Národný bezpečnostný úrad SR

Sekcia informačnej bezpečnosti a elektronického podpisu

Certifikačný poriadok pre koreňovú CA a akreditované CA vydávajúce kvalifikované certifikáty v súlade s platnými právnymi predpismi SR, najmä zákonom č. 215/2002 Z.z. o elektronickom podpise

Verzia: 2.1

Dokument nadobúda účinnosť dňom: 15. 6. 2009

Obsah

Zoznam použitých pojmov

Adresárové služby	Špecializovaná databáza, v ktorej sú publikované certifikáty a zoznamy zrušených certifikátov.
Aktivácia certifikátu	Aktivácia certifikátu sa vzťahuje na dáta, iné než kľúče, ktoré sú potrebné na prevádzkovanie kryptografických modulov (HSM moduly a smartkarty), a ktoré vyžadujú primeranú ochranu.
Certifikačná autorita *(CA)*	Dôveryhodná autorita, ktorá generuje certifikáty a zoznamy zrušených certifikátov (komponent infraštruktúry PKI).
Certifikačný poriadok *(CP)*	Pomenovaný zoznam pravidiel, ktoré označujú použiteľnosť certifikátu v príslušnej skupine alebo triede aplikácií, zdieľajúcimi spoločné bezpečnostné požiadavky.
Pravidlá na výkon certifikačných činností *(CPS)*	Zoznam predpisov a praktík, ktoré certifikačné autority používajú pri vydávaní certifikátov.
Certifikačné služby	Pojem je definovaný v zákone č. 215 / 2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
Certifikácia	Proces, počas ktorého certifikačná autorita na základe štandardizovanej žiadosti vydá k príslušnému verejnému kľúču certifikát.
Certifikát	Reťazec údajov, ktorý spája identifikátor (Distinguished Name) koncového subjektu s verejným kľúčom pomocou digitálneho podpisu. Formát tohto reťazca údajov je definovaný v ISO/IEC 9594-8. Tento reťazec údajov taktiež obsahuje identifikátor vydavateľa certifikátu, špecifické sériové číslo certifikátu, dobu platnosti a ďalšie údaje.
Digitálny podpis	Jedinečná digitálna identifikácia entity, ktorá sa využíva na autentifikáciu zdroja, integrity dát a nepopierateľnosť. Digitálny podpis využíva súkromný kľúč, ktorému zodpovedá príslušný verejný kľúč, matematickú funkciu známu ako „message digest“ a princípy asymetrickej kryptografie.
Infraštruktúra PKI	Technické a programové vybavenie použité na zaistenie služieb na vydávanie a správu certifikátov.
KCA	Koreňová certifikačná autorita Národného bezpečnostného úradu.
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.
Kryptografický modul	Hardvérové zariadenie umožňujúce vykonávať kryptografické operácie (napr. smartkarta, HSM modul).
KvCSR	Kvalifikovaný certifikát fyzickej osoby vydaný v súlade s platnými právnymi predpismi SR a vydaný v certifikačnej ceste s koreňovým certifikátom KCA NBÚ. Na identifikáciu KvCSR slúži certifikačný poriadok s OID identifikátorom 1.3.158.36061701.0.0.0.1.2.2
Obnova certifikátu *(Certificate Renewal)*	Obnova certifikátu v kontexte tohto dokumentu znamená vydanie nového certifikátu s veľmi podobnými charakteristikami ako pôvodný (obnovovaný) certifikát. Dvojica kľúčov prislúchajúcich k certifikátu sa v tomto prípade negeneruje nanovo, ale prevezme sa z pôvodného certifikátu.

Obnova kľúčov ***(Keys Renewal)***	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.
Odtlačok verejného kľúča ***(Fingerprint)***	Tzv. *haš* verejného kľúča. Haš je matematická funkcia, ktorá vytvára „skratku" dát (*message digest*). Z dát rôznej veľkosti vytvorí skrátenú správu fixnej veľkosti. Zo správy nie je možné spätne získať pôvodné dáta. Akákoľvek zmena vstupných dát sa preukáže tým, že sa vytvorí iný message digest.
Súkromný kľúč	Súkromná časť dvojice asymetrických kľúčov. Používa sa na podpisovanie a (alebo) dešifrovanie správ.
Registračná autorita	Komponent infraštruktúry PKI, používaný na posúvanie schválených žiadostí o vydanie certifikátu do certifikačnej autority.
Registračné miesto	Priestory úradu, v ktorých sa prijímajú a schvaľujú žiadosti o kvalifikované certifikáty. Registračné miesto obsluhuje registračný operátor.
Kľúčový pár	Dvojica asymetrických kľúčov, ktorá pozostáva z verejného a súkromného kľúča.
Spoliehajúca strana ***(Relying Party)***	Subjekt alebo komponent, ktorý požaduje od PKI infraštruktúry overenie stavu certifikátu.
Verejný kľúč	Verejná časť dvojice asymetrických kľúčov. Používa sa na šifrovanie a overovanie správ.
Zrušenie certifikátu ***(Certificate Revocation)***	Ukončenie platnosti certifikátu. Platnosť certifikátu nie je možné obnoviť.
Zoznam zrušených certifikátov	Zoznam certifikátov, ktorých platnosť bola zrušená. Zoznam môže mať formát CRL (zoznam všetkých zrušených neexpirovaných certifikátov vydaných CA) alebo OCSP(zoznam len požadovaných certifikátov).
Zoznam zrušených certifikátov certifikačných autorít ***(Authority Revocation List)***	Zoznam certifikátov verejných kľúčov certifikačných autorít (vrátane KCA), ktorých platnosť bola zrušená. Zoznam vydáva a podpisuje KCA. Zoznam je publikovaný v adresári LDAP.

Skratky

ARL	zoznam zrušených certifikátov certifikačných autorít *(Authority Revocation List)*
C	krajina *(Country)*
CA	certifikačná autorita *(Certification Authority)*
CMLC	životný cyklus správy certifikátu *(Certificate Management Life Cycle)*
CN	bežné meno (Common Name)
CP	certifikačný poriadok *(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)*
ETSI	European Telecommunications Standards Institute
HSM	kryptografický modul hardvérovej ochrany kľúča *(Hardware Security Module)*
HTTP	Hypertext Transfer Protocol
IBEP	sekcia informačnej bezpečnosti a elektronického podpisu
IČO	identifikačné číslo organizácie
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KCA	koreňová certifikačná autorita
KCA1	koreňová certifikačná autorita 1
KCA2	prvý následník koreňovej certifikačnej autority
KvCSR	kvalifikovaný certifikát fyzickej osoby
L	lokalita (Locality)
LDAP	protokol pre prístup k adresárovým službám *(Lightweight Directory Access Protocol)*
O	organizácia *(Organization)*
OCSP	Online Certificate Status Protocol
OID	objektový identifikátor *(Object Identifier Descriptor)*

OU	organizačná jednotka *(Organizational Unit)*
PKCS	Public Key Cryptography Standards
PKI	infraštruktúra verejného kľúča (Public Key Infrastructure)
QCP	kvalifikovaný certifikačný poriadok (Qualified Certificate Policy)
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SK	Slovensko (Slovakia)
SR	Slovenská republika *(Slovak Republic)*
SSCD	bezpečné zariadenie na vyhotovovanie elektronického podpisu *(Secure Signature Creation Device)*
SW TWS	Software for Trustworthy System
TS	technická špecifikácia *(Technical Specification)*
Z.z.	zbierka zákonov

1. Úvod

1.1 Účel certifikačného poriadku

Certifikačný poriadok (ďalej len „CP“) pre certifikáty koreňovej certifikačnej autority NBÚ, upravuje metodiku, záväzné postupy a povinnosti Národného bezpečnostného úradu (ďalej len „NBÚ“) pre vydávanie a správu certifikátov koreňovej certifikačnej autority NBÚ (ďalej len „KCA“).

Tento CP zároveň profiluje aj certifikačné poriadky, použité pri vydávaní a zrušovaní certifikátov na správu a kvalifikovaných certifikátov akreditovanými certifikačnými autoritami (ďalej len „akreditované CA“) a uznanými zahraničnými certifikačnými autoritami (ďalej len „uznané zahraničné CA“) v súlade s platnými právnymi predpismi Slovenskej republiky (ďalej len „SR“), najmä zákonom č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 215/2002 Z.z. o elektronickom podpise“). Napríklad, ak je použitá európska kvalifikovaná certifikačná politika s objektovým identifikátorom (ďalej len „OID“) 0.4.0.1456.1.1 (QCP Public + SSCD) z dokumentu ETSI TS 101 456 V1.3.1 pre vydávanie kvalifikovaného certifikátu fyzickej osoby alebo ETSI TS 102 023 V1.2.1, tak podľa slovenskej legislatívy je zakázané pozastavenie platnosti certifikátu, pričom politika identifikovaná s OID 0.4.0.1456.1.1 to umožňuje a preto aj pri použití politiky OID 0.4.0.1456.1.1 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.

Ak body v tomto CP špecifikujú požiadavky pre KCA, tak potom sa požiadavky pre dané body odsekov pre akreditované CA a uznané zahraničné CA prevezmú z vyhlášky NBÚ č. 133/2009 Z.z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností.

1.2 Identifikácia CP

Certifikačný poriadok identifikujúci certifikáty KCA, certifikáty na správu a kvalifikované certifikáty vydávané akreditovanými CA a uznanými zahraničnými CA spĺňajúce požiadavky platných právnych predpisov SR je identifikovaný pomocou OID odvodeným od OID NBÚ.

OID tohto 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 priradený organizáciou ISO (IČO)
0	vyhradené pre ďalšie použitie v NBÚ
0	vyhradené pre ďalšie použitie v NBÚ
0	vyhradené pre ďalšie použitie v NBÚ
1	KCA
2	Dokument „Certifikačný poriadok pre certifikáty KCA“
2	Certifikačný poriadok pre koreňovú CA a akreditované CA vydávajúce kvalifikované certifikáty v súlade s platnými právnymi predpismi SR, najmä zákonom č. 215/2002 Z.z. o elektronickom podpise

1.3 Charakteristika, použitie a subjekty pracujúce s certifikátmi

1.3.1 Charakteristika certifikátu

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

Certifikáty na správu a kvalifikované certifikáty, ktoré vytvárajú certifikačnú cestu v strome dôvery KCA, môžu byť vydané podľa vlastného CP, ale ich vydávanie je v pravidlách na výkon certifikačných činností (ďalej len „CPS“) profilované podľa požiadaviek tohto CP, ktoré musia byť dodržané.

Kvalifikované certifikáty fyzických osôb vydané podľa platných právnych predpisov SR sa budú v tomto CP ďalej označovať ako „KvCSR“.

1.3.2 Certifikačné kľúče KCA

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

1.3.3 Použitie certifikátu KCA, certifikátov na správu a KvCSR

Certifikáty KCA môžu byť použité na:

a) overovanie platnosti certifikátov akreditovaných CA,
b) overovanie platnosti certifikátov uznaných zahraničných CA,
c) overovanie platnosti certifikátov na správu KCA,
d) overovanie platnosti zoznamov zrušených certifikátov akreditovaných CA,
e) overovanie platnosti zoznamov zrušených certifikátov uznaných zahraničných CA,
f) overovanie platnosti zoznamov zrušených certifikátov na správu KCA.

Certifikáty na správu vydávané akreditovanými CA a uznanými zahraničnými CA môžu byť použité na:

a) overovanie platnosti certifikátov na správu a KvCSR,
b) overenie platnosti zoznamov zrušených certifikátov,
c) overovanie platnosti nepriamych zoznamov zrušených certifikátov (aj v on-line režime),
d) overenie platnosti časových pečiatok.

KvCSR môžu byť použité na overovanie platnosti zaručených elektronických podpisov.

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

1.3.3.1 Dôležité obmedzenia certifikátov KCA, certifikátov na správu a KvCSR požadované v tomto CP

1) Certifikát sa nesmie nachádzať v stave pozastavenia platnosti, teda v stavoch certificateHold a removeFromCRL.
2) Čas zrušenia certifikátu v zozname zrušených certifikátov nesmie byť pred časom, po ktorom bol vydaný iný zoznam zrušených certifikátov, podľa ktorého bol certifikát platný.
3) Súkromný kľúč prislúchajúci k verejnému kľúču, na ktorý bol KvCSR vydaný, sa musí nachádzať na bezpečnom zariadení na vyhotovovanie elektronického podpisu (SSCD), ktoré je certifikované NBÚ a nijakým spôsobom neumožňuje export súkromného kľúča zo SSCD. Za overenie SSCD zariadenia zodpovedá akreditovaná CA a uznaná zahraničná CA, a ak SSCD zariadenie fyzická osoba žiadajúca o KvCSR nevlastní, tak aj za jeho dodanie žiadateľovi o vydanie KvCSR.

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

Certifikáty KCA, certifikáty na správu a KvCSR musia spĺňať požiadavky, ktoré definuje NBÚ v štandardoch zverejnených na vlastných internetových stránkach. Dokumenty podrobne definujú požiadavky na formáty certifikátov KCA, certifikátov na správu, KvCSR, zoznamov zrušených certifikátov a rovnako i požiadavky na formáty zaručených elektronických podpisov, na ktorých vyhotovovanie sú KvCSR použité.

Podrobné informácie o formátoch, ktoré musia byť pri vydávaní certifikátov dodržané sa nachádzajú na nasledujúcej internetovej stránke:

http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html

Akreditované CA a uznané zahraničné CA musia pri vydávaní spĺňať požiadavky definované v dokumente NBÚ „Kontrola certifikačnej cesty“, ktorý popisuje vytvorenie a overenie certifikačnej cesty a nachádza sa na nasledujúcej internetovej stránke:

http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/legislativa/kontrola_cert_cesty.pdf

1.3.4 Subjekty pracujúce s certifikátom KCA

1.3.4.1 Koreňová certifikačná autorita (KCA)

Koreňovou certifikačnou autoritou (KCA) sa v rámci tohto CP rozumie koreňová certifikačná autorita zriadená a prevádzkovaná NBÚ podľa ustanovení zákona č. 215/2002 Z.z. o elektronickom podpise.

1.3.4.2 Registračná autorita KCA

Služby registračnej autority KCA v zmysle tohto CP vykonáva NBÚ.

1.3.4.3 Správca adresárov KCA

Správcom adresárov KCA v zmysle tohto CP je NBÚ.

1.3.4.4 Držiteľ certifikátu KCA

Držiteľom certifikátu KCA je NBÚ.

1.3.4.5 Používatelia certifikátu KCA

Používateľmi certifikátu KCA sú:

a) akreditované CA,

b) uznané zahraničné CA,

c) klienti akreditovaných CA a uznaných zahraničných CA.

1.3.4.6 Druhy certifikátov vydávaných KCA

KCA vydáva v zmysle § 5 a § 10 zákona č. 215/2002 Z.z. o elektronickom podpise nasledovné druhy certifikátov:

a) certifikát vlastného verejného kľúča,

b) certifikáty následníkov KCA,

c) krížové certifikáty KCA a následníka KCA počas procesu výmeny kľúčov KCA,

d) certifikáty pre akreditované CA,

e) certifikáty pre uznané zahraničné CA,

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

1.4 Kontaktné informácie KCA

1.4.1 Špecifikácia administrátorskej organizácie

Tento CP je spravovaný sekciou informačnej bezpečnosti a elektronického podpisu Národného bezpečnostného úradu.

1.4.2 Kontaktná adresa

Sekcia informačnej bezpečnosti a elektronického podpisu
Národný bezpečnostný úrad
Budatínska 30
P.O.BOX 16
850 07 Bratislava 57
Slovenská republika

http://www.nbusr.sk
http://ep.nbusr.sk

1.4.3 Kontaktná osoba

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

Bezpečnostný správca KCA
Sekcia informačnej bezpečnosti a elektronického podpisu
Národný bezpečnostný úrad
P.O.BOX 16
850 07 Bratislava 57
Slovenská republika

Telefón: +421 2/6869 2114 (sekretariát sekcie informačnej bezpečnosti a elektronického podpisu)
+421 903 993 167 (prevádzka KCA)

Fax: +421 2/6869 1701

E-mail: info@nbusr.sk
secadmin@nbusr.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

Podľa zákona č. 215/2002 Z.z. o elektronickom podpise je KCA 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 certifikátu

Používateľ (spoliehajúca sa strana) certifikátu je povinní používať certifikát KCA, certifikáty na správu a KvCSR v súlade ustanoveniami definovanými v bode 1.3.3 tohto CP.

2.1.4 Povinnosti správcov adresárov

Správca adresárov je povinný zabezpečiť:

a) včasné a presné publikovanie certifikátov,

b) včasné a presné publikovanie zoznamov zrušených certifikátov.

2.2 Právne záruky

Právne záruky a obmedzenia záruk v rámci tohto CP vyplývajú z platných právnych predpisov SR a ustanovení CPS.

2.3 Finančná zodpovednosť KCA

V rámci tohto 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) tento CP,

b) vydané certifikáty (okrem certifikátov obslužného personálu KCA),

c) aktuálne zoznamy zrušených certifikátov (CRL) a zoznamy zrušených certifikátov certifikačných autorít (ARL),

d) archív vydaných zoznamov zrušených certifikátov (CRL) a zoznamov zrušených certifikátov certifikačných autorít (ARL),

e) informácie o stave certifikátov,

f) žiadosť o vydanie certifikátu pre akreditované CA a uznané zahraničné CA,

g) žiadosť o zrušenie certifikátu pre akreditované CA a uznané zahraničné CA.

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 sekcii informačnej bezpečnosti a elektronického podpisu 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 počas procesu výmeny kľúčov KCA,

d) certifikáty vydané pre akreditované CA,

e) certifikáty vydané pre uznané zahraničné CA.

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 sekcii informačnej bezpečnosti a elektronického podpisu 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

KCA aktualizuje zoznam vydaných certifikátov pri každom vydaní nového certifikátu.

2.5.3 Zverejňovanie zoznamov zrušených certifikátov KCA

KCA publikuje zoznamy zrušených certifikátov (CRL) a zoznamy zrušených certifikátov (ARL) nasledovne:

KCA1

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

Archív CRL a ARL (HTTP): http://ep.nbusr.sk/kca/archive

Archív CRL a ARL (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.crl

Aktuálne CRL (HTTP): http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl

Aktuálne ARL (HTTP): http://ep.nbusr.sk/kca/crls2/kcanbusr2a.crl

Archív CRL a ARL (HTTP): http://ep.nbusr.sk/kca/archive

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

2.5.4 Periodicita publikovania informácií KCA

Zoznamy zrušených certifikátov (CRL) a zoznamy zrušených certifikátov certifikačných autorít (ARL) 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 jeho číslo neuplynulo viac ako 24 hodín – § 6 vyhlášky NBÚ 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).

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

2.6 Audit zhody

Tento CP sa riadi platnými právnymi predpismi SR.

2.7 Dôvernosť

Tento CP sa riadi platnými právnymi predpismi SR.

2.8 Ochrana práv duševného vlastníctva

Tento 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

Rozlišovacie meno (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

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

Krížový certifikát vydaný KCA1 pre KCA2

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

Krížový certifikát vydaný KCA2 pre KCA1

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

3.1.1.2 Pravidlá na zabezpečenie jednoznačnosti mien KCA

Jednoznačnosť mena KCA je zabezpečená jej postavením v systéme.

3.1.1.3 Riešenie sporov týkajúcich sa mien KCA

V rámci tohto CP nemôže dôjsť ku kolízií mien, a teda riešenie sporov nemá zmysel.

3.1.2 Certifikáty na správu

Menná konvencia certifikátov na správu je navrhovaná akreditovanou CA a uznanou zahraničnou CA tak, aby jednoznačne identifikovala držiteľa certifikátu.

3.1.3 Kvalifikované certifikáty fyzických osôb

KvCSR musí v rozlišovacom mene držiteľa obsahovať minimálne commonName a countryName a to tak, ako je definované v dokumente NBÚ „Formáty kvalifikovaných certifikátov“.

V zmysle § 5 zákona č. 215/2002 Z.z. o elektronickom podpise platí, že ak sa v styku s orgánmi verejnej moci alebo orgánmi verejnej správy používa zaručený elektronický podpis, kvalifikovaný certifikát musí byť vydaný akreditovanou CA alebo uznanou zahraničnou CA a musí obsahovať rodné číslo držiteľa certifikátu.

Rozlišovacie meno držiteľa certifikátu potom musí obsahovať aj položku serialNumber, v ktorej pre jednoznačnú identifikáciu osoby musí byť uvedené rodné číslo podľa pravidiel uvedených v dokumente NBÚ „Formáty kvalifikovaných certifikátov“, ktorý sa nachádza na nasledujúcej internetovej stránke:

http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/formats/formaty_qc.pdf

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 autentizáciu KCA v procese iniciálnej registrácie slúži zákon č. 215/2002 Z.z o elektronickom podpise a rozhodnutie riaditeľa sekcie informačnej bezpečnosti a elektronického podpisu 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 autentizáciu následníka KCA v procese iniciálnej registrácie slúži zákon č. 215/2002 Z.z o elektronickom podpise a rozhodnutie riaditeľa sekcie informačnej bezpečnosti a elektronického podpisu 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.

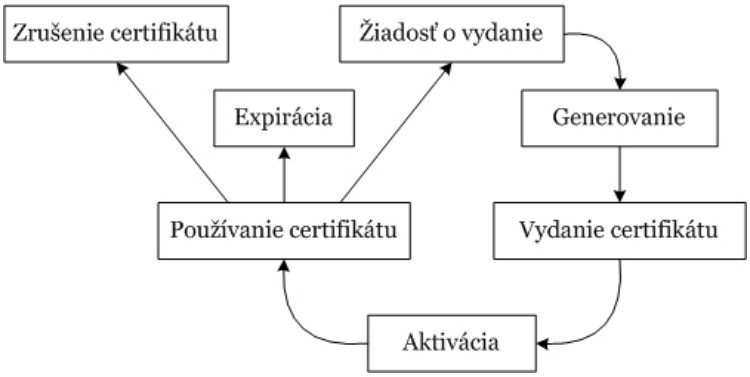
3.6 Žiadosť o zrušenie certifikátu KCA

Žiadosť o zrušenie certifikátu 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 § 15 zákona č. 215/2002 Z.z. o elektronickom podpise.

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

4. Prevádzkové postupy

Táto kapitola rieši životný cyklus správy certifikátu (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 životného cyklu správy certifikátu sú:

a) žiadosť o vydanie,
b) generovanie,
c) vydanie certifikátu,
d) aktivácia,
e) používanie certifikátu,
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) určené na certifikáciu 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 tohto CP. Ochrana certifikačných kľúčov KCA je riešená podľa ustanovení bodu 6.2 tohto CP. Certifikácia (vydanie certifikátu) verejného kľúča KCA sa vykonáva okamžite po jeho vygenerovaní.

4.1.2 Generovanie podpisových kľúčov pre KvCSR fyzických osôb

Kľúčový pár prislúchajúci ku KvCSR musí byť generovaný len na bezpečnom certifikovanom SSCD zariadení, ktoré musí byť certifikované NBÚ v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise. SSCD nesmie umožňovať export súkromného kľúča alebo nekontrolované použitie súkromného kľúča. Operácie so súkromným kľúčom musia byť výhradne pod kontrolou vlastníka SSCD.

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 kvalifikovaného certifikátu KCA

Certifikát verejného kľúča 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) nezávislý externý audítor,

d) jeden zamestnanec NBÚ.

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

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

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

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

Aby bolo možné využiť certifikačné kľúče následníka KCA pri poskytovaní certifikačných služieb, musia byť vydané vzájomné krížové certifikáty používaného verejného kľúča KCA a verejného kľúča následníka KCA.

Po vydaní certifikátu následníka KCA a krížových certifikátov verejného kľúča KCA a verejného kľúča následníka KCA zverejní NBÚ certifikát následníka KCA a krížové certifikáty podľa bodu 2.5.2 tohto CP.

4.4 Prevzatie certifikátu KCA

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

4.5 Zrušenie certifikátu

4.5.1 Okolnosti na zrušenie

KCA zruší certifikát v prípade:

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

b) úmyselného zneužitia kľúčov a certifikátov autorizovanou osobou,

c) podstatného závažného porušenia prevádzkových požiadaviek identifikovaných v tomto CP a príslušných 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 opísaná v CPS.

4.5.4 Interval na zrušenie certifikátu

Interval na zrušenie certifikátu je maximálne 24 hodín.

4.5.5 Periodicita publikovania zoznamu zrušených certifikátov KCA

Zoznamy zrušených certifikátov (CRL) a zoznamy zrušených certifikátov certifikačných autorít (ARL) 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 – § 6 vyhlášky NBÚ 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).

4.5.6 Zisťovanie stavu certifikátov

Stav certifikátov vydaných KCA je možné zisťovať:

a) na základe zoznamov zrušených certifikátov (CRL) a zoznamov zrušených certifikátov certifikačných autorít (ARL) (bod 2.5.3 tohto CP),

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

4.5.7 Iné možnosti informovania o zrušení certifikátov

Informácie o zrušení certifikátov kľúča KCA budú prístupné na sekcii informačnej bezpečnosti a elektronického podpisu 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. Popis auditu je definovaný v CPS.

4.7 Archivácia záznamov KCA

Záznamy vznikajúce pri certifikačných činnostiach spojených s certifikátmi KCA sa, v zmysle § 18 zákona č. 215/2002 Z.z. o elektronickom podpise, archivujú po dobu najmenej 10 rokov. Rozsah archivovaných údajov je stanovený v CPS.

4.8 Zmena certifikačných kľúčov KCA

Zmena certifikačných kľúčov KCA sa realizuje ako úplná výmena kľúčov pozostávajúca z generovania nového páru certifikačných kľúčov následníka KCA, jeho certifikácie a zabezpečenia kontinuity overovania vydaných certifikátov krížovou certifikáciou nového kľúča s jeho predchodcom (pokiaľ predchodca nebol kompromitovaný) v zmysle pravidiel stanovených v RFC 2510.

Prevádzkové a bezpečnostné procedúry zmeny kľúčov sú navrhnuté tak, aby minimalizovali riziká pri tejto operácií 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 kapitolou 4.2 tohto CP.

Plánovaná zmena kľúčov KCA musí byť oznámená 2 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 zákona č. 215/2002 Z.z. o elektronickom podpise. Činnosť KCA môže byť ukončená iba zmenou alebo zrušením tohto zákona alebo inou zákonnou úpravou. Zákonná úprava, ktorá ukončí činnosť KCA stanoví aj spôsob ukončenia činnosti.

5. Fyzické procedurálne a personálne bezpečnostné opatrenia

5.1 Opatrenia na zaistenie fyzickej bezpečnosti KCA

Opatrenia na zaistenie fyzickej bezpečnosti 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 KCA

Na zaistenie procedurálnej bezpečnosti sú vypracované bezpečnostné smernice 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 viacerých očí a podobne).

5.3 Opatrenia na zaistenie personálnej bezpečnosti KCA

Personál KCA je preverovaný v zmysle vyhlášky NBÚ č. 331/2004 Z. z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca.

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 elektronickými podpismi. 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 KCA k internetu.

6.2 Kryptografické prostriedky ochrany kľúčov KCA

Certifikačné kľúče KCA sú generované a uchovávané v kryptografickom module hardvérovej ochrany kľúča (ďalej len „HSM“) certifikovanom NBÚ podľa zákona č. 215/2002 Z.z. o elektronickom podpise a spĺňajúcich minimálne FIPS 140-1 úroveň 3.

HSM KCA má zabudované preverené algoritmy na generovanie náhodných čísel vyhovujúce požiadavkám vyhlášky NBÚ č. 134/2009 Z.z., ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis (o produktoch elektronického podpisu).

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

HSM KCA dovoľuje zabezpečiť certifikačné kľúče KCA proti možnosti ich čítania alebo exportu. 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)

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

Pole	Kritickosť	Obsah
Version		3
Serial number		01
Signature algorithm		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.
Public Key		RSA (2048 bits)
SubjectKeyIdentifier		30F4 A871 CE72 9F99 B429 BAF9 03B1 4110 5F24 DC99
BasicConstraints	Critical	Subject Type=CA Path Lenght 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	Certificate Signing, Off-line CRL Signing, CRL Signing (06)

Tab. 7.1a Profil certifikátu KCA (KCA1)

7.2 Profil certifikátu následníka KCA (KCA2)

V nasledujúcej tabuľke je uvedený profil certifikátu verejného kľúča následníka KCA (KCA2).

Pole	Kritickosť	Obsah
Version		3
Serial number		01
Signature algorithm		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.
Public Key		RSA (2048 bits)
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		06DA 89E7 D38E 533A 7977 E9EB F9A6 B632 653F 4624
BasicConstraints	Critical	Subject Type=CA Path Lenght Constraint=None
KeyUsage	Critical	Certificate Signing, Off-line CRL Signing, CRL Signing (06)

Tab. 7.2a Profil certifikátu následníka KCA (KCA2)

7.3 Profil krížového certifikátu následníka KCA (KCA2) vydaného KCA (KCA1)

V nasledujúcej tabuľke je uvedený profil krížového certifikátu verejného kľúča následníka KCA (KCA2) vydaného KCA (KCA1).

Pole	Kritickosť	Obsah
Version		3
Serial number		213C
Signature algorithm		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.
Public Key		RSA (2048 bits)
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
Authority Key Identifier		30F4 A871 CE72 9F99 B429 BAF9 03B1 4110 5F24 DC99

CRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ep.nbusr.sk/kca/crls/current_a.crl
SubjectKeyIdentifier		06DA 89E7 D38E 533A 7977 E9EB F9A6 B632 653F 4624
BasicConstraints	Critical	Subject Type=CA Path Lenght Constraint=None
KeyUsage	Critical	Certificate Signing, Off-line CRL Signing, CRL Signing (06)

Tab. 7.3a Profil krížového certifikátu následníka KCA (KCA2) vydaného KCA (KCA1)

7.4 Profil krížového certifikátu KCA (KCA1) vydaného následníkom KCA (KCA2)

V nasledujúcej tabuľke je uvedený profil krížového certifikátu verejného kľúča KCA (KCA1) vydaného následníkom KCA (KCA2).

Pole	Kritickosť	Obsah
Version		3
Serial number		09
Signature algorithm		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.
Public Key		RSA (2048 bits)
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
Authority Key Identifier		06DA 89E7 D38E 533A 7977 E9EB F9A6 B632 653F 4624

CRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl
SubjectKeyIdentifier		30F4 A871 CE72 9F99 B429 BAF9 03B1 4110 5F24 DC99
BasicConstraints	Critical	Subject Type=CA Path Lenght Constraint=None
KeyUsage	Critical	Certificate Signing, Off-line CRL Signing, CRL Signing (06)

Tab. 7.4a Profil krížového certifikátu KCA (KCA1) vydaného následníkom KCA (KCA2)

7.5 Profil certifikátu akreditovanej CA

Profil certifikátu akreditovanej CA, resp. uznanej zahraničnej CA je uvedený v dokumente NBÚ „Formáty kvalifikovaných certifikátov“, ktorý sa nachádza na nasledujúcej internetovej stránke:

http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/formats/formaty_qc.pdf

7.6 Profil kvalifikovaného certifikátu fyzickej osoby

Profil KvCSR je uvedený v dokumente NBÚ „Formáty kvalifikovaných certifikátov“, ktorý sa nachádza na nasledujúcej internetovej stránke:

http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/formats/formaty_qc.pdf

V rozšírení certifikačnej politiky kvalifikovaného certifikátu môže byť uvedených aj viac politík, okrem 1.3.158.36061701.0.0.0.1.2.2, ktorá identifikuje kvalifikovaný certifikát vydaný v súlade s platnými právnymi predpismi SR. Ak sa do certifikačnej politiky certifikátu uvedie aj OID európskej certifikačnej politiky OID 0.4.0.1456.1.1 (QCP Public + SSCD), potom v CPS sa musia uviesť požiadavky politiky (QCP Public + SSCD) tak, aby platili a neboli porušené požiadavky platných právnych predpisov SR. Napríklad (QCP Public + SSCD) umožňuje pozastavenie platnosti certifikátu, ale platné právne predpisy SR to neumožňujú, tak v CPS sa uvedie, že pozastavenie platnosti nie je povolené.

7.7 Profil zoznamov zrušených certifikátov

Profil zoznamov zrušených certifikátov je v súlade s medzinárodným štandardom RFC 5280.

Profil KvCSR je uvedený v dokumente NBÚ „Formáty zoznamu zrušených kvalifikovaných certifikátov“, ktorý sa nachádza na nasledujúcej internetovej stránke:

http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/legislativa/9/formaty_crl.pdf

8. Administrácia špecifikácií

Tento CP je revidovaný 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 tohto CP). Všetky formálne podané požiadavky na zmeny posúdi NBÚ a rozhodne o ich realizácii.

Pred schválením zmien v nasledujúcej verzii CP upozorní NBÚ všetky akreditované CA a uznané zahraničné CA, 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 CA, 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 certifikačného poriadku sú identifikované dvojmiestnym číslom. Číslovaná verzia má označenie v tvare:

Verzia A.B

Zmeny textu certifikačného poriadku, ktoré nemenia význam dokumentu (napr. opravy gramatických chýb, náhrada niektorých slov synonymami, zmena formátovania a pod.) sa v čísle verzie neodrážajú.

Zmeny textu certifikačného poriadku, ktoré menia význam dokumentu, ale zmeny nezasahujú do podstaty zverejňovaných zásad (napríklad zmena distribučných bodov a pod.) sa zachycujú v čísle verzie na pozícii B.

Podstatné zmeny certifikačného poriadku sa v čísle verzie odrážajú na pozícií A.

8.2 Schvaľovanie verzií

Tento CP schvaľuje riaditeľ sekcie informačnej bezpečnosti a elektronického podpisu NBÚ.

9. Účinnosť certifikačného poriadku

Tento CP kľúča nadobúda účinnosť dňom 15. 6. 2009.