                38 B3 D9 00 A5 F6 81 B9 4B 0D 9B 2A DB 4D 65 67
                B1 A5 1B CC
              }
            }
          }
        SEQUENCE {
          OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
          OCTET STRING, encapsulates {
            OCTET STRING
              38 94 23 FE 2B 7E 2C C8 5B 1E E3 D4 19 87 C6 54
              6A 93 BC B0
            }
          }
        SEQUENCE {
          OBJECT IDENTIFIER keyUsage (2 5 29 15)
          BOOLEAN TRUE       -- critical
          OCTET STRING, encapsulates {
            BIT STRING 6 unused bits
              '10'B (bit 1)  -- nonRepudiation
            }
          }
        SEQUENCE {
          OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
          OCTET STRING, encapsulates {
            SEQUENCE {
              SEQUENCE {           -- QCP public + SSCD
                OBJECT IDENTIFIER '0 4 0 1456 1 1'
                }
              SEQUENCE {           -- QCP SK
                OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
                  SEQUENCE {
                    SEQUENCE {
                      OBJECT IDENTIFIER unotice (1 3 6 1 5 5 7 2 2)
                      SEQUENCE {
                        UTF8String 'EN: Qualified certificate of mandate
pursuant to Act No. 215/2002 Coll. and Decree No. 131/2009 Coll. SK:
```

```
Kvalifikovaný mandátny certifikát podľa zákona č. 215/2002 Z. z. a vyhlášky č.
131/2009 Z. z. '
                        }
                      }
                    }
                  }
                SEQUENCE {          -- Oprávnenie 346 Zákonný zástupca
                  OBJECT IDENTIFIER '1 3 158 36061701 1 1 346'
                    SEQUENCE {
                      SEQUENCE {
                        OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
                        IA5String http://qes.test.eu/resources/cps1_346
                        }
                      SEQUENCE {
                        OBJECT IDENTIFIER unotice (1 3 6 1 5 5 7 2 2)
                        SEQUENCE {
                          UTF8String 'EN: Authorization 346, Legal
Representative, pursuant to Article 10a of the Act No. 215/2002 Coll. SK:
Oprávnenie 346, Zákonný zástupca, podľa § 10a zákona č. 215/2002 Z. z. '
                        }
                      }
                    }
                  }
                }
              }
            SEQUENCE {
              OBJECT IDENTIFIER basicConstraints (2 5 29 19)
              OCTET STRING, encapsulates {
                SEQUENCE {}      -- end entity certificate
                }
              }
            SEQUENCE {
              OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
              OCTET STRING, encapsulates {
                SEQUENCE {
                  SEQUENCE {
                    [0] {
                      [0] {
                        [6] 'http://qes.test.eu/test/testca.crl'
                        }
                      }
                    }
                  SEQUENCE {
                    [0] {
                      [0] {
                        [6]
                      'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
                      'n,l=Test locality,c=EU?certificateRevocationList'
                      ';binary'
                        }
                      }
                    }
                  SEQUENCE {
                    [0] {
                      [0] {
                        [6]
                      'ldap:///cn=Test CA,o=Test organization,l=Test lo'
                      'cality,c=EU?certificateRevocationList;binary'
                        }
                      }
                    }
                  }
                }
```

```
        }
      SEQUENCE {
        OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
        OCTET STRING, encapsulates {
          SEQUENCE {
            SEQUENCE {
              OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
              [6] 'http://ocsp.test.eu/ocsp'
              }
           -- certificate and cross-certificates
            SEQUENCE {
              OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
              [6] 'http://qes.test.eu/test/testca.p7c'
              }
            SEQUENCE {
              OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
              [6]
                'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
                'n,l=Test locality,c=EU?caCertificate;binary'
              }
            SEQUENCE {
              OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
              [6]
                'ldap:///cn=Test CA,o=Test organization,l=Test lo'
                'cality,c=EU?caCertificate;binary'
              }
            }
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
        OCTET STRING, encapsulates {
          SEQUENCE {
            SEQUENCE {          -- etsi-qcs-QcCompliance
              OBJECT IDENTIFIER '0 4 0 1862 1 1'
              }
            SEQUENCE {          -- etsi-qcs-QcSSCD
              OBJECT IDENTIFIER '0 4 0 1862 1 4'
              }
            }
          }
        }
      }
    }
  SEQUENCE {          -- signatureAlgorithm
    OBJECT IDENTIFIER
      sha256WithRSAEncryption (1 2 840 113549 1 1 11)
    NULL
    }
  BIT STRING          -- signatureValue
    A3 64 00 CC E5 ED 4A 20 5E D4 AD D9 E3 49 76 53
    3E 22 8D EB 5E B2 D3 53 B6 FB F2 58 21 4A 66 8C
    41 BC 6A D2 58 AC 1D 6A 09 F2 0C 1A 52 8E 67 15
    6B F0 4F AB 98 A9 C8 85 A4 19 1F 17 06 2D F1 45
    93 FC 7A 97 D3 1D 75 F3 3E E0 DA 5C 3D 50 02 4C
    68 7B AD 3B DB 92 6B 62 DC 65 64 50 98 F8 6B 55
    25 4B EC D6 6C 49 8E 7A 0A B8 C2 8E 2E 43 1D 52
    3F 37 A8 CC C6 FE D0 03 FC 55 87 A4 65 82 68 8E
           [ Another 128 bytes skipped ]
  }
```

A.3 Príklad systémového kvalifikovaného certifikátu

```
SEQUENCE {
  SEQUENCE {
    [0] {
      INTEGER 2  -- version
      }
    INTEGER 30883      -- serialNumber
    SEQUENCE {   -- signature
      OBJECT IDENTIFIER
        sha256WithRSAEncryption (1 2 840 113549 1 1 11)
      NULL
      }
    SEQUENCE {   -- issuer
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER countryName (2 5 4 6)
          PrintableString 'EU'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER localityName (2 5 4 7)
          UTF8String 'Test locality'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER organizationName (2 5 4 10)
          UTF8String 'Narodny bezpecnostny urad'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER commonName (2 5 4 3)
          UTF8String 'Test CA'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER serialNumber (2 5 4 5)
                    -- organisation unique identification data
          PrintableString 'NTRSK-36061701'
          }
        }
      }
    SEQUENCE {
      UTCTime 21/11/2006 15:21:16 GMT -- notBefore
      UTCTime 21/11/2007 15:21:16 GMT -- notAfter
      }
    SEQUENCE {   -- subject
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER countryName (2 5 4 6)
          PrintableString 'EU'
          }
        }
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER localityName (2 5 4 7)
          UTF8String 'Test locality'
          }
        }
```

```
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER commonName (2 5 4 3)
        UTF8String 'Podatelna'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationName (2 5 4 10)
        UTF8String 'Narodny bezpecnostny urad'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
        UTF8String 'SIBEP'
        }
      }
    SET {
      SEQUENCE {
        OBJECT IDENTIFIER serialNumber (2 5 4 5)
                  -- unique identification data
        PrintableString 'NTRSK-36061701'
        }
      }
    }
  SEQUENCE {   -- subjectPublicKeyInfo
    SEQUENCE {
      OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
      NULL
      }
    BIT STRING, encapsulates {
      SEQUENCE {
        INTEGER
          00 8A 32 3D 82 25 5D 31 DB CD 59 8B A2 8C 82 56
          0D F5 DE 0F 5A 3F 83 4F 88 41 62 7E 27 56 A6 88
          D8 8F CB D8 07 65 EE 32 3C C3 E8 46 15 3C F6 00
          C8 A8 67 43 1E CD 1D BF 32 DB 2B EC 33 BC 63 2D
          50 4E 1C 76 66 E7 88 C5 68 58 87 ED E1 DF 46 26
          BC 21 76 BF 91 33 54 0F BE 45 82 92 8D 41 31 1D
          A8 83 8E F1 EB 57 2A 5F 53 DA F9 FE 3A 28 CD FE
          25 CE E3 FA BD 0D 0E 9E DA 06 C6 93 CC 0D CF FF
                  [ Another 129 bytes skipped ]
        INTEGER 65537
        }
      }
    }
  [3] {        -- extensions
    SEQUENCE {
      SEQUENCE {
        OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
        OCTET STRING, encapsulates {
          SEQUENCE {
            [0]
              38 B3 D9 00 A5 F6 81 B9 4B 0D 9B 2A DB 4D 65 67
              B1 A5 1B CC
            }
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
        OCTET STRING, encapsulates {
          OCTET STRING
            38 94 23 FE 2B 7E 2C C8 5B 1E E3 D4 19 87 C6 54
```

```
            6A 93 BC B0
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER keyUsage (2 5 29 15)
        BOOLEAN TRUE       -- critical
        OCTET STRING, encapsulates {
          BIT STRING 6 unused bits
            '10'B (bit 1)  -- nonRepudiation
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
        OCTET STRING, encapsulates {
          SEQUENCE {
            SEQUENCE {           -- QCP public + SSCD
              OBJECT IDENTIFIER '0 4 0 1456 1 1'
              }
            SEQUENCE {           -- QCP SK
              OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
                SEQUENCE {
                  SEQUENCE {
                    OBJECT IDENTIFIER unotice (1 3 6 1 5 5 7 2 2)
                    SEQUENCE {
                      UTF8String 'EN: A certificate is issued as a qualified
certificate for seal pursuant to the Act No. 215/2002 Coll. and the NSA Decree
No. 131/2009 Coll. SK: Kvalifikovaný systémový certifikát podľa zákona č.
215/2002 Z. z. a vyhlášky č. 131/2009 Z. z.'
                        }
                      }
                    }
                  }
                }
              }
            }
        }
      SEQUENCE {
        OBJECT IDENTIFIER basicConstraints (2 5 29 19)
        OCTET STRING, encapsulates {
          SEQUENCE {}      -- end entity certificate
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
        OCTET STRING, encapsulates {
          SEQUENCE {
            SEQUENCE {
              [0] {
                [0] {
                  [6] 'http://qes.test.eu/test/testca.crl'
                  }
                }
              }
            SEQUENCE {
              [0] {
                [0] {
                  [6]
                'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
                'n,l=Test locality,c=EU?certificateRevocationList'
                ';binary'
                  }
                }
              }
            SEQUENCE {
              [0] {
```

```
                [0] {
                  [6]
                'ldap:///cn=Test CA,o=Test organization,l=Test lo'
                'cality,c=EU?certificateRevocationList;binary'
                  }
                }
              }
            }
          }
        }
        SEQUENCE {
          OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
          OCTET STRING, encapsulates {
            SEQUENCE {
              SEQUENCE {
                OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
                [6] 'http://ocsp.test.eu/ocsp'
                }
             -- certificate and cross-certificates
                SEQUENCE {
                  OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
                  [6] 'http://qes.test.eu/test/testca.p7c'
                  }
                SEQUENCE {
                  OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
                  [6]
                    'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
                    'n,l=Test locality,c=EU?caCertificate;binary'
                  }
                SEQUENCE {
                  OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
                  [6]
                    'ldap:///cn=Test CA,o=Test organization,l=Test lo'
                    'cality,c=EU?caCertificate;binary'
                  }
                }
              }
            }
          }
          SEQUENCE {
            OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
            OCTET STRING, encapsulates {
              SEQUENCE {
                SEQUENCE {          -- etsi-qcs-QcCompliance
                  OBJECT IDENTIFIER '0 4 0 1862 1 1'
                  }
                SEQUENCE {          -- etsi-qcs-QcSSCD
                  OBJECT IDENTIFIER '0 4 0 1862 1 4'
                  }
                }
              }
            }
          }
        }
      }
    }
  SEQUENCE {          -- signatureAlgorithm
    OBJECT IDENTIFIER
      sha256WithRSAEncryption (1 2 840 113549 1 1 11)
    NULL
    }
  BIT STRING          -- signatureValue
    A3 64 00 CC E5 ED 4A 20 5E D4 AD D9 E3 49 76 53
    3E 22 8D EB 5E B2 D3 53 B6 FB F2 58 21 4A 66 8C
    41 BC 6A D2 58 AC 1D 6A 09 F2 0C 1A 52 8E 67 15
    6B F0 4F AB 98 A9 C8 85 A4 19 1F 17 06 2D F1 45
```

```
    93 FC 7A 97 D3 1D 75 F3 3E E0 DA 5C 3D 50 02 4C
    68 7B AD 3B DB 92 6B 62 DC 65 64 50 98 F8 6B 55
    25 4B EC D6 6C 49 8E 7A 0A B8 C2 8E 2E 43 1D 52
    3F 37 A8 CC C6 FE D0 03 FC 55 87 A4 65 82 68 8E
            [ Another 128 bytes skipped ]
  }
```

A.4 Príklad certifikátu časovej pečiatky pre zaručený elektronický podpis

```
  0 1541: SEQUENCE {
  4 1261:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2    -- version
       :       }
 13    1:     INTEGER 33     -- serialNumber
 16   13:     SEQUENCE {     -- signature
 18    9:       OBJECT IDENTIFIER
       :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 29    0:       NULL
       :       }
 31   83:     SEQUENCE {     -- issuer
 33   11:       SET {
 35    9:         SEQUENCE {
 37    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 42    2:           PrintableString 'EU'
       :           }
       :         }
 46   22:       SET {
 48   20:         SEQUENCE {
 50    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
 55   13:           UTF8String 'Test locality'
       :           }
       :         }
 70   26:       SET {
 72   24:         SEQUENCE {
 74    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 79   25:           UTF8String 'Narodny bezpecnostny urad'
       :           }
       :         }
 98   16:       SET {
100   14:         SEQUENCE {
102    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
107    7:           UTF8String 'Test CA'
       :           }
       :         }
258   21:       SET {
260   19:         SEQUENCE {
262    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
                               -- organisation unique identification data
267   14:           PrintableString 'NTRSK-36061701'
       :           }
       :         }
       :       }
116   30:     SEQUENCE {
118   13:       UTCTime 21/07/2006 08:48:17 GMT -- notBefore
133   13:       UTCTime 20/07/2011 08:48:17 GMT -- notAfter
       :       }
148   91:     SEQUENCE {     -- subject
150   11:       SET {
152    9:         SEQUENCE {
154    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
```

```
159    2:           PrintableString 'EU'
        :           }
        :         }
163   22:       SET {
165   20:         SEQUENCE {
167    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
172   13:           UTF8String 'Test locality'
        :           }
        :         }
187   30:       SET {
189   28:         SEQUENCE {
191    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
196   21:           UTF8String 'Test TSA organization'
        :           }
        :         }
219   20:       SET {
221   18:         SEQUENCE {
223    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
228   11:           UTF8String 'TSA for QES'
        :           }
        :         }
        :       }
241  290:     SEQUENCE {     -- subjectPublicKeyInfo
245   13:       SEQUENCE {
247    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
258    0:         NULL
        :         }
260  271:       BIT STRING, encapsulates {
265  266:         SEQUENCE {
269  257:           INTEGER
        :             00 D5 53 25 C5 4B 2B 83 9B FB 6A CE 4E 17 ED FA
        :             F5 32 B2 F1 85 C3 72 97 E4 F2 76 58 D9 19 1F 39
        :             B9 40 6C 87 1B 24 7C E4 9B E8 91 9D 71 4A C2 CF
        :             00 4F 7B 46 8E E1 C1 65 31 2C C6 DC B5 40 F7 3B
        :             77 0D EB B1 F1 A2 48 10 E5 3F 5B B7 12 AA 52 B4
        :             1E CB 13 C6 4C 14 E1 3E FC 1F 89 BA 3F A1 0C 9C
        :             32 0E BC 61 89 88 17 FE 75 4C F5 FF 0C BC 4E 9A
        :             52 B5 BE D0 F3 DD E0 83 C4 EB 94 7E 72 C1 33 CD
        :                     [ Another 129 bytes skipped ]
530    3:           INTEGER 65537
        :           }
        :         }
        :       }
535  730:     [3] {          -- extensions
539  726:       SEQUENCE {
543   31:         SEQUENCE {
545    3:           OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
550   24:           OCTET STRING, encapsulates {
552   22:             SEQUENCE {
554   20:               [0]
        :                 38 B3 D9 00 A5 F6 81 B9 4B 0D 9B 2A DB 4D 65 67
        :                 B1 A5 1B CC
        :               }
        :             }
        :           }
576   29:         SEQUENCE {
578    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
583   22:           OCTET STRING, encapsulates {
585   20:             OCTET STRING
        :               35 78 32 78 AF D2 98 62 FF 05 9E B9 3D 9C 2A 0C
        :               95 8E 18 52
        :             }
        :           }
607   11:         SEQUENCE {
```

```
609    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
614    4:           OCTET STRING, encapsulates {
616    2:             BIT STRING 6 unused bits
       :               '10'B (bit 1)    -- nonRepudiation
       :             }
       :           }
620   36:         SEQUENCE {
622    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
627   29:           OCTET STRING, encapsulates {
629   27:             SEQUENCE {
631   15:               SEQUENCE {       -- QCP SK
633   13:                 OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
       :                 }
648    8:               SEQUENCE {       -- NCP+: Normalized Certificate Policy
                                          -- requiring a secure user device
650    6:                 OBJECT IDENTIFIER '0 4 0 2042 1 2'
       :                 }
       :               }
       :             }
       :           }
658    9:         SEQUENCE {
660    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
665    2:           OCTET STRING, encapsulates {
667    0:             SEQUENCE {}  -- end entity certificate
       :             }
       :           }
669   22:         SEQUENCE {
671    3:           OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
676    1:           BOOLEAN TRUE   -- critical
679   12:           OCTET STRING, encapsulates {
681   10:             SEQUENCE {
683    8:               OBJECT IDENTIFIER timeStamping (1 3 6 1 5 5 7 3 8)
       :               }
       :             }
       :           }
693  265:         SEQUENCE {
697    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
702  256:           OCTET STRING, encapsulates {
706  253:             SEQUENCE {
709   40:               SEQUENCE {
711   38:                 [0] {
713   36:                   [0] {
715   34:                     [6] 'http://qes.test.eu/test/testca.crl'
       :                     }
       :                   }
       :                 }
751  109:               SEQUENCE {
753  107:                 [0] {
755  105:                   [0] {
757  103:                     [6]
       :                     'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
       :                     'n,l=Test locality,c=EU?certificateRevocationList'
       :                     ';binary'
       :                     }
       :                   }
       :                 }
862   98:               SEQUENCE {
864   96:                 [0] {
866   94:                   [0] {
868   92:                     [6]
       :                     'ldap:///cn=Test CA,o=Test organization,l=Test lo'
       :                     'cality,c=EU?certificateRevocationList;binary'
       :                     }
       :                   }
```

```
         :                 }
         :               }
         :             }
         :           }
 962  303:         SEQUENCE {
 966    8:           OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
 976  289:           OCTET STRING, encapsulates {
 980  285:             SEQUENCE {
 984   36:               SEQUENCE {
 986    8:                 OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
 996   24:                 [6] 'http://ocsp.test.eu/ocsp'
         :                 }
                          -- certificate and cross-certificates
1022   46:               SEQUENCE {
1024    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1034   34:                 [6] 'http://qes.test.eu/test/testca.p7c'
         :                 }
1070  103:               SEQUENCE {
1072    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1082   91:                 [6]
         :                   'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
         :                   'n,l=Test locality,c=EU?caCertificate;binary'
         :                 }
1175   92:               SEQUENCE {
1177    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1187   80:                 [6]
         :                   'ldap:///cn=Test CA,o=Test organization,l=Test lo'
         :                   'cality,c=EU?caCertificate;binary'
         :                 }
         :               }
         :             }
         :           }
         :         }
         :       }
         :     }
1269   13:   SEQUENCE {
1271    9:     OBJECT IDENTIFIER
         :       sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1282    0:     NULL
         :     }
1284  257:   BIT STRING
         :     27 2F 6F FA CC 27 7F 8A E1 6C 0B 10 A5 0F 31 E7
         :     02 5F 15 5C C6 B6 31 87 12 F6 D7 6B 37 E8 62 B2
         :     4E FF B7 92 5A F4 EF 31 90 4C 67 B9 46 DF CC 05
         :     CC BF F6 63 A7 45 D7 5F 92 0D 8E BB B7 4A 3C A3
         :     BD 20 4E 93 F0 35 28 79 FC 79 79 77 EF 4A E0 83
         :     E3 3D 4B 70 CE 25 BE 80 8D E5 E8 E9 2A 67 86 CF
         :     4D 79 EB 5F 9D 54 6B 9D AD AA DC 81 37 63 7D 39
         :     56 26 E3 9B 2C E1 A6 14 8C E9 BD 20 35 0F A8 7A
         :             [ Another 128 bytes skipped ]
         :   }
```

A.5 Príklad CA certifikátu

```
   0 1926: SEQUENCE {
   4 1646:   SEQUENCE {
   8    3:     [0] {
  10    1:       INTEGER 2    -- version
         :       }
  13    2:     INTEGER 8558   -- serialNumber
  17   13:     SEQUENCE {     -- signature
  19    9:       OBJECT IDENTIFIER
```

```
        :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 30    0:       NULL
        :       }
 32   85:     SEQUENCE {     -- issuer
 34   11:       SET {
 36    9:         SEQUENCE {
 38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43    2:           PrintableString 'EU'
        :           }
        :         }
 47   22:       SET {
 49   20:         SEQUENCE {
 51    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
 56   13:           UTF8String 'Test locality'
        :           }
        :         }
 71   26:       SET {
 73   24:         SEQUENCE {
 75    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 80   17:           UTF8String 'Test organization'
        :           }
        :         }
 99   18:       SET {
101   16:         SEQUENCE {
103    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
108    9:           UTF8String 'Test Root'
        :           }
        :         }
        :       }
119   30:     SEQUENCE {
121   13:       UTCTime 24/08/2006 11:18:13 GMT -- notBefore
136   13:       UTCTime 24/08/2011 11:17:27 GMT -- notAfter
        :       }
151   83:     SEQUENCE {     -- subject
153   11:       SET {
155    9:         SEQUENCE {
157    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
162    2:           PrintableString 'EU'
        :           }
        :         }
166   22:       SET {
168   20:         SEQUENCE {
170    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
175   13:           UTF8String 'Test locality'
        :           }
        :         }
190   26:       SET {
192   24:         SEQUENCE {
194    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
199   25:           UTF8String 'Narodny bezpecnostny urad'
        :           }
        :         }
218   16:       SET {
220   14:         SEQUENCE {
222    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
227    7:           UTF8String 'Test CA'
        :           }
        :         }
258   21:       SET {
260   19:         SEQUENCE {
262    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
                              -- organisation unique identification data
267   14:           PrintableString 'NTRSK-36061701'
        :           }
```

```
        :         }
        :       }
 236  290:     SEQUENCE {     -- subjectPublicKeyInfo
 240   13:       SEQUENCE {
 242    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
 253    0:         NULL
        :         }
 255  271:       BIT STRING, encapsulates {
 260  266:         SEQUENCE {
 264  257:           INTEGER
        :             00 B2 D4 6C 5A D4 86 6B E5 BA 28 4F 87 4D F7 E2
        :             20 78 5F 02 E8 0F FA E3 EF EF 2A 09 CC 4A 74 0A
        :             36 4E B5 95 C1 FC 59 23 36 85 E6 6B 5F 6F 29 84
        :             9A 3F D1 08 ED 30 2E 17 3B 96 23 E8 67 68 C4 68
        :             78 84 D4 D2 AA 56 37 47 0F AD 1C E1 88 B5 39 5D
        :             B6 C1 22 30 08 BA DB 0D BB BF 53 2A 8E AD 48 E6
        :             D0 12 DB 02 A9 F9 DF AA E4 E9 01 A3 DD 39 E2 0C
        :             C5 C0 A0 EC 36 5C 93 99 AC 31 4B 09 18 71 31 FF
        :                     [ Another 129 bytes skipped ]
 525    3:           INTEGER 65537
        :           }
        :         }
        :       }
 530 1120:     [3] {          -- extensions
 534 1116:       SEQUENCE {
 538   31:         SEQUENCE {
 540    3:           OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
 545   24:           OCTET STRING, encapsulates {
 547   22:             SEQUENCE {
 549   20:               [0]
        :                 06 DA 89 E7 D3 8E 53 3A 79 77 E9 EB F9 A6 B6 32
        :                 65 3F 46 24
        :               }
        :             }
        :           }
 571   29:         SEQUENCE {
 573    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
 578   22:           OCTET STRING, encapsulates {
 580   20:             OCTET STRING
        :               38 B3 D9 00 A5 F6 81 B9 4B 0D 9B 2A DB 4D 65 67
        :               B1 A5 1B CC
        :             }
        :           }
 602   14:         SEQUENCE {
 604    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
 609    1:           BOOLEAN TRUE   -- critical
 612    4:           OCTET STRING, encapsulates {
 614    2:             BIT STRING 1 unused bit
        :               '1100000'B -- keyCertSign, cRLSign
        :             }
        :           }
 618   29:         SEQUENCE {
 620    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 625    1:           BOOLEAN TRUE   -- critical
 628   19:           OCTET STRING, encapsulates {
 630   17:             SEQUENCE {
 632   15:               SEQUENCE { -- QCP SK
 634   13:                 OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
        :                 }
        :               }
        :             }
        :           }
 649   69:         SEQUENCE {
 651    3:           OBJECT IDENTIFIER policyMappings (2 5 29 33)
```

```
656    1:           BOOLEAN TRUE   -- is optional
659   59:           OCTET STRING, encapsulates {
661   57:             SEQUENCE {
663   23:               SEQUENCE {
                          -- issuerDomainPolicy  - QCP SK
665   13:                 OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
                          -- subjectDomainPolicy - QCP public + SSCD
680    6:                 OBJECT IDENTIFIER '0 4 0 1456 1 1'
       :                 }
688   30:               SEQUENCE {
                          -- issuerDomainPolicy  - QCP SK
690   13:                 OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
                          -- subjectDomainPolicy - QCP SK
705   13:                 OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
       :                 }
       :               }
       :             }
       :           }
720   18:         SEQUENCE {
722    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
727    1:           BOOLEAN TRUE   -- critical
730    8:           OCTET STRING, encapsulates {
732    6:             SEQUENCE {
734    1:               BOOLEAN TRUE     -- CA certificate
737    1:               INTEGER 1        -- pathLenConstraint
       :               }
       :             }
       :           }
740   15:         SEQUENCE {
742    3:           OBJECT IDENTIFIER policyConstraints (2 5 29 36)
747    1:           BOOLEAN TRUE   -- critical
750    5:           OCTET STRING, encapsulates {
752    3:             SEQUENCE {
754    1:               [0] 00           -- requireExplicitPolicy SkipCerts
       :               }
       :             }
       :           }
757  272:         SEQUENCE {
761    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
766  263:           OCTET STRING, encapsulates {
770  259:             SEQUENCE {
774   42:               SEQUENCE {
776   40:                 [0] {
778   38:                   [0] {
780   36:                     [6] 'http://qes.test.eu/test/testroot.crl'
       :                     }
       :                   }
       :                 }
818  111:               SEQUENCE {
820  109:                 [0] {
822  107:                   [0] {
824  105:                     [6]
       :                     'ldap://qes.test.eu/cn=Test Root,o=Test organizat'
       :                     'ion,l=Test locality,c=EU?certificateRevocationLi'
       :                     'st;binary'
       :                     }
       :                   }
       :                 }
931  100:               SEQUENCE {
933   98:                 [0] {
935   96:                   [0] {
937   94:                     [6]
       :                     'ldap:///cn=Test Root,o=Test organization,l=Test '
       :                     'locality,c=EU?certificateRevocationList;binary'
```

```
          :                     }
          :                   }
          :                 }
          :               }
          :             }
          :           }
1033  310:         SEQUENCE {
1037    8:           OBJECT IDENTIFIER authorityInfoAccess (1 3 6 1 5 5 7 1 1)
1047  296:           OCTET STRING, encapsulates {
1051  292:             SEQUENCE {
1055   37:               SEQUENCE {
1057    8:                 OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
1067   25:                 [6] 'http://ocsp.test.eu/ocspr'
          :                 }
                           -- certificate and cross-certificates
1094   48:               SEQUENCE {
1096    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1106   36:                 [6] 'http://qes.test.eu/test/testroot.p7c'
          :                 }
1144  105:               SEQUENCE {
1146    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1156   93:                 [6]
          :                   'ldap://qes.test.eu/cn=Test Root,o=Test organizat'
          :                   'ion,l=Test locality,c=EU?caCertificate;binary'
          :                 }
1251   94:               SEQUENCE {
1253    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1263   82:                 [6]
          :                   'ldap:///cn=Test Root,o=Test organization,l=Test '
          :                   'locality,c=EU?caCertificate;binary'
          :                 }
          :               }
          :             }
          :           }
1347  303:         SEQUENCE {
1351    8:           OBJECT IDENTIFIER subjectInfoAccess (1 3 6 1 5 5 7 1 11)
1361  289:           OCTET STRING, encapsulates {
1365  285:             SEQUENCE {
1369   36:               SEQUENCE {
1371    8:                 OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
1381   24:                 [6] 'http://ocsp.test.eu/ocsp'
          :                 }
                           -- certificate and cross-certificates
1407   46:               SEQUENCE {
1409    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1419   34:                 [6] 'http://qes.test.eu/test/testca.p7c'
          :                 }
1455  103:               SEQUENCE {
1457    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1467   91:                 [6]
          :                   'ldap://qes.test.eu/cn=Test CA,o=Test organizatio'
          :                   'n,l=Test locality,c=EU?caCertificate;binary'
          :                 }
1560   92:               SEQUENCE {
1562    8:                 OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1572   80:                 [6]
          :                   'ldap:///cn=Test CA,o=Test organization,l=Test lo'
          :                   'cality,c=EU?caCertificate;binary'
          :                 }
          :               }
          :             }
          :           }
          :         }
          :       }
```

```
         :     }
1654   13:   SEQUENCE {       -- signatureAlgorithm
1656    9:     OBJECT IDENTIFIER
         :       sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1667    0:     NULL
         :     }
1669  257:   BIT STRING       -- signatureValue
         :     C0 D9 11 F1 AE 65 1E C3 76 B3 7C 6B A3 6C 06 E1
         :     52 2D 70 05 49 12 B4 5B 6E ED 94 B7 2A 64 3F 62
         :     41 16 C6 5D 3F 0D 4B CF 3E C4 4B C2 51 78 10 C6
         :     DF 8A F5 B9 6D 51 D5 5E 42 19 4B F7 86 B3 25 7A
         :     9B 1C F0 95 44 6E 81 1E 03 E0 58 11 A6 2B F5 02
         :     BC 97 4A 46 35 F2 7A 29 E7 95 EF 0B 7C A4 B1 A3
         :     8B DE 76 FE 4C A8 70 A0 5B D4 5A F9 B4 B1 0E A3
         :     F4 E1 C2 6A D3 6F CF 9A 84 F7 A3 00 28 8A 99 1B
         :             [ Another 128 bytes skipped ]
         :   }
```

A.6 Príklad koreňového certifikátu

```
  0 1493: SEQUENCE {
  4 1213:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2    -- version
       :       }
 13    1:     INTEGER 1      -- serialNumber
 16   13:     SEQUENCE {     -- signature
 18    9:       OBJECT IDENTIFIER
       :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 29    0:       NULL
       :       }
 31   85:     SEQUENCE {     -- issuer
 33   11:       SET {
 35    9:         SEQUENCE {
 37    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 42    2:           PrintableString 'EU'
       :           }
       :         }
 46   22:       SET {
 48   20:         SEQUENCE {
 50    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
 55   13:           UTF8String 'Test locality'
       :           }
       :         }
 70   26:       SET {
 72   24:         SEQUENCE {
 74    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 79   17:           UTF8String 'Test organization'
       :           }
       :         }
 98   18:       SET {
100   16:         SEQUENCE {
102    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
107    9:           UTF8String 'Test Root'
       :           }
       :         }
       :       }
118   30:     SEQUENCE {
120   13:       UTCTime 22/02/2005 16:13:37 GMT -- notBefore
135   13:       UTCTime 22/02/2015 15:43:57 GMT -- notAfter
       :       }
150   85:     SEQUENCE {     -- subject
152   11:       SET {
154    9:         SEQUENCE {
156    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
161    2:           PrintableString 'EU'
       :           }
       :         }
165   22:       SET {
167   20:         SEQUENCE {
169    3:           OBJECT IDENTIFIER localityName (2 5 4 7)
174   13:           UTF8String 'Test locality'
       :           }
       :         }
189   26:       SET {
191   24:         SEQUENCE {
193    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
198   17:           UTF8String 'Test organization'
       :           }
       :         }
217   18:       SET {
```

```
219   16:         SEQUENCE {
221    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
226    9:           UTF8String 'Test Root'
             :         }
             :       }
             :     }
237  290:     SEQUENCE {     -- subjectPublicKeyInfo
241   13:       SEQUENCE {
243    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
254    0:         NULL
             :         }
256  271:       BIT STRING, encapsulates {
261  266:         SEQUENCE {
265  257:           INTEGER
             :             00 F2 6F 8E C9 BD 3F 65 65 41 BE 5F DC 51 AB 4D
             :             C5 A4 8D E2 0C 4B 7C 52 75 9A 80 23 36 FB B4 53
             :             77 1D 8F D1 D7 BD DA 14 79 8E DB 13 51 66 C7 4A
             :             33 AD 0F 95 4F E8 83 BA 03 42 70 2E BE 9C F1 74
             :             6F 83 84 6C 5D F6 32 63 9E 6E DE 63 C0 DF 6B 31
             :             70 81 D6 21 BA D7 3A 81 F7 F1 95 7B C1 AA 36 39
             :             74 0B 2F F2 9B 6D 08 AA 05 A7 6C DA 2E 5B FD B5
             :             0D B8 FD 8B 75 53 9D A5 01 9E 1E E3 98 9B D3 29
             :                       [ Another 129 bytes skipped ]
526    3:           INTEGER 65537
             :           }
             :         }
             :       }
531  686:     [3] {          -- extensions
535  682:       SEQUENCE {
539   29:         SEQUENCE {
541    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
546   22:           OCTET STRING, encapsulates {
548   20:             OCTET STRING
             :               06 DA 89 E7 D3 8E 53 3A 79 77 E9 EB F9 A6 B6 32
             :               65 3F 46 24
             :             }
             :           }
570   14:         SEQUENCE {
572    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
577    1:           BOOLEAN TRUE   -- critical
580    4:           OCTET STRING, encapsulates {
582    2:             BIT STRING 1 unused bit
             :               '1100000'B -- keyCertSign, cRLSign
             :             }
             :           }
586   26:         SEQUENCE {
588    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
593   19:           OCTET STRING, encapsulates {
595   17:             SEQUENCE {
597   15:               SEQUENCE { -- QCP SK
599   13:                 OBJECT IDENTIFIER '1 3 158 36061701 0 0 0 1 2 2'
             :                 }
             :               }
             :             }
             :           }
614   15:         SEQUENCE {
616    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
621    1:           BOOLEAN TRUE   -- critical
624    5:           OCTET STRING, encapsulates {
626    3:             SEQUENCE {
628    1:               BOOLEAN TRUE     -- CA certificate
             :               }
             :             }
             :           }
```

```
 631  272:          SEQUENCE {
 635    3:            OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
 640  263:            OCTET STRING, encapsulates {
 644  259:              SEQUENCE {
 648   42:                SEQUENCE {
 650   40:                  [0] {
 652   38:                    [0] {
 654   36:                      [6] 'http://qes.test.eu/test/testroot.crl'
         :                      }
         :                    }
         :                  }
 692  111:                SEQUENCE {
 694  109:                  [0] {
 696  107:                    [0] {
 698  105:                      [6]
         :                      'ldap://qes.test.eu/cn=Test Root,o=Test organizat'
         :                      'ion,l=Test locality,c=EU?certificateRevocationLi'
         :                      'st;binary'
         :                      }
         :                    }
         :                  }
 805  100:                SEQUENCE {
 807   98:                  [0] {
 809   96:                    [0] {
 811   94:                      [6]
         :                      'ldap:///cn=Test Root,o=Test organization,l=Test '
         :                      'locality,c=EU?certificateRevocationList;binary'
         :                      }
         :                    }
         :                  }
         :                }
         :              }
         :            }
 907  310:          SEQUENCE {
 911    8:            OBJECT IDENTIFIER subjectInfoAccess (1 3 6 1 5 5 7 1 11)
 921  296:            OCTET STRING, encapsulates {
 925  292:              SEQUENCE {
 929   37:                SEQUENCE {
 931    8:                  OBJECT IDENTIFIER ocsp (1 3 6 1 5 5 7 48 1)
 941   25:                  [6] 'http://ocsp.test.eu/ocspr'
         :                  }
                           -- certificate and cross-certificates
 968   48:                SEQUENCE {
 970    8:                  OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
 980   36:                  [6] 'http://qes.test.eu/test/testroot.p7c'
         :                  }
1018  105:                SEQUENCE {
1020    8:                  OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1030   93:                  [6]
         :                    'ldap://qes.test.eu/cn=Test Root,o=Test organizat'
         :                    'ion,l=Test locality,c=EU?caCertificate;binary'
         :                  }
1125   94:                SEQUENCE {
1127    8:                  OBJECT IDENTIFIER caIssuers (1 3 6 1 5 5 7 48 2)
1137   82:                  [6]
         :                    'ldap:///cn=Test Root,o=Test organization,l=Test '
         :                    'locality,c=EU?caCertificate;binary'
         :                  }
         :                }
         :              }
         :            }
         :          }
         :        }
         :      }
```

```
1221   13:   SEQUENCE {       -- signatureAlgorithm
1223    9:     OBJECT IDENTIFIER
         :       sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1234    0:     NULL
         :     }
1236  257:   BIT STRING       -- signatureValue
         :     F2 3B 29 D1 58 61 09 BF 48 18 10 57 4B BA AF 87
         :     78 0B 29 F9 BA AE 41 DD F1 6C 7E 1B C9 29 3E F6
         :     4A E8 40 9C 6A DF 6B 70 E9 27 F8 A0 27 1B 90 3F
         :     7C 18 A1 76 48 1D 17 7C 6E 8F C2 6E EB D3 F4 A5
         :     1D A6 2F 37 DB D2 29 EA 11 5F 51 55 BF D4 52 FB
         :     85 71 8F 9A 58 D8 8F 4C 44 E3 51 CD 30 4F BE A1
         :     D9 BD 99 BD C8 CC 71 5C B5 D8 C4 95 B9 A1 8A 3A
         :     48 35 64 68 0B 0D A7 24 F0 D3 D4 EF 96 6F 96 72
         :             [ Another 128 bytes skipped ]
         :   }
```

Príloha B (informatívna) Revízie vykonané od predošlého vydania

B.1 Pridané požiadavky

Pridané položky, ktoré významne zmenili význam predchádzajúcich požiadaviek:

V kapitole 5 sú uvedené požiadavky na identifikáciu kvalifikovaných certifikátov a mandátnych certifikátov.

B.2 Upravené požiadavky

Položky, ktoré upravujú predchádzajúce požiadavky:

Meno vydavateľa musí pre nové certifikáty vydané pre nový kľúčový pár vydavateľa obsahovať jednoznačnú identifikáciu v položke *serialNumber*.
Dokumenty vo formáte PDF obsahujúce napríklad CP alebo CPS by mali byť chránené minimálne podľa požiadaviek ETSI TS 102 778-3 Part 3 [19].

B.3 Vysvetlenia

Položky, ktoré boli zmenené pre vysvetlenie predchádzajúcich požiadaviek:

B.4 Publikačné zmeny

Zmeny, ktoré neovplyvňujú technický význam dokumentu:

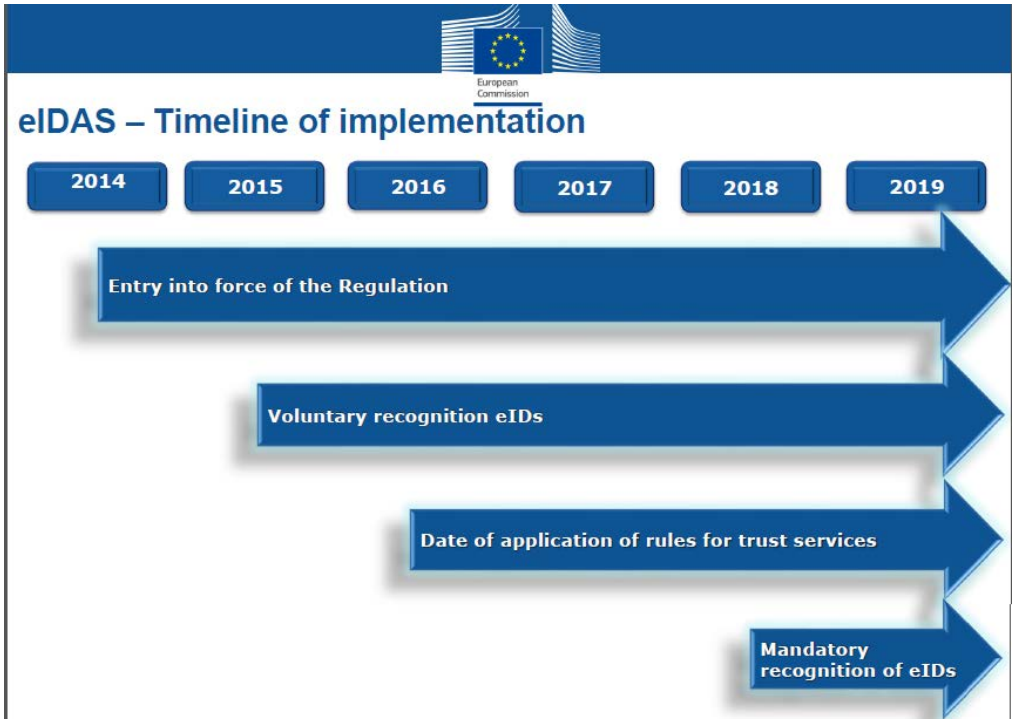
Pridanie novej podkapitoly 5.1 a 5.2.

Príloha C (informatívna) Zoznam použitej literatúry

Základná legislatíva Slovenskej republiky pre elektronický podpis:
http://www.nbusr.sk/sk/pravne-predpisy/elektronicky-podpis.1.html
Štandardy NBÚ:
http://www.nbusr.sk/sk/elektronicky-podpis/standardy-nbu.1.html
Zostavenie certifikačnej cesty a overenie platnosti certifikátov:
http://www.nbusr.sk/sk/elektronicky-podpis/overovanie.1.html
Rozhodnutia Komisie pre elektronický podpis:
VYKONÁVACIE ROZHODNUTIE KOMISIE 2013/662/EÚ zo 14. októbra 2013, ktorým sa mení rozhodnutie 2009/767/ES, pokiaľ ide o zostavovanie, vedenie a uverejňovanie zoznamov dôveryhodných informácií o poskytovateľoch certifikačných služieb, ktorí podliehajú dohľadu členského štátu alebo sú v ňom akreditovaní
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:306:0021:0039:EN:PDF
VYKONÁVACIE ROZHODNUTIE KOMISIE 2014/148/EÚ zo 17. marca 2014, ktorým sa mení rozhodnutie 2011/130/EÚ, ktorým sa ustanovujú minimálne požiadavky na cezhraničné spracovanie dokumentov elektronicky podpísaných príslušnými orgánmi v zmysle smernice Európskeho parlamentu a Rady 2006/123/ES o službách na vnútornom trhu
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2014:080:0007:0009:EN:PDF

Legislatíva EÚ, ktorá ruší smernicu o elektronickom podpise a požiadavky národných legislatív prijatých na základe tejto smernice:
http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES http://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX:32014R0910



Príloha D História

Verzia	Dátum	Poznámka	Vypracoval
V 1.0	30.9.2004	Prvé vydanie	Ing. Peter Rybár
V 1.1	14.8.2005	Ruší verziu 1.0	Ing. Peter Rybár, NBÚ
Verzia 1.2	6.11.2005	Zmena kritických rozšírení	Ing. Peter Rybár, NBÚ
Verzia 2.0 Č.: 3198/2007/IBEP-001	8.4.2007	Pridanie odkazu na identitu fyzickej osoby do X.509 kvalifikovaného certifikátu	Ing. Peter Rybár, NBÚ
Verzia 2.1 Č.: 3198/2007/IBEP-017	18.9.2007	Výnimka pre označenie kvalifikovaného certifikátu podľa slovenskej legislatívy.	Ing. Peter Rybár, NBÚ
Verzia 2.2 Č.: 2739/2008/IBEP-004	6.6.2008	Zmena identifikácie osoby podľa novely zákona o EP z roku 2008.	Ing. Peter Rybár, NBÚ
Verzia 3.0 Č.: 584/2009/IBEP-008	30.6.2009	Štandardy formátov KC pred verziou 3.0 sú zrušené. Zmena podľa novely vyhlášky z roku 2009.	Ing. Peter Rybár, NBÚ
Verzia 4.0 Č.: 3109/2014/IBEP/OA-001	10.7.2014	Zmena na základe novely legislatívy.	Ing. Peter Rybár, NBÚ