Národný bezpečnostný úrad SR

Sekcia elektronického podpisu

Certifikačný poriadok
pre certifikáty certifikačného kľúča
Koreňovej certifikačnej autority

Verzia: 1.0

Dokument nadobúda účinnosť dňom: 25.06.2003

Obsah

Pojmy

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).
Certifikačná politika *(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	Služby, ktoré poskytuje Úrad, napr. registrácia, certifikácia, overenie platnosti a funkčnosti certifikátu, pozastavenie platnosti certifikátu, zrušenie pozastavenia platnosti certifikátu, zrušenie certifikátu, obnova certifikátu, obnova kľúčov.
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 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).
NBUCA	Je organizačná zložka Sekcie NBÚ SR pre elektronický podpis spolu so svojou infraštruktúrou, ktorá zaisťuje akreditované certifikačné služby v zmysle Zákona č. 215 / 2002 Z.z. o elektronickom podpise.
Obnova certifikátu ***(Certificate Renewal)***	Obnova certifikátu v kontexte tohto dokumentu znamená vydanie nového certifikátu s rovnakými alebo 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. *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 *(CRL)*	Zoznam certifikátov, ktorých platnosť bola pozastavená alebo zrušená. Zoznam vydáva a podpisuje Certifikačná autorita a je publikovaný v adresári LDAP.
Zoznam zrušených certifikátov certifikačných autorít *(ARL)*	Zoznam kvalifikovaných certifikátov certifikačných kľúčov certifikačných autorít (vrátane KCA), ktorých platnosť bola pozastavená alebo zrušená. Zoznam vydáva a podpisuje Koreňová Certifikačná autorita. 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 *(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)*
IT	Informačná technológia *(Information Technology)*
KCA	Koreňová certifikačná autorita
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 certifikáty certifikačných kľúčov koreňovej certifikačnej autority NBÚ SR (v ďalšom iba „CP“), prezentuje metodiku, záväzné postupy a zodpovednosti Národného bezpečnostného úradu (v ďalšom iba „Úrad) pre vydávanie a správe certifikátov certifikačných kľúčov koreňovej certifikačnej autority (v ďalšom iba „KCA“)

CP je v súlade s Pravidlami pre výkon certifikačných činností (Certification Practice Statement, ďalej len „CPS“) OID 1.3.158.36061701.0.0.0.1.1.1, ktoré poskytujú detailné informácie o postupoch a opatreniach na výkon certifikačných činností.

CP je záväzným dokumentom, slúžiacim ako štandard zásad, procedúr a postupov, ktoré musia dodržiavať všetky zúčastnené strany.

1.2 Identifikácia CP

Certifikačný poriadok pre certifikáty certifikačných kľúčov koreňovej certifikačnej autority NBÚ SR je identifikovaný objektovým identifikátorom odvodeným od objektového identifikátora NBÚ SR.

Objektový identifikátor CP pre certifikačné kľúče KCA (OID) má tvar:

1.3.158.36061701.0.0.0.1.2.1

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	Koreňová CA NBÚ
2	Dokument „Certifikačný poriadok pre certifikáty certifikačných kľúčov KCA“
1	verzia 1 dokumentu „Certifikačný poriadok pre certifikáty certifikačných kľúčov KCA“

1.3 Charakteristika, použiteľnosť a subjekty pracujúce s certifikátmi

1.3.1 Charakteristika certifikátu

Certifikát certifikačného kľúča koreňovej certifikačnej autority je certifikát, ktorý Koreňová certifikačná autorita (KCA) vydáva na vlastný verejný kľúč Úradu v podobe autocertifikátu (self-signed certifikat), ktorého zaručený elektronický podpis je vyhotovený súkromným kľúčom, ktorý je súčasťou toho istého kľúčového páru ako verejný kľúč z certifikátu, a ktorý patrí Úradu.

1.3.2 Certifikačné kľúče NBÚ

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

1.3.3 Použiteľnosť certifikátu

Certifikáty certifikačných kľúčov koreňovej certifikačnej autority NBÚ SR môžu byť použité:

1) Overovanie platnosti kvalifikovaných certifikátov certifikačných kľúčov akreditovaných certifikačných autorít vydaných Úradom.
2) Overovanie platnosti krížových certifikátov uznaných zahraničných certifikačných autorít, ktoré vydal Úrad.
3) Overovanie platnosti zoznamov zrušených kvalifikovaných certifikátov certifikačných kľúčov akreditovaných certifikačných autorít, ktoré vydal Úrad.
4) Overovanie platnosti zoznamov zrušených krížových certifikátov uznaných zahraničných certifikačných autorít, ktoré vydal Úrad.
5) Overovanie platnosti technologických certifikátov KCA.
6) Overovanie platnosti zoznamov zrušených Technologických certifikátov KCA.

Akékoľvek iné použitie kvalifikovaného certifikátu certifikačného kľúča KCA sa považuje za neoprávnené použitie certifikátu.

1.3.4 Subjekty pracujúce s certifikátom certifikačného kľúča KCA

1.3.4.1 Certifikačná autorita

Certifikačnou autoritou sa v rámci tohto CP rozumie koreňová certifikačná autorita (KCA) Úradu, zriadená a prevádzkovaná podľa ustanovení Zákona o elektronickom podpise č. 215/2002 Z.z..

1.3.4.2 Registračná autorita

Služby registračnej autority v zmysle tohoto CP vykonáva Úrad.

1.3.4.3 Správca adresárov

Správcom adresárov v zmysle tohoto CP je Úrad.

1.3.4.4 Držiteľ certifikátu

Držiteľom certifikátu je Úrad.

1.3.4.5 Používatelia certifikátu

Používateľmi certifikátu certifikačného kľúča KCA sú:

a) Akreditované certifikačné autority.

b) Zahraničné certifikačné autority uznané v SR.

c) Klienti akreditovaných certifikačných autorít a zahraničných certifikačných autorít.

1.4 Kontaktné informácie

Špecifikácia administrátorskej organizácie

Tento certifikačný poriadok je plne spravovaný Sekciou pre elektronický podpis 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 Záväzky jednotlivých subjektov

2.1.1 Záväzky Certifikačnej autority

KCA ako certifikátor svojho vlastného certifikačného kľúča je povinná.

a) Zaistiť kontrolu vlastníctva a správneho priradenia súkromného kľúča z patričného kľúčového páru k certifikovanému verejnému kľúču.

b) Zabezpečiť správnosť všetkých informácií v tele certifikátu certifikačného kľúča a ich súlad s jeho certifikačným profilom.

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

d) Včas zverejniť informácie o novovydanom 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 Záväzky držiteľa certifikátu

Podľa zákona č. 215/2002 Z.z. je KCA je povinná:

a) Používať súkromné kľúče prislúchajúce k certifikátu certifikačného kľúča 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 Záväzky používateľa certifikátu (spoliehajúcej sa strany)

Používatelia certifikáty sú povinní používať certifikát certifikačného kľúča KCA NBÚ v súlade s použiteľnosťou certifikátu definovanou v kapitole č 1.3.3. „Použiteľnosť certifikátu“

2.1.4 Záväzky správcov adresárov

Správca adresárov je povinný zabezpečiť:

a) Včasné a presné publikovanie certifikátu.

b) Včasné a presné publikovanie zoznamov zrušených certifikátov, ktoré sa týkajú certifikátu certifikačného kľúča KCA NBÚ.

2.2 Právne záruky

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

2.3 Finančná zodpovednosť

V rámci tohto CP nie je stanovená žiadna finančná zodpovednosť.

2.4 Rozhodcovské konanie a riešenie sporov

Spory, ktoré sa týkajú používania certifikátov certifikačného kľúča koreňovej CA sa riešia v zmysle platných zákonov a ostatných všeobecne záväzných predpisov SR.

2.5 Zverejňovanie informácií

Úrad 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

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

V listinnej podobe je dokumentácia k dispozícii na Sekcii elektronického podpisu NBÚ.

2.5.2 Zverejňovanie certifikátov

Kvalifikovaný certifikát certifikačného kľúča KCA zverejňuje Úrad:

a) V adresárových službách dostupných 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?cacertifikate?

b) Samostatne na internetovej stránke http://ep.nbusr.sk.

c) V listinnej podobe je dokumentácia k dispozícii na Sekcii elektronického podpisu NBÚ.

d) V dennej tlači.

2.5.3 Zverejňovanie zoznamov zrušených certifikátov

Úrad publikuje zoznamy zrušených kvalifikovaných certifikátov KCA na internetových stránkach:

CRL: http://ep.nbusr.sk/kca/crls/current_master_c.crl

ARL: http://ep.nbusr.sk/kca/crls/current_master_a.crl

ARLDP: http://ep.nbusr.sk/kca/crls/current_a.crl

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 v oblasti auditu zhody riadi ustanoveniami CPS.

2.7 Dôvernosť

Tento CP sa v oblasti dôvernosti riadi ustanoveniami CPS.

2.8 Ochrana intelektuálnych práv

Tento CP sa v oblasti ochrany intelektuálnych práv riadi ustanoveniami príslušného CPS.

3. Identifikácia a autentifikácia

3.1 Mená konvencia

Pre certifikát certifikačného kľúča koreňovej CA platí nasledovná menná konvencia

Subject (držiteľ) certifikátu:

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

Vydavateľ certifikátu:

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

3.1.1 Pravidlá na zabezpečenie jednoznačnosti mien

Jednoznačnosť mena KCA je zabezpečená jej postavením v systéme.

3.1.2 Riešenie sporov týkajúcich sa mien

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

3.2 Iniciálna registrácia Koreňovej certifikačnej autority

Iniciálna registrácia Koreňovej certifikačnej autority sa vykonáva v procese formálneho založenia koreňovej certifikačnej autority v procedúre jej vytvárania. Na autentizáciu koreňovej certifikačnej autority v procese iniciálnej registrácie slúži Zákon č 215/2002 Z.Z o elektronickom podpise a rozhodnutie riaditeľa Sekcie NBÚ pre elektronický podpis o zriadení Koreňovej certifikačnej autority.

3.3 Spôsob preukázania vlastníctva súkromného kľúča

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

3.4 Vydanie následného certifikátu

Vydávanie následného certifikátu metódou výmeny kľúčov v existujúcom certifikáte nie je povolené v zmysle tohoto CP.

3.5 Vydanie následného certifikátu po zrušení certifikátu

Vydávanie následného certifikátu metódou výmeny kľúčov po zrušení certifikátu v existujúcom certifikáte nie je povolené v zmysle tohoto CP.

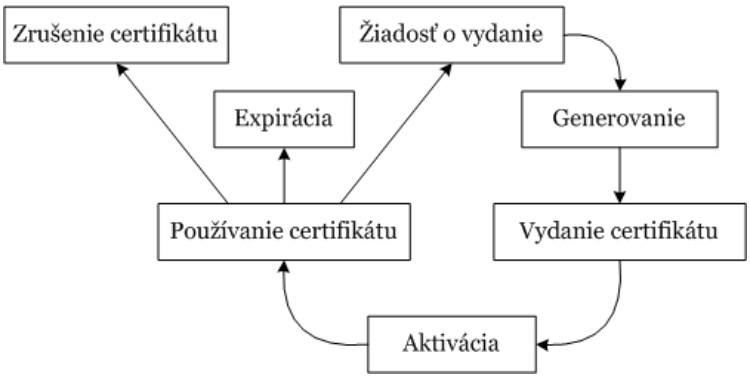
3.6 Žiadosť o zrušenie certifikátu

Žiadosť o zrušenie certifikátu certifikačného 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 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,
- Expirácia,
- Archivácia.

Sekundárnym stavom je zrušenie certifikátu.

4.1 Generovanie certifikačných kľúčov KCA

Kľúčový pár KCA – verejný a súkromný kľúč KCA – určené na certifikáciu a preverovanie certifikátov (certifikačný 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 certifikačného páru sa vykonáva okamžite po jeho vygenerovaní.

4.2 Žiadosť o vydanie certifikátu certifikačného kľúča KCA

Žiadosť o vydanie certifikátu certifikačného kľúča KCA podáva Úrad sám sebe z formálnych dôvodov (naplnenie požiadavky zákona 215, §15, ods. 4) písomnou formou. S ohľadom na charakter certifikátu a postup pri certifikácii certifikačného kľúča KCA nie je potrebná žiadosť o vydanie certifikátu vo formáte PKCS#10.

4.3 Vydanie kvalifikovaného certifikátu certifikačného kľúča KCA

Kvalifikovaný certifikát verejného kľúča KCA je vydaný podľa postupu, označovaného ako Certificate Signing Event (CSE). V rámci tohto postupu vyžadujú nasledovné osoby ako svedkovia:

- Bezpečnostný správca KCA
- Bezpečnostný audítor KCA
- jeden zamestnanec Úradu a
- jeden nezávislý svedok

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

Po zadaní certifikačných informácií do príslušnej aplikácie sa vygeneruje certifikačný kľúčový pár KCA a certifikát certifikačného kľúča KCA. Uloženie a zálohovanie súkromného kľúča je vykonané v súlade s procedúrami popísanými v CPS.

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

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

Aby bolo možné využiť certifikačné kľúče následníka KCA pri poskytovaní certifikačných služieb, musia byť vydané vzájomné krížové certifikáty pre používaný verejný certifikačný kľúč KCA a verejný certifikačný kľúč následníka KCA.

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

4.4 Prevzatie certifikátu

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 v CPS.

d.) Ak zrušenie certifikátu nariadila oprávnená tretia strana (súd, alebo vláda SR).

e.) Ak KCA ukončila svoju činnosť.

4.5.2 Strany, ktoré môžu žiadať o zrušenie

O zrušenie certifikátu certifikačného kľúča KCA môže požiadať:

a) KCA.

b) Oprávnená tretia strana (súd, alebo vláda SR).

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 hierarchie NBUCA je kľúčové bezodkladné overenie a spracovanie požiadavky na zrušenie certifikátu certifikačného kľúča KCA. Procedúra zrušenia certifikátu je opísaná v CPS.

4.5.4 Interval na zrušenie certifikátu

Interval na zrušenie certifikátu je 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 certifikačného kľúča KCA budú prístupné na Sekcii elektronického podpisu a zverejnené v dennej tlači.

4.6 Audit bezpečnosti

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

Záznamy vznikajúce pri certifikačných činnostiach spojených s certifikátmi certifikačných kľúčov 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 operácii a zabezpečovali minimalizáciu prerušenia poskytovaniea 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

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 vniknuté prípadnou havarijnou situáciou.

4.10 Skončenie činnosti KCA

Činnosť KCA NBÚ sa zakladá na ustanoveniach Zákona 215/2002 Z.z. o elektronickom podpise. Činnosť KCA NBÚ môže byť ukončená iba zmenou alebo zrušením tohoto 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. 88/2002 Z.z. o fyzickej a objektovej bezpečnosti.

5.2 Opatrenia na zaistenie procedurálnej bezpečnosti

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

Personál KCA NBÚ je preverovaný v zmysle Vyhlášky NBÚ č. 2/2002 Z.z. o personálnej bezpečnosti. 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

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 hardvérovom kryptografickom module Private Server/GP firmy Algorithmic Research. Hardvérový kryptografický modul bol certifikovaný NSA podľa FIPS 140-1 na bezpečnostnú úroveň 3.

Kryptografický modul Server/GP 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, passfráza) a obmedziť používane aktív podmienkou kontroly výkonu viacerými používateľmi.

Kryptografický modul Private Server/GP 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 certifikačného kľúča:

Pole	Kritické	Obsah
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 Organizational 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 Authority Key Identifier		
2.1.1 Key Identifier		SKID vydavateľa tohto certifikátu
2.1.2 AuthorityCertIssuer		Nenachádza sa

Pole	Kritické	Obsah
2.1.3 AuthorityCertSerialNumber		Nenachádza sa
2.2 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“).
2.3 Key Usage	Critical	
2.3.1 Digital Signature		
2.3.2 Non Repudiation		
2.3.3 Key Encipherment		
2.3.4 Data Encipherment		
2.3.5 Key Agreement		
2.3.6 Key Certificate Signature		Zvolené
2.3.7 CRL Signature		
2.4 Certificate Policies	Critical	
2.4.1 Policy Identifier		1.3.158.36061701.0.0.0.1.2.1
2.4.2 Policy Qualifier Infor		
2.4.2.1 Policy Qualifier ID		CPS (1.3.6.1.5.5.7.2.1)
2.4.2.2 Policy Qualifier		http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_1.pdf
2.4.3 Policy Qualifier Infor		
2.4.3.1 Policy Qualifier ID		User Notice (1.3.6.1.5.5.7.2.2)
2.4.3.2 Policy Qualifier		Tento certifikat je vydany ako kvalifikovany certifikat „Korenovej CA pre kvalifikovane certifikaty“ v sulade so zakonom c. 215/2002 Z.z.
2.5 Subject Alternate Name		
2.5.1 RFC822Name		(voliteľné)
2.6 CRL Distribution Point		Nenachádza sa
2.7 Basic Constraints	Critical	Nachádza sa
2.7.1 Subject Type		CA
2.7.2 Path Length Constraint		2
2.8 Authority Information Access		Nenachádza sa.

7.2 Profil ARL

Zoznam zneplatnených certifikátov certifikačných kľúčov KCA (Authority Revocation List) obsahuje záznamy o zneplatnených certifikátoch a certifikátoch s pozastavenou platnosťou v čase vydania ARL. ARL je potvrdený digitálnym podpisom KCA. Digitálny podpis je vytvorený kombináciou algoritmov SHA1 a RSA. Dĺžka podpisovacieho kľúča RSA externej CA je 2048 bitov.

Zoznam odvolaných certifikátov pre túto triedu certifikátov vydáva PKI VUB každých 12 hodín.

Pole ARL	Kritické	Obsah poľa
1. ARL Body		
1.1 Version		v2
1.2 signatureAlgorithm		SHA 1 + RSA
1.3 Issuer Distinguished Name		
1.3.1 Common Name (CN)		Korenova CA pre kvalifikovane certifikaty 1*
1.3.2 Locality (L)		Bratislava
1.3.3 Organization Unit (OU)		Sekcia elektronickeho podpisu
1.3.4 Organization (O)		Narodny bezpecnostny urad
1.3.5 Country (C)		SK
1.4 thisUpdate		Dátum a čas vydania ARL
1.5 nextUpdate		Dátum a čas vydania najbližšieho ARL
1.7 revokedCertificates		Zoznam odvolaných certifikátov
1.7.1 userCertificate		Sériové číslo revokovaného certifikátu
1.7.2. revocationDate		Čas revokácie certifikátu
1.8 crlEntryExtensions		
1.8.1 Reason Code		Príčina revokácie certifikátu
2. arl Extensions		
2.1. Authority Key Identifier		Identifikátor certifikačného kľúča, použitého na podpísanie ARL, pozostávajúci z 160-bitového SHA-1 hashu informácie uvedenej v subjectPublicKey (s výnimkou „tag“, „length“ a „number of unused bits“).
2.2 ARL Number		Pridelené pri generovaní ARL
2.3 IssuingDistributionPoint	critical	http://ep.nbusr.sk/kca/crls/current_a.crl

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 realizácii.

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 rovnovýznamovými slovami, 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 pozícii A.

8.2 Schvaľovanie verzií

Tento CP schvaľuje riaditeľ Sekcie NBÚ pre elektronický podpis.

9. Účinnosť certifikačného poriadku

Certifikačný poriadok certifikačného kľúča nadobúda účinnosť dňom 25.06.2003.