Národný bezpečnostný úrad SR

Sekcia IBEP

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: 2.0

Dokument nadobúda účinnosť dňom: 3.4.2006

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
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 NBÚ.
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 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	Obnova kľúčov v kontexte tohto dokumentu znamená vydanie nového certifikátu s rovnakými alebo veľmi podobnými charakteristikami ako

(Keys Renewal)	pôvodný (obnovovaný) certifikát. Generuje sa nová dvojica kľúčov prislúchajúca k certifikátu.
Odtlačok verejného kľúča ***(Fingerprint)***	tzv. *hash* verejného kľúča. Hash 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 *(RA)*	Komponent infraštruktúry PKI, používaný na posúvanie schválených žiadostí o vydanie certifikátu do CA.
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. Účinnosť 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 uvedenými CA), alebo OCSP(zoznam len požadovaných certifikátov).
Zoznam zrušených certifikátov certifikačných autorít *(ARL)*	Zoznam kvalifikovaných certifikátov certifikačných kľúčov certifikačných autorít (vrátane KCA), ktorých platnosť bola zrušená. Zoznam vydáva a podpisuje KCA. Zoznam je publikovaný v adresári LDAP.

Skratky

ACA	Akreditovaná certifikačná autorita
ARL	Zoznam zrušených certifikátov certifikačných autorít *(Authority Revocation List)*
CA	Certifikačná autorita *(Certification Authority)*
CP	Certifikačný poriadok alebo tiež certifikačná politika *(Certificate Policy)*
CPS	Pravidlá na výkon certifikačných činností *(Certification Practice Statement)*
CRL	Zoznam zrušených certifikátov *(Certificate Revocation List)*
HSM	Hardvérový kryptografický modul *(Hardware Security Module)*
HW	Hardvér *(Hardware)*
IBEP	Sekcia informačnej bezpečnosti a elektronického podpisu
IT	Informačná technológia *(Information Technology)*
KCA	Koreňová certifikačná autorita NBÚ
KCA1	Koreňová certifikačná autorita 1 NBÚ
KCA2	Následník koreňovej certifikačnej autority NBÚ
LDAP	Protokol pre prístup k adresárovým službám *(Lightweight Directory Access Protocol)*
OID	Identifikátor klasifikácie objektov *(Object Identifier Descriptor)*
PC	Osobný počítač *(Personal Computer)*
RA	Registračná autorita *(Registration Authority)*
SC	Smartkarta *(SmartCard)*
SW	Softvér *(Software)*

1. Úvod

1.1 Účel certifikačného poriadku

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

Tento CP zároveň profiluje aj certifikačné poriadky, použité pri vydávaní kvalifikovaných certifikátov akreditovanými certifikačnými autoritami v súlade s platnými právnymi predpismi SR, najmä zákonom č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej ako „zákon č. 215/2002 Z.z. o elektronickom podpise"). Napríklad, ak je použitá európska kvalifikovaná certifikačná politika OID 0.4.0.1456.1.1 (QCP Public + SSCD) z dokumentu ETSI TS 101 456 V1.3.1 pre vydávanie kvalifikovaného certifikátu koncového používateľa, 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 ACA prevezmú z vyhlášky č. 541/2002 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 NBÚ, kvalifikované certifikáty akreditovaných CA spĺňajúcich požiadavky slovenských právnych predpisov je identifikovaný objektovým identifikátorom odvodeným od objektového identifikátora NBÚ.

Objektový identifikátor CP pre certifikačné kľúče KCA (OID) 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 Národného Bezpečnostného Úradu 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 NBÚ
2	Dokument „Certifikačný poriadok pre certifikáty KCA"
2	Certifikačný poriadok pre certifikáty KCA a kvalifikované certifikáty akreditovaných CA

spĺňajúcich platné právne predpisy SR.

1.3 Charakteristika, použitie a subjekty pracujúce s certifikátmi

1.3.1 Charakteristika certifikátu

Certifikát KCA je certifikát, ktorý KCA vydáva na vlastný verejný kľúč Úradu v podobe self-signed certifikátu KCA, ktorého zaručený elektronický podpis je vyhotovený súkromným kľúčom, ktorý je súčasťou toho istého kľúčového páru ako verejný kľúč certifikátu, a ktorý patrí NBÚ.

Kvalifikované certifikáty, ktoré vytvárajú certifikačnú cestu v podstrome KCA NBÚ, môžu byť vydané podľa vlastnej CP, ale ich vydávanie je v CPS profilované podľa požiadaviek tohoto poriadku, ktorý musia dodržať. Ďalej sa tieto kvalifikované certifikáty, vydané podľa platných právnych predpisov SR, budú označovať ako KvCSR.

1.3.2 Certifikačné kľúče NBÚ

Na zabezpečenie certifikačných služieb používa KCA NBÚ kľúčové páry RSA o minimálnej dĺžke 2048 bitov alebo ECDSA s minimálnou dĺžkou 256 bitov.

1.3.3 Použitie certifikátu KCA a KvCSR

Certifikáty KCA môžu byť použité na:

1) overovanie platnosti kvalifikovaných certifikátov ACA,
2) overovanie platnosti krížových certifikátov uznaných zahraničných CA,
3) overovanie platnosti zoznamov zrušených kvalifikovaných certifikátov ACA,
4) overovanie platnosti zoznamov zrušených krížových certifikátov uznaných zahraničných CA,
5) overovanie platnosti technologických certifikátov KCA,
6) overovanie platnosti zoznamov zrušených technologických certifikátov KCA.

KvCSR akreditovaných CA môžu byť použité na:

1) overovanie platnosti užívateľských certifikátov a kvalifikovaných certifikátov,
2) overenie platnosti zoznamu zrušených certifikátov.

KvCSR koncových užívateľov môžu byť použité na:

1) overovanie platnosti zaručených elektronických podpisov,
2) overovanie platnosti nepriamych zoznamov zrušených certifikátov (aj v on-line režime),
3) overenie platnosti časových pečiatok.

Akékoľvek iné použitie kvalifikovaného certifikátu KCA a KvCSR sa považuje za neoprávnené použitie certifikátu.

1.3.3.1 Dôležité obmedzenia certifikátu KCA 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 pre ktorého verejnú časť bol kvalifikovaný certifikát vydaný, sa musí nachádzať na bezpečnom zariadení SSCD, ktoré je certifikované NBÚ a nijakým spôsobom neumožňuje export súkromného kľúča zo SSCD. Pričom za overenie SSCD zariadenia zodpovedá akreditovaná certifikačná autorita a ak SSCD zariadenie osoba žiadajúca o kvalifikovaný certifikát nevlastní, tak aj za jeho dodanie žiadateľovi o kvalifikovaný certifikát.

1.3.3.2 Špecifikácie formátu, obsahu a použitia KvCSR

Certifikáty KCA a KvCSR musia spĺňať požiadavky, ktoré definuje NBÚ v dokumentoch zverejnených na NBÚ stránkach. Dokumenty podrobne definujú požiadavky na kvalifikované certifikáty, zoznamy zrušených certifikátov a rovnako aj na formáty kvalifikovaných podpisov, v ktorých sa kvalifikované certifikáty používajú.

Podrobné informácie o formátoch, ktoré musia byť pri vydávaní splnené je možné nájsť na NBÚ stránke:

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

Akreditované certifikačné autority musia pri vydávaní spĺňať požiadavky definované v dokumente, ktorý popisuje vytvorenie a overenie certifikačnej cesty a nachádza sa na NBÚ stránke:

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

1.3.4 Subjekty pracujúce s certifikátom KCA

1.3.4.1 KCA

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

1.3.4.2 Registračná autorita

Služby registračnej autority KCA v zmysle tohto CP vykonáva NBÚ.

1.3.4.3 Správca adresárov

Správcom adresárov KCA v zmysle tohto CP je NBÚ.

1.3.4.4 Držiteľ certifikátu

Držiteľom certifikátu KCA je NBÚ.

1.3.4.5 Používatelia certifikátu

Používateľmi certifikátu KCA sú:

a) Akreditované certifikačné autority,

b) Zahraničné certifikačné autority uznané v SR,

c) Klienti akreditovaných certifikačných autorít a zahraničných certifikačných autorít.

1.3.4.6 Druhy certifikátov vydávaných KCA

KCA vydáva v zmysle § 10 a § 5 zákona č. 215 / 2002 Z. z. tieto druhy certifikátov:

a) kvalifikované certifikáty pre akreditované certifikačné autority,

b) krížové certifikáty pre uznané zahraničné certifikačné autority,

c) kvalifikované certifikáty svojich vlastných kľúčov,

d) kvalifikované certifikáty následníka KCA,

e) technologické certifikáty: certifikáty personálu KCA (operátori CA) a certifikáty pre ďalšie entity NBÚ CA (napr. server časových pečiatok).

1.4 Kontaktné informácie KCA

Špecifikácia administrátorskej organizácie

Tento certifikačný poriadok je plne spravovaný sekciou IBEP Národného bezpečnostného úradu SR.

Kontaktná Adresa

Národný bezpečnostný úrad SR,
Budatínska 30,
P.O.BOX 16
850 07 Bratislava 57,
Slovenská republika,
http://ep.nbusr.sk

Kontaktná osoba

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

Bezpečnostný správca KCA
Národný bezpečnostný úrad SR
P.O.BOX 16
850 07 Bratislava 57,

Telefón: 02 6869 2114 (sekretariát sekcie informačnej bezpečnosti a elektronického podpisu)
0903 993 167 (prevádzka KCA)
Fax: 02 6869 1701
e-mail: secadmin@nbusr.sk

2. Všeobecné ustanovenia

2.1 Povinnosti jednotlivých subjektov

2.1.1 Povinnosti Certifikačnej autority KCA

KCA ako vydavateľ certifikátu svojho vlastného 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 kľúča,

d) včas zverejniť informácie o novo vydanom certifikáte,

e) včas informovať používateľov o pripravovanej zmene 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. je KCA povinná:

a) používať súkromné kľúče prislúchajúce 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, 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 (spoliehajúcej sa strany)

Používatelia certifikátu sú povinní používať certifikát KCA NBÚ a KvCSR v súlade s použiteľnosťou certifikátu definovanou v kapitole č 1.3.3 Použitie certifikátu KCA a KvCSR.

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 KCA

Právne záruky a obmedzenia záruk v rámci tohto CP vyplývajú z právnych predpisov platných v 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 zákonov a ostatných všeobecne záväzných právnych predpisov SR.

2.5 Zverejňovanie informácií KCA

NBÚ zverejňuje:

1) Dokumentáciu v rozsahu
   a) Certifikačné poriadky pre všetky triedy verejných certifikátov vydávaných KCA NBÚ
   b) Pravidlá na výkon certifikačných činností
2) Vydané certifikáty
3) Zoznamy zrušených certifikátov
4) Stavové informácie o certifikátoch

2.5.1 Zverejňovanie dokumentácie KCA

Dokumentácia je zverejnená elektronicky na internetovej stránke Úradu http://ep.nbusr.sk/kca.

V listinnej podobe je dokumentácia k dispozícií na sekcii IBEP NBÚ.

2.5.2 Zverejňovanie certifikátov KCA

Dokumentácia ako aj ďalšie všeobecné informácie týkajúce sa KCA sú zverejnené elektronicky na internetovej stránke úradu http://ep.nbusr.sk/kca.

V listinnej podobe je dokumentácia k dispozícií na sekcii IBEP NBÚ.

Úrad zverejňuje nasledujúce certifikáty KCA:

- kvalifikovaný certifikát KCA,
- kvalifikované certifikáty vydané KCA pre akreditované certifikačné autority,
- kvalifikované krížové certifikáty uznaných zahraničných certifikačných autorít,
- kvalifikovaný certifikát následníka KCA počas procesu výmeny kľúčov KCA,
- krížové kvalifikované certifikáty KCA a následníka KCA počas procesu výmeny kľúčov KCA.

Tieto informácie sú verejne prístupné nasledovnými spôsobmi:

a) samostatne na internetovej stránke http://ep.nbusr.sk/kca,

b) v listinnej podobe na registračnom mieste NBÚ,

c) v dennej tlači - kvalifikovaný certifikát KCA,

d) kvalifikovaný certifikát KCA 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?

e) kvalifikovaný certifikát vlastného kľúča následníka KCA 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?

KCA aktualizuje zoznam vydaných certifikátov pri každom vydaní nového kvalifikovaného certifikátu. Odkazy, na ktorých je možné získať potrebné informácie o vydaných kvalifikovaných certifikátoch zverejňuje KCA na svojej kontaktnej internetovej adrese.

2.5.3 Zverejňovanie zoznamov zrušených certifikátov KCA

Úrad publikuje aktuálny zoznam zrušených vlastných certifikátov KCA, kvalifikovaných certifikátov ACA, krížových kvalifikovaných certifikátov (ARL), všetkých zrušených certifikátov vydaných KCA (CRL) a zverejňuje ich na adrese:

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

Po dobu jedného roka odo dňa vydania úrad publikuje každý zoznam zrušených certifikátov (tzv. archívne CRL) prostredníctvom:

1) protokolu LDAP na adrese:

Pre KCA1

archívne CRL
ldap://ep.nbusr.sk/ou=crls,ou=Sekcia elektronickeho podpisu,o=Narodny bezpecnostny urad,c=sk?cRLDistributionPoint?sub?

Pre KCA2

archívne CRL
ldap://ep.nbusr.sk/ou=arch crls KCA2,ou=Sekcia IBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?cRLDistributionPoint?sub?

2) Web stránky:
http://ep.nbusr.sk/kca/crl.html

Spôsob vyhľadávania archívnych CRL v adresári LDAP a na Web stránkach je popísaný na informačnej stránke KCA: http://ep.nbusr.sk/kca.

2.5.4 Periodicita publikovania informácií

Zoznamy zrušených certifikátov (ARL, CRL) sa vytvárajú a zverejňujú s periódou maximálne 24 hodín a zároveň tak, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, v ktorom sa zverejňuje zrušenie príslušného certifikátu, neuplynulo viac ako 24 hodín, pokiaľ to neznemožní havarijný stav systému, alebo iné technické okolnosti (napr. § 5, Vyhlášky NBÚ č 538/2002 Z. z.).

Ostatné informácie sú zverejňované staticky.

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 KCA

Subject (držiteľ) certifikátu:

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

Vydavateľ certifikátu:

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

3.1.2 Následník KCA

Subject (držiteľ) certifikátu:

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

Vydavateľ certifikátu:

Common Name:	KCA NBU SR

Organization Unit: Sekcia IBEP
Organization: Narodny bezpecnostny urad
Locality: Bratislava
Country: sk

3.1.3 Krížové kvalifikované certifikáty KCA1 a následníka KCA2

Krížové kvalifikované certifikáty KCA1 a následníka KCA2 spĺňajú nasledovnú mennú konvenciu:

3.1.3.1 Krížový certifikát vydaný KCA1 pre KCA2

Issuer (vydavateľ) certifikátu:

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

Subject (držiteľ) certifikátu:

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

3.1.3.2 Krížový certifikát vydaný KCA2 pre KCA1

Issuer (vydavateľ) certifikátu:

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

Subject (držiteľ) certifikátu:

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

3.1.4 Pravidlá na zabezpečenie jednoznačnosti mien

Jednoznačnosť mena KCA je zabezpečená jej postavením v systéme.

3.1.5 Riešenie sporov týkajúcich sa mien KCA

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

3.1.6 Používateľské kvalifikované certifikáty

Kvalifikovaný certifikát používateľa musí v položke Subject obsahovať minimálne commonName a countryName a to tak, ako je definované v dokumente formáty kvalifikovaných certifikátov: http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html

Položka Subject certifikátu môže obsahovať aj serialNumber, v ktorej pre jednoznačnú identifikáciu osoby môže byť uvedené číslo občianskeho preukazu, s dátumom vydania občianskeho preukazu.

Formát textu v položke serialNumber „ID Card XX 999999-YYYYMMDD“

Kde XX je séria, 9 čísla, YYYY rok, MM mesiac a DD je deň vydania OP.

3.2 Iniciálna registrácia

3.2.1 Koreňová certifikačná autorita KCA1

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 IBEP o zriadení KCA.

3.2.2 Následník koreňovej certifikačnej autority KCA2

Iniciálna registrácia Následníka KCA sa vykonáva v procese formálneho zriadenia následníka KCA. Na autentifikáciu následníka KCA v procese iniciálnej registrácie slúži zákon č 215/2002 Z.z o elektronickom podpise a rozhodnutie riaditeľa sekcie IBEP o zriadení KCA

3.3 Spôsob preukázania vlastníctva súkromného kľúča

Preukazovanie vlastníctva súkromného kľúča prislúchajúceho k verejnému kľúču v žiadosti o certifikát je dané procedúrami overenia KCA.

3.4 Vydanie následného certifikátu KCA

Pri vydávaní následného certifikátu KCA, musí dôjsť ku generovaniu nového kľúča.

3.5 Vydanie následného certifikátu po zrušení certifikátu KCA

Pri vydávaní následného certifikátu KCA, po zrušení certifikátu KCA, musí dôjsť ku generovaniu nového kľúča.

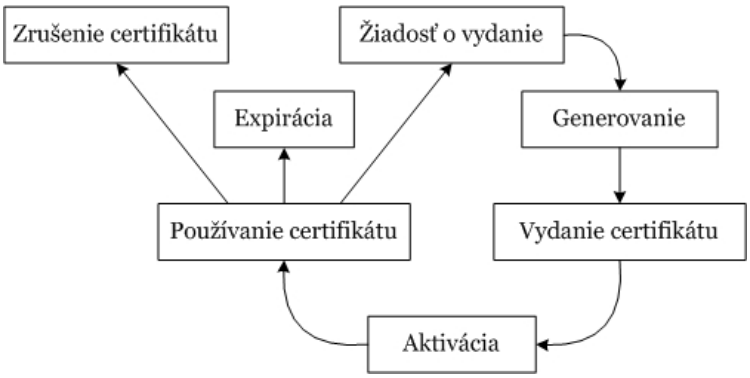
3.6 Žiadosť o zrušenie certifikátu KCA

Žiadosť o zrušenie certifikátu 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 požiadavky zákona o elektronickom podpise (zákon č. 215 / 2002 Z. z., § 15, ods. 4).

Žiadosť musí obsahovať, mimo ostatných dôvodov uvedených v CPS, najmä dátum a čas podania žiadosti, dôvod žiadosti a identifikáciu osoby organizácie, ktorá žiadosť podala.

4. Prevádzkové postupy

Táto kapitola odzrkadľuje životný cyklus kvalifikovaného certifikátu (Certificate Management LifeCycle, CMLC). Životný cyklus kvalifikovaného certifikátu pozostáva z primárnych a sekundárnych stavov. Každý vydaný certifikát prechádza všetkými primárnymi stavmi, zatiaľ čo sekundárne stavy sú výnimočné.



Primárnymi stavmi sú:

- Žiadosť o vydanie certifikátu,
- Generovanie certifikátu,
- Vydanie certifikátu,
- Aktivácia,
- Používanie certifikátu,
- Expirácia,
- Archivácia.

Sekundárnym stavom je zrušenie certifikátu.

4.1 Generovanie kľúčov KCA

Kľúčový pár KCA – verejný a súkromný kľúč KCA – určené na certifikáciu a overovanie certifikátov (kľúčový pár KCA) sa generuje ako jeden kľúčový pár na prostriedkoch KCA pri zaistení požadovanej bezpečnosti generovania. Procedúra je sledovaná komisiou podľa postupu popísaného v kapitole 4.3 „Vydanie kvalifikovaného certifikátu“. Ochrana certifikačných kľúčov KCA je popísaná v kapitole 6.2 „Kryptografické prostriedky ochrany kľúčov KCA“. Certifikácia verejného kľúča z kľúčového páru sa vykonáva okamžite po jeho vygenerovaní.

4.1.1 Generovanie podpisových kľúčov pre KvCSR koncových používateľov

Kľúčový pár musí byť generovaný len na certifikovanom SSCD, ktoré nesmie umožniť 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 Úrad sám sebe z formálnych dôvodov (naplnenie požiadavky § 15, ods. 4 zákona č. 215/2002 Z.z. o elektronickom podpise,) v písomnej forme. S ohľadom na charakter certifikátu a postup pri certifikácii KCA, nie je potrebná žiadosť o vydanie certifikátu vo formáte PKCS#10.

4.3 Vydanie kvalifikovaného certifikátu KCA

Kvalifikovaný 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:

- Bezpečnostný správca KCA
- Interný bezpečnostný audítor KCA
- Externý bezpečnostný audítor KCA
- jeden zamestnanec Úradu

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 aplikácie sa vygeneruje certifikačný kľúčový pár KCA a certifikát KCA.

Po vydaní kvalifikovaného certifikátu KCA Úrad zverejní kvalifikovaný certifikát KCA na prostriedkoch určených na distribúciu certifikátov.

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 pre používaný verejný kľúč KCA a verejný kľúč následníka KCA.

Po vydaní kvalifikovaného certifikátu následníka KCA a krížových certifikátov verejného kľúča KCA a verejného kľúča následníka KCA Úrad zverejní kvalifikovaný certifikát následníka KCA a krížové certifikáty na prostriedkoch určených na distribúciu certifikátov.

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 príslušnom CP a CPS,

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

e.) ak KCA ukončila svoju činnosť.

4.5.2 Strany, ktoré môžu žiadať o zrušenie

O zrušenie certifikátu KCA môže požiadať:

a) KCA

b) Oprávnená tretia strana (súd)

4.5.3 Postup pri zrušení KCA certifikátu

Proces zrušenia certifikátu je iniciovaný prijatím žiadosti o zrušenie certifikátu obsahujúcej všetky potrebné náležitosti. Na zachovanie integrity v rámci hierarchie NBÚ CA je kľúčové bezodkladné overenie a spracovanie požiadavky na zrušenie certifikátu KCA. 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

Zoznamy zrušených certifikátov (ARL, CRL) sa vytvárajú a zverejňujú s periódou maximálne 24 hodín a zároveň tak, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, ktorý obsahuje jeho číslo, neuplynulo viac ako 24 hodín, pokiaľ to neznemožní havarijný stav systému, alebo iné technické okolnosti (§ 5 Vyhlášky NBÚ č. 538/2002).

4.5.6 On-line zisťovanie stavu certifikátov

Stav certifikátov je možné zisťovať:

1) porovnaním záznamu CRL v adresárových službách,

2) z informácií uverejnených na príslušnej webovej stránke.

4.5.7 Iné možnosti informovania o zrušení certifikátov

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

4.6 Audit bezpečnosti KCA

Postupy a procedúry pri vydávaní a zrušovaní certifikačných kľúčov KCA sú podrobované pravidelnému bezpečnostnému auditu zabezpečovanému NBÚ. Popis auditu je definovaný v CPS.

4.7 Archivácia záznamov KCA

Záznamy vznikajúce pri certifikačných činnostiach spojených s certifikátmi KCA sa archivujú na obdobie 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 Protokolom na manažment certifikátov (Certificate Management Protocol) definovaným 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 4.1. tohto dokumentu.

Plánovaná zmena kľúčov KCA musí byť oznámená 2 mesiace vopred všetkým podriadeným ACA a krížovo certifikovaným 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 a minimalizovať prerušenie poskytovania certifikačných služieb KCA a ostatné škody vzniknuté prípadnou havarijnou situáciou.

4.10 Skončenie činnosti KCA

Činnosť KCA NBÚ sa zakladá na ustanoveniach zákona č. 215/2002 Z. z. o elektronickom podpise. Činnosť KCA NBÚ môže byť ukončená iba zmenou alebo zrušením tohto zákona alebo inou zákonnou úpravou. Zákonná úprava, ktorá ukončí činnosť KCA NBÚ stanoví aj spôsob ukončenia činnosti.

5. Fyzické procedurálne a personálne bezpečnostné opatrenia

5.1 Opatrenia na zaistenie fyzickej bezpečnosti

Opatrenia na zaistenie fyzickej bezpečnosti sú v súlade s Vyhláškou NBÚ č. 336/2004 Z. z. o fyzickej a objektovej bezpečnosti.

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

Personál KCA NBÚ má kvalifikáciu potrebnú na zabezpečovanie certifikačných činností KCA NBÚ.

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

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

6. Technické bezpečnostné opatrenia

6.1 Opatrenia na zaistenie bezpečnej prevádzky KCA

Jadro systému KCA NBÚ je komponované ako samostatná entita komunikačne izolovaná od zvyšku systému. Zvyšné časti systému sú rozdelené do viacerých sekcií, 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 NBÚ sa uskutočňuje na médiách. Komunikácia, ktorá prebieha po vnútornej sieti medzi jednotlivými komponentmi systému KCA NBÚ je chránená šifrovaním.

Prvky oddelenia sieťovej komunikácie vymedzujú spôsob vzájomnej komunikácie komponentov systému.

Integrita citlivých údajov používaných v KCA NBÚ 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 NBÚ 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 NBÚ z vonkajšieho prostredia.

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

6.2 Kryptografické prostriedky ochrany kľúčov KCA

Certifikačné kľúče KCA sú generované a uchovávané v HSM spĺňajúcich minimálne FIPS 140-2 úroveň 3 a v doteraz používanom HSM Private Server firmy Algorithmic Research, ktorý bol certifikovaný NBÚ podľa FIPS 140-1 na bezpečnostnú úroveň 3.

Kryptografický modul Server firmy Algorithmic Research podporuje kryptografické algoritmy na symetrické šifrovanie DES, 3xDES a AES na asymetrickú kryptografiu RSA, DSA na hašovanie SHA1, MD5, ARDFP. Má zabudované preverené algoritmy na generovanie náhodných čísel vyhovujúce požiadavkám vyhlášky 539/2002 Z. z.

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

Kryptografický modul Private Server firmy Algorithmic Research dovoľuje zabezpečiť kľúče aplikácií 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

V nasledujúcej tabuľke sa nachádza profil certifikátu kľúča KCA.

Field	Criticality	Content
1 X509v1 Field		
1.1 Version		v3
1.2 Serial Number		*alokované automaticky vydávajúcou CA*
1.3 Signature Algorithm		SHA-1 s RSA podpisom
1.4 Issuer Distinguished Name		
1.4.1 Common Name (CN)		Korenova CA pre kvalifikovane certifikaty 1
1.4.2 Locality (L)		Bratislava
1.4.3 Organizational Unit (OU)		Sekcia elektronickeho podpisu
1.4.4 Organization (O)		Narodny bezpecnostny urad
1.4.5 Country (C)		SK
1.5 Validity		
1.5.1 Not before		Napr.., “10:00:00 02. Februar 2003”
1.5.2 Not After		Napr.., “10:00:00 02. Februar 2004”
1.6 Subject		
1.6.1 Common Name (CN)		Korenova CA pre kvalifikovane certifikaty 1*
1.6.2 Locality (L)		Bratislava
1.6.3 Organization Unit (OU)		Sekcia elektronickeho podpisu
1.6.4 Organization (O)		Narodny bezpecnostny urad
1.6.5 Country (C)		SK
1.7 Subject Public Key Info		2048-bit RSA verejný kľúč zakódovaný v súlade RFC2459 a PKCS#1
2 X509v3 Extensions		
2.1 Subject Key Identifier		Identifikátor kľúča pozostávajúci z 160-bitového SHA-1 hashu informácie uvedenej v subjectPublicKey (s výnimkou „tag“, „length“ a „number of unused bits“).
2.2 Key Usage	Critical	
2.2.1 Certificate Signing		Zvolené
2.2.2 CRL Signing		Zvolené
2.3 Certificate Policies	Critical	
2.3.1 Policy Identifier		1.3.158.36061701.0.0.0.1.2.1
2.3.1.1 Policy Qualifier ID		CPS (1.3.6.1.5.5.7.2.1)
2.3.1.2 Policy Qualifier		http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_1.pdf
2.3.2 Policy Qualifier Info		
2.3.2.1 Policy Qualifier ID		User Notice (1.3.6.1.5.5.7.2.2)
2.3.2.2 Policy Qualifier		Tento certifikat je vydany ako kvalifikovany certifikat „Korenovej CA pre kvalifikovane certifikaty“ v sulade so zakonom c. 215/2002 Z.z.
2.4 Basic Constraints	Critical	
2.4.1 Subject Type		CA
2.4.2 Path Length Constraint		3

7.2 Profil certifikátu kľúča následníka KCA

V nasledujúcej tabuľke sa nachádza profil certifikátu následníka kľúča KCA.

Field	Criticality	Content
1 X509v1 Field		
1.1 Version		v3
1.2 Serial Number		*alokované automaticky vydávajúcou CA*
1.3 Signature Algorithm		SHA-1 s RSA podpisom
1.4 Issuer Distinguished Name		
1.4.1 Common Name (CN)		KCA NBU SR
1.4.2 Organizational Unit (OU)		Sekcia IBEP
1.4.3 Organization (O)		Narodny bezpecnostny urad
1.4.4 Locality (L)		Bratislava
1.4.5 Country (C)		SK
1.5 Validity		
1.5.1 Not before		Napr.., “10:00:00 02. Februar 2005”
1.5.2 Not After		Napr.., “10:00:00 02. Februar 2010”
1.6 Subject		
1.6.1 Common Name (CN)		KCA NBU SR
1.6.2 Organization Unit (OU)		Sekcia IBEP
1.6.3 Organization (O)		Narodny bezpecnostny urad
1.6.4 Locality (L)		Bratislava
1.6.5 Country (C)		SK
1.7 Subject Public Key Info		2048-bit RSA verejný kľúč zakódovaný v súlade RFC2459 a PKCS#1
2 X509v3 Extensions		
2.1 Subject Key Identifier		Identifikátor kľúča pozostávajúci z 160-bitového SHA-1 hashu informácie uvedenej v subjectPublicKey (s výnimkou „tag“, „length“ a „number of unused bits“).
2.2 Key Usage	Critical	
2.2.1 Certificate Signing		Zvolené
2.2.2 CRL Signing		Zvolené
2.3 Certificate Policies		
2.3.1 Policy Identifier		1.3.158.36061701.0.0.0.1.2.2
2.3.1.1 Policy Qualifier ID		CPS (1.3.6.1.5.5.7.2.1)
2.3.1.2 Policy Qualifier		http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf
2.3.2 Policy Qualifier Info		
2.3.2.1 Policy Qualifier ID		User Notice (1.3.6.1.5.5.7.2.2)
2.3.2.2 Policy Qualifier		Certifikat je vydany ako kvalifikovany certifikat KCA NBU SR v sulade s platnymi pravnymi predpismi SR.
2.4 Certificate Policies		
2.4.1 Policy Identifier		0.4.0.1862.1.1
2.5 CRL Distribution Points		http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl
2.6 Basic Constraints	Critical	
2.6.1 Subject Type		CA

7.3 Profil krížového certifikátu vydaného KCA1 pre KCA2

Položky stromu	Položky menu	Obsah poľa	Kritický
CA Signing Algorithm			
	SHA-1 With RSA Encryption		
DN String Type Preference		UTF8	
Distinquished Name Issuer			
	Common Name	Korenova CA pre kvalifikovane certifikaty 1	
	Locality	Bratislava	
	Organizational Unit	Sekcia elektronickeho podpisu	
	Organization	Narodny bezpecnostny urad	
	Country	SK	
Validity			
	Start	Nastaviť požadovaný začiatočný čas	
	End	14.1.2006, 16:56:21	
Distinquished Name Śubject			
	Common Name	KCA NBU SR	
	Organizational Unit	Sekcia IBEP	
	Organization	Narodny bezpecnostny urad	
	Locality	Bratislava	
	Country	SK	
Key Properties			
	Key Size	2048	
	Key Algorithm	RSA	
	Key Usage	CRL Signing	Critical
		Certificate Signing	
Extensions			
	Basic Constraints	IsCA	Critical
	Subject Key ID	160bit SHA-1	
	Autority Key ID	160bit SHA-1	
	Certificate Policies		
	Policy Identifier	1.3.158.36061701.0.0.0.1.2.1	
	Certificate Practice Statement URI	http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf	
	User Notice	Certifikat je vydany ako krizovy (cross) certifikat pre naslednika KCA NBU SR v sulade s platnymi pravnymi predpismi SR.	
	Certificate Policies		
	Policy Identifier	0.4.0.1862.1.1	

	Authority Information Access		
	OID	1.3.6.1.5.5.7.48.2	
	Name Type	URI	
	Access Descriptor	http://ep.nbusr.sk/kca/certs/kca/certifikat_der.cer	
	CRL Distribution Points	http://ep.nbusr.sk/kca/crls/current_a.crl	

7.4 Profil krížového certifikátu vydaného KCA1 pre KCA2

Položky stromu	Položky menu	Obsah poľa	Kritický
CA Signing Algorithm			
	SHA-1 With RSA Encryption		
DN String Type Preference		UTF8	
Distinquished Name Issuer			
	Common Name	Korenova CA pre kvalifikovane certifikaty 1	
	Locality	Bratislava	
	Organizational Unit	Sekcia elektronickeho podpisu	
	Organization	Narodny bezpecnostny urad	
	Country	SK	
Validity			
	Start	Nastaviť požadovaný začiatočný čas	
	End	14.1.2006, 16:56:21	
Distinquished Name Śubject			
	Common Name	KCA NBU SR	
	Organizational Unit	Sekcia IBEP	
	Organization	Narodny bezpecnostny urad	
	Locality	Bratislava	
	Country	SK	
Key Properties			
	Key Size	2048	
	Key Algorithm	RSA	
	Key Usage	CRL Signing	Critical
		Certificate Signing	
Extensions			
	Basic Constraints	IsCA	Critical
	Subject Key ID	160bit SHA-1	

	Autority Key ID	160bit SHA-1	
	Certificate Policies		
	Policy Identifier	1.3.158.36061701.0.0.0.1.2.1	
	Certificate Practice Statement URI	http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf	
	User Notice	Certifikat je vydany ako krizovy (cross) certifikat pre naslednika KCA NBU SR v sulade s platnymi pravnymi predpismi SR.	
	Certificate Policies		
	Policy Identifier	0.4.0.1862.1.1	
	Authority Information Access		
	OID	1.3.6.1.5.5.7.48.2	
	Name Type	URI	
	Access Descriptor	http://ep.nbusr.sk/kca/certs/kca/certifikat_der.cer	
	CRL Distribution Points	http://ep.nbusr.sk/kca/crls/current_a.crl	

7.5 Profil používateľského kvalifikovaného certifikátu

Profil je podrobne popísaný v dokumente Formáty kvalifikovaných certifikátov na stránke:

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

kde obsah jednotlivých rozšírení je uvedený hlavne v tabuľke 12.

Pre kvalifikované certifikáty sa odporúča používať algoritmus RSA s kľúčom veľkosti 2048 bitov.

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.

7.6 Profil zoznamu zrušených certifikátov

Profil zoznamov zrušených certifikátov (CRL) a zoznamov zrušených certifikátov certifikačných autorít (ARL) je v súlade s normou RFC 3280.

Profil zoznamu zrušených certifikátov je definovaný v dokumente „Formáty zoznamu zrušených kvalifikovaných certifikátov“, ktoré vydalo NBÚ.

Dokument je zverejnený na stránke:

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

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 vedením KCA NBÚ. Všetky formálne podané požiadavky na zmeny posúdi NBÚ a rozhodne o ich realizácií.

Pred schválením zmien v nasledujúcej verzii CP upozorní NBÚ všetky CA, ktorým vydal certifikát a všetky priamo krížovo certifikované CA.

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 IBEP NBÚ.

9. Účinnosť certifikačného poriadku

Certifikačný poriadok certifikačného kľúča nadobúda účinnosť dňom 3.4.2006.