Národný bezpečnostný úrad

Certifikačná politika pre koreňovú CA a dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný bezpečnostný úrad

Verzia: 4.0

Dokument nadobúda účinnosť dňa 1.11.2016

Obsah

Odkazy na štandardy a legislatívu

[1] IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, pozri https://tools.ietf.org/html/rfc3647

[2] Recommendation ITU-T X.509 | ISO/IEC 9594-8 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, pozri http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509

[3] 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, Nariadenie (EÚ) č. 910/2014 a Korigendum

[4] SD Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu, pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf

[5] ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, pozri http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/

[6] ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, pozri http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/

Zoznam použitých pojmov

adresárové služby	Špecializovaná databáza, v ktorej sú zverejňované certifikáty a zoznamy zrušených certifikátov.
certifikačná autorita	Dôveryhodná autorita, ktorá generuje certifikáty a zoznamy zrušených certifikátov (komponent infraštruktúry PKI). Kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných certifikátov podľa nariadenia (EÚ) č. 910/2014. Rec. ITU-T X.509 [2] - 3.5.16 certification authority (CA): An authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the subjects' keys.
certifikačné služby	Služby, ktoré poskytuje certifikačná autorita (registrácia, vydávanie certifikátu, overenie platnosti a funkčnosti certifikátu, zrušenie certifikátu, výmena kľúčov…).
certifikačná politika	Pomenovaný zoznam pravidiel, ktoré označujú použiteľnosť certifikátu v príslušnej skupine alebo triede aplikácií zdieľajúcej spoločné bezpečnostné požiadavky. Rec. ITU-T X.509 [2] - 3.5.10 certificate policy: A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate the applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
vydávanie certifikátu	Proces, počas ktorého certifikačná autorita vydá certifikát na základe štandardizovanej žiadosti k príslušnému preverenému verejnému kľúču a preverenej identite subjektu.
certifikát	Reťazec údajov, ktorý spája identifikátor (Distinguished Name) subjektu s verejným kľúčom subjektu pomocou digitálneho podpisu. Formát tohto reťazca údajov je definovaný v Rec. ITU-T X.509 alebo ISO/IEC 9594-8. Tento reťazec údajov taktiež obsahuje identifikátor vydavateľa certifikátu, špecifické sériové číslo certifikátu, dobu platnosti a ďalšie údaje. Rec. ITU-T X.509 [2] - 3.5.53 public-key certificate (PKC): The public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it.
certifikát na správu	Certifikát slúžiaci na overenie platnosti kvalifikovaného certifikátu – certifikát úradu, certifikát akreditovanej certifikačnej autority, certifikát časovej pečiatky, certifikát na overenie potvrdenia existencie a platnosti certifikátov (OCSP) a certifikát na overenie zoznamu zrušených certifikátov.
digitálny podpis	Digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient Pozri Recommendation ITU-T X.800 alebo ISO/IEC 7498-2 Rec. ITU-T X.509 [2] - 6.1 Digital signatures
HSM	Kryptografický modul hardvérovej ochrany kľúča umožňujúci vykonávať kryptografické operácie.

infraštruktúra PKI	Technické a programové vybavenie použité na zaistenie poskytovania certifikačných služieb.
KCA	Koreňová certifikačná autorita Národného bezpečnostného úradu.
kľúčový pár	Dvojica asymetrických kľúčov, ktorá pozostáva zo súkromného a verejného kľúča.
kompromitácia súkromného kľúča	Zneužitie, použitie alebo sprístupnenie súkromného kľúča bez vedomia jeho vlastníka, ako aj prezradenie hesla na prístup k revokačnému heslu. Ak certifikačná autorita zistí kompromitáciu súkromného kľúča, certifikát zviazaný s týmto kľúčom zruší.
nariadenie (EÚ) č. 910/2014	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
obnova kľúčov	Obnova kľúčov v kontexte tohto dokumentu znamená vydanie nového certifikátu s rovnakými alebo veľmi podobnými charakteristikami ako pôvodný (obnovovaný) certifikát. Generuje sa nová dvojica kľúčov prislúchajúca k certifikátu.
pravidlá na výkon certifikačných činností	Zoznam predpisov a praktík, ktoré certifikačné autority používajú pri vydávaní certifikátov.
registračná autorita	Komponent infraštruktúry PKI používaný na posúvanie schválených žiadostí o vydanie certifikátu do certifikačnej autority. Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates mainly. This service includes proof of possession of non-CA generated subject private keys. Pozri IETF RFC 3647 [1] a Rec. ITU-T X.509 [2]
schéma dohľadu	Schému dohľadu kvalifikovaných dôveryhodných služieb definuje orgán dohľadu (NBÚ), pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf
spoliehajúca sa strana	Subjekt alebo komponent, ktorý požaduje od PKI infraštruktúry overenie stavu certifikátu. Rec. ITU-T X.509 [2] -3.5.55 relying party: A user or agent that relies on the data in a certificate in making decisions.
súkromný kľúč	Súkromná časť dvojice asymetrických kľúčov, ktorá sa používa na podpisovanie a (alebo) zašifrovanie správ.
verejný kľúč	Verejná časť dvojice asymetrických kľúčov, ktorá sa používa na overovanie a (alebo) odšifrovanie správ.
zrušenie certifikátu	Predčasné ukončenie platnosti certifikátu. Platnosť certifikátu nie je možné obnoviť.
zoznam zrušených certifikátov	Zoznam všetkých zrušených certifikátov vydaných CA.

Skratky

C	krajina *(Country)*
CA	certifikačná autorita *(Certification Authority)*
CMLC	životný cyklus správy certifikátu *(Certificate Management Life Cycle)*
CN	bežné meno *(Common Name)*
CP	certifikačná politika *(Certificate Policy)*
CPS	pravidlá na výkon certifikačných činností *(Certification Practice Statement)*
CRL	zoznam zrušených certifikátov *(Certificate Revocation List)*
CSE	Certificate Signing Event
DN	rozlišovacie meno *(Distinguished Name)*
eIDAS	Nariadenie (EÚ) č. 910/2014 [3]
eQCP	ETSI certifikačné politiky QCP-n-qscd, QCP-l-qscd, QCP-n, QCP-l, QCP-w
ETSI	Európsky inštitút pre telekomunikačné štandardy (European Telecommunications Standards Institute)
ESI	elektronické podpisy a infraštruktúra (Electronic Signatures and Infrastructures)
EÚ	Európska únia *(European Union)*
FIPS	federálne štandardy pre informačné procesy (Federal Information Processing Standards)
HSM	kryptografický modul hardvérovej ochrany kľúča *(Hardware Security Module)*
HTTP	hypertextový protokol prenosu (Hypertext Transfer Protocol)
IČO	identifikačné číslo organizácie
IDC	číslo identifikačnej karty
IEC	medzinárodná elektrotechnická komisia (International Electrotechnical Commission)
ISO	medzinárodná organizácia pre štandardy (International Organization for Standardization)
KCA	koreňová certifikačná autorita
KCA1	koreňová certifikačná autorita 1
KCA2	prvý následník koreňovej certifikačnej autority, druhá verzia koreňovej certifikačnej autority
KCA3	druhý následník koreňovej certifikačnej autority, tretia verzia koreňovej certifikačnej autority
L	lokalita *(Locality)*

LDAP	protokol pre prístup k adresárovým službám *(Lightweight Directory Access Protocol)*
NBÚ	Národný bezpečnostný úrad
NTR	Identifikačné číslo organizácie
O	Názov organizácie *(Organization)*
OID	objektový identifikátor *(Object Identifier Descriptor)*
OU	organizačná jednotka *(Organizational Unit)*
PKCS	šifrovacie štandardy verejného kľúča (Public Key Cryptography Standards)
PKI	infraštruktúra verejného kľúča *(Public Key Infrastructure)*
PNO	osobné číslo
QCA	kvalifikovaný poskytovateľ dôveryhodných služieb vydávajúci kvalifikované certifikáty, ktorému kvalifikovaný štatút udelil Národný bezpečnostný úrad
QCP	kvalifikovaná certifikačná politika *(Qualified Certificate Policy)*
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman algoritmus
SD	Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu (NBÚ), pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf
SHA	bezpečný hašovací algoritmus (Secure Hash Algorithm)
SK	Slovensko *(Slovakia)*
SR	Slovenská republika *(Slovak Republic)*
QSCD	Zariadenia na vyhotovenie kvalifikovaných elektronických podpisov/pečatí *(Qualified electronic signature/seal creation devices)*
SW TWS	softvér pre dôveryhodné systémy (Software for Trustworthy System)
TS	technická špecifikácia *(Technical Specification)*
TSL	dôveryhodný zoznam *(Trusted List)*
V	verzia *(Version)*
VAT	daňové identifikačné číslo
Z. z.	zbierka zákonov

1. Úvod

1.1 Účel certifikačnej politiky

Táto certifikačná politika, angl. Certificate Policy (ďalej len „CP“) upravuje metodiku, záväzné postupy a povinnosti Národného bezpečnostného úradu (ďalej len „NBÚ“ alebo „úrad“) pre vydávanie a správu certifikátov verejných kľúčov (ďalej len „certifikáty“) koreňovej certifikačnej autority (ďalej len „KCA“).

Táto CP zároveň profiluje aj certifikačné politiky, použité pri vydávaní a zrušovaní certifikátov na správu a kvalifikovaných certifikátov kvalifikovaných poskytovateľov dôveryhodných služieb vydávajúcich kvalifikované certifikáty (ďalej len „QCA“), ktorým kvalifikovaný štatút udelil úrad v súlade s platnými právnymi predpismi Slovenskej republiky (ďalej len „SR“). Napríklad, ak je použitá ETSI ESI certifikačná politika pre vydanie kvalifikovaných certifikátov s objektovým identifikátorom (ďalej len „OID“) 0.4.0.194112.1.2 (QCP-n-qscd) z dokumentu ETSI EN 319 411-2 pre vydávanie kvalifikovaných certifikátov, tak podľa slovenskej legislatívy je zakázané pozastavenie platnosti certifikátu, pričom politika identifikovaná s OID 0.4.0.194112.1.2 to umožňuje, a preto aj pri použití požiadaviek certifikačnej politiky OID 0.4.0.194112.1.2 v certifikačnej politike definovanej v tomto dokumente, nebude povolené pozastavenie platnosti certifikátu.

CP je záväzným dokumentom slúžiacim ako štandard zásad, procedúr a postupov, ktoré musia dodržiavať všetky zúčastnené strany a zjednodušuje identifikáciu certifikátov vydávaných v súlade s platnými právnymi predpismi SR.

Body v tejto CP po kapitolu 10 špecifikujú požiadavky pre KCA.

Od kapitoly 10 táto CP špecifikuje požiadavky pre QCA, ktorej úrad udelil kvalifikovaný štatút pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov podľa nariadenia (EÚ) č. 910/2014.

1.2 Identifikácia CP

CP identifikuje certifikáty KCA, certifikáty na správu a kvalifikované certifikáty vydané QCA, ktorým kvalifikovaný štatút udelil úrad.

OID tejto CP má tvar:

1.3.158.36061701.0.0.0.1.2.2

kde jednotlivé zložky OID majú nasledovný význam:

1	ISO
3	ISO Identified Organization
158	Slovakia
36061701	jedinečný identifikátor NBÚ (IČO)
0	riaditeľ NBÚ
0	útvar NBÚ
0	KCA
1	dokumentácia KCA
2	certifikačné politiky
2	Certifikačná politika identifikujúca certifikáty KCA, certifikáty na správu a kvalifikované certifikáty vydaná QCA, ktorej kvalifikovaný štatút udelil úrad.

1.3 Charakteristika, použitie a subjekty pracujúce s certifikátmi

1.3.1 *Charakteristika certifikátov*

Certifikát KCA je self-signed certifikát, ktorý KCA vydáva na vlastný verejný kľúč, ktorého digitálny podpis je vyhotovený súkromným kľúčom, ktorý je súčasťou toho istého kľúčového páru ako verejný kľúč certifikátu, a ktorého vlastníkom (držiteľom) je NBÚ.

Kvalifikované certifikáty sa vydávajú podľa pravidiel uvedených v kapitole 10.

1.3.2 *Kľúče KCA*

Na zabezpečenie certifikačných služieb používa KCA kľúčové páry RSA o minimálnej dĺžke modulusu 2048 bitov.

1.3.3 *Použitie certifikátov*

Certifikáty KCA môžu byť použité na:

a) overovanie platnosti certifikátov QCA,

b) overovanie platnosti certifikátov na správu KCA,

c) overovanie platnosti zoznamov zrušených certifikátov (ďalej len „CRL“) vydávaných KCA.

Certifikáty na správu vydávané QCA môžu byť použité na:

a) overovanie platnosti kvalifikovaných certifikátov – kvalifikovaných certifikátov pre elektronický podpis / pečať a kvalifikovaných certifikátov pre autentifikáciu webových sídiel,

b) overovanie certifikátov na správu (napr. certifikát časovej pečiatky, OCSP odpovede),

c) overovanie platnosti zoznamov CRL vydávaných QCA.

Akékoľvek iné použitie certifikátov KCA a certifikátov na správu sa považuje za neoprávnené použitie certifikátov.

1.3.3.1 Dôležité obmedzenia certifikátov požadované v tejto CP

a) Certifikáty na správu a kvalifikované certifikáty, ktoré vytvárajú certifikačnú cestu v strome dôvery KCA, alebo certifikáty vydávané dôveryhodnou službou, ktorej kvalifikovaný štatút udelil úrad, musia obsahovať v rozšírení *certificatePolicies* objektový identifikátor tejto CP (1.3.158.3606.1701.0.0.0.1.2.2).

b) Žiadne certifikáty vytvárajúce certifikačnú cestu v strome dôvery KCA nesmú okrem self-signed certifikátov obsahovať v rozšírení *certificatePolicies* objektový identifikátor anyPolicy (2.5.29.32.0).

c) Certifikát sa nesmie nachádzať v stave pozastavenia platnosti, teda v stavoch certificateHold a removeFromCRL.

d) Čas zrušenia certifikátu v zozname zrušených certifikátov nesmie byť pred časom, po ktorom bol vydaný iný zoznam zrušených certifikátov (položka *thisUpdate*), podľa ktorého bol certifikát platný.

e) Ak kvalifikovaný certifikát deklaruje v rozšírení *QCStatements* OID (1.3.6.1.5.5.7.1.3) pomocou položky QcSSCD/QcQSCD OID (0.4.0.1862.1.4), že súkromný kľúč prislúchajúci k verejnému kľúču, na ktorý bol vydaný kvalifikovaný certifikát sa nachádza na zariadení na vyhotovenie kvalifikovaných elektronických podpisov (QSCD), postupuje sa podľa požiadaviek v kapitole 10 a toto zariadenie musí byť certifikované NBÚ, alebo zverejnené v zozname podľa článku 31 ods. 2 nariadenia (EÚ) č. 910/2014.

1.3.3.2 Špecifikácie formátu, obsahu a použitia certifikátov KCA, certifikátov na správu a kvalifikovaných certifikátov

Certifikáty KCA, certifikáty na správu a kvalifikované certifikáty musia spĺňať požiadavky, ktoré definuje NBÚ v schéme dohľadu, pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf. NBÚ zverejňuje štandardy, ktoré podrobne definujú požiadavky na formáty certifikátov KCA, certifikátov na správu, kvalifikovaných certifikátov, zoznamov CRL a OCSP odpovedí.

Ak certifikát QCA vydal úrad, QCA musí pri vydávaní spĺňať požiadavky definované v dokumente NBÚ „Kontrola certifikačnej cesty“, ktorý popisuje vytvorenie a overenie certifikačnej cesty a nachádza sa na webovom sídle úradu.

1.3.4 Subjekty pracujúce s certifikátom KCA

1.3.4.1 Koreňová certifikačná autorita (KCA)

Koreňovou certifikačnou autoritou (KCA) sa v rámci tejto CP rozumie koreňová certifikačná autorita zriadená a prevádzkovaná NBÚ podľa ustanovení národnej legislatívy.

1.3.4.2 Registračná autorita KCA

Služby registračnej autority KCA v zmysle tejto CP vykonáva NBÚ.

1.3.4.3 Správca adresárov KCA

Správcom adresárov KCA v zmysle tejto CP je NBÚ.

1.3.4.4 Držiteľ certifikátu KCA

Držiteľom certifikátu KCA je NBÚ.

1.3.4.5 Používatelia certifikátu KCA (Relying Party)

Používateľmi certifikátu KCA sú:

a) QCA,

b) klienti QCA,

c) držitelia špecifických certifikátov na správu vydávaných KCA (napr. na podpisovanie / pečatenie dôveryhodných zoznamov).

1.3.4.6 Druhy certifikátov vydávané KCA

KCA vydáva nasledovné druhy certifikátov na správu:

a) certifikát vlastného verejného kľúča,

b) certifikáty následníkov KCA,

c) krížové certifikáty KCA a následníka KCA vydávané v rámci procesu výmeny kľúčov KCA,

d) certifikáty pre QCA,

e) špecifické certifikáty na správu: certifikáty obslužného personálu KCA (operátori KCA) a certifikáty pre podpisovanie schválených podpisových politík a dôveryhodných zoznamov.

1.4 Kontaktné informácie KCA

1.4.1 Špecifikácia administrátorskej organizácie

Táto CP je spravovaná NBÚ.

1.4.2 Kontaktná adresa

Národný bezpečnostný úrad
Budatínska 30
P.O.BOX 16
850 07 Bratislava 57
Slovenská republika

http://ep.nbusr.sk

1.4.3 Kontaktná osoba

Všetky otázky, pripomienky a návrhy k tejto CP posielajte na adresu:

bezpečnostný správca KCA
Národný bezpečnostný úrad
P.O.BOX 16
850 07 Bratislava 57
Slovenská republika

Telefón: +421 2/ 6869 2014 (útvar spravujúci túto CP)
+421 903 993 167 (prevádzka KCA)

Fax: +421 2/ 6869 1710

E-mail: podatelna@nbu.gov.sk
secadmin@nbu.gov.sk

2. Všeobecné ustanovenia

2.1 Povinnosti jednotlivých subjektov

2.1.1 Povinnosti KCA

KCA ako vydavateľ certifikátu vlastného verejného kľúča je povinná:

a) zaistiť kontrolu vlastníctva a správneho priradenia súkromného kľúča z príslušného kľúčového páru k verejnému kľúču,

b) zabezpečiť správnosť všetkých informácií v tele certifikátu a ich súlad s jeho certifikačným profilom,

c) potvrdiť vlastníctvo a správne priradenie súkromného a verejného kľúča, ako aj správnosť informácií obsiahnutých v tele certifikátu vydaním certifikátu verejného kľúča,

d) včas zverejniť informácie o novo vydanom certifikáte,

e) včas informovať používateľov o pripravovanej zmene kľúčov a certifikátov,

f) zverejnením certifikátu (resp. jeho charakteristík) viacerými prostriedkami vytvoriť podmienky na bezpečné overenie platnosti a správnosti certifikátu.

2.1.2 Povinnosti držiteľa certifikátu KCA

KCA je povinná:

a) používať súkromný kľúč prislúchajúci k certifikátu KCA iba na účely, na ktoré bol určený,

b) zaobchádzať so svojím súkromným kľúčom s náležitou starostlivosťou tak, aby nemohlo dôjsť k jeho zneužitiu,

c) neodkladne zrušiť certifikát KCA ak zistí, že došlo k neoprávnenému použitiu jeho súkromného kľúča, alebo ak hrozí neoprávnené použitie jeho súkromného kľúča,

d) dodržiavať všetky podmienky a obmedzenia týkajúce sa používania súkromných kľúčov a certifikátov.

2.1.3 Povinnosti používateľa certifikátov

Používateľ (spoliehajúca sa strana) certifikátu je povinný používať certifikát KCA, certifikáty na správu a kvalifikované certifikáty v súlade s ustanoveniami definovanými v bode 1.3.3 tejto CP.

2.1.4 Povinnosti správcov adresárov

Správca adresárov je povinný zabezpečiť:

a) včasné a presné publikovanie certifikátov,

b) včasné a presné publikovanie zoznamov CRL.

2.2 Právne záruky

Právne záruky a obmedzenia záruk v rámci tejto CP vyplývajú z platných právnych predpisov SR.

2.3 Finančná zodpovednosť KCA

V rámci tejto CP nie je stanovená žiadna finančná zodpovednosť.

2.4 Rozhodcovské konanie a riešenie sporov

Spory, ktoré sa týkajú používania certifikátov KCA, sa riešia v zmysle platných právnych predpisov SR.

2.5 Zverejňovanie informácií KCA

KCA zverejňuje:

a) túto CP,
b) CPS KCA,
c) certifikáty vydané KCA (okrem certifikátov obslužného personálu KCA),
d) aktuálne zoznamy CRL vydávané KCA,
e) archív zoznamov CRL vydaných KCA,
f) informácie o stave certifikátov vydaných KCA,
g) formulár žiadosti o vydanie certifikátu pre QCA,
h) formulár žiadosti o zrušenie certifikátu pre QCA.

2.5.1 Zverejňovanie dokumentácie KCA

Verejne prístupná dokumentácia KCA je zverejnená elektronicky na nasledujúcej internetovej stránke: http://ep.nbusr.sk/kca/index.html

V listinnej podobe je dokumentácia k dispozícií na NBÚ.

2.5.2 Zverejňovanie certifikátov KCA

KCA zverejňuje nasledovné typy vydaných certifikátov:

a) certifikát vlastného verejného kľúča KCA,
b) certifikáty následníkov KCA,
c) krížové certifikáty KCA a následníka KCA vydávané počas procesu výmeny kľúčov KCA (ak sú vydané),
d) certifikáty vydané pre QCA,
e) certifikáty pre podpisovanie slovenského TSL a schválených podpisových politík.

Tieto informácie sú verejne prístupné nasledovnými spôsobmi:

a) na nasledujúcich internetových stránkach

http://ep.nbusr.sk/kca/certifikat.html

http://ep.nbusr.sk/kca/zoznam_certifikatov.html

b) v listinnej podobe na NBÚ,

c) v dennej tlači – platí pre certifikáty KCA a certifikáty následníkov KCA,

d) certifikát vlastného verejného kľúča KCA (KCA1) je dostupný prostredníctvom adresárových služieb na adrese:

ldap://ep.nbusr.sk/cn=Korenova CA pre kvalifikovane certifikaty 1,l=Bratislava,ou=Sekcia elektronickeho podpisu,o=Narodny bezpecnostny urad,c=sk?caCertificate;binary

e) certifikát vlastného verejného kľúča následníka KCA (KCA2) je dostupný prostredníctvom adresárových služieb na adrese:

ldap://ep.nbusr.sk/cn=KCA NBU SR,ou=Sekcia IBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?caCertificate;binary

f) certifikát vlastného verejného kľúča druhého následníka KCA (KCA3) je dostupný prostredníctvom adresárových služieb na adrese:

ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?caCertificate;binary

KCA aktualizuje zoznam vydaných certifikátov pri každom vydaní nového certifikátu podliehajúcemu zverejňovaniu.

2.5.3 Zverejňovanie zoznamov zrušených certifikátov KCA

KCA publikuje zoznamy CRL nasledovne:

KCA1

Prehľad zrušených certifikátov (HTTP): http://ep.nbusr.sk/kca/crl1.html

Archív CRL (HTTP):	http://ep.nbusr.sk/kca/archive
Archív CRL (LDAP):	ldap://ep.nbusr.sk/ou=crls,ou=Sekcia elektronickeho podpisu,o=Narodny bezpecnostny urad,c=sk?cRLDistributionPoint?sub?

KCA2

Prehľad zrušených certifikátov (HTTP): http://ep.nbusr.sk/kca/crl2.html

Aktuálne CRL (HTTP):	http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl
Aktuálne CRL (LDAP)	ldap://ep.nbusr.sk/cn=KCA NBU SR,ou=Sekcia IBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList

Archív CRL (HTTP):	http://ep.nbusr.sk/kca/archive2
Archív CRL (LDAP):	ldap://ep.nbusr.sk/ou=arch crls KCA2,ou=Sekcia IBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?cRLDistributionPoint?sub?

KCA3

Prehľad zrušených certifikátov (HTTP): http://ep.nbusr.sk/kca/crl3.html

Aktuálne CRL (HTTP):	http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl
Aktuálne CRL (LDAP)	ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList
Archív CRL (HTTP):	http://ep.nbusr.sk/kca/archive3
Archív CRL (LDAP):	ldap://ep.nbusr.sk/ou=arch crls KCA3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?cRLDistributionPoint?sub?

2.5.4 Periodicita publikovania informácií KCA

Zoznamy CRL vydávané KCA sa vydávajú a zverejňujú minimálne raz za 24 hodín.

Zároveň musí byť zabezpečené, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, ktorý obsahuje číslo zrušeného certifikátu, neuplynulo viac ako 24 hodín.

Ostatné informácie sú zverejňované staticky a aktualizované iba v prípade zmeny.

2.6 Audit zhody

Táto CP sa riadi platnými právnymi predpismi SR.

2.7 Dôvernosť

Táto CP sa riadi platnými právnymi predpismi SR.

2.8 Ochrana práv duševného vlastníctva

Táto CP sa riadi platnými právnymi predpismi SR.

3. Identifikácia a autentifikácia

3.1 Menná konvencia

3.1.1 Certifikáty KCA

3.1.1.1 Menná konvencia pre KCA

KCA1 (self-signed)

Rozlišovacie meno, angl. Distinguished Name (ďalej len „DN“) vydavateľa certifikátu:

Common Name:	Korenova CA pre kvalifikovane certifikaty 1
Locality:	Bratislava
Organizational Unit:	Sekcia elektronického podpisu
Organization:	Narodny bezpecnostny urad
Country:	SK

DN držiteľa certifikátu:

Common Name:	Korenova CA pre kvalifikovane certifikaty 1
Locality:	Bratislava
Organizational Unit:	Sekcia elektronického podpisu
Organization:	Narodny bezpecnostny urad
Country:	SK

KCA2 (self-signed)

DN vydavateľa certifikátu:

Common Name:	KCA NBU SR
Organizational Unit:	Sekcia IBEP
Organization:	Narodny bezpecnostny urad
Locality:	Bratislava
Country:	SK

DN držiteľa certifikátu:

Common Name:	KCA NBU SR
Organizational Unit:	Sekcia IBEP
Organization:	Narodny bezpecnostny urad
Locality:	Bratislava
Country:	SK

KCA3 (self-signed)

DN vydavateľa certifikátu:

Common Name:	KCA NBU SR 3
Organizational Unit:	SIBEP
Organization:	Narodny bezpecnostny urad
Locality:	Bratislava
Country:	SK

DN držiteľa certifikátu:

Common Name:	KCA NBU SR 3
Organizational Unit:	SIBEP
Organization:	Narodny bezpecnostny urad
Locality:	Bratislava
Country:	SK

3.1.1.2 Pravidlá na zabezpečenie jednoznačnosti mien KCA

Jednoznačnosť mena KCA je zabezpečená povinnosťou KCA zvoliť pre každú verziu (inkarnáciu) KCA odlišné DN.

3.1.1.3 Riešenie sporov týkajúcich sa mien KCA

V rámci tejto CP nemôže dôjsť ku kolízii mien, a teda riešenie sporov nemá zmysel.

3.1.2 Certifikáty na správu

Menná konvencia certifikátov na správu musí byť navrhovaná KCA a QCA tak, aby jednoznačne identifikovala držiteľa certifikátu.

V certifikátoch na správu musí byť uvedený identifikátor CP 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 na správu vydaných QCA, ktorým kvalifikovaný štatút udelil NBÚ.

3.1.3 Kvalifikované certifikáty

Pravidlá mennej konvencie kvalifikovaných certifikátov sú uvedené v schéme dohľadu kvalifikovaných dôveryhodných služieb (ktorú definuje orgán dohľadu NBÚ, pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf) v tabuľke T1 v riadku T1.I,III,IV(b), T1.I(c), T1.III(c) a T1.IV(c) a v časti "SD článku 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014 - nepovinné dodatočné osobitné atribúty".

Na základe SD musí byť v kvalifikovaných certifikátoch uvedený identifikátor certifikačnej politiky 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 na správu vydanými QCA, ktorým kvalifikovaný štatút udelil NBÚ.

Kvalifikovaný certifikát spája identitu vlastníka súkromného kľúča s verejným kľúčom slúžiacim na overenie jeho podpisov / pečatí, 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.

Kvalifikovaný certifikát musí obsahovať minimálne údaje podľa tabuľky T1 SD a doplňujúci identifikátor podľa "SD článku 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014 - nepovinné dodatočné osobitné atribúty".

3.2 Iniciálna registrácia

3.2.1 Koreňová certifikačná autorita KCA

Iniciálna registrácia KCA sa vykonáva v procese formálneho založenia KCA v procedúre jej vytvárania. Na autentifikáciu KCA v procese iniciálnej registrácie slúži národná legislatíva a rozhodnutie riaditeľa príslušného útvaru NBÚ o zriadení KCA.

3.2.2 Následník KCA

Iniciálna registrácia následníka KCA sa vykonáva v procese formálneho zriadenia následníka KCA v procedúre jeho vytvárania. Na autentifikáciu následníka KCA v procese iniciálnej registrácie slúži národná legislatíva a rozhodnutie riaditeľa príslušného útvaru NBÚ o zriadení následníka KCA.

3.3 Spôsob preukázania vlastníctva súkromného kľúča KCA

Preukazovanie vlastníctva súkromného kľúča KCA prislúchajúceho k verejnému kľúču uvedenému v žiadosti o certifikát je dané internými predpismi KCA.

3.4 Vydanie následného certifikátu KCA

Pri vydávaní následného certifikátu KCA musí dôjsť ku generovaniu nového kľúčového materiálu a nového self-signed certifikátu.

3.5 Vydanie následného certifikátu po zrušení certifikátu KCA

Pri vydávaní následného certifikátu KCA po zrušení certifikátu KCA musí dôjsť ku generovaniu nového kľúčového materiálu a nového certifikátu KCA.

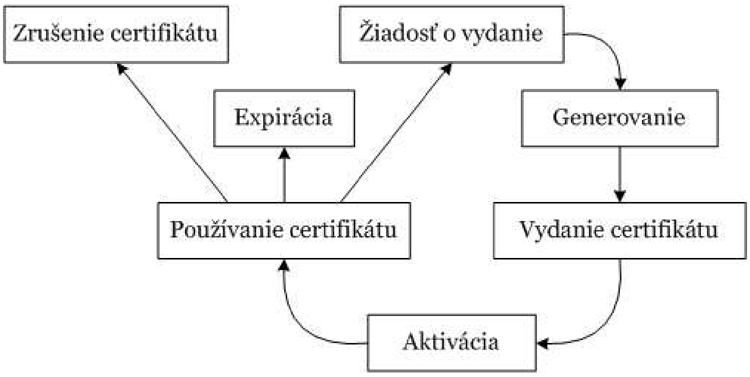
3.6 Žiadosť o zrušenie certifikátu KCA

Žiadosť o zrušenie certifikátu vlastného verejného kľúča KCA môže podať KCA alebo oprávnená tretia strana. Formálna žiadosť musí byť podaná písomnou formou a musí byť podpísaná osobami oprávnenými na podanie žiadosti o zrušenie, aby sa predišlo neautorizovanému zrušeniu certifikátu, a aby boli naplnené ustanovenia národnej legislatívy.

Žiadosť musí obsahovať najmä dátum a čas podania žiadosti, dôvod žiadosti a identifikáciu osoby alebo organizácie, ktorá žiadosť podala.

4. Prevádzkové postupy

V tejto kapitole je popísaný životný cyklus certifikátu označovaný aj ako Certificate Management Life Cycle (CMLC). Životný cyklus certifikátu pozostáva z primárnych a sekundárnych stavov. Každý vydaný certifikát prechádza všetkými primárnymi stavmi, zatiaľ čo sekundárne stavy sú výnimočné.



Primárnymi stavmi sú:

a) žiadosť o vydanie certifikátu,

b) generovanie certifikátu,

c) vydanie certifikátu,

d) aktivácia,

e) používanie,

f) expirácia,

g) archivácia.

Sekundárnym stavom životného cyklu správy certifikátu je zrušenie certifikátu.

4.1 Generovanie kľúčov

4.1.1 Generovanie kľúčov KCA

Kľúčový pár KCA (súkromný a verejný kľúč KCA) určený na vydávanie a overovanie certifikátov sa generuje na technologických prostriedkoch KCA pri zaistení požadovanej bezpečnosti generovania. Procedúra je sledovaná komisiou podľa postupu popísaného v bode 4.3 tejto CP. Ochrana kľúčov KCA je riešená podľa ustanovení bodu 6.2 tejto CP. Vydanie certifikátu KCA sa vykonáva ihneď po vygenerovaní kľúčového páru.

4.1.2 Generovanie podpisových kľúčov pre kvalifikované certifikáty

Kľúčový pár prislúchajúci ku kvalifikovanému certifikátu musí byť generovaný výhradne na technickom zariadení označovanom ako zariadenia na vyhotovenie kvalifikovaných elektronických podpisov, resp. zariadenia na vyhotovenie kvalifikovaných elektronických pečatí, ktoré musia byť certifikované NBÚ alebo zverejnené v zozname podľa článku 31 ods. 2 nariadenia (EÚ) č. 910/2014. Bezpečný produkt nesmie umožňovať export súkromného kľúča alebo nekontrolované použitie súkromného kľúča. Operácie so súkromným kľúčom musia byť výhradne pod kontrolou vlastníka bezpečného produktu.

4.2 Žiadosť o vydanie certifikátu KCA

Žiadosť o vydanie certifikátu KCA podáva z formálnych dôvodov prevádzkovateľ KCA sám sebe v písomnej forme. S ohľadom na charakter certifikátu a postup pri certifikácii KCA, nie je potrebná elektronická žiadosť o vydanie certifikátu vo formáte PKCS#10.

4.3 Vydanie certifikátu KCA

Certifikát KCA je vydaný podľa postupu označovaného ako Certificate Signing Event (CSE). V rámci tohto postupu sú vyžadované minimálne nasledovné osoby ako svedkovia:

a) bezpečnostný správca KCA,

b) interný audítor KCA,

c) jeden príslušník alebo zamestnanec NBÚ.

Svedkovia musia podpísať svedecké potvrdenie, v ktorom potvrdzujú generovanie certifikátu a skutočnosť, že certifikát zodpovedá štruktúre definovanej v príslušnej dokumentácii KCA.

Po zadaní certifikačných informácií do SW TWS aplikácie používanej v KCA sa vygeneruje kľúčový pár KCA a certifikát KCA.

Po vydaní certifikátu KCA zverejní NBÚ certifikát KCA podľa bodu 2.5.2 tejto CP.

Vydanie certifikátu následníka KCA prebieha rovnakým spôsobom ako vydanie certifikátu KCA.

Počas výmeny kľúčov KCA môžu byť vydané vzájomné krížové certifikáty používaného verejného kľúča KCA a verejného kľúča následníka KCA.

Po vydaní certifikátu následníka KCA, prípadne krížových certifikátov verejného kľúča KCA a verejného kľúča následníka KCA, NBÚ zverejní certifikáty podľa bodu 2.5.2 tejto CP.

4.4 Prevzatie certifikátu KCA

V rámci tejto CP sa za prevzatie certifikátu považuje podpísanie protokolu o generovaní certifikátu svedkami.

4.5 Zrušenie certifikátu KCA

4.5.1 Okolnosti na zrušenie

KCA zruší certifikát vlastného verejného kľúča v prípade:

a) ak súkromný kľúč patriaci k verejnému kľúču uvedeného v certifikáte bol ukradnutý, stratený, pozmenený alebo inak kompromitovaný,

b) úmyselného zneužitia kľúčov a certifikátov autorizovanou osobou,

c) podstatného a závažného porušenia prevádzkových požiadaviek identifikovaných v tejto CP a príslušnom CPS,

d) ak zrušenie certifikátu nariadila oprávnená tretia strana (súd),

e) ak KCA ukončila svoju činnosť.

4.5.2 Oprávnení žiadatelia o zrušenie certifikátu

O zrušenie certifikátu KCA môže požiadať:

a) KCA,

b) oprávnená tretia strana (súd).

4.5.3 Postup pri zrušení certifikátu

Proces zrušenia certifikátu je iniciovaný prijatím žiadosti o zrušenie certifikátu obsahujúcej všetky potrebné náležitosti. Na zachovanie integrity v rámci stromu dôvery KCA je kľúčové bezodkladné overenie a spracovanie požiadavky na zrušenie certifikátu. Procedúra zrušenia certifikátu je podrobne popísaná v CPS KCA.

4.5.4 Interval na zrušenie certifikátu

Interval na zrušenie certifikátu je maximálne 24 hodín.

4.5.5 Periodicita publikovania zoznamu CRL

Zoznamy CRL sa vydávajú a zverejňujú minimálne raz za 24 hodín.

Zároveň musí byť zabezpečené, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, ktorý obsahuje jeho číslo neuplynulo viac ako 24 hodín.

4.5.6 Zisťovanie stavu certifikátov

Stav certifikátov vydaných KCA je možné zisťovať:

a) na základe zoznamov CRL (bod 2.5.3 tejto CP),

b) z informácií uverejnených na internetovej stránke (bod 2.5.3 tejto CP).

4.5.7 Iné možnosti informovania o zrušení certifikátov

Informácie o zrušení certifikátov kľúča KCA budú prístupné na NBÚ a zverejnené v dennej tlači.

4.6 Audit bezpečnosti poskytovania certifikačných činností KCA

Postupy a procedúry pri vydávaní a zrušovaní certifikátov na KCA sú podrobované pravidelnému internému a externému auditu bezpečnosti poskytovania certifikačných činností. Podrobný popis spôsobu vykonávania auditu bezpečnosti je definovaný v CPS.

4.7 Archivácia záznamov KCA

Záznamy vznikajúce pri certifikačných činnostiach spojených s certifikátmi KCA sa archivujú po dobu najmenej 10 rokov. Rozsah archivovaných údajov je stanovený v CPS.

4.8 Výmena kľúčov KCA

Výmena kľúčov KCA sa realizuje ako úplná výmena kľúčov pozostávajúca z generovania nového kľúčového páru následníka KCA a vydania nového certifikátu následníka KCA. Počas procesu výmeny vlastného kľúčového páru môže KCA vydať krížové certifikáty KCA a následníka KCA. Tieto certifikáty je možné použiť na vzájomné overenie certifikátov KCA a následníka KCA.

Prevádzkové a bezpečnostné procedúry zmeny kľúčov sú navrhnuté tak, aby minimalizovali riziká pri tejto operácii a zabezpečovali minimalizáciu prerušenia poskytovania certifikačných služieb KCA.

Zmena kľúčov musí byť plánovaná (mimo riešenia havarijných situácií). Požiadavka na zmenu kľúčov musí byť riešená formálnou žiadosťou o vydanie certifikátu v súlade s bodom 4.2 tejto CP.

Plánovaná zmena kľúčov KCA musí byť oznámená dva mesiace vopred všetkým akreditovaným CA a uznaným zahraničným CA.

4.9 Havarijný plán KCA

Výnimočné stavy KCA sú riešené v súlade s havarijným plánom KCA vypracovaným na riešenie havarijných situácií s cieľom aktívne predchádzať havarijným situáciám, minimalizovať prerušenie poskytovania certifikačných služieb KCA a minimalizovať ostatné škody vzniknuté prípadnou havarijnou situáciou.

4.10 Ukončenie činnosti KCA

Činnosť KCA sa zakladá na ustanoveniach národnej legislatívy. Činnosť KCA môže byť ukončená iba zmenou alebo zrušením v zákone o dôveryhodných službách alebo inou zákonnou úpravou. Zákonná úprava, ktorá ukončí činnosť KCA, stanoví aj spôsob ukončenia činnosti.

5. Fyzické procedurálne a personálne bezpečnostné opatrenia KCA

5.1 Opatrenia na zaistenie fyzickej bezpečnosti

Opatrenia na zaistenie fyzickej bezpečnosti KCA sú v súlade s vyhláškou NBÚ č. 336/2004 Z. z. o fyzickej a objektovej bezpečnosti v znení vyhlášky NBÚ č. 315/2006 Z. z.

5.2 Opatrenia na zaistenie procedurálnej bezpečnosti

Na zaistenie procedurálnej bezpečnosti sú vypracované bezpečnostné smernice KCA pokrývajúce jednotlivé procedúry, činnosti a postupy pri výkone certifikačných činností. Výkon jednotlivých bezpečnostne kritických procedúr zabezpečujú pracovníci zaradení do identifikovaných rolí definovaných na základe bezpečnostných požiadaviek a technologických podmienok používaného systému KCA. Na zaistenie požadovaného stupňa bezpečnosti certifikačných služieb KCA je stanovený systém kontroly vykonávania jednotlivých procesov a procedúr (vedenie prevádzkových záznamov, pravidlo štyroch očí a podobne).

5.3 Opatrenia na zaistenie personálnej bezpečnosti

Personál KCA je preverovaný v zmysle vyhlášky Vyhláška 134/2016 Z. z. Národného bezpečnostného úradu o personálnej bezpečnosti.

Personál KCA má kvalifikáciu potrebnú na zabezpečovanie certifikačných činností KCA.

Každý príslušník personálu KCA má jednoznačne stanovenú bezpečnostnú rolu zahrnutú v popise jeho pracovnej náplne.

Personál je pravidelne preškoľovaný a preverovaný v oblasti bezpečnosti, znalosti oprávnení svojich rolí a technologických zručností potrebných na poskytovanie certifikačných služieb KCA.

6. Technické bezpečnostné opatrenia

6.1 Opatrenia na zaistenie bezpečnej prevádzky KCA

Jadro systému KCA je komponované ako samostatná entita, komunikačne izolovaná od zvyšku systému. Zvyšné časti systému sú rozdelené do viacerých celkov, ktoré si navzájom vymieňajú údaje špeciálnym, na tento účel navrhnutým spôsobom zaručujúcim plnú kontrolu nad prenášanými informáciami. Prenos údajov medzi jadrom a zvyšnými časťami systému KCA sa uskutočňuje na prenosných médiách. Komunikácia, ktorá prebieha po vnútornej sieti medzi jednotlivými komponentmi systému KCA je chránená šifrovaním.

Prvky oddelenia sieťovej komunikácie vymedzujú spôsob vzájomnej komunikácie komponentov systému.

Integrita citlivých údajov používaných v KCA je chránená využitím mechanizmov digitálneho podpisu. Na zabezpečenie integrity systému slúži systém zálohovania údajov, ktorý chráni dôležité údaje proti strate alebo poškodeniu v prípade technickej poruchy systému.

Najdôležitejšie komponenty systému KCA sú zdvojené alebo zálohované formou studenej zálohy.

Na ochranu pred preniknutím škodlivých infiltrácií sa vykonáva antivírová kontrola informácií a to hlavne informácií vstupujúcich do systému KCA z vonkajšieho prostredia.

Dostupnosť k on-line službám KCA a k informáciám KCA zverejňovaným formou internetových stránok je zaistená redundantným pripojením technologických prvkov KCA k internetu.

6.2 Kryptografické prostriedky ochrany kľúčov KCA

Kľúče KCA sú generované a uchovávané v kryptografickom module hardvérovej ochrany kľúča (ďalej len „HSM“) certifikovanom NBÚ alebo zverejnené v zozname podľa článku 31 ods. 2 nariadenia (EÚ) č. 910/2014.

HSM KCA má zabudované preverené algoritmy na generovanie náhodných čísel.

HSM KCA vyhovuje bezpečnostným požiadavkám podľa FIPS-140-2 Bezpečnostné požiadavky na kryptografické moduly na úrovni 3.

Na zaistenie riadenia logického prístupu k aktívam uchovávaným v HSM poskytuje modul možnosť chrániť aktíva pomocou aktivačných údajov (PIN) a obmedziť používanie aktív podmienkou kontroly výkonu viacerými používateľmi.

HSM KCA dovoľuje zabezpečiť kľúče KCA proti možnosti ich čítania alebo exportu v nezašifrovanej podobe. Má zabudovanú ochranu proti pokusom o vniknutie, ktorá chráni uchovávaný kryptografický materiál pred možnosťou násilnej kompromitácie.

7. Profily certifikátov a zoznamov zrušených certifikátov

7.1 Profil certifikátu KCA (KCA1)

Haš certifikátu KCA (KCA1) je nasledovný:

<u>SHA1:</u> A6D7D70982CB73BE7FA69470029E7EF9360EEA68

<u>SHA256:</u> 6FBF021174831BE8B5889C9077F7BD6C385B5541B759E2F096D7D3BDBF774CDB

V nasledujúcej tabuľke je uvedený profil certifikátu KCA (KCA1).

Pole	**Kritickosť**	**Obsah**
Version		v3
serialNumber		01
signatureAlgorithm		sha1withRSAEncryption (1.2.840.113549.1.1.5)
issuer		CN=Korenova CA pre kvalifikovane certifikaty 1 L=Bratislava OU=Sekcia elektronickeho podpisu O=Narodny bezpecnostny urad C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
validity		040114163833Z UTC 060114155622Z UTC
subject		CN=Korenova CA pre kvalifikovane certifikaty 1 L=Bratislava OU=Sekcia elektronickeho podpisu O=Narodny bezpecnostny urad C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (2048 bits) 30 82 01 0a 02 82 01 01 00 eb 28 d7 38 ed 1d 7f b7 c5 b2 76 fa 0d 21 29 07 c3 30 ea c5 a4 cc 50 6d 65 8b 09 47 3e f0 25 d9 ca 8b 38 95 b4 61 4c fe 21 25 6b 48 5b 71 21 f0 27 e1 71 5d ae cf cf 71 31 67 17 16 f4 45 60 75 7d f6 71 b2 66 66 32 0f 04 ad c2 38 c6 42 0e 03 3e a1 fe 76 e8 02 0c 7a 04 d4 b7 6b c8 d7 32 41 cc 60 95 77 1f 5f fa cd 13 76 7a fe 69 62 b5 ac bb b5 b2 c1 c1 37 1e 62 4a 93 6f c1 6a 7c 17 cb c1 b1 76 2a ce 74 e9 3d e6 82 03 64 8d 0b 14 c9 4f ce 7a 16 da b5 f2 8a 83 0a 84 07 12 c8 30 2e d0 c0 58 13 4b 65 d0 9c b9 e2 93 ac d0 8e aa 36 de f9 36 77 00 e2 d7 9a d8 a3 a9 f1 2d 98 3a 99 51 e3 46 52 39 6e e1 5c ef 99 9f ed 29 29 6a 96 45 02 e3 07 16 21 ed eb b1 b1 63 31 38 4b 75 6b 13 f6 2c 80 54 9e e2 f9 26 47 c4 86 be 47 ef 8d 0d 19 95 ad c8 d1 95 62 0e b2 54 09 a3 e5 58 f3 02 03 01 00 01
subjectKeyIdentifier (SHA1)		**30 f4 a8 71 ce 72 9f 99 b4 29 ba f9 03 b1 41 10 5f 24 dc 99**
basicConstraints	**Critical**	Subject Type=CA Path Length Constraint=3

certificatePolicies	**Critical**	[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Tento certifikat je vydany ako kvalifikovany certifikat "Korenovej CA pre kvalifikovane certifikaty 1" v sulade so zakonom c. 215/2002 Z. z.. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_1.pdf
keyUsage	**Critical**	keyCertSign, cRLSign

Tab. 7.1a Profil certifikátu KCA (KCA1)

7.2 Profil certifikátu nástupníka KCA (KCA2)

Haš certifikátu nástupníka KCA (KCA2) je nasledovný:

SHA1: 4EA3F1135F43A4D521973DAA1FBEB3CDF2DCF75A

SHA256: E17E8EC51F376C0371B45BBEB5BD8416584A9E8A44B51E7CA1AE0E36731CCE0F

V nasledujúcej tabuľke je uvedený profil certifikátu nástupníka KCA (KCA2).

Pole	Kritickosť	Obsah
version		v3
serialNumber		01
signatureAlgorithm		sha1withRSAEncryption (1.2.840.113549.1.1.5)
issuer		CN=KCA NBU SR OU=Sekcia IBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
validity		050222161337Z UTC 150222154357Z UTC
subject		CN=KCA NBU SR OU=Sekcia IBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (2048 bits) 30 82 01 0a 02 82 01 01 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 10 3b d4 39 eb 61 d6 1a a4 65 78 fe 63 88 91 b8 de f1 98 e0 67 58 e0 af 18 63 ab 29 ec 83 c3 e9 1a b3 d9 13 27 93 9c 5f 90 d0 54 2c 96 34 94 8c cb ef 05 62 82 eb ad a3 b6 b9 85 2e 54 1b fc 2b 3b ae 51 22 24 60 c6 85 3a ea c8 c9 a5 9d a9 f4 df 9c 0b 9d e5 35 67 f0 e1 d2 1f 3b 5c 9f fb 21 bd 9c 19 7d f6 b8 86 7e 70 59 0d 3a a4 03 13 cd b6 88 46 5c 84 34 34 c3 50 e6 31 b4 3f 7c 9d d8 e1 02 03 01 00 01
certificatePolicies		[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Certifikat je vydany ako kvalifikovany certifikat KCA NBU SR v sulade s platnymi pravnymi predpismi SR. [1,2]Policy Qualifier Info:

		Policy Qualifier Id=CPS Qualifier: http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf [2]Certificate Policy: Policy Identifier=0.4.0.1862.1.1
cRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl
subjectKeyIdentifier (SHA1)		**06 da 89 e7 d3 8e 53 3a 79 77 e9 eb f9 a6 b6 32 65 3f 46 24**
basicConstraints	**Critical**	Subject Type=CA Path Length Constraint=None
keyUsage	**Critical**	keyCertSign, cRLSign

Tab. 7.2a Profil certifikátu následníka KCA (KCA2)

7.3 Profil certifikátu druhého následníka KCA (KCA3)

Haš certifikátu druhého následníka KCA (KCA3) je nasledovný:

SHA1: 21F73B27BBBF2811BBEAB4F1799E7DD892F3FE85

SHA256: D83477E0388C40BA092FECA484A5EBD3AD3028BF60220132E95158C00DDCE98F

V nasledujúcej tabuľke je uvedený profil certifikátu druhého následníka KCA (KCA3).

Pole	Kritickosť	Obsah
Version		v3
serialNumber		01
signatureAlgorithm		sha256withRSAEncryption (1.2.840.113549.1.1.11)
issuer		CN=KCA NBU SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
validity		091106095939Z UTC 251106072909Z UTC
subject		CN=KCA NBU SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (4096 bits) 30 82 02 0a 02 82 02 01 00 db aa d0 8f 2f 4a 97 12 d5 b9 eb 7d 59 dc 83 5c 8b 31 17 f2 e5 6e 5e ce 2c d2 c5 27 dc 67 ea b3 8e f0 d7 05 21 97 d2 94 0d 54 49 b1 1f 2b ed e4 30 9c 8d 60 93 72 16 2f 0e 19 0a b7 be ff 7f c9 18 c9 e4 40 11 cd 59 67 b3 84 4e 84 8f e7 c4 46 a1 bb 81 13 e1 5c 55 bb 23 b9 87 47 e6 c8 98 86 74 5c 09 20 fc c5 53 15 d8 77 66 7e bb 63 a9 2d b3 4b ca 78 f8 1c 6f 64 d8 22 ba a7 94 c1 d0 25 f3 8f 83 14 af ba db 5c 5d 2c 57 e2 77 89 0c 1c 15 22 68 97 c0 b8 80 69 67 f7 00 b8 73 30 b8 e2 31 d6 7d 95 12 bd 0d ef 2b d8 6b 48 16 c9 27 76 d8 2d 95 7f 45 ac 0a bd 1e 12 91 60 f1 9c 58 8e b6 2e ee 8d 42 eb 5a 97 e4 82 20 a8 d9 30 d5 e0 d4 86 b1 a1 9e 5c 42 33 a0 14 a1 61 1b 69 a6 26 c7 8e 6b 8b c8 5c 19 9a f8 20 63 6f ee c7 e1 15 c2 de 9b 82 b9 5f b5 02 e9 39 11 76 ad 34 00 76 dd 74 3b 26 4d b8 c4 69 86 42 ae 0f 08 1d d4 48 4a e2 f5 bd 5e e6 cb 35 b0 42 0c 14 61 1c 6f 1d a7 b5 63 fd 63 88 54 93 ee 40 a4 77 d4 ed a7 82 73 62 57 82 2d 14 b7 d5 4d 4e a1 e7 8f c8 80 de 16 0c 83 3b d8 09 3b e7 25 48 9e 4a 94 6e ad 6e 61 e1 c8 df be 70 21 55 11 d5 e2 e4 5b 51 6e b1 3f b0 31 8b d5 02 96 4a 83 fd 06 5f a9 4d 2d 19 a9 40 e3 85 bf b8 8f 5d aa 0e e1 84 8d ef ad 4f 90 72 5f e6 a2 55 c9 84 bc 74 23 3f 79 ca 40 4d 12 91 fd 17 dd 25 23 66 1d c3 c7 79 af 14 f9 9a f9 bf ed 1f f4 39 16 27 fc f0 cc b0 16 35 d5 37 e0 2e 2c d4 b0 66 2c 0e ae 18 01 9f 8f cb 9e b1 0f b9 19 12 82 0d c6 70 50 0d 7d e5 72 cd da 8d 09 62 77 ab f5 96 39 2f e0 c1 4e 08 db c6 87 31 7b 2e 79 aa fb 04 a9 68 62 24 ed 0a c2 48 30 33 ff ed 1e 23 b9 5b 14 bf 45 6e a4 d6 db 35 e8 e3 02 03 01 00 01

certificatePolicies		[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://ep.nbusr.sk/kca/doc/kca_cps.pdf
cRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList; [3]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap:///cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;
subjectInfoAccess		URL=http://ep.nbusr.sk/kca/certs/kca3/kcanbusr3.p7c URL=ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary URL=ldap:///cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary
subjectKeyIdentifier (SHA1)		**7f f1 3d 21 c2 97 5a 2e 97 07 0e b1 69 83 25 fd 21 86 3e 07**
basicConstraints	**Critical**	Subject Type=CA Path Length Constraint=None
keyUsage	**Critical**	keyCertSign, cRLSign

Tab. 7.3a Profil certifikátu druhého následníka KCA (KCA3)

7.4 Profil krížového certifikátu vydaného KCA1 pre KCA2

Haš krížového certifikátu vydaného KCA1 pre KCA2 je nasledovný:

<u>SHA1:</u> F03FFB2B949CB98DBF746659A1337DAA8427DE92

<u>SHA256:</u> 7F7953F8ADDD9C9939CB4E272162455A6643F73E40A4900C75288CB8269BB0FF

V nasledujúcej tabuľke je uvedený profil krížového certifikátu vydaného KCA1 pre KCA2.

Pole	Kritickosť	Obsah
Version		v3
serialNumber		213C
signatureAlgorithm		sha1withRSAEncryption (1.2.840.113549.1.1.5)
Issuer		CN=Korenova CA pre kvalifikovane certifikaty 1 L=Bratislava OU=Sekcia elektronickeho podpisu O=Narodny bezpecnostny urad C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
Validity		050222230000Z UTC 060114155622Z UTC
subject		CN=KCA NBU SR OU=Sekcia IBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (2048 bits) 30 82 01 0a 02 82 01 01 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 10 3b d4 39 eb 61 d6 1a a4 65 78 fe 63 88 91 b8 de f1 98 e0 67 58 e0 af 18 63 ab 29 ec 83 c3 e9 1a b3 d9 13 27 93 9c 5f 90 d0 54 2c 96 34 94 8c cb ef 05 62 82 eb ad a3 b6 b9 85 2e 54 1b fc 2b 3b ae 51 22 24 60 c6 85 3a ea c8 c9 a5 9d a9 f4 df 9c 0b 9d e5 35 67 f0 e1 d2 1f 3b 5c 9f fb 21 bd 9c 19 7d f6 b8 86 7e 70 59 0d 3a a4 03 13 cd b6 88 46 5c 84 34 34 c3 50 e6 31 b4 3f 7c 9d d8 e1 02 03 01 00 01
certificatePolicies		[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Certifikat je vydany ako krizovy (cross) certifikat pre naslednika KCA NBU SR v sulade s platnymi pravnymi predpismi SR.

		[1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf [2]Certificate Policy: Policy Identifier=0.4.0.1862.1.1
authorityInfoAccess		[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ep.nbusr.sk/kca/certs/kca/certifikat_der.cer
authorityKeyIdentifier (SHA1)		KeyID=30 f4 a8 71 ce 72 9f 99 b4 29 ba f9 03 b1 41 10 5f 24 dc 99
cRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ep.nbusr.sk/kca/crls/current_a.crl
subjectKeyIdentifier (SHA1)		06 da 89 e7 d3 8e 53 3a 79 77 e9 eb f9 a6 b6 32 65 3f 46 24
basicConstraints	**Critical**	Subject Type=CA Path Length Constraint=None
keyUsage	**Critical**	keyCertSign, cRLSign

Tab. 7.4a Profil krížového certifikátu vydaného KCA1 pre KCA2

7.5 Profil krížového certifikátu vydaného KCA2 pre KCA1

Haš krížového certifikátu vydaného KCA2 pre KCA1 je nasledovný:

SHA1: 4B28494356B78C09336B30FB8887BCBC17C130E2

SHA256: FC06ADEDA98C9A625720B3C1E7BF9491466A01345D7267817CC28BF138FDDB87

V nasledujúcej tabuľke je uvedený profil krížového certifikátu vydaného KCA2 pre KCA1.

Pole	Kritickosť	Obsah
version		v3
serialNumber		09
signatureAlgorithm		sha1withRSAEncryption (1.2.840.113549.1.1.5)
issuer		CN=KCA NBU SR OU=Sekcia IBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
validity		050222230000Z UTC 060114155621Z UTC
subject		CN=Korenova CA pre kvalifikovane certifikaty 1 L=Bratislava OU=Sekcia elektronickeho podpisu O=Narodny bezpecnostny urad C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (2048 bits) 30 82 01 0a 02 82 01 01 00 eb 28 d7 38 ed 1d 7f b7 c5 b2 76 fa 0d 21 29 07 c3 30 ea c5 a4 cc 50 6d 65 8b 09 47 3e f0 25 d9 ca 8b 38 95 b4 61 4c fe 21 25 6b 48 5b 71 21 f0 27 e1 71 5d ae cf cf 71 31 67 17 16 f4 45 60 75 7d f6 71 b2 66 66 32 0f 04 ad c2 38 c6 42 0e 03 3e a1 fe 76 e8 02 0c 7a 04 d4 b7 6b c8 d7 32 41 cc 60 95 77 1f 5f fa cd 13 76 7a fe 69 62 b5 ac bb b5 b2 c1 c1 37 1e 62 4a 93 6f c1 6a 7c 17 cb c1 b1 76 2a ce 74 e9 3d e6 82 03 64 8d 0b 14 c9 4f ce 7a 16 da b5 f2 8a 83 0a 84 07 12 c8 30 2e d0 c0 58 13 4b 65 d0 9c b9 e2 93 ac d0 8e aa 36 de f9 36 77 00 e2 d7 9a d8 a3 a9 f1 2d 98 3a 99 51 e3 46 52 39 6e e1 5c ef 99 9f ed 29 29 6a 96 45 02 e3 07 16 21 ed eb b1 b1 63 31 38 4b 75 6b 13 f6 2c 80 54 9e e2 f9 26 47 c4 86 be 47 ef 8d 0d 19 95 ad c8 d1 95 62 0e b2 54 09 a3 e5 58 f3 02 03 01 00 01
certificatePolicies		[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Certifikat je vydany ako krizovy (cross) certifikat pre Korenovu certifikacnu autoritu NBU SR v sulade s platnymi pravnymi predpismi SR.

		[1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf [2]Certificate Policy: Policy Identifier=0.4.0.1862.1.1
authorityInfoAccess		[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ep.nbusr.sk/kca/certs/kca2/kcanbusr2.cer
authorityKeyIdentifier (SHA1)		KeyID=06 da 89 e7 d3 8e 53 3a 79 77 e9 eb f9 a6 b6 32 65 3f 46 24
cRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl
subjectKeyIdentifier (SHA1)		30 f4 a8 71 ce 72 9f 99 b4 29 ba f9 03 b1 41 10 5f 24 dc 99
basicConstraints	**Critical**	Subject Type=CA Path Length Constraint=None
keyUsage	**Critical**	keyCertSign, cRLSign

Tab. 7.5a Profil krížového certifikátu vydaného KCA2 pre KCA1

7.6 Profil certifikátu QCA

V nasledujúcej tabuľke je uvedený profil certifikátu vydávaného KCA pre QCA.

Pole	Kritickosť	Obsah
version		v3
serialNumber		jednoznačné sériové číslo pridelené KCA
signatureAlgorithm		sha256withRSAEncryption (1.2.840.113549.1.1.11)
issuer		CN=KCA NBU SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
validity		začiatok platnosti certifikátu - (X) koniec platnosti certifikátu (X) + (N) rokov – koniec platnosti certifikátu QCA nesmie presiahnuť koniec platnosti certifikátu KCA
subject		Rozlišovacie meno (DN) QCA Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String. DN meno musí spĺňať podmienky uvedené v schéme dohľadu kvalifikovaných dôveryhodných služieb, ktorú definuje orgán dohľadu – NBÚ (pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf), v tabuľke T1 v riadku T1.I,III,IV(b).

subjectPublicKeyInfo		RSA (najmenej 2048 bits) verejný kľúč QCA
authorityInfoAccess		[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ep.nbusr.sk/kca/certs/kca3/kcanbusr3_p7c.p7c [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary
authorityKeyIdentifier (SHA1)		KeyID=7f f1 3d 21 c2 97 5a 2e 97 07 0e b1 69 83 25 fd 21 86 3e 07
cRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList; [3]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap:///cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;
subjectKeyIdentifier (SHA1)		haš verejného kľúča akreditovanej CA / uznanej zahraničnej CA
basicConstraints	**Critical**	Subject Type=CA Path Length Constraint=0
certificatePolicies	**Critical**	[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://ep.nbusr.sk/kca/doc/kca_cps.pdf
policyConstraints	**Critical**	Required Explicit Policy Skip Certs=0
keyUsage	**Critical**	keyCertSign, cRLSign

Tab. 7.6a Profil certifikátu akreditovanej CA / uznanej zahraničnej CA vydávaného KCA

7.7 Profil certifikátu pre pečatenie slovenského TSL a schválených podpisových politík vydávaného KCA

V nasledujúcej tabuľke je uvedený profil certifikátu vydávaného pre účely pečatenia slovenského TSL a schválených podpisových politík.

Pole	Kritickosť	Obsah
Version		v3
serialNumber		jednoznačné sériové číslo pridelené KCA
signatureAlgorithm		sha256withRSAEncryption (1.2.840.113549.1.1.11)
Issuer		CN=KCA NBU SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
Validity		začiatok platnosti certifikátu (X) koniec platnosti certifikátu (X) + 3 roky
Subject		serialNumber=NTRSK-36061701 CN=TL and Signature Policy List x OU=CIS Operation division O=NATIONAL SECURITY AUTHORITY L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (2048 bits) verejný kľúč podpisovateľa slovenského TSL a schválených podpisových politík
basicConstraints		Subject Type=End Entity Path Length Constraint=None
certificatePolicies		[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://ep.nbusr.sk/kca/doc/kca_cps.pdf [2]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.1.10.5.0.1
authorityInfoAccess		[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ep.nbusr.sk/kca/certs/kca3/kcanbusr3_p7c.p7c [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)

		Alternative Name: URL=ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary
subjectAltName		RFC822 Name=podatelna@nbusr.sk URL=http://…
extKeyUsage		tslSigning (0.4.0.2231.3.0)
authorityKeyIdentifier (SHA1)		KeyID=7f f1 3d 21 c2 97 5a 2e 97 07 0e b1 69 83 25 fd 21 86 3e 07
cRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList; [3]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap:///cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;
subjectKeyIdentifier (SHA1)		haš verejného kľúča podpisovateľa slovenského TSL a schválených podpisových politík
keyUsage	**Critical**	nonRepudiation

7.7a Profil certifikátu pre podpisovanie slovenského TSL a schválených podpisových politík vydávaného KCA

7.8 Profil kvalifikovaného certifikátu

Profil kvalifikovaného certifikátu je uvedený v kapitole 10.2 v odseku "**Kapitola 6.6.1 ETSI EN 319 411-2 V2.1.1 (Certificate Profile)"**

7.9 Profil zoznamu CRL vydávaného KCA

V nasledujúcej tabuľke je uvedený profil zoznamu CRL generovaného KCA.

Pole	**Kritickosť**	**Obsah**
Version		2
Signature algorithm		sha256withRSAEncryption (1.2.840.113549.1.1.11)
Issuer		CN=KCA NBU SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK
thisUpdate		(X)
nextUpdate		max. (X) + 4 hodiny + 72000 sekúnd
cRLNumber		jednoznačné číslo CRL pridelené KCA
authorityKeyIdentifier		KeyID=7f f1 3d 21 c2 97 5a 2e 97 07 0e b1 69 83 25 fd 21 86 3e 07

7.10a Profil zoznamu CRL vydávaného KCA

8. Administrácia špecifikácií

Táto CP je revidovaná ako celok raz za 12 mesiacov. Požiadavky na úpravy sa podávajú v podobe formálnej žiadosti na úpravu CP osobe poverenej bezpečnostným vedením KCA (kontakt je uvedený v bode 1.4.3 tejto CP). Všetky formálne podané požiadavky na zmeny posúdi NBÚ a rozhodne o ich realizácii.

Pred schválením zmien v nasledujúcej verzii CP upozorní NBÚ všetky QCA, ktorým vydal certifikát.

Upozornenie bude realizované písomnou formou a bude obsahovať súhrn navrhovaných zmien, konečný dátum na prijatie pripomienok a dátum, kedy zmeny vstúpia v platnosť. NBÚ môže požiadať QCA, aby upozornili svojich zákazníkov a informovali ich o zmenách v CP.

Perióda na prijatie pripomienok je 30 dní odo dňa odoslania upozornenia, pokiaľ nie je uvedené inak.

8.1 Identifikácia verzií

Verzie certifikačnej politiky sú identifikované dvojmiestnym číslom. Číslovaná verzia má označenie v tvare:

Verzia A.B

Zmeny textu CP, ktoré nemenia význam dokumentu (napr. opravy gramatických chýb, náhrada niektorých slov rovnako významovými slovami, zmena formátovania a pod.) alebo zmeny textu CP, ktoré menia význam dokumentu, ale nezasahujú do podstaty zverejňovaných zásad (napríklad zmena distribučných bodov a pod.) sa zachycujú v čísle verzie na pozícii B.

Podstatné zmeny certifikačnej politiky sa v čísle verzie odrážajú na pozícii A.

8.2 Schvaľovanie verzií

CP schvaľuje riaditeľ odboru akreditácie NBÚ.

9. Účinnosť certifikačnej politiky

CP nadobúda účinnosť dňom 1.11.2016.

10. Certifikačná politika kvalifikovaných certifikátov

Vzhľadom na nesúlad certifikačných politík (QCP-n-qscd, QCP-l-qscd, QCP-n, QCP-l, QCP-w) definovaných v ETSI EN 319 411-2 V2.1.1 (2016-02) (ďalej len "eQCP") s niektorými požiadavkami nariadenia (EÚ) č. 910/2014, nie je možné priamo uvádzať identifikátory eQCP v kvalifikovanom certifikáte, ale len OID CP 1.3.158.36061701.0.0.0.1.2.2, ktorý ich profiluje.

10.1 Identifikácia

Identifikácia CP kvalifikovaných certifikátov je na základe OID CP 1.3.158.36061701.0.0.0.1.2.2. OID CP je uvedený v rozšírení certifikátu *certificatePolicies* OID (2.5.29.32) (kapitola 8.1.1 a 8.2.2.6 Rec. ITU-T X.509). CP OID 1.3.158.36061701.0.0.0.1.2.2 profiluje eQCP s cieľom dosiahnuť súlad s požiadavkami nariadenia (EÚ) č. 910/2014 a s národnou legislatívou.

Ak v tomto dokumente nie je uvedené inak, plnia sa požiadavky z profilovanej eQCP.

OID identifikátory eQCP:

OID 0.4.0.194112.1.0 (QCP-n): the certificate policy for EU qualified certificates issued to natural persons,

OID 0.4.0.194112.1.1 (QCP-l): the certificate policy for EU qualified certificates issued to legal persons,

OID 0.4.0.194112.1.2 (QCP-n-qscd): the certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD,

OID 0.4.0.194112.1.3 (QCP-l-qscd): the certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD,

OID 0.4.0.194112.1.4 (QCP-w): the certificate policy for EU qualified web site authentication certificates.

10.2 Doplnené a upravené požiadavky certifikačných politík eQCP

Ďalej sa uvádzajú len tie kapitoly z ETSI EN 319 411-2 V2.1.1 (2016-02) a z neho odkazovaných dokumentov, ktoré sú doplnené alebo upravené.

Kapitola 4.2.5 ETSI EN 319 411-2 V2.1.1 (Certificate policy)

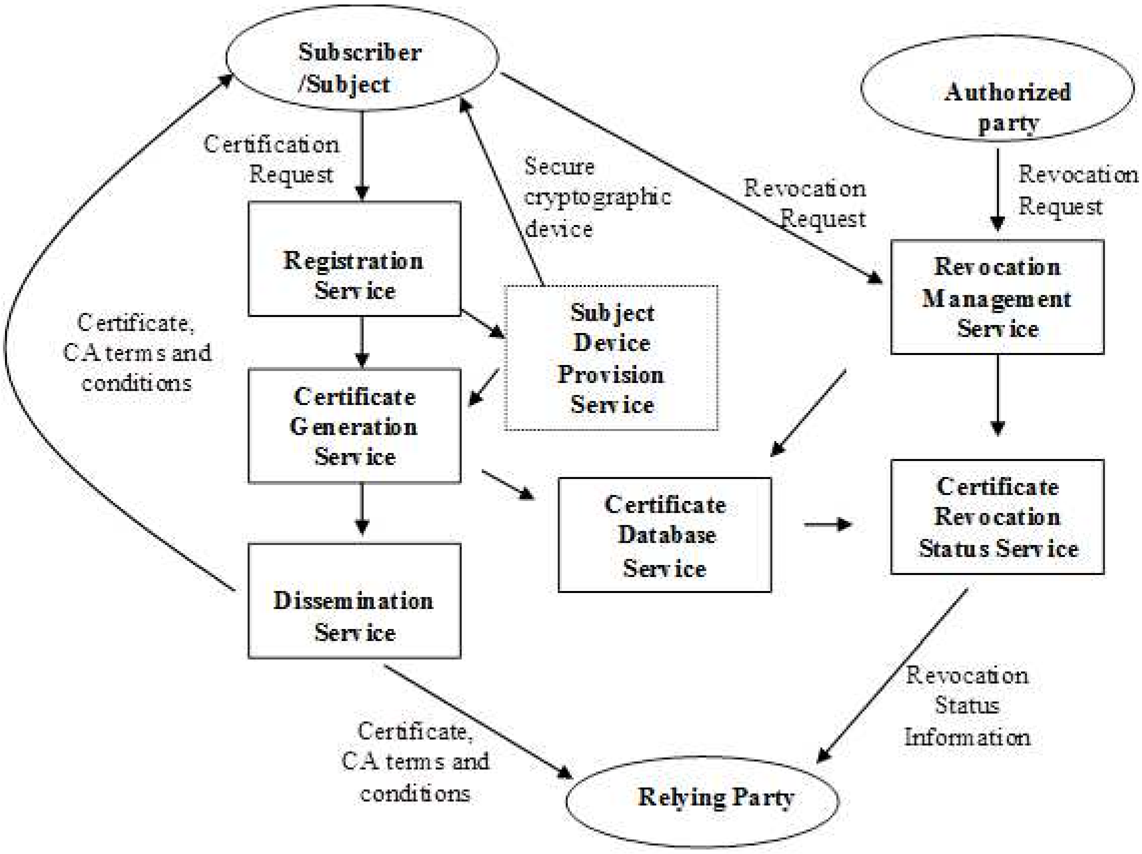
Identifikácia CP je definovaná v kapitole 10.1.

Jednotlivé typy certifikátov sa rozlišujú na základe podmienok uvedených v schéme dohľadu kvalifikovaných dôveryhodných služieb (ktorú definuje orgán dohľadu - NBÚ, pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf) v tabuľke T1 v riadku T1.I,III,IV(a).

Kapitola 4.4 ETSI EN 319 411-2 V2.1.1 (Certification services)

Na základe čl. 24 ods. 2 písm. k) nariadenia (EÚ) č. 910/2014, ktoré požaduje, aby kvalifikovaný poskytovateľ dôveryhodných služieb zriadil a aktualizoval databázu certifikátov, sa povinne prevádzkuje aj služba - **databáza certifikátov**. Databáza certifikátov obsahuje najmä vydané kvalifikované certifikáty a obsahuje aj informáciu vo forme CRL alebo OCSP odpovede, v ktorej bol buď certifikát zrušený, alebo ak počas platnosti certifikátu nedošlo k zrušeniu certifikátu a certifikát expiroval, tak potvrdenie vo forme CRL alebo OCSP odpovede, že certifikát bol počas celej doby platnosti platný, na základe CRL alebo OCSP odpovede obsahujúcej v položke *thisUpdate* hodnotu dátumu a času neskoršiu ako je dátum a čas expirovania kvalifikovaného certifikátu.

Databáza certifikátov slúži ako zdroj informácií pre vydávanie OCSP odpovedí, najmä po expirovaní kvalifikovaného certifikátu.



Kapitola 5.3 ETSI EN 319 411-2 V2.1.1 (Certificate Policy name and identification)

Identifikácia je na základe postupu uvedeného v kapitole 10.1.

Kapitola 6.2.2 ETSI EN 319 411-2 V2.1.1 (Initial Identity Validation)

Okrem požiadaviek uvedených v kapitole 6.2.2 ETSI EN 319 411-2 V2.1.1, sa musí postupovať podľa požiadaviek uvedených v schéme dohľadu v tabuľke T1 v riadku T1.I,III,IV(a) a podľa "SD článku 24 ods. 2 písm. d) nariadenia (EÚ) č. 910/2014".

Zodpovednosť za vydanie kvalifikovaného certifikátu, najmä za správnosť údajov uvedených v kvalifikovanom certifikáte v čase vydania kvalifikovaného certifikátu (čas je uvedený v položke *validity.notBefore* certifikátu) a za overenie, že osoba ktorej je kvalifikovaný certifikát vydaný, súhlasila s vydaním kvalifikovaného certifikátu, nie je možné preniesť na inú osobu a je len v zodpovednosti vydavateľa kvalifikovaného certifikátu (kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných certifikátov podľa nariadenia (EÚ) č. 910/2014).

Kapitola 6.3.10 ETSI EN 319 411-2 V2.1.1 (Certificate Status Services)

Hodnoty uvedené v CRL alebo v OCSP odpovedi musia splniť požiadavky podľa SD pre službu "kvalifikovaná dôveryhodná služba overenia (verification) kvalifikovaných certifikátov", obsahujúce najmä "SD článku 24 ods. 3 nariadenia (EÚ) č. 910/2014" a "SD článku 24 ods. 4 nariadenia (EÚ) č. 910/2014".

Platnosť certifikátu nesmie byť pozastavená podľa "SD článku 28 ods. 5 a čl. 38 ods. 5 nariadenia (EÚ) č. 910/2014".

Obmedzenia uvedené v kapitole 6.3.10 ETSI EN 319 411-2 V2.1.1 pre OCSP sú chybné. OCSP môže obsahovať informáciu aj o expirovanom certifikáte.

Postupuje sa podľa profilu v SD v tabuľke T1 v riadku T1.I,III(i)T1.IV(j) a podľa "SD - profil OCSP odpovede".

Kapitola 6.5.1 ETSI EN 319 411-2 V2.1.1 (Key Pair Generation and Installation)

Podľa písm. b) ods. i) kapitoly 6.5.1 ETSI EN 319 411-2 V2.1.1, sa jedná o splnenie ods. 3 prílohy II nariadenia (EÚ) č. 910/2014, kde generovať alebo spravovať údaje na vyhotovenie elektronického podpisu v mene podpisovateľa môže výhradne kvalifikovaný poskytovateľ dôveryhodných služieb – to znamená, len poskytovateľ dôveryhodných služieb, ktorý má aspoň jednu dôveryhodnú službu s kvalifikovaným štatútom.

Zodpovednosť za vygenerovanie kľúčového páru v QSCD alebo overenie, že kľúčový pár je uložený v QSCD, nie je možné preniesť na inú osobu a je len v zodpovednosti vydavateľa kvalifikovaného certifikátu (kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných certifikátov podľa nariadenia (EÚ) č. 910/2014).

Kapitola 6.6.1 ETSI EN 319 411-2 V2.1.1 (Certificate Profile)

Požiadavky uvedené v písm. a) v kapitole 6.6.1 ETSI EN 319 411-2 V2.1.1 sa menia z "musí" na "môže".

Podľa požiadaviek uvedených v písm. d) až h) v kapitole 6.6.1 ETSI EN 319 411-2 V2.1.1 musí certifikát obsahovať aspoň OID certifikačnej politiky 1.3.158.36061701.0.0.0.1.2.2 podľa kapitoly 10.1.

Musia byť splnené požiadavky uvedené v schéme dohľadu pre službu "kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných certifikátov" a najmä požiadaviek v tabuľke T1, ako nepovinné dodatočné osobitné atribúty sa použijú minimálne atribúty definované v "SD článku čl. 28 ods. 3 a čl. 38 ods. 3 nariadenia (EÚ) č. 910/2014 - nepovinné dodatočné osobitné atribúty".

Pri vydaní mandátnych certifikátov sa postupuje podľa "SD článku 28 ods. 3, čl. 38 ods. 3 a odôvodnenia 58 nariadenia (EÚ) č. 910/2014".

Požiadavky uvedené v druhej vete v kapitole 6.6.1 ETSI EN 319 411-1 V1.1.1 sa menia z "musí" na "môže".

Kapitola 6.6.2 ETSI EN 319 411-2 V2.1.1 (CRL Profile)

Musí sa postupovať podľa požiadaviek uvedených v schéme dohľadu v tabuľke T1 v riadku T1.I,III (i)T1.IV(j), podľa "SD článku 24 ods. 3 nariadenia (EÚ) č. 910/2014" a "SD článku 24 ods. 4 nariadenia (EÚ) č. 910/2014".

Kapitola 6.6.3 ETSI EN 319 411-2 V2.1.1 (OCSP Profile)

Musí sa postupovať podľa požiadaviek uvedených v schéme dohľadu pre službu "kvalifikovaná dôveryhodná služba overenia (verification) kvalifikovaných certifikátov", najmä podľa požiadaviek v SD v tabuľke T1 v riadku T1.I,III (i)T1.IV(j), podľa "SD článku 24 ods. 3 nariadenia (EÚ) č. 910/2014", "SD článku 24 ods. 4 nariadenia (EÚ) č. 910/2014" a podľa "SD - profil OCSP odpovede".

Kapitola 6.9.4 ETSI EN 319 411-2 V2.1.1 (Terms and conditions)

Požiadavky uvedené v písm. b) v kapitole 6.9.4 ETSI EN 319 411-2 V2.1.1 sa menia z "musí" na "môže".