Národný bezpečnostný úrad

sekcia informačnej bezpečnosti a elektronického podpisu

Pravidlá na výkon certifikačných činností koreňovej certifikačnej autority

Verzia: 3.0

Dokument nadobúda účinnosť dňa 17. 8. 2010

Obsah

Zoznam použitých pojmov

adresárové služby	špecializovaná databáza, v ktorej sú zverejňované certifikáty a zoznamy zrušených certifikátov
certifikačná autorita	dôveryhodná autorita, ktorá generuje certifikáty a zoznamy zrušených certifikátov (komponent infraštruktúry PKI)
certifikačné služby	služby, ktoré poskytuje certifikačná autorita (registrácia, certifikácia, overenie platnosti a funkčnosti certifikátu, zrušenie certifikátu, výmena kľúčov)
certifikačný poriadok	pomenovaný zoznam pravidiel, ktoré označujú použiteľnosť certifikátu v príslušnej skupine alebo triede aplikácií zdieľajúcej spoločné bezpečnostné požiadavky.
certifikácia	proces, počas ktorého certifikačná autorita na základe štandardizovanej žiadosti vydá k príslušnému verejnému kľúču certifikát
certifikát	Reťazec údajov, ktorý spája identifikátor (Distinguished Name) entity 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.
certifikát na správu	certifikát slúžiaci na overenie platnosti kvalifikovaného certifikátu – certifikát úradu, certifikát akreditovanej certifikačnej autority, certifikát časovej pečiatky, certifikát na overenie potvrdenia existencie a platnosti certifikátov a certifikát na overenie zoznamu zrušených certifikátov
digitálny podpis	Jedinečná digitálna identifikácia entity, ktorá sa využíva na autentifikáciu zdroja, integrity dát a nepopierateľnosti. 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 poskytovania certifikačných služieb
KCA	Koreňová certifikačná autorita Národného bezpečnostného úradu.
kľúčový pár	dvojica asymetrických kľúčov, ktorá pozostáva zo súkromného a verejného kľúča
kompromitácia súkromného kľúča	Zneužitie, použitie alebo sprístupnenie súkromného kľúča bez vedomia jeho vlastníka, ako aj prezradenie hesla na prístup k revokačnému heslu. Ak certifikačná autorita zistí kompromitáciu súkromného kľúča, certifikát zviazaný s týmto kľúčom zruší.
HSM	kryptografický modul hardvérovej ochrany kľúča umožňujúci vykonávať kryptografické operácie
KvCSR	Kvalifikovaný certifikát fyzickej osoby vydaný v súlade s platnými právnymi predpismi Slovenskej republiky a vydaný v certifikačnej ceste Koreňovej certifikačnej autority Národného bezpečnostného úradu. Na identifikáciu KvCSR slúži certifikačný poriadok s OID identifikátorom 1.3.158.36061701.0.0.0.1.2.2.
obnova kľúčov	Obnova kľúčov v kontexte tohto dokumentu znamená vydanie nového certifikátu s rovnakými alebo veľmi podobnými charakteristikami ako pôvodný (obnovovaný) certifikát. Generuje sa nová dvojica kľúčov prislúchajúca k certifikátu.

pravidlá na výkon certifikačných činností	zoznam predpisov a praktík, ktoré certifikačné autority používajú pri vydávaní certifikátov
registračná autorita	komponent infraštruktúry PKI používaný na posúvanie schválených žiadostí o vydanie certifikátu do certifikačnej autority
spoliehajúca strana	subjekt alebo komponent, ktorý požaduje od PKI infraštruktúry overenie stavu certifikátu
súkromný kľúč	súkromná časť dvojice asymetrických kľúčov, ktorá sa používa na podpisovanie a (alebo) dešifrovanie správ
verejný kľúč	verejná časť dvojice asymetrických kľúčov, ktorá sa používa na overovanie a (alebo)dešifrovanie správ
zrušenie certifikátu	Predčasné ukončenie platnosti certifikátu. Platnosť certifikátu nie je možné obnoviť.
zoznam zrušených certifikátov	zoznam všetkých zrušených neexpirovaných certifikátov vydaných CA

Skratky

ANSI	American National Standards Institute
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
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, druhá inkarnácia koreňovej certifikačnej autority
KCA3	druhý následník koreňovej certifikačnej autority, tretia inkarnácia koreňovej certifikačnej autority
KvCSR	kvalifikovaný certifikát fyzickej osoby
L	lokalita (Locality)
LDAP	protokol pre prístup k adresárovým službám *(Lightweight Directory Access Protocol)*
NBÚ	Národný bezpečnostný úrad
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)
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SIBEP	sekcia informačnej bezpečnosti a elektronického podpisu
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
TSL	dôveryhodný zoznam poskytovateľov (Trusted List)
Z.z.	zbierka zákonov

1. Úvod

1.1 Účel dokumentu

Dokument „Pravidlá na výkon certifikačných činností koreňovej certifikačnej autority“ prezentuje vykonávacie postupy a praktiky, ktoré Národný bezpečnostný úrad (ďalej len „NBÚ“) využíva na zabezpečenie certifikačných služieb poskytovaných koreňovou certifikačnou autoritou (ďalej len „KCA“) v zmysle zákona 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“).

Tento dokument obsahujúci pravidlá na výkon certifikačných činností, angl. Certification Practice Statement (ďalej len „CPS“) slúži používateľom a spoliehajúcim sa tretím stranám ako podklad pre posúdenie dôveryhodnosti poskytovania certifikačných služieb KCA.

1.2 Identifikácia CPS

Tieto CPS sú identifikované pomocou objektového identifikátora (ďalej len „OID“) odvodeného od OID NBÚ.

OID týchto CPS má tvar:

1.3.158.36061701.0.0.0.1.1.2

kde jednotlivé zložky OID majú nasledovný význam:

1	ISO
3	ISO Identified Organization
158	Slovakia
36061701	jedinečný identifikátor NBÚ priradený organizáciou ISO (IČO)
0	riaditeľ NBÚ
0	sekcia informačnej bezpečnosti a elektronického podpisu
0	KCA
1	dokumentácia KCA
1	Pravidlá na výkon certifikačných činností
2	Pravidlá na výkon certifikačných činností KCA

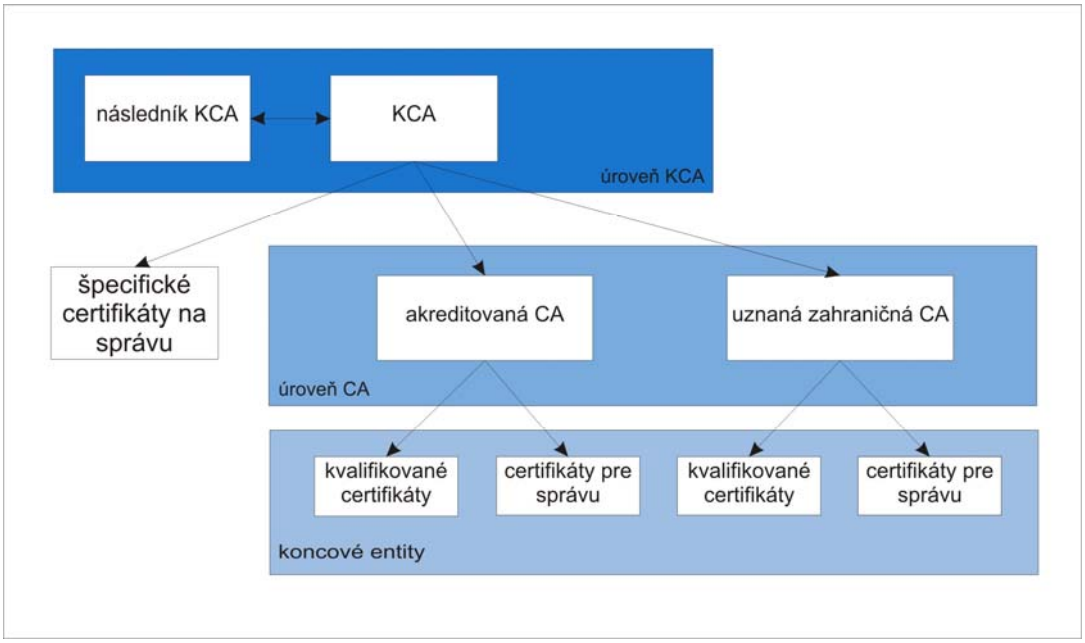
1.3 Podporované certifikačné poriadky

Tieto CPS podporujú „Certifikačný poriadok pre koreňovú CA a akreditované CA vydávajúce kvalifikované certifikáty a certifikáty na správu v súlade s platnými právnymi predpismi SR, najmä zákonom č. 215/2002 Z.z. o elektronickom podpise, OID: 1.3.158.36061701.0.0.0.1.2.2 (ďalej len „CP“).

1.4 Komunita a účel použitia CPS

Tieto CPS špecifikujú certifikačné služby poskytované pri vydávaní a správe certifikátov verejných kľúčov (ďalej len „certifikáty“) vydávaných KCA spolu s pravidlami a postupmi, ktoré NBÚ ako prevádzkovateľ KCA využíva na zabezpečenie týchto služieb.

V nasledujúcom diagrame je zobrazený model dôvery certifikačných služieb poskytovaných KCA.



1.4.1 Koreňová certifikačná autorita

Koreňovou certifikačnou autoritou (KCA) sa v rámci týchto CPS rozumie koreňová certifikačná autorita Slovenskej republiky zriadená a prevádzkovaná NBÚ podľa ustanovení zákona č. 215/2002 Z.z. o elektronickom podpise. KCA je z technologického hľadiska vybudovaná ako off-line certifikačná autorita.

1.4.2 Registračná autorita KCA

Služby registračnej autority v zmysle týchto CPS vykonáva NBÚ. NBÚ prevádzkuje registračnú autoritu KCA, ktorá slúži na registráciu a overovanie žiadostí o vydanie a zrušenie certifikátov vydávaných KCA. Registračná autorita KCA je z technologického hľadiska vybudovaná ako off-line registračná autorita.

Kontaktné údaje na registračnú autoritu sú uvedené v bode 1.7.4 týchto CPS.

1.4.3 Držitelia certifikátov vydávaných KCA (Subscribing Party)

Držiteľmi certifikátov vydávaných KCA sú:

a) NBÚ ako zriaďovateľ a prevádzkovateľ KCA,
b) akreditované certifikačné autority (ďalej len „akreditované CA“),
c) uznané zahraničné certifikačné autority (ďalej len „uznané zahraničné CA“),
d) držitelia špecifických certifikátov na správu vydávaných KCA.

1.4.4 Používatelia certifikátov vydávaných KCA (Relying Party)

Používateľmi certifikátov vydaných KCA sú:

a) akreditované CA,
b) uznané zahraničné CA,
c) klienti akreditovaných CA a uznaných zahraničných CA,
d) držitelia špecifických certifikátov na správu vydávaných KCA.

1.5 Druhy certifikátov vydávané KCA

KCA podľa § 10 zákona č. 215/2002 Z.z. o elektronickom podpise vydáva nasledovné druhy certifikátov:

a) certifikát vlastného verejného kľúča,
b) certifikáty následníkov KCA,
c) krížové certifikáty KCA a následníka KCA vydávané v rámci procesu výmeny kľúčov KCA,
d) certifikáty pre akreditované CA,
e) certifikáty pre uznané zahraničné CA,
f) špecifické certifikáty na správu: certifikáty obslužného personálu KCA (operátori KCA) a certifikáty pre podpisovanie slovenského dôveryhodného zoznamu poskytovateľov (ďalej len „TSL“) a schválených podpisových politík.

1.6 Použiteľnosť certifikátov vydávaných KCA

1.6.1 Certifikát KCA

Certifikát KCA vygenerovaný ako sebou podpísaný (self-signed) certifikát je možné používať výlučne na:

a) overovanie platnosti certifikátov akreditovaných CA vydávaných KCA,
b) overovanie platnosti certifikátov uznaných zahraničných CA vydávaných KCA,
c) overovanie platnosti špecifických certifikátov na správu vydávaných KCA,
d) overovanie platnosti zoznamov zrušených certifikátov (ďalej len „CRL“) vydávaných KCA.

Akékoľvek iné použitie certifikátu KCA sa považuje za neoprávnené použitie certifikátu.

1.6.2 Certifikát následníka KCA

Certifikát následníka KCA vygenerovaný ako sebou podpísaný (self-signed) sa používa na zabezpečenie kontinuity certifikačných činností KCA. Kľúčový pár následníka KCA nahradí kľúčový pár KCA a certifikát následníka KCA sa stane aktuálne platným certifikátom KCA.

Od okamihu vydania certifikátu následníka KCA je možné vydávať nové certifikáty len využitím kľúčového páru následníka KCA s výnimkou vydania krížového certifikátu pre následníka KCA, ktorý je možné vydať na pôvodnej KCA. Nahradzovaný kľúčový pár KCA je od okamihu vydania certifikátu následníka KCA možné používať len na zrušovanie už vydaných certifikátov a vydávanie zoznamov CRL.

Použitie certifikátu následníka KCA je po výmene kľúčov obdobné ako použitie certifikátu KCA a je uvedené v bode 1.6.1 týchto CPS. Popis procesu výmeny kľúčov KCA je uvedený v bode 4.10 týchto CPS.

Akékoľvek iné použitie certifikátu následníka KCA sa považuje za neoprávnené použitie certifikátu.

1.6.3 Krížové certifikáty KCA a následníka KCA vydávané v rámci procesu výmeny kľúčov KCA

KCA môže počas procesu výmeny vlastného kľúčového páru vydať krížové certifikáty KCA a následníka KCA. Tieto certifikáty je možné použiť na vzájomné overenie certifikátov KCA a následníka KCA.

Akékoľvek iné použitie certifikátu následníka KCA sa považuje za neoprávnené použitie certifikátu.

1.6.4 Certifikáty akreditovaných CA

Certifikát akreditovanej CA vydaný KCA môže byť použitý na:

a) overovanie platnosti kvalifikovaných certifikátov fyzických osôb vydávaných podľa platných právnych predpisov Slovenskej republiky (ďalej len „KvCSR“) vydávaných akreditovanou CA,

b) overovanie platnosti certifikátov na správu vydávaných akreditovanou CA,

c) overovanie platnosti zoznamov CRL vydávaných akreditovanou CA,

d) overovanie platnosti nepriamych zoznamov zrušených certifikátov (aj v on-line režime),

e) overenie platnosti časových pečiatok.

Akékoľvek iné použitie certifikátu akreditovanej CA vydaného KCA sa považuje za neoprávnené použitie certifikátu.

1.6.5 Certifikáty uznaných zahraničných CA

Certifikát uznanej zahraničnej CA vydaný KCA môže byť použitý na:

a) overovanie platnosti KvCSR vydávaných uznanou zahraničnou CA,

b) overovanie platnosti certifikátov na správu vydávaných uznanou zahraničnou CA,

c) overovanie platnosti zoznamov CRL vydávaných uznanou zahraničnou CA,

d) overovanie platnosti nepriamych zoznamov zrušených certifikátov (aj v on-line režime),

e) overenie platnosti časových pečiatok.

Akékoľvek iné použitie certifikátu uznanej zahraničnej CA vydaného KCA sa považuje za neoprávnené použitie certifikátu.

1.6.6 Špecifické certifikáty na správu

1.6.6.1 Certifikáty obslužného personálu KCA

Certifikát obslužného personálu KCA (operátori KCA) vydaný KCA môže byť použitý na autentizáciu operátora KCA k aktívam KCA.

Akékoľvek iné použitie certifikátu obslužného personálu KCA vydaného KCA sa považuje za neoprávnené použitie certifikátu.

Postupy generovania kľúčov, iniciálnej registrácie, vydávania certifikátov, vydávania následných certifikátov a zrušovania certifikátov obslužného personálu KCA sú súčasťou interných technických predpisov KCA.

1.6.6.2 Certifikáty pre podpisovanie slovenského TSL a schválených podpisových politík

Certifikát určený pre podpisovanie slovenského TSL a schválených podpisových politík sa používa na overovanie podpisu slovenského TSL a podpisu schválených podpisových politík.

Akékoľvek iné použitie certifikátu pre podpisovanie slovenského TSL a schválených podpisových politík sa považuje za neoprávnené použitie certifikátu.

Postupy generovania kľúčov, iniciálnej registrácie, vydávania certifikátov, vydávania následných certifikátov a zrušovania certifikátov podpisovateľa slovenského TSL a schválených podpisových politík sú súčasťou interných technických postupov KCA.

1.7 Kontaktné informácie KCA

1.7.1 Špecifikácia administrátorskej organizácie

Tieto CPS sú spravované sekciou informačnej bezpečnosti a elektronického podpisu NBÚ.

1.7.2 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

1.7.3 Kontaktná osoba

Všetky otázky, pripomienky a návrhy k týmto CPS 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
podatelna@nbusr.sk
secadmin@nbusr.sk

1.7.4 Kontaktné informácie registračnej autority

Adresa registračného miesta registračnej autority KCA:

Sekcia informačnej bezpečnosti a elektronického podpisu
Národný bezpečnostný úrad
Budatínska 30
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
podatelna@nbusr.sk
secadmin@nbusr.sk

Stránkové hodiny registračného miesta registračnej autority KCA:

Pondelok	7:30 – 15:30
Utorok	7:30 – 15:30
Streda	7:30 – 15:30
Štvrtok	7:30 – 15:30
Piatok	7:30 – 15:30

2. Všeobecné ustanovenia

2.1 Povinnosti

2.1.1 Povinnosti KCA pri správe certifikátov

Povinnosti certifikačnej autority pri správe certifikátov podľa § 16 zákona č. 215/2002 Z.z. o elektronickom podpise, ktoré sa vzťahujú i na KCA sú:

a) KCA vydaním certifikátu potvrdzuje pravosť predloženého verejného kľúča a skutočnosť, že držiteľ certifikátu disponuje súkromným kľúčom, ku ktorému patrí predložený verejný kľúč,

b) KCA potvrdzuje pravosť verejného kľúča držiteľa certifikátu tak, že po overení potrebných náležitostí vydá žiadateľovi certifikát, ktorý KCA podpíše elektronickým podpisom využitím svojho súkromného kľúča,

c) overenie potrebných náležitostí žiadateľa o vydanie certifikátu (dokladov, vlastníctva súkromného kľúča patriaceho k predloženému verejnému kľúču) realizuje KCA prostredníctvom registračnej autority konajúcej v mene KCA,

d) KCA je povinná vytvoriť podmienky, ktoré umožnia overovateľovi overiť platnosť certifikátu, ktorý KCA vydala. Na tento účel je KCA povinná zabezpečiť, aby jej verejný kľúč bol pre overovateľa dostupný z viacerých informačných zdrojov.

2.1.2 Povinnosti registračnej autority KCA

Podľa § 21 ods. 4 zákona č. 215/2002 Z.z. o elektronickom podpise registračná autorita KCA najmä:

a) prijíma žiadosti o vydanie certifikátu,

b) kontroluje súlad údajov v žiadosti o vydanie certifikátu s údajmi v predloženom preukaze totožnosti žiadateľa o vydanie certifikátu,

c) odosiela žiadosti o vydanie certifikátu certifikačnej autorite,

d) odovzdáva certifikáty žiadateľom o vydanie certifikátu.

Registračná autorita KCA rovnako slúži na prijímanie a schvaľovanie, resp. zamietanie žiadostí o zrušenie certifikátu.

Registračná autorita KCA je povinná riadiť sa internými predpismi vydávanými KCA, ktoré upravujú jej činnosť.

2.1.3 Povinnosti držiteľov certifikátov vydaných KCA

Podľa § 22 zákona č. 215/2002 Z.z. o elektronickom podpise sú povinnosti držiteľa certifikátu vydaného KCA nasledovné:

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

b) uvádzať presné, pravdivé a úplné informácie vo vzťahu k certifikátu svojho verejného kľúča,

c) neodkladne požiadať KCA, ktorá spravuje jeho certifikát, o zrušenie certifikátu, ak zistí, že došlo k neoprávnenému použitiu jeho súkromného kľúča, alebo ak hrozí neoprávnené použitie jeho súkromného kľúča alebo ak nastali zmeny v údajoch uvedených v certifikáte v súlade s predpísaným postupom popísaným v bode 4.6 týchto CPS.

Držiteľ certifikátu môže certifikáty používať výhradne v súlade s týmito CPS a v súlade s CP. Musí dodržiavať všetky lehoty, podmienky a obmedzenia týkajúce sa používania súkromných kľúčov a certifikátov v súlade s týmito CPS a v súlade s CP.

Podľa § 21 zákona č. 215/2002 Z.z. o elektronickom podpise za škodu spôsobenú porušením povinností zodpovedá držiteľ certifikátu podľa všeobecných predpisov o náhrade škody.

2.1.4 Povinnosti používateľov certifikátov vydaných KCA

Používatelia certifikátov vydaných KCA sú povinní používať tieto certifikáty v súlade s použiteľnosťou certifikátov definovanou v bode 1.6 týchto CPS a v súlade s CP.

2.1.5 Povinnosti správcu adresárov KCA

Správcom adresárových služieb KCA je NBÚ. Správca adresárových služieb KCA je povinný zabezpečiť:

a) včasné a presné zverejňovanie všetkých certifikátov vydaných KCA s výnimkou certifikátov obslužného personálu KCA,

b) včasné a presné zverejňovanie aktuálnych zoznamov CRL vydaných KCA tak, aby interval medzi zverejnením dvoch po sebe nasledujúcich zoznamov CRL a ARL nepresiahol 24 hodín,

c) nepretržitú prevádzku služby zverejňovania aktuálnych zoznamov CRL vydávaných KCA,

d) nepretržitú prevádzku služby zverejňovania archívu zoznamov všetkých CRL vydaných KCA.

2.2 Právne záruky

Zodpovednosť KCA za škodu je nasledovná:

a) KCA nie je zodpovedná za prevádzku ktorejkoľvek akreditovanej CA alebo uznanej zahraničnej CA,

b) KCA nie je zodpovedná za akékoľvek následky trestných činov, priestupkov alebo porušení zmluvy vyplývajúcich z prevádzky akreditovanej CA alebo uznanej zahraničnej CA,

c) za škodu spôsobenú porušením povinností zodpovedá KCA podľa platných právnych predpisov Slovenskej republiky (ďalej len „SR“),

d) KCA ručí za to, že použije vlastné súkromné kľúče prislúchajúce k vlastným certifikátom pri podpisovaní ňou vydávaných certifikátov a zoznamov CRL,

e) v rámci každej inkarnácie (následníka), KCA poskytuje záruky na jedinečnosť sériového čísla ňou vydávaných certifikátov,

f) KCA poskytuje záruku na zrušenie ňou vydaného certifikátu, pokiaľ bola žiadosť o zrušenie certifikátu podaná spôsobom definovaným v bode 4.6 týchto CPS,

g) ak je rozsah použitia certifikátu vydávaného KCA obmedzený, KCA nezodpovedá za škodu spôsobenú tým, že certifikát bol použitý v rozpore s obmedzeniami uvedenými v certifikáte,

h) ak je v KvCSR vydanom akreditovanou CA alebo uznanou zahraničnou CA uvedené obmedzenie na výšku transakcií, na ktoré sa môže použiť, KCA nezodpovedá za škody spôsobené prekročením tejto hodnoty.

2.3 Finančná zodpovednosť

Finančná zodpovednosť jednotlivých strán je určená platnými právnymi predpismi SR.

2.4 Rozhodcovské konanie a riešenie sporov

Spory, ktoré sa týkajú používania certifikátov KCA sa riešia v zmysle platných právnych predpisov SR. Pokiaľ vznikne spor v súvislosti s týmito CPS, strany sa zaväzujú v dobrej viere vynaložiť maximálne úsilie ukončiť spor dohodou alebo s pomocou tretej strany.

Ak strany nie sú schopné riešiť spor v primeranom čase, potom sa strany spoločne dohodnú na nezávislom rozhodcovi s primeranou kvalifikáciou a praktickými skúsenosťami s riešením sporov a dohodnú sa na záväznosti výroku rozhodcu.

Spory so zahraničnými CA, ktoré nie sú slovenskými právnymi subjektmi, ale boli v zmysle § 17 zákona č. 215/2002 Z.z. o elektronickom podpise uznané NBÚ, týkajúce sa otázok poskytovania certifikačných služieb a zodpovednosti za škody spôsobené pri poskytovaní certifikačných služieb sa riešia v zmysle platných právnych predpisov SR, pričom miestom konania sporu je SR.

V prípade, že ktorékoľvek ustanovenie týchto CPS je z nejakých dôvodov uznané za neplatné, nezákonné alebo právne nevynútiteľné, toto nemá vplyv na ostatné ustanovenia týchto CPS. CPS sa v takomto prípade vykladajú tak, ako keby neplatné ustanovenia vôbec neobsahovali a aktualizácia CPS sa vykoná v súlade s ustanoveniami kapitoly 8 týchto CPS.

Ak sa tieto CPS preložia do iného jazyka ako do slovenského, bude slovenská verzia rozhodujúca.

2.5 Poplatky za služby KCA

Certifikačné služby poskytované KCA nie sú spoplatňované.

2.6 Zverejňovanie informácií KCA

KCA zverejňuje:

a) CP,

b) tieto CPS,

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

d) aktuálne zoznamy CRL vydávané KCA,

e) archív zoznamov CRL vydaných KCA,

f) informácie o stave certifikátov vydaných KCA,

g) formulár žiadosti o vydanie certifikátu pre akreditované CA a uznané zahraničné CA,

h) formulár žiadosti o zrušenie certifikátu pre akreditované CA a uznané zahraničné CA.

2.6.1 Zverejňovanie dokumentácie

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.

2.6.2 Zverejňovanie certifikátov

KCA zverejňuje nasledovné typy vydaných certifikátov:

a) certifikát vlastného verejného kľúča KCA,

b) certifikáty následníkov KCA,

c) krížové certifikáty KCA a následníka KCA vydávané v rámci procesu výmeny kľúčov KCA (ak sú vydané),

d) certifikáty vydané pre akreditované CA,

e) certifikáty vydané pre uznané zahraničné CA,

f) certifikáty pre podpisovanie slovenského TSL a schválených podpisových politík.

Tieto informácie sú verejne prístupné nasledovnými spôsobmi:

a) na nasledujúcich internetových stránkach

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

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

b) v listinnej podobe na 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

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

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

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

2.6.3 Zverejňovanie zoznamov zrušených certifikátov

KCA publikuje zoznamy CRL nasledovne:

KCA1

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

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

KCA2

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

Aktuálne CRL (HTTP):	http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl
Aktuálne CRL (LDAP)	ldap://ep.nbusr.sk/cn=KCA NBU SR,ou=Sekcia IBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList
Archív CRL (HTTP):	http://ep.nbusr.sk/kca/archive2
Archív CRL (LDAP):	ldap://ep.nbusr.sk/ou=arch crls KCA2,ou=Sekcia IBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?cRLDistributionPoint?sub?

KCA3

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

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

2.6.4 Periodicita zverejňovania informácií

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

Zároveň musí byť zabezpečené, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, ktorý obsahuje 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), ďalej len „vyhláška NBÚ č. 131/2009 Z.z.“.

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

2.6.5 Adresárové služby

Adresárové služby KCA sú poskytované prostredníctvom adresárov v správe NBÚ. Adresáre poskytujú:

a) prístup ku všetkým certifikátom vydaným KCA podliehajúcim zverejneniu,

b) informácie o stave certifikátov vydaných KCA,

c) prístup k aktuálnym zoznamom CRL vydávaných KCA,

d) prístup k archívu všetkých zoznamov CRL vydaných KCA.

2.6.5.1 Funkcie adresárov

Adresáre umožňujú vyhľadávanie v rámci adresárovej štruktúry tak, aby bolo možné:

a) zistiť informácie o všetkých certifikátoch vydaných KCA podliehajúcim zverejneniu,

b) zistiť stav každého certifikátu vydaného KCA, ktorý podlieha zverejneniu (platný, zrušený alebo expirovaný),

c) prehľadne pristúpiť k archívu všetkých zoznamov CRL vydaných KCA.

2.6.5.2 Dostupnosť adresárov

Adresárové služby sú prístupné sedem dní v týždni, 24 hodín denne s výnimkou závažnej technickej príčiny.

2.6.5.3 Obmedzenia

Prístup k informáciám nie je obmedzený na vyhľadávanie jedného mena v rámci adresárov. Adresárové služby v rozsahu uvedenom v bode 2.6.5.1 týchto CPS sú verejne prístupné.

Adresárové služby neumožňujú:

a) poskytnúť prístup k adresárom KCA iným spôsobom než je uvedené v týchto CPS,

b) poskytnúť iné informácie alebo služby v rámci KCA než je uvedené v týchto CPS.

2.6.5.4 Zverejňovanie adresárových informácií

Adresáre sú prístupné na adresách uvedených v bodoch 2.6.1, 2.6.2 a 2.6.3 týchto CPS.

Kópie adresárov môžu byť zverejňované aj na iných miestach, pokiaľ je to oprávnene požadované z hľadiska efektívnej prevádzky KCA. Tieto kópie môžu obsahovať buď celú adresárovú štruktúru alebo jej časť.

2.7 Audit bezpečnosti poskytovania certifikačných činností KCA

Na zabezpečenie bezpečnosti poskytovania certifikačných činností KCA je prevádzkovateľ KCA povinný opakovane sa podrobovať auditu bezpečnosti poskytovania certifikačných činností (ďalej len „audit bezpečnosti“).

2.7.1 Frekvencia a periodicita auditu bezpečnosti

Frekvencia a periodicita auditu bezpečnosti KCA musia byť prispôsobené tak, aby bol ukončený najneskôr do 12 mesiacov odo dňa ukončenia predchádzajúceho auditu (§ 25 zákona č. 215/2002 Z.z. o elektronickom podpise).

2.7.2 Audítor

Výber audítora vykonávajúceho audit bezpečnosti KCA sa riadi podľa § 6 ods. 2 vyhlášky NBÚ č. 132/2009 Z.z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov (ďalej len „vyhláška NBÚ č. 132/2009 Z.z.“).

Audítor vykonávajúci audit bezpečnosti KCA musí byť s prevádzkovateľom KCA vo zmluvnom vzťahu na vykonanie externého auditu a musí byť organizačne oddelený od prevádzkovateľa KCA tak, aby bol audit nezainteresovaný a nezávislý.

2.7.3 Rozsah auditu bezpečnosti

Výkon auditu pozostáva KCA pozostáva z overenia všetkých náležitostí uvedených v § 6 ods. 3 vyhlášky NBÚ č. 132/2009 Z.z.

Rozsah auditu bezpečnosti je zameraný na preverenie zhody prevádzky KCA s požiadavkami platných právnych predpisov SR, najmä s požiadavkami zákona č. 215/2002 Z.z. o elektronickom podpise a súvisiacich vykonávacích predpisov a zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „zákon č. 428/2002 Z.z. o ochrane osobných údajov“).

2.7.4 Výsledky auditu bezpečnosti

Výkon auditu bezpečnosti sa v zmysle § 6 ods. 4 vyhlášky NBÚ č. 132/2009 Z.z. končí záverečnou správou, ktorá pozostáva z výroku audítora a zo zhodnotenia celkového stavu bezpečnosti KCA v čase výkonu auditu bezpečnosti, popisu zistení o nedostatkoch bezpečnostného charakteru a odporúčaní na odstránenie zistených nedostatkov.

Rozpory medzi prevádzkou KCA a ustanoveniami uvedenými v týchto CPS, CP, bezpečnostnej politike a prevádzkovej dokumentácii musia byť zaznamenané v popise zistení o nedostatkoch bezpečnostného charakteru. Nedostatky budú odstránené v určenom termíne na základe zoznamu odporúčaní na odstránenie zistených nedostatkov.

Výsledky auditu bezpečnosti sú považované za citlivú obchodnú informáciu. Pokiaľ nie je táto skutočnosť dohodnutá inak, sú výsledky chránené v súlade s ustanoveniami uvedenými v bode 2.8 týchto CPS.

Implementácia nápravných opatrení bude oznámená príslušnej autorite. Môže sa požadovať špeciálny audit bezpečnosti na potvrdenie implementácie a efektívnosti nápravných opatrení.

NBÚ môže sprístupniť výsledky auditu verejnosti v celom rozsahu alebo čiastočne. Spôsob a rozsah zverejnenia volí NBÚ, musí však byť v súlade s ustanoveniami bodu 2.8 týchto CPS.

2.8 Dôvernosť informácií KCA

2.8.1 Typy informácií považované za citlivé

Citlivými informáciami KCA sú:

a) dáta pre vytváranie elektronických podpisov prislúchajúce k dátam pre overovanie elektronických podpisov obsiahnutých vo vlastných certifikátoch KCA,

b) niektoré kryptografické informácie potrebné pri prevádzke KCA,

c) prevádzková a bezpečnostná dokumentácia KCA okrem dokumentácie uvedenej v bode 2.6 týchto CPS,

d) všetky osobné údaje klientov podliehajúce ochrane osobných údajov v zmysle zákona č. 428/2002 Z.z. o ochrane osobných údajov.

2.8.1.1 Prístup k citlivým informáciám

Prevádzkový personál KCA má prístup iba k informáciám, ktoré nevyhnutne potrebuje na vykonávanie svojich povinností.

Záznamy v papierovej podobe a ďalšie dokumenty obsahujúce citlivé informácie sú uchovávané v zmysle vnútorných bezpečnostných postupov NBÚ.

2.8.1.2 Zhromažďovanie a využívanie osobných informácií

Zhromažďovanie a využívanie osobných informácií, poskytnutých NBÚ ako výsledok postupov popísaných v týchto CPS, podlieha príslušným platným právnym predpisom SR, najmä zákonu č. 428/2002 Z.z. o ochrane osobných údajov.

2.8.1.3 Informácie o registrácii

Všetky záznamy o registrácii sa považujú za citlivé informácie vrátane:

a) schválených aj zamietnutých žiadostí o vydanie certifikátu,

b) dokumentácie dokazujúcej identifikáciu žiadateľa,

c) informácií o certifikáte zozbieraných ako časť registračných záznamov (napr. pasfrázy na autentifikáciu zrušenia certifikátu), čo však nebráni zverejňovaniu informácií o certifikáte v adresároch.

2.8.1.4 Dokumentácia

Za citlivé sa považujú nasledovné dokumenty KCA:

a) bezpečnostné smernice vydané v zmysle 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 (ďalej len „vyhláška NBÚ č. 133/2009 Z.z.“) s výnimkou bezpečnostnej politiky,

b) informácie o konfiguráciách zariadení,

c) prevádzková dokumentácia s výnimkou CP a CPS.

2.8.2 Typy informácií nepovažované za citlivé

Za citlivé informácie sa nepovažujú informácie uvedené v certifikátoch vydaných KCA a v zoznamoch CRL, ako aj akékoľvek súhrny takýchto informácií.

Za citlivé sa nepovažujú nasledovné dokumenty KCA:

a) CP,

b) CPS,

c) bezpečnostná politika.

2.8.3 Oznámenie o zrušení certifikátu

NBÚ oznámi zrušenie certifikátu držiteľovi písomnou formou. Informácie o dôvodoch zrušenia certifikátov, ktoré sú uvedené v zoznamoch zrušených certifikátov, nie sú považované za citlivé a preto môžu byť zverejnené. Dôvod zrušenia platnosti certifikátu uvedený v zozname CRL je jediná verejne prístupná informácia. Ďalšie podrobnosti ohľadne dôvodu zrušenia platnosti certifikátu KCA neposkytuje.

V prípade zrušenia certifikátu na základe podnetu, NBÚ písomne oboznámi držiteľa certifikátu s výsledkom šetrenia.

Informácia o zrušení certifikátu bude dostupná aj v zoznamoch CRL vydaných KCA. Spôsob zverejňovania zoznamov CRL je uvedený v bode 2.6.3 týchto CPS.

2.8.4 Poskytovanie informácií vyžadovaných podľa zákona

Akékoľvek informácie, ktoré sú chránené zákonom č. 428/2002 Z.z. o ochrane osobných údajov, poskytne NBÚ bez súhlasu dotknutej osoby len na základe písomného vyžiadania oprávnených osôb určených zákonom č. 428/2002 Z.z. o ochrane osobných údajov alebo vo všeobecne záväzných právnych predpisoch SR.

2.9 Ochrana intelektuálnych práv

NBÚ zaručuje, že na všetok hardvér a softvér použitý v KCA má licenciu alebo je vo vlastníctve NBÚ. Používanie RFC 3647 „Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework“ a ANSI X9.79 je uznané. NBÚ si nenárokuje práva na intelektuálne vlastníctvo na vydané certifikáty.

3. Identifikácia a autentifikácia

3.1 Iniciálna registrácia

3.1.1 Menná konvencia

Menná konvencia jednotlivých subjektov komunity používajúcej certifikáty vydávané KCA je definovaná v nasledujúcich podkapitolách.

3.1.1.1 Menná konvencia pre certifikáty KCA

KCA1 (self-signed)

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

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

DN držiteľa certifikátu:

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

KCA2 (self-signed)

DN vydavateľa certifikátu:

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

DN držiteľa certifikátu:

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

KCA3 (self-signed)

DN vydavateľa certifikátu:

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

DN držiteľa certifikátu:

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

V rámci procesu výmeny kľúčov KCA môže KCA vydať krížový certifikát následníkovi KCA. Následník KCA potom vydá krížový certifikát pôvodnej KCA. Menná konvencia takýchto certifikátov je zrejmá.

3.1.1.2 Menná konvencia pre akreditované certifikačné autority a uznané zahraničné certifikačné autority

KCA v certifikátoch vydávaných pre akreditované CA uznané zahraničné CA podporuje nasledovné atribúty uvádzané v DN držiteľa:

Common Name

Organization Unit

Organization

Locality

Country

Voľba DN je v kompetencii akreditovanej CA, resp. uznanej zahraničnej CA. Podmienkou je, aby zvolené DN bolo jedinečné, a aby jednoznačne identifikovalo poskytovateľa.

Povinným atribútom DN je „Country“ a jeden z dvojice atribútov „Common Name“ alebo „Organization“.

3.1.2 Kontrola mien

NBÚ po obdržaní žiadosti o vydanie certifikátu skontroluje žiadosť v písomnej aj v elektronickej forme voči konvencii podľa bodu 3.1.1 týchto CP podľa nasledujúcich pravidiel:

a) skontrolovanie syntaxe mien,

b) skontrolovanie vecnej správnosti mien,

c) skontrolovanie prítomnosti všetkých povinných položiek.

3.1.3 Jednoznačnosť a zmysluplnosť mien

KCA zodpovedá za jednoznačnosť mien v rámci KCA. Identifikačné údaje akreditovaných CA a uznaných zahraničných CA musia jednoznačne identifikovať poskytovateľa spomedzi ostatných, ktorým KCA vydala certifikát.

Okrem identifikačných údajov uvedených v tele certifikátu je každá akreditovaná CA a uznaná zahraničná CA identifikovaná prostredníctvom registračného čísla, ktoré prideľuje NBÚ. Registračné čísla akreditovaných CA a uznaných zahraničných CA sú zverejnené na nasledujúcej internetovej stránke:

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

3.1.4 Spôsob riešenia sporov týkajúcich sa mien

Kolízie v menách akreditovaných CA rieši NBÚ. NBÚ rešpektuje práva k ochranným známkam. NBÚ nepovolí žiadateľovi používať meno, o ktorom súd rozhodol, že ho nemá právo používať. Na druhej strane nie je povinnosťou prideliť dané meno oprávnenému držiteľovi, pokiaľ už má pridelené meno vyhovujúce jeho jednoznačnej autentifikácii. NBÚ nie je povinný kontrolovať zoznamy ochranných značiek a súdnych rozhodnutí.

3.1.5 Preukazovanie vlastníctva súkromného kľúča

Všetky žiadosti o vydanie certifikátov musia byť predložené vo formáte PKCS# 10 (definovaný v RFC 2314 „PKCS #10: Certification Request Syntax"), podľa ktorého je žiadosť podpísaná súkromným kľúčom žiadateľa.

3.1.6 Preukazovanie pravosti verejného kľúča

Žiadateľ o vydanie certifikátu akreditovanej CA alebo uznanej zahraničnej CA na KCA predloží ako prílohu k žiadosti o vydanie certifikátu kryptografickú charakteristiku verejného kľúča, pre ktorý požaduje vydanie certifikátu.

Kryptografická charakteristika verejného kľúča priložená k žiadosti o vydanie certifikátu musí byť transponovaná do čitateľného tvaru, vytlačená na papieri a podpísaná štatutárnym zástupcom akreditovanej CA alebo uznanej zahraničnej CA.

3.1.7 Proces iniciálnej registrácie a autentifikácia organizácií a jej zástupcov

3.1.7.1 Iniciálna registrácia KCA

Iniciálna registrácia KCA sa vykonáva v procese formálneho založenia KCA počas procedúry jej vytvorenia. Na jej autentifikáciu 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.

Iniciálna registrácia následníka KCA sa vykonáva v procese formálneho zriadenia následníka KCA počas procedúry jeho vytvorenia. Na autentifikáciu 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.

3.1.7.2 Iniciálna registrácia akreditovanej CA

Iniciálna registrácia akreditovanej CA sa vykonáva pri ukončení procesu akreditácie certifikačnej autority. Podkladom pre iniciálnu registráciu akreditovanej CA sú:

a) rozhodnutie NBÚ o udelení akreditácie akreditovanej CA,

b) žiadosť o vydanie certifikátu na KCA.

Žiadateľ o vydanie prvého certifikátu pre akreditovanú CA predloží:

a) preukaz totožnosti,

b) splnomocnenie o zastupovaní akreditovanej CA.

3.1.7.3 Iniciálna registrácia uznanej zahraničnej CA

Iniciálna registrácia uznanej zahraničnej certifikačnej autority sa vykonáva po uznaní zahraničnej CA v zmysle ustanovení § 17 zákona č. 215/2002 Z.z. o elektronickom podpise. Podkladom pre iniciálnu registráciu zahraničnej CA sú:

a) rozhodnutie NBÚ o uznaní zahraničnej CA,

b) žiadosť o vydanie certifikátu uznanej zahraničnej CA na KCA.

Žiadateľ o vydanie prvého certifikátu pre zahraničnú CA predloží:

a) preukaz totožnosti uznávaný v SR,

b) splnomocnenie o zastupovaní uznanej zahraničnej CA.

3.2 Vydanie následného certifikátu

Vydanie následného certifikátu podlieha rovnakému procesu ako iniciálna registrácia (viď bod 3.1 týchto CPS).

3.3 Vydanie certifikátu po zrušení certifikátu

Vydanie certifikátu po zrušení certifikátu podlieha rovnakému procesu ako iniciálna registrácia (viď bod 3.1 týchto CPS).

3.4 Recertifikácia akreditovaných CA a uznaných zahraničných CA

V prípade výmeny certifikačných kľúčov KCA podľa bodu 4.10 týchto CPS NBÚ umožní opätovné prevydanie všetkých platných certifikátov akreditovaných CA a uznaných zahraničných CA.

Recertifikácia akreditovaných CA a uznaných zahraničných CA podlieha rovnakému procesu ako iniciálna registrácia (viď bod 3.1 týchto CPS).

3.5 Žiadosť o zrušenie certifikátu

Žiadosť o zrušenie certifikátov vydaných KCA je možné podať na registračnom mieste registračnej autority KCA alebo telefonicky.

3.5.1 Podanie žiadosti o zrušenie certifikátu na registračnom mieste

Na registračnom mieste registračnej autority KCA je možné podať žiadosť o zrušenie certifikátu písomnou formou počas stránkových hodín registračnej autority (kontaktné informácie sú uvedené v bode 1.7.4 týchto CPS).

Na registračnom mieste registračnej autority KCA musí žiadateľ o zrušenie certifikátu predložiť nasledovné dokumenty:

a) vlastný preukaz totožnosti,

b) splnomocnenie akreditovanej CA alebo uznanej zahraničnej CA o zastupovaní žiadateľom,

c) žiadosť o zrušenie certifikátu uvedenú na nasledujúcej internetovej stránke:

http://ep.nbusr.sk/kca/doc/ziadost_o_zrusenie_cert.rtf

Ďalší postup spracovania žiadosti o zrušenie certifikátu sa riadi ustanoveniami bodu 4.6 týchto CPS.

3.5.2 Podanie žiadosti o zrušenie certifikátu telefonicky

Telefonicky je možné podať žiadosť o zrušenie certifikátu 24 hodín denne (kontaktné telefónne číslo je uvedené v bode 1.7.4 týchto CPS).

Ak žiadosť o zrušenie certifikátu akreditovanej CA alebo uznanej zahraničnej CA bude prebiehať telefonicky na definovanej telefónnej linke NBÚ, žiadateľ musí okrem nahlásenia žiadosti o zrušenie certifikátu správne odpovedať na vybrané kontrolné otázky operátora registračnej autority KCA. Zoznam otázok a odpovedí obdrží splnomocnený zástupca akreditovanej CA alebo uznanej zahraničnej CA (držiteľ certifikátu) počas registrácie.

Na potvrdenie telefonickej žiadosti o zrušenie certifikátu je povinný žiadateľ zaslať faxom kópie nasledovných dokumentov:

a) vyplnenú žiadosť o zrušenie certifikátu,

b) kópiu preukazu totožnosti žiadateľa o zrušenie certifikátu.

Na tento účel je vyhradené kontaktné faxové číslo NBÚ uvedené v bode 1.7.4 týchto CPS.

Ak žiadosť o zrušenie certifikátu nie je možné akceptovať (napríklad ak žiadateľ nesprávne odpovedal na kontrolné otázky alebo nebolo možné spoľahlivo overiť totožnosť žiadateľa), bude táto žiadosť zamietnutá.

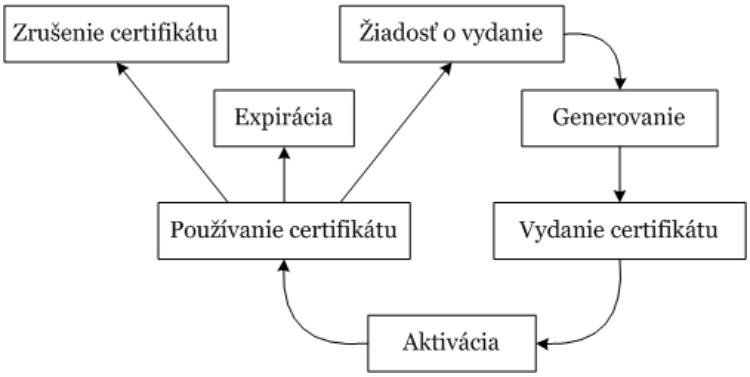
V prípade že žiadosť o zrušenie certifikátu bola zamietnutá, o zrušenie certifikátu bude môcť opätovne požiadať iba poverený zástupca akreditovanej CA alebo uznanej zahraničnej CA pri osobnej návšteve na registračnom mieste registračnej autority KCA.

Zrušenie certifikátu akreditovanej CA alebo uznanej zahraničnej CA bez zodpovedania kontrolných otázok je možné iba osobne na registračnom mieste registračnej (bod 3.5.1 týchto CPS).

Ďalší postup spracovania žiadosti o zrušenie certifikátu sa riadi ustanoveniami bodu 4.6 týchto CPS.

4. Prevádzkové postupy platné pre KCA

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



Primárnymi stavmi sú:

a) žiadosť o vydanie certifikátu,
b) generovanie certifikátu,
c) vydanie certifikátu,
d) aktivácia,
e) používanie,
f) expirácia,
g) archivácia.

Sekundárnym stavom je zrušenie certifikátu.

NBÚ vydáva certifikáty pre akreditované CA a certifikáty pre uznané zahraničné CA s dobou platnosti, ktorú určuje NBÚ.

Akreditovaná CA alebo uznaná zahraničná CA, ktorá požiada o vydanie certifikátu sa musí zúčastniť iniciálnej registrácie. Nevyhnutným predpokladom pre vydanie certifikátu pre akreditovanú CA je úspešné absolvovanie procesu akreditácie podľa zákona č. 215/2002 Z.z. o elektronickom podpise. V prípade zahraničnej CA je nevyhnutným predpokladom pre vydanie certifikátu uznanie zahraničnej CA v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise.

Iniciálna registrácia prebieha na registračnom mieste registračnej autority KCA a pokrýva činnosti:

a) podanie formálnej žiadosti o vydanie certifikátu,
b) overenie totožnosti žiadateľa,
c) skontrolovanie elektronickej žiadosti o vydanie certifikátu vo formáte PKCS#10,
d) odoslanie elektronickej žiadosti o vydanie certifikátu do KCA,
e) generovanie a vydanie certifikátu,
f) prevzatie a odovzdanie certifikátu žiadateľovi.

Počas doby platnosti certifikátu môže držiteľ certifikátu požiadať o zrušenie certifikátu.

Pred uplynutím platnosti certifikátu (expiráciou) držiteľ certifikátu požiada NBÚ o vydanie následného certifikátu pre nový kľúčový pár.

4.1 Žiadosť o vydanie certifikátu

4.1.1 Žiadosť o vydanie certifikátu KCA

Žiadosť o vydanie certifikátu vlastného verejného kľúča KCA podáva písomnou formou prevádzkovateľ KCA na registračnom mieste registračnej autority KCA na základe zákona č. 215/2002 Z.z. o elektronickom podpise. S ohľadom na charakter certifikátu a postup pri vydaní certifikátu KCA nie je potrebná elektronická žiadosť o vydanie certifikátu vo formáte PKCS#10.

Pri procese vydania certifikátu KCA sa postupuje podľa postupu uvedeného v bode 4.2.1 týchto CPS.

4.1.2 Žiadosť o vydanie certifikátu akreditovanej CA

Podaniu žiadosti o vydanie certifikátu pre akreditovanú CA musí predchádzať úspešné ukončenie procesu akreditácie certifikačnej autority v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise.

Žiadosť o vydanie certifikátu akreditovanej CA môže podať:

a) štatutárny zástupca akreditovanej CA osobne,

b) zástupca akreditovanej CA poverený štatutárnym zástupcom akreditovanej CA na zastupovanie akreditovanej CA vo veci vydania certifikátu.

Osoba podávajúca žiadosť o certifikáciu realizuje nasledovné kroky:

a) vyplní alebo doručí formálnu žiadosť o vydanie certifikátu uvedenú na nasledujúcej internetovej stránke:

   http://ep.nbusr.sk/kca/doc/ziadost_o_vydanie_kval_cert.rtf

b) ak nie je štatutárnym zástupcom akreditovanej CA, predloží operátorovi registračnej autority KCA notársky overené poverenie na zastupovanie akreditovanej CA vo veci vydania certifikátu podpísané štatutárnym zástupcom akreditovanej CA,

c) odovzdá operátorovi registračnej autority KCA na záznamovom médiu elektronickú žiadosť o vydanie certifikátu vo formáte PKCS#10,

d) odovzdá operátorovi registračnej autority KCA záznam z generovania kľúčového materiálu.

V nadväznosti na predchádzajúce kroky operátor registračnej autority KCA:

a) overí skutočnosť či CA, ktorú žiadateľ zastupuje, získala akreditáciu NBÚ,

b) overí totožnosť žiadateľa a jeho poverenie od akreditovanej CA,

c) formálne a obsahovo skontroluje papierovú a elektronickú žiadosť o vydanie certifikátu.

V prípade zamietnutia žiadosti o vydanie certifikátu je:

a) žiadateľ o zamietnutí vyrozumený osobne na registračnom mieste registračnej autority KCA,

b) akreditovaná CA je o zamietnutí vyrozumená písomnou formou.

V prípade, že žiadosť o vydanie certifikátu je platná a boli splnené aj ostatné požiadavky na vydania certifikátu, činnosť pokračuje podľa postupu uvedeného v bode 4.2.2 týchto CPS.

4.1.3 Žiadosť o vydanie certifikátu uznanej zahraničnej CA

Podaniu žiadosti o vydanie certifikátu uznanej zahraničnej CA musí predchádzať formálne uznanie zahraničnej CA v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise.

Žiadosť o vydanie certifikátu uznanej zahraničnej CA môže podať:

a) štatutárny zástupca uznanej zahraničnej CA osobne,

b) zástupca uznanej zahraničnej CA poverený štatutárnym zástupcom na zastupovanie uznanej zahraničnej CA vo veci vydania certifikátu.

Osoba podávajúca žiadosť o vydanie certifikátu uznanej zahraničnej CA realizuje nasledovné kroky:

a) vyplní alebo doručí formálnu žiadosť o vydanie certifikátu uvedenú na nasledujúcej internetovej stránke:

   http://ep.nbusr.sk/kca/doc/ziadost_o_vydanie_cert.rtf

b) ak nie je štatutárnym zástupcom uznanej zahraničnej CA, predloží operátorovi registračnej autority KCA notársky overené poverenie na zastupovanie uznanej zahraničnej CA vo veci vydania certifikátu,

c) odovzdá operátorovi registračnej autority KCA na záznamovom médiu elektronickú žiadosť o vydanie certifikátu vo formáte PKCS#10,

d) odovzdá operátorovi registračnej autority KCA záznam z generovania kľúčového materiálu.

V nadväznosti na predchádzajúce kroky operátor registračnej autority KCA:

a) overí skutočnosť, či CA, ktorú žiadateľ zastupuje, bola uznaná NBÚ,

b) overí totožnosť žiadateľa a jeho poverenie od uznanej zahraničnej CA,

c) formálne a obsahovo skontroluje elektronickú a papierovú žiadosť o vydanie certifikátu.

V prípade zamietnutia žiadosti o vydanie certifikátu je:

a) žiadateľ o zamietnutí vyrozumený osobne na registračnom mieste registračnej autority KCA,

b) zahraničná CA je o zamietnutí vyrozumená písomnou formou.

K vyrozumeniu o odmietnutí žiadosti o vydanie certifikátu je pripojené zdôvodnenie odmietnutia.

V prípade, že žiadosť o vydanie certifikátu zahraničnej CA je platná a boli splnené aj ostatné požiadavky potrebné pre vydanie certifikátu, činnosť pokračuje podľa postupu uvedeného v bode 4.2.3 týchto CPS.

4.2 Vydávanie certifikátov

4.2.1 Vydanie certifikátu KCA

Certifikát vlastného verejného kľúča KCA je vydaný podľa postupu označovaného ako Certificate Signing Event (CSE). V rámci tohto postupu sa požaduje minimálne účasť nasledovných osôb:

a) bezpečnostný správca KCA,

b) interný audítor KCA,

c) jeden príslušník alebo zamestnanec NBÚ.

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

Po zadaní certifikačných informácií do SW TWS aplikácie používanej v KCA sa vygeneruje kľúčový pár KCA a self-signed certifikát KCA. Uloženie a zálohovanie súkromného kľúča je vykonané v súlade s internými predpismi KCA. Po vydaní certifikátu KCA ho NBÚ zverejnení prostredníctvom prostriedkov určených na distribúciu certifikátov.

Vydanie certifikátu následníka KCA prebieha rovnakým spôsobom ako vydanie certifikátu KCA. V prípade potreby môžu byť vydané vzájomné krížové certifikáty pre používaný verejný kľúč KCA a verejný kľúč následníka KCA. Po vydaní certifikátu následníka KCA, prípadne krížových certifikátov KCA a následníka KCA, NBÚ zverejní certifikáty prostredníctvom prostriedkov určených na distribúciu certifikátov. Detailnejší postup procesu je popísaný v bode 4.10 týchto CPS.

4.2.2 Vydanie certifikátu akreditovanej CA

Po prijatí žiadosti o vydanie certifikátu akreditovanej CA a pri kladnom výsledku preverenia požadovaných náležitostí žiadosti, jej správnosti a správnosti údajov obsiahnutých v tele žiadosti, KCA:

a) vydá certifikát akreditovanej CA,

b) zverejní certifikát akreditovanej CA na prostriedkoch určených na distribúciu certifikátov.

4.2.3 Vydanie certifikátu uznanej zahraničnej CA

Po prijatí žiadosti o vydanie certifikátu uznanej zahraničnej CA a pri kladnom výsledku preverenia požadovaných náležitostí žiadosti, jej správnosti a správnosti údajov obsiahnutých v tele žiadosti, KCA:

a) vydá certifikát uznanej zahraničnej CA,

b) zverejní certifikát uznanej zahraničnej CA prostredníctvom prostriedkov určených na distribúciu certifikátov.

4.3 Odovzdanie certifikátu žiadateľovi

Po vydaní certifikátu akreditovanej CA alebo uznanej zahraničnej CA registračný operátor KCA zabezpečí odovzdanie certifikátu žiadateľovi.

Certifikát akreditovanej CA alebo certifikát uznanej zahraničnej CA je odovzdaný jej poverenému zástupcovi osobne na registračnom mieste registračnej autority KCA.

Certifikáty vydané KCA sú tiež dostupné prostredníctvom adresárových služieb NBÚ (viď bod 2.6.2 týchto CPS). Podporované formáty distribuovaných certifikátov sú: DER, Base64 a PKCS#7.

4.4 Prevzatie certifikátu

Žiadateľ je povinný prevziať vydaný certifikát. Ak ho prevziať odmietne, musí požiadať o jeho zrušenie v súlade s ustanoveniami týchto CPS a ustanoveniami CP. Pri prevzatí certifikátu podpisuje žiadateľ preberací protokol o prevzatí certifikátu držiteľom.

Prevzatím certifikátu žiadateľ:

a) potvrdzuje a zaručuje, že uvedené informácie v certifikáte sú platné,

b) potvrdzuje, že žiadny neoprávnený subjekt nevlastní alebo nemá prístup k príslušnému súkromnému kľúču z kľúčového páru, na ktorého verejný kľúč bol vydaný preberaný certifikát,

c) potvrdzuje, že sú mu známe a akceptuje práva a povinnosti držiteľa certifikátu ustanovené v tomto CPS a v CP pre príslušný typ certifikátu.

4.5 Používanie certifikátov

Certifikát sa smie používať len na účely, na ktoré je vydaný. Podrobnejšie informácie a pravidlá týkajúce sa použiteľnosti certifikátov vydaných KCA sú uvedené v bode 1.5 týchto CPS a v CP.

4.6 Zrušenie certifikátu

Bezodkladné overenie a spracovanie požiadavky na zrušenie certifikátu je kľúčové pre zachovanie integrity v rámci hierarchie KCA.

4.6.1 Oprávnené dôvody na zrušenie certifikátu

Na zrušenie certifikátu existuje oprávnený dôvod ak:

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

b) v prípade úmyselného zneužitia kľúčov a certifikátov autorizovanou osobou alebo neautorizovanou osobou,

c) v prípade závažného porušenia prevádzkových požiadaviek identifikovaných v príslušných zmluvách alebo v príslušnom CP alebo v tomto CPS,

d) certifikát bol vydaný na základe nepravdivých údajov,

e) subjekt, ktorému bol certifikát vydaný, ukončil svoju činnosť,

f) oprávnený subjekt alebo osoba (viď bod 4.6.2 týchto CPS) požiada o zrušenie certifikátu,

g) v prípade zmeny identifikačných údajov alebo atribútov v certifikáte pred uplynutím doby platnosti certifikátu,

h) zrušenie certifikátu nariadil súd,

i) bol zrušený certifikát KCA.

4.6.2 Kto môže požiadať o zrušenie certifikátu

O zrušenie certifikátu môže požiadať:

a) držiteľ certifikátu alebo jeho splnomocnený zástupca,

b) autorizovaný zástupca KCA,

c) tretia strana v súlade s platnými právnymi predpismi SR (napr. súd).

4.6.3 Postup pre spracovanie žiadosti o zrušenie certifikátu akreditovanej CA alebo uznanej zahraničnej CA

Proces zrušenia certifikátu je iniciovaný prijatím vyplnenej žiadosti o zrušenie certifikátu uvedenej na nasledujúcej internetovej stránke:

http://ep.nbusr.sk/kca/doc/ziadost_o_zrusenie_cert.rtf

Viac informácií o spôsobe podávania žiadostí o zrušenie certifikátu je uvedené v bode 3.5 týchto CPS.

Po prijatí žiadosti budú realizované nasledovné kroky:

a) prevzatie a zaevidovanie žiadosti o zrušenie certifikátu podanú písomne alebo telefonicky,

b) formálna kontrola správnosti prijatej žiadosti o zrušenie certifikátu,

c) kontrola oprávnenia požadovať zrušenie certifikátu v zmysle bodu 4.6.2 týchto CPS,

d) preverenie autenticity osoby podávajúcej žiadosť o zrušenie certifikátu a jej oprávnení na podanie žiadosti (preverenie musí prebehnúť podľa vopred definovanej procedúry s kontrolovateľnými výsledkami),

e) posúdenie žiadosti o zrušenie certifikátu (akceptovanie – neakceptovanie),

f) po akceptovaní žiadosti o zrušenie certifikátu realizácia zrušenia certifikátu,

g) zverejňovanie zrušeného certifikátu v zozname CRL.

4.6.4 Časový interval na zrušenie certifikátu

Zrušenie certifikátu vydaného KCA sa v prípade akceptovanej žiadosti o zrušenie certifikátu uskutoční do 24 hodín.

4.7 Služby na overenie stavu certifikátu

Na overenie stavu certifikátov KCA poskytuje službu zverejňovania zoznamov CRL.

4.7.1 Zoznam zrušených certifikátov

4.7.1.1 Zverejňovanie zoznamov zrušených certifikátov

Prístupové adresy a komunikačné protokoly pre zverejňovanie zoznamov CRL vydaných KCA sú popísané v bode 2.6.3 týchto CPS.

4.7.1.2 Periodicita zverejňovania zoznamu zrušených certifikátov

Zoznamy 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 sériové číslo, neuplynulo viac ako 24 hodín (v zmysle § 6 vyhlášky NBÚ č. 131/2009 Z.z.).

4.7.1.3 Odporúčanie na sledovanie zoznamu zrušených certifikátov

Používatelia certifikátov musia overovať certifikáty voči aktuálne platnému CRL vydaného KCA, pokiaľ je tento dostupný. Odporúča sa kontrola platnosti certifikátu pri každej transakcii. V prípade, že CRL je dočasne nedostupný, používatelia musia odmietnuť použitie certifikátu alebo sa zodpovedne rozhodnúť prijať riziko používania certifikátu, ktorého platnosť nie je garantovaná týmto CPS.

4.7.2 OCSP

On-line overovanie stavu certifikátov vydaných KCA prostredníctvom protokolu OCSP nie je implementované.

4.7.3 Iné možnosti informovania o zrušení certifikátu KCA

Informácie o zrušení certifikátu vlastného verejného kľúča KCA budú zverejnené na internetovej adrese http://ep.nbusr.sk/kca/crl.html a v dennej tlači.

4.8 Prevádzkové procedúry

Tento bod dokumentu popisuje spôsob vedenia, uchovávania, spracovania, udržiavania a zabezpečovania prevádzkových záznamov KCA, ktoré sa vyhodnocujú v procese auditu bezpečnosti.

V súlade s § 9 ods. 7 písm. f) vyhlášky NBÚ č. 133/2009 Z.z. má KCA vypracovaný a do prevádzky uvedený systém priebežného dokumentovania všetkých kľúčových aktivít.

4.8.1 Vedenie prevádzkových záznamov

Pre kontrolu činnosti KCA sa vedú prevádzkové záznamy, ktoré zaznamenávajú požiadavky na činnosť KCA, zachytávajú postupy vykonávania prevádzkových procedúr KCA a uchovávajú záznamy o činnosti jednotlivých komponentov KCA.

Prevádzkové záznamy a dokumenty sú uchovávané v papierovej alebo elektronickej forme.

Prevádzkové záznamy vedené v elektronickej forme musia byť zálohované tak, aby nemohlo dôjsť k ich porušeniu alebo strate.

4.8.2 Typy uchovávaných prevádzkových záznamov

Ako prevádzkové záznamy sa v prevádzke KCA uchovávajú:

a) požiadavky na generovanie kľúčov KCA s pripojeným výsledkom o generovaní kľúčov,
b) žiadosti o vydanie certifikátov spolu s výsledkom preverenia žiadosti,
c) záznamy o vydaní certifikátov,
d) záznamy o odovzdaní certifikátov,
e) žiadosti o zrušenie certifikátov spolu s výsledkom preverenia žiadosti,
f) záznamy o zrušení certifikátov,
g) záznamy o vydávaní a zverejňovaní zoznamu CRL,
h) záznamy o manipulácii so súkromným kľúčom KCA,

i) záznamy zmien konfigurácií a inštalácie systémov a aplikácií KCA,

j) systémové a aplikačné logy komponentov KCA,

k) hlásenia výskytu prípadných prevádzkových a bezpečnostných incidentov,

l) protokoly o riešení ohlásených bezpečnostných incidentov.

4.8.3 Frekvencia spracovania a auditu prevádzkových záznamov

Prevádzkové záznamy KCA sa spracovávajú v pravidelných týždenných, mesačných a ročných intervaloch. Na vyhodnocovanie prevádzkových záznamov KCA je vypracovaný systém pravidelného ako aj náhodného auditu v súlade s internými predpismi KCA.

4.8.4 Doba uchovávania záznamov

Záznamy priebežného dokumentovania kľúčových aktivít KCA sú uchovávané minimálne tri roky v zmysle § 9 ods. 7 písm. g) vyhlášky NBÚ č. 133/2009 Z.z. Ostatné prevádzkové záznamy sa uchovávajú ako aktívne záznamy po dobu jedného roku od ich vzniku. Po uplynutí definovanej doby aktívneho života sú záznamy preradené do archívu. Podrobnosti o vedení archívu sú uvedené v bode 4.9 týchto CPS.

4.8.5 Ochrana prevádzkových záznamov

Prevádzkové záznamy vedené v elektronickej forme sú zálohované tak, aby nemohlo dôjsť k ich porušeniu alebo strate. Integrita prevádzkových záznamov je zabezpečená prostredníctvom elektronického podpisu záznamov použitím kľúčového páru a certifikátu generovaného špeciálne pre tento účel. Vlastníkom súkromného kľúča používaného pre podpisovanie auditných záznamov je bezpečnostný správca KCA.

Prevádzkové záznamy vedené listinnou formou sú spravované v režime, ktorý zabezpečí, aby nemohlo dôjsť k ich porušeniu, znehodnoteniu alebo strate.

4.8.6 Zálohovanie prevádzkových záznamov

NBÚ zabezpečuje zálohovanie prevádzkových záznamov v súlade s internými predpismi KCA a platnými právnymi predpismi SR.

4.8.7 Systém zberu prevádzkových záznamov vedených v elektronickej forme

Systém zberu elektronických prevádzkových záznamov je kombináciou automatických činností vykonávaných operačnými systémami, aplikáciami komponentov KCA a manuálnych činností vykonávaných personálom prevádzky.

Proces zberu elektronických prevádzkových záznamov je aktivovaný pri štarte systémov KCA a uzavrie sa len pri vypnutí celého informačného systému KCA.

V prípade prerušenia činnosti automatizovaného systému zberu prevádzkových záznamov budú vykonané príslušné kroky na obnovu jeho činnosti alebo budú využité náhradné možnosti, ktoré boli vopred schválené ako náhradné riešenie.

4.9 Archivácia záznamov

4.9.1 Typy archivovaných udalostí

Archívne záznamy KCA sú uchovávané v rozsahu dostatočnom na zaručenie platnosti podpisu a správnej funkčnosti infraštruktúry manažmentu certifikátov. Minimálne musia byť archivované nasledovné informácie:

a) prevádzkové záznamy podľa bodu 4.8.2 týchto CPS,

b) certifikáty vydané KCA,

c) zoznamy CRL,

d) oficiálna korešpondencia,

e) dokumentácia programového vybavenia KCA,

f) bezpečnostná dokumentácia KCA,

g) inštalačné média a popisy konfiguračných súborov programového vybavenia KCA.

Každý archívny záznam je opatrený časovým údajom jeho vytvorenia.

4.9.2 Doba uchovávania archívu

Doba uchovávania archivovaných údajov je v zmysle § 18 zákona č. 215/2002 Z.z. stanovená najmenej na 10 rokov.

4.9.3 Ochrana archívu

Archívne záznamy sú chránené kombináciou fyzickej bezpečnosti, kryptografickej ochrany a režimových opatrení. Archivačné médiá sú chránené pred vplyvmi prostredia ako je teplota, vlhkosť a magnetizmus.

4.9.4 Procedúry zálohovania archívu

Procedúry zálohovania archívu sú navrhnuté tak, aby zaisťovali kompletné obnovenie služieb. Podrobnosti sú špecifikované v bezpečnostných a prevádzkových smerniciach KCA.

4.9.5 Časové údaje záznamov

Každý archívny záznam je opatrený časovým údajom jeho vytvorenia.

4.9.6 Systém archivácie

Archivácia je vykonávaná osobami obslužného personálu KCA, ktoré ňou boli poverené. Zoznam poverených osôb a detailné popisy procedúr archivácie sú súčasťou interných predpisov KCA.

4.10 Výmena kľúčov

4.10.1 Výmena kľúčov KCA

Výmena kľúčov KCA sa realizuje ako úplná výmena kľúčov pozostávajúca z generovania nového kľúčového páru následníka KCA a vydania self-signed certifikátu následníka KCA. Na zabezpečenie kontinuity overovania vydaných certifikátov je možné realizovať krížovú certifikáciu nového kľúča s jeho predchodcom (pokiaľ predchodca nebol kompromitovaný) v zmysle pravidiel stanovených v RFC 4210 „Internet X.509 Public Key Infrastructure: Certificate Management Protocols".

Proces výmeny kľúčov KCA pozostáva z nasledovných krokov:

1) Vydanie certifikátu následníka KCA

   a) NBÚ oznámi plánovanú výmenu kľúčov KCA všetkým akreditovaným CA, uznaným zahraničným CA a verejnosti prostredníctvom internetovej stránky http://ep.nbusr.sk/kca najmenej dva mesiace vopred,

   b) NBÚ vydá certifikát následníka KCA v súlade s platnými právnymi predpismi SR,

   c) NBÚ vyzve splnomocnených zástupcov akreditovaných CA a uznaných zahraničných CA na recertifikáciu (viď bod 3.4 týchto CPS) alebo na vydanie následného certifikátu (viď bod 3.4 týchto CPS),

   d) certifikáty následníka KCA budú vydané v zmysle platnej mennej konvencie (viď bod 3.1.1.1 týchto CPS),

   e) certifikát následníka KCA budú zverejnené prostredníctvom adresárových služieb NBÚ (viď bod 2.6.2 týchto CPS),

   f) od okamihu spustenia následníka KCA do produkčnej prevádzky až po ukončenie činosti pôvodnej KCA budú súbežne poskytovať certifikačné služby KCA a následník KCA v nasledujúcom rozsahu:

      - KCA bude zabezpečovať certifikačné služby zrušovania certifikátov, vydávania a zverejňovania zoznamov CRL,

      - následník KCA bude poskytovať certifikačné služby vydávania a zverejňovania certifikátov podľa bodu 1.5 týchto CPS, služby zrušovania certifikátov a služby vydávania a zverejňovania zoznamov CRL.

2) Recertifikácia platných certifikátov akreditovaných CA a uznaných zahraničných CA následníkom KCA alebo vydanie následných certifikátov akreditovaných CA a uznaných zahraničných CA následníkom KCA

   Rozhodnutie o recertifikácii (bod 3.4 týchto CPS) alebo o vydaní následného certifikátu (bod 3.2 týchto CPS) uskutoční akreditovaná CA alebo uznaná zahraničná CA na základe požiadaviek platných právnych predpisov SR. V prípade, že neexistuje legislatívna požiadavka na použitie jedného z uvedených spôsobov, rozhodne podľa svojich možností, zámerov a potrieb akreditovaná CA alebo uznaná zahraničná ACA.

   V prípade **recertifikácie** platných certifikátov akreditovaných CA a uznaných zahraničných CA platia nasledovné pravidlá:

   a) následník KCA vydá certifikát akreditovanej CA alebo uznanej zahraničnej CA na verejný kľúč, na ktorý vydala certifikát KCA,

   b) certifikát recertifikovaného verejného kľúča vydaný KCA musí byť v čase recertifikácie platný,

c) certifikát akreditovanej CA alebo uznanej zahraničnej CA vydaný procesom recertifikácie následníkom KCA musí mať rovnaké rozlišovacie meno a verejný kľúč ako pôvodný platný certifikát vydaný KCA,

d) po recertifikácii certifikátu akreditovanej CA alebo uznanej zahraničnej CA následníkom KCA, NBÚ zabezpečí zverejnenie certifikátu vydaného následníkom KCA prostredníctvom adresárových služieb KCA (viď bod 2.6.5 týchto CPS).

V prípade **vydania následných certifikátov** akreditovaných CA a uznaných zahraničných CA následníkom KCA platia nasledovné pravidlá:

a) následník KCA vydá certifikát akreditovanej CA alebo uznanej zahraničnej CA na nový verejný kľúč,

b) vydanie následného certifikátu akreditovanej CA alebo uznanej zahraničnej CA následníkom KCA sa uskutoční podľa pravidiel popísaných v bode 3.2 týchto CPS,

c) menná konvencia následných certifikátov akreditovaných CA a uznaných zahraničných CA je popísaná v bode 3.1.1.2 týchto CPS,

d) po vydaní následného certifikátu akreditovanej CA alebo uznanej zahraničnej CA následníkom KCA, NBÚ zabezpečí zverejnenie nových vydaných certifikátov prostredníctvom adresárových služieb (viď bod 2.6.5 týchto CPS).

Prevádzkové a bezpečnostné procedúry výmeny kľúčov KCA sú navrhnuté tak, aby minimalizovali riziká pri tejto operácii a zabezpečovali minimalizáciu prerušenia poskytovania certifikačných služieb KCA. Výmena kľúčov musí byť plánovaná (mimo riešenia havarijných situácií). Požiadavka na výmenu kľúčov musí byť riešená formálnou žiadosťou o vydanie certifikátu v súlade s bodom 4.1 týchto CPS.

4.10.2 Zmena certifikačných kľúčov ACA

Zmena kľúčov akreditovanej CA sa riadi podľa ustanovení CPS príslušnej akreditovanej CA.

4.10.3 Zmena certifikačných kľúčov uznanej zahraničnej CA

Zmena certifikačných kľúčov uznanej zahraničnej CA sa riadi podľa ustanovení CPS príslušnej uznanej zahraničnej CA.

4.11 Ukončenie činnosti

KCA je ustanovená na základe zákona č. 215/2002 Z.z. o elektronickom podpise. Činnosť KCA môže byť ukončená iba zmenou alebo zrušením tohto zákona, prípadne inou legislatívnou úpravou. Predpokladá sa, že legislatívna úprava, ktorá ukončí činnosť KCA stanoví aj spôsob ukončenia jej činnosti.

4.12 Interný audit bezpečnosti

Interný audit bezpečnosti realizuje interný audítor KCA na základe schváleného plánu interných auditov KCA. Rozsah interného auditu bezpečnosti sa riadi internými predpismi KCA.

Výsledky interného auditu bezpečnosti sú predkladané formou správy z interného auditu.

5. Fyzické, procedurálne a personálne bezpečnostné opatrenia platné pre KCA

5.1 Opatrenia na fyzickú bezpečnosť

Fyzická bezpečnosť KCA je riešená v zmysle ustanovení vyhlášky NBÚ č. 336/2004 Z.z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky NBÚ č. 315/2006 Z.z. (ďalej len „vyhláška NBÚ č. 336/2004 Z.z.“).

5.1.1 Lokalizácia a konštrukcia prevádzkových priestorov

Všetky systémy a zariadenia KCA (hardvér, softvér, sieťové komponenty) sú umiestnené v bezpečných priestoroch chránených pred neautorizovaným prístupom nepovolaných osôb, pred živelnými pohromami a haváriami v inžinierskych sieťach.

5.1.2 Fyzický prístup

Bezpečnostné opatrenia na fyzickú a objektovú bezpečnosť spĺňajú požiadavky vyhlášky NBÚ č. 336/2004 Z.z. Prístup do priestorov KCA je riadený prísnou bezpečnostnou politikou a pravidelne auditovanými procedúrami. NBÚ má pripravené spôsoby a postupy na ochranu svojich počítačových systémov, údajov a archívov proti neoprávnenej manipulácii, krádeži a prezradeniu.

5.1.3 Napájanie a vzduchotechnika

Komponenty systému KCA sú chránené neprerušiteľnými zdrojmi elektrického napájania. Priestory, v ktorých sa nachádza systém KCA, sú vybavené klimatizáciou.

5.1.4 Rozvody vody a kanalizácie

Priestory KCA sú chránené proti nebezpečenstvu pôsobenia vody.

5.1.5 Protipožiarne opatrenia

NBÚ prevádzkuje dymové a požiarne detektory na ochranu priestorov NBUCA.

5.1.6 Uchovávanie médií

NBÚ uskladňuje všetky médiá KCA ako pásky a dokumenty v bezpečnom prostredí.

Médiá sú uchovávané tak, aby boli chránené pred poškodením (voda, oheň, elektromagnetické poškodenie). Médiá obsahujúce záznamy pre audit, archívne alebo zálohované informácie sú uchovávané v priestoroch, ktoré nie sú fyzicky spojené s prevádzkovými priestormi KCA v súlade s príslušnými internými predpismi KCA a právnymi predpismi SR.

5.1.7 Odpadové hospodárstvo

Nosiče informácií obsahujúce údaje KCA, sú likvidované v zmysle postupov stanovených záväznými internými predpismi NBÚ.

5.1.8 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, rovnako ako minimalizovať ostatné škody vniknuté prípadnou havarijnou situáciou.

KCA vedie podrobnú dokumentáciu zahrňujúcu:

a) procedúry na obnovu činností v prípade poruchy technických prostriedkov, programového vybavenia alebo údajov,

b) procedúry obnovy pre prípad, že certifikát KCA je zrušený,

c) procedúry obnovy pre prípad kompromitácie súkromného kľúča KCA,

d) procedúry pre prevádzku a obnovu prevádzky v prípade prírodnej katastrofy,

e) plány zálohovania, archivácie a uchovávania médií,

f) zoznam konfiguračných parametrov komponentov KCA.

Uvedená dokumentácia je súčasťou bezpečnostných smerníc.

Prevádzkovateľ KCA poskytuje školenia o procedúrach v prípade havárie pre obslužný personál a minimálne raz ročne testuje havarijný plán.

5.1.9 Záložné prevádzkové priestory

Okrem primárnych prevádzkových priestorov KCA disponuje záložnými prevádzkovými priestormi určenými na dislokáciu záložnej technológie KCA a pravidelné ukladanie záložných kópií a archívnych dát.

5.2 Procedurálne opatrenia

Činnosti vykonávané v prevádzke KCA sú popísané formou definície prevádzkových postupov a procedúr. Prevádzkové postupy obsahujú definíciu nadväznosti jednotlivých procedúr, ktoré sú krokmi konkrétneho postupu. Prevádzkové procedúry sú špecifikáciou základných činností pri obsluhe komponentov KCA. Špecifikácia prevádzkovej procedúry obsahuje popis činností pri obsluhe, pravidlá na bezpečnú realizáciu činností a identifikáciu roly, ktorá smie dané činnosti vykonávať.

Na zabezpečenie činností boli pre jednotlivých pracovníkov prevádzky definované roly. Definícia roly pokrýva: rozsah činností ktoré môže pracovník vykonávať, rozsah zodpovednosti pracovníka za vykonávané činnosti, počet osôb potrebných na vykonávanie pridelených činností, pravidlá na obmedzenie fyzického prístupu do priestorov NBUCA, spôsob autentizácie pracovníka pri vykonávaní činností, požiadavky na znalosti a skúsenosti a zlučiteľnosť príslušnej roly s ďalšími rolami.

Pre prevádzkovanie KCA sú definované nasledujúce základné roly:

a) bezpečnostný správca,

b) interný audítor,

c) administrátor PKI (operátor CA),

d) operátor HSM modulu,

e) technický administrátor,

f) registračný operátor.

Spôsob a bezpečnosť vykonávania prevádzkových procedúr sú kontrolované auditom bezpečnosti.

5.2.1 Bezpečnostný správca

Hlavnou úlohou bezpečnostného správcu KCA je prideľovanie rolí a prístupových práv v systéme KCA, odsúhlasovanie zmien v konfigurácii komponentov, vypracovávanie vrcholových dokumentov (CP, CPS), atď.

5.2.2 Interný audítor

Interný audítor predstavuje nezávislý spôsob kontrolovania správy KCA. Rola interného audítora nie je zlučiteľná s rolami, ktoré sa podieľajú na správe a obsluhe komponentov.

5.2.3 Administrátor PKI (CA operátor)

Zodpovednosti CA operátor spočívajú v administrácii (inštalácia, zmeny v konfigurácii) KCA. Operátor CA generuje všetky typy certifikátov vydávaných KCA (bod 1.5 týchto CPS). Zabezpečuje zrušovanie certifikátov vydaných KCA. Všetkých operácií, ktoré PKI administrátor vykonáva sa musí zúčastniť minimálne ďalšia osoba (pravidlo štyroch očí).

5.2.4 Operátor HSM modulov

Činnosti spojené so správou HSM modulov vykonávajú jeden alebo dvaja operátori. Počet operátorov, ktorí sú potrební na vykonanie príslušnej činnosti závisí od typu a úrovne bezpečnosti danej činnosti.

5.2.5 Technický administrátor

Hlavnou úlohou technických administrátorov je spravovanie komponentov tvoriacich technologickú architektúru KCA. Medzi technických administrátorov patria systémoví, databázoví, sieťoví, web, LDAP a backup administrátori.

5.2.6 Registračný operátor

Operátor, ktorý zabezpečuje registračné procesy k vydaniu a zrušovaniu certifikátov vydaných KCA.

5.2.7 Počet osôb potrebných na konkrétnu úlohu

Pri zabezpečovaní bezpečnostne kritických činností (vydávanie a zrušovanie certifikátov, záloha a obnova HSM modulu, zálohovanie a obnova databázy) sa musia zúčastniť minimálne dve osoby (pravidlo štyroch očí).

5.3 Personálne bezpečnostné opatrenia

Každý príslušník NBÚ, ktorý je súčasťou obslužného personálu KCA má vo svojej pracovnej náplni pridelenú jednu alebo viacero rolí. Roly pracovníkov sú jednoznačne definované internými predpismi KCA. Každý pracovník je preukázateľne poučený o svojich povinnostiach, bezpečnostných a pracovných postupoch požadovaných pri plnení úloh vyplývajúcich z jeho roly. Rotácia pracovníkov v jednotlivých rolách sa riadi internými predpismi KCA.

Osoby zabezpečujúce činnosti v rámci prevádzky KCA sú pravidelne preškoľované z tém špecifických pre prevádzku KCA. Témy školení zahrňujú obsluhu technického a programového vybavenia informačného systému KCA, bezpečnostné predpisy KCA a prevádzkové predpisy KCA. Rozsah školení jednotlivých osôb zabezpečujúcich prevádzku je definovaný povahou rolí, ktoré sú im pridelené.

5.3.1 Preverovanie osôb

Osoby zabezpečujúce činnosti v rámci prevádzky KCA sú preverované v zmysle vyhlášky NBÚ č. 331/2004 Z.z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca.

5.3.2 Personálna bezpečnosť pri zmluvne zabezpečovaných činnostiach

Každý pracovník zabezpečujúci zmluvné činnosti musí byť preukázateľne poučený o svojich povinnostiach, bezpečnostných a pracovných postupoch požadovaných pri plnení úloh vyplývajúcich z jeho roly.

5.3.3 Sankcie za neoprávnené činnosti

Udeľovanie sankcií za neoprávnené činnosti sa riadi vnútorným poriadkom NBÚ a platnými právnymi predpismi SR.

5.3.4 Dokumentácia poskytovaná obslužnému personálu KCA

Na definovanie povinností a procedúr pre každú rolu je poskytnutá príslušníkom NBÚ vykonávajúcim túto rolu dokumentácia v potrebnom rozsahu.

Obslužný personál KCA je povinný používať dokumenty, ktoré im boli poskytnuté len na účely, na ktoré sú určené. Každá osoba zabezpečujúca prevádzku KCA je oboznámená s politikou ochrany osobných údajov a dát v rámci KCA.

6. Technické bezpečnostné opatrenia platné pre KCA

Technické bezpečnostné opatrenia zahrňujú opatrenia na ochranu kľúčového materiálu a aktivačných údajov, počítačové bezpečnostné opatrenia (riadenie prístupu, audit, testovanie), bezpečnostné opatrenia na vývoj a riadenie bezpečnosti, sieťové bezpečnostné opatrenia a opatrenia pre kryptografické moduly hardvérovej ochrany kľúča (ďalej len „HSM“).

6.1 Pravidlá pre generovanie kľúčov

6.1.1 Koreňová certifikačná autorita

6.1.1.1 Generovanie párových dát

Generovanie párových dát KCA sa vykonáva prostriedkami HSM modulu v súlade s podpisovými schémami definovanými vyhláškou Národného bezpečnostného úradu č. 135/2009 Z.z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, podmienkach platnosti pre zaručený elektronický podpis, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky), ďalej len „vyhláška NBÚ č. 135/2009 Z.z.“.

HSM modul KCA vyhovuje bezpečnostným požiadavkám podľa FIPS-140-2 Bezpečnostné požiadavky na kryptografické moduly na úrovni 3 (ďalej len „FIPS-140-2 úroveň 3“).

KCA podporuje asymetrický algoritmus RSA s parametrami podľa prílohy č. 1 vyhlášky NBÚ č. 135/2009 Z.z a hašovaciu funkciu sha256.

6.1.1.2 Doručenie súkromného kľúča držiteľovi certifikátu

KCA negeneruje kľúčové páry akreditovaných CA a uznaných zahraničných CA, preto nezabezpečuje doručenie súkromného kľúča.

6.1.1.3 Doručenie verejného kľúča KCA používateľom

Verejný kľúč KCA obsiahnutý v certifikáte, ako aj všetky certifikáty vydané KCA pre akreditované CA a uznané zahraničné CA, sú zverejnené prostredníctvom adresárových služieb NBÚ. Okrem toho sú, v zmysle § 12 ods. 2 vyhlášky NBÚ č. 135/2009 Z.z., certifikáty KCA a jej následníkov zverejňované v tlači. Detailnejšie informácie o spôsobe zverejňovania informácií KCA sa nachádzajú v bode 2.6.2 týchto CPS.

6.1.1.4 Dĺžka kľúčov

Všetky kľúče generované KCA NBÚ majú dĺžku najmenej 2048 bitov. V rámci KCA je použitý asymetrický algoritmus RSA.

6.1.1.5 Parametre verejného kľúča

Zákon č. 215/2002 Z.z. nestanovuje požiadavky na ďalšie špecifické parametre verejných kľúčov.

6.1.1.6 Kontrola kvality parametrov

NBÚ zabezpečí kontrolu nasledovných parametrov kľúčového páru KCA, resp. následníka KCA:

a) algoritmus použitý na generovanie kľúčov,

b) dĺžku kľúčov,

c) jedinečnosť verejného kľúča v zmysle § 4 písm. d) vyhlášky NBÚ č. 131/2009 Z.z.

V prípade, že kľúčový pár nespĺňa požadované parametre, nie je možné vydať certifikát prislúchajúci k príslušnému kľúčovému páru. NBÚ musí zabezpečiť zopakovanie procesu vydávania certifikátu od začiatku.

6.1.1.7 Generovanie kľúčov

Všetky kľúče KCA sú generované v HSM module, ktorý vyhovuje bezpečnostným požiadavkám podľa FIPS-140-2 úroveň 3.

6.1.1.8 Použiteľnosť kľúčov (X.509 v3 Key Usage)

Certifikáty KCA a jej následníkov sú generované s použiteľnosťou kľúčov nastavenou na keyCertSign a cRLSign. Certifikát KCA a certifikát následníka KCA vydáva NBÚ na účely vydávania certifikátov (bod 4.2 týchto CPS) a vydávania zoznamu CRL (bod 4.7.1 týchto CPS).

6.1.2 Akreditované CA a uznané zahraničné CA

6.1.2.1 Generovanie kľúčov

NBÚ neposkytuje službu generovania kľúčového páru pre akreditované CA na svojich zariadeniach.

Kľúčový pár (súkromný a verejný) kľúč akreditovanej CA alebo uznanej zahraničnej CA určený na vydávanie certifikátov sa generuje na prostriedkoch akreditovanej alebo zahraničnej CA pri zaistení požadovanej bezpečnosti generovania.

Zodpovednosť za zaistenie bezpečnosti a kvality generovania kľúčového páru, za zaistenie ochrany súkromného kľúča a za správnosť priradenia súkromného a verejného kľúča z kľúčového páru nesie akreditovaná CA alebo uznaná zahraničná CA.

6.1.2.2 Doručenie súkromného kľúča držiteľovi certifikátu

KCA negeneruje kľúčový pár pre akreditované CA alebo uznané zahraničné CA, preto nezabezpečuje doručenie súkromného kľúča akreditovanej CA alebo uznanej zahraničnej CA.

6.1.2.3 Doručenie verejného kľúča do KCA

Po vygenerovaní kľúčového páru akreditovaná CA alebo uznaná zahraničná CA doručí svoj verejný kľúč do KCA vo forme štandardizovanej elektronickej žiadosti o vydanie certifikát (PKCS#10 žiadosť). Podrobnejšie informácie sú uvedené bodoch 4.1.2 a 4.1.3 týchto CPS.

6.1.2.4 Doručenie certifikátu akreditovanej CA alebo uznanej zahraničnej CA

Postup doručenia certifikátu vydaného KCA akreditovanej CA alebo uznanej zahraničnej CA je popísaný v bode 4.3 týchto CPS.

6.1.2.5 Dĺžka kľúčov

Na generovanie kľúčov musia akreditované CA alebo uznané zahraničné CA využívať algoritmy v súlade s prílohou č. 1 vyhlášky NBÚ č. 135/2009 Z.z. KCA podporuje asymetrický algoritmus RSA s minimálnou dĺžkou kľúčov 2048 bitov.

6.1.2.6 Parametre verejného kľúča

Verejný kľúč akreditovanej CA, ktorý sa má uviesť v certifikáte ako verejný kľúč akreditovanej CA, nesmie byť zhodný s verejným kľúčom uvedenom v ktoromkoľvek inom certifikáte, ktorý vydala KCA v zmysle § 4 písm. d) vyhlášky NBÚ č. 131/2009 Z.z. Pravidlo platí aj pre vydávanie certifikátov pre uznané zahraničné CA a všetky ďalšie certifikáty vydávané KCA.

Zákon č. 215/2002 Z.z. o elektronickom podpise nestanovuje požiadavky na ďalšie parametre verejných kľúčov.

6.1.2.7 Kontrola kvality parametrov

Pri každej žiadosti o certifikát pre akreditované CA alebo uznané zahraničné CA, KCA kontroluje požadované parametre tak, aby verejný kľúč akreditovanej CA alebo uznanej zahraničnej CA spĺňal požiadavky platných právnych predpisov SR.

Operátor RA KCA pri prijatí žiadosti skontroluje, či neexistuje k dodanému verejnému kľúču certifikát vydaný KCA. Ak bol takýto certifikát nájdený, požiada klienta o vygenerovanie nového kľúčového páru a zároveň zruší certifikát, ktorý obsahuje rovnaký verejný kľúč ako kľúč dodaný klientom. Vlastník zrušeného certifikátu je okamžite o tejto udalosti informovaný a je požiadaný o vygenerovanie nového kľúčového páru a o doručenie nového verejného kľúča na vydanie následného certifikátu.

V prípade, že verejný kľúč akreditovanej CA alebo uznanej zahraničnej CA nespĺňa hore uvedené parametre, KCA požiada akreditovanú CA alebo uznanú zahraničnú CA o vygenerovanie nového kľúčového páru a novej PKCS#10 žiadosti.

6.1.2.8 Generovanie kľúčov

Pri procese generovania kľúčov musí akreditovaná CA alebo uznaná zahraničná CA spĺňať požiadavky platných právnych predpisov SR.

6.1.2.9 Využiteľnosť kľúčov (X.509 v3 Key Usage)

Certifikáty pre akreditované CA alebo uznané zahraničné CA sú generované s použiteľnosťou kľúčov (Key Usage) nastavenou na účely podpisovania certifikátov a zoznamov CRL (keyCertSign, cRLSign).

6.2 Ochrana súkromného kľúča

6.2.1 Štandardy pre HSM moduly

Súkromný kľúč KCA a súkromný kľúč následníka KCA sú uložené v HSM moduloch. HSM moduly použité v KCA sú odolné voči nedovolenej manipulácii a vyhovujú bezpečnostným požiadavkám podľa FIPS-140-2 úroveň 3.

6.2.2 Kontrola prístupu k súkromným kľúčom

Na vykonanie kritických činností na kryptografickom module (napr. záloha súkromného kľúča KCA) je nutná súčasná autorizácia dvoch určených pracovníkov NBÚ.

6.2.3 Rozdelenie súkromných kľúčov

Súkromný kľúč KCA je exportovaný v zašifrovanej forme za účelom zálohovania (viď bod 6.2.4 týchto CPS). Neexistuje možnosť získania súkromného kľúča KCA a jej následníkov inými metódami.

6.2.4 Zálohovanie a archivácia súkromných kľúčov

Súkromné kľúče KCA sú zálohované v zašifrovanej forme. Na obnovu týchto kľúčov je nutná súčasná autorizácia dvoch určených príslušníkov NBÚ. Po ukončení platnosti certifikátu KCA, ktorý je zviazaný s verejným kľúčom prislúchajúcim k zálohovanému súkromnému kľúču, bude záloha súkromného kľúča zničená. Toto pravidlo platí aj o súkromnom kľúči následníkov KCA.

KCA nezabezpečuje zálohovanie a archiváciu súkromných kľúčov akreditovaných CA alebo uznaných zahraničných CA.

6.2.5 Uloženie súkromného kľúča

Súkromný kľúč KCA sa generuje priamo prostriedkami kryptografického modulu. Na vygenerovanie súkromného kľúča KCA je potrebná súčasná autorizácia dvoch určených príslušníkov NBÚ. Súkromný kľúč KCA je uložený v zašifrovanom tvare. Funkčné, technické a bezpečnostné vlastnosti HSM modulu, v ktorom je uložený súkromný kľúč KCA, spĺňajú požiadavky vyhlášky NBÚ č. 134/2009 Z.z. Tieto pravidlá platia aj pre súkromné kľúče následníkov KCA.

6.2.6 Aktivácia, deaktivácia a zničenie súkromného kľúča

Aktivácia súkromného kľúča KCA sa uskutočňuje vždy v prítomnosti minimálne dvoch určených príslušníkov NBÚ. Súkromný kľúč KCA je po jeho použití deaktivovaný. Súkromný kľúč KCA môže byť zničený iba za podmienok dvojitej kontroly. Vyššie uvedené pravidlá platia aj pre súkromné kľúče následníkov KCA.

6.3 Manažment párových dát

6.3.1 Archivácia verejných kľúčov

Archivácia verejných kľúčov sa zabezpečuje prostredníctvom archivovania certifikátov, v ktorých sa verejné kľúče nachádzajú. NBÚ zabezpečuje archiváciu všetkých certifikátov vydaných KCA.

Archív certifikátov vydaných KCA je chránený pred neautorizovaným prístupom. Každý archívny záznam je opatrený elektronickým podpisom, ktorý umožňuje kontrolu integrity archívneho záznamu a zabezpečuje autorizáciu pre prácu s archívom. Archívne záznamy sú vytvorené vo viacerých kópiách, minimálne jedna kópia sa uchováva na bezpečnom mieste mimo primárnych prevádzkových priestorov KCA.

6.3.2 Doba použitia súkromných a verejných kľúčov

Doba použitia kľúčových párov je zhodná s dobou platnosti príslušných certifikátov vydaných KCA.

6.4 Aktivačné údaje

6.4.1 Generovanie a inštalácia aktivačných údajov

Na ochranu prístupu k používaniu súkromného kľúča sa používajú čipové karty s definovaným prístupovým heslom. Aktivačné údaje sa vydávajú užívateľovi osobne.

6.4.2 Ochrana aktivačných údajov

Aktivačné údaje musia byť chránené na úrovni údajov chránených HSM modulom a nesmú byť uložené s HSM modulom. Aktivačné údaje nie sú nikdy zdieľané.

6.5 Počítačové bezpečnostné opatrenia

Všetky počítačové komponenty KCA spĺňajú požiadavky na spoľahlivé a bezpečné prevádzkovanie certifikačných služieb v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise.

V systéme KCA sú používané bezpečné produkty certifikované v zmysle zákona č. 215/2002 Z.z. o elektronickom podpise a produkty s medzinárodnou certifikáciou (Common Criteria, ITSEC, NIST).

Základné bezpečnostné opatrenia systému KCA:

a) komponenty systému KCA (hardvér, softvér, sieťové prvky) sú použité výhradne na činnosti spojené s poskytovaním certifikačných služieb,

b) prístup ku komponentom KCA na úrovni logickej bezpečnosti vyžaduje identifikáciu a autentizáciu používateľov,

c) diferenciácia prístupu ku komponentom systému KCA na základe separácie rolí a rôznych funkcií obslužného personálu,

d) nepretržitá dostupnosť služby vydávania a zverejňovania zoznamov CRL,

e) využitie monitorovacieho systému na včasnú detekciu, zaznamenanie a zastavenie pokusov o neautorizovaný prístup k systému KCA,

f) ďalšie bezpečnostné opatrenia popísané v interných predpisoch KCA.

6.6 Bezpečnostné opatrenia na vývoj a riadenie bezpečnosti

6.6.1 Bezpečnostné opatrenia na vývoj

Na zabezpečovanie certifikačných služieb KCA používa bezpečné produkty certifikované podľa zákona č. 215/2002 Z.z. o elektronickom podpise, ISO/IEC 15408 a FIPS-140-2. Pri vývoji produktov museli byť splnené požiadavky na bezpečnosť vývoja, ktoré tieto štandardy stanovujú.

Pri vývoji špecializovaného programového vybavenia sú uplatňované ustanovenia interných predpisov KCA, ktoré predpisujú zásady bezpečnosti vývoja programového vybavenia a riadenie bezpečnosti pri poskytovaní certifikačných služieb.

6.6.2 Opatrenia na riadenie bezpečnosti

Riadenie bezpečnosti KCA vychádza z bezpečnostnej politiky, identifikuje organizáciu riadenia bezpečnosti, zahŕňa manažment rizík pozostávajúci z analýzy rizík, vytvorenia bezpečnostných odporúčaní, systémovej bezpečnostnej politiky, bezpečnostného projektu informačných technológii a implementácie bezpečnosti pozostávajúcej z implementácie bezpečnostných opatrení a budovania bezpečnostného povedomia.

Na zaistenie účinnosti riadenia bezpečnosti slúži pravidelné vykonávanie auditu bezpečnosti (interného a externého), pravidelné vyhodnocovanie účinnosti bezpečnostných opatrení a mechanizmov, prípadný návrh ich zmien a prispôsobovania bezpečnostných opatrení novým podmienkam a ich zapracovávanie do procesu riadenia bezpečnosti.

6.7 Sieťové bezpečnostné opatrenia

Technológia KCA zabezpečujúca funkcie vydávania a zrušovania certifikátov a vydávania zoznamov CRL je striktne oddelená od sieťových a publikačných komponentov KCA a nie je dostupná z verejnej siete Internet. Bezpečnosť siete a sieťových prvkov je pravidelne testovaná.

6.8 Opatrenia pre HSM moduly

HSM moduly KCA vyhovujú bezpečnostným požiadavkám podľa FIPS-140-2 úroveň 3. Bezpečnosť HSM modulov je pravidelne monitorovaná a testovaná. Všetky činnosti súvisiace s prevádzkou HSM modulov sú zaznamenávané a vyhodnocované.

7. Profily certifikátov a zoznamov CRL vydávaných KCA

7.1 Profil certifikátu KCA (KCA1)

Haš certifikátu KCA (KCA1) je nasledovný:

SHA1: A6D7D70982CB73BE7FA69470029E7EF9360EEA68

SHA256: 6FBF021174831BE8B5889C9077F7BD6C385B5541B759E2F096D7D3BDBF774CDB

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

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

Tab. 7.1a Profil certifikátu KCA (KCA1)

7.2 Profil certifikátu následníka KCA (KCA2)

Haš certifikátu následníka KCA (KCA2) je nasledovný:

SHA1: 4EA3F1135F43A4D521973DAA1FBEB3CDF2DCF75A

SHA256: E17E8EC51F376C0371B45BBEB5BD8416584A9E8A44B51E7CA1AE0E36731CCE0F

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

Pole	Kritickosť	Obsah
version		v3
serialNumber		01
signatureAlgorithm		sha1withRSAEncryption (1.2.840.113549.1.1.5)
issuer		CN=KCA NBU SR OU=Sekcia IBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
validity		050222161337Z UTC 150222154357Z UTC
subject		CN=KCA NBU SR OU=Sekcia IBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (2048 bits) 30 82 01 0a 02 82 01 01 00 f2 6f 8e c9 bd 3f 65 65 41 be 5f dc 51 ab 4d c5 a4 8d e2 0c 4b 7c 52 75 9a 80 23 36 fb b4 53 77 1d 8f d1 d7 bd da 14 79 8e db 13 51 66 c7 4a 33 ad 0f 95 4f e8 83 ba 03 42 70 2e be 9c f1 74 6f 83 84 6c 5d f6 32 63 9e 6e de 63 c0 df 6b 31 70 81 d6 21 ba d7 3a 81 f7 f1 95 7b c1 aa 36 39 74 0b 2f f2 9b 6d 08 aa 05 a7 6c da 2e 5b fd b5 0d b8 fd 8b 75 53 9d a5 01 9e 1e e3 98 9b d3 29 10 3b d4 39 eb 61 d6 1a a4 65 78 fe 63 88 91 b8 de f1 98 e0 67 58 e0 af 18 63 ab 29 ec 83 c3 e9 1a b3 d9 13 27 93 9c 5f 90 d0 54 2c 96 34 94 8c cb ef 05 62 82 eb ad a3 b6 b9 85 2e 54 1b fc 2b 3b ae 51 22 24 60 c6 85 3a ea c8 c9 a5 9d a9 f4 df 9c 0b 9d e5 35 67 f0 e1 d2 1f 3b 5c 9f fb 21 bd 9c 19 7d f6 b8 86 7e 70 59 0d 3a a4 03 13 cd b6 88 46 5c 84 34 34 c3 50 e6 31 b4 3f 7c 9d d8 e1 02 03 01 00 01
certificatePolicies		[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Certifikat je vydany ako kvalifikovany certifikat KCA NBU SR v sulade s platnymi pravnymi predpismi SR.

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

Tab. 7.2a Profil certifikátu následníka KCA (KCA2)

7.3 Profil certifikátu druhého následníka KCA (KCA3)

Haš certifikátu druhého následníka KCA (KCA3) je nasledovný:

SHA1: 21F73B27BBBF2811BBEAB4F1799E7DD892F3FE85

SHA256: D83477E0388C40BA092FECA484A5EBD3AD3028BF60220132E95158C00DDCE98F

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

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

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

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

7.4 Profil krížového certifikátu vydaného KCA1 pre KCA2

Haš krížového certifikátu vydaného KCA1 pre KCA2 je nasledovný:

SHA1: F03FFB2B949CB98DBF746659A1337DAA8427DE92

SHA256: 7F7953F8ADDD9C9939CB4E272162455A6643F73E40A4900C75288CB8269BB0FF

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

Pole	Kritickosť	Obsah
Version		v3
serialNumber		213C
signatureAlgorithm		sha1withRSAEncryption (1.2.840.113549.1.1.5)
Issuer		CN=Korenova CA pre kvalifikovane certifikaty 1 L=Bratislava OU=Sekcia elektronickeho podpisu O=Narodny bezpecnostny urad C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
Validity		050222230000Z UTC 060114155622Z UTC
subject		CN=KCA NBU SR OU=Sekcia IBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (2048 bits) 30 82 01 0a 02 82 01 01 00 f2 6f 8e c9 bd 3f 65 65 41 be 5f dc 51 ab 4d c5 a4 8d e2 0c 4b 7c 52 75 9a 80 23 36 fb b4 53 77 1d 8f d1 d7 bd da 14 79 8e db 13 51 66 c7 4a 33 ad 0f 95 4f e8 83 ba 03 42 70 2e be 9c f1 74 6f 83 84 6c 5d f6 32 63 9e 6e de 63 c0 df 6b 31 70 81 d6 21 ba d7 3a 81 f7 f1 95 7b c1 aa 36 39 74 0b 2f f2 9b 6d 08 aa 05 a7 6c da 2e 5b fd b5 0d b8 fd 8b 75 53 9d a5 01 9e 1e e3 98 9b d3 29 10 3b d4 39 eb 61 d6 1a a4 65 78 fe 63 88 91 b8 de f1 98 e0 67 58 e0 af 18 63 ab 29 ec 83 c3 e9 1a b3 d9 13 27 93 9c 5f 90 d0 54 2c 96 34 94 8c cb ef 05 62 82 eb ad a3 b6 b9 85 2e 54 1b fc 2b 3b ae 51 22 24 60 c6 85 3a ea c8 c9 a5 9d a9 f4 df 9c 0b 9d e5 35 67 f0 e1 d2 1f 3b 5c 9f fb 21 bd 9c 19 7d f6 b8 86 7e 70 59 0d 3a a4 03 13 cd b6 88 46 5c 84 34 34 c3 50 e6 31 b4 3f 7c 9d d8 e1 02 03 01 00 01
certificatePolicies		[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Certifikat je vydany ako krizovy (cross) certifikat pre naslednika KCA NBU SR v sulade s platnymi pravnymi predpismi

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

Tab. 7.4a Profil krížového certifikátu vydaného KCA1 pre KCA2

7.5 Profil krížového certifikátu vydaného KCA2 pre KCA1

Haš krížového certifikátu vydaného KCA2 pre KCA1 je nasledovný:

SHA1: 4B28494356B78C09336B30FB8887BCBC17C130E2

SHA256: FC06ADEDA98C9A625720B3C1E7BF9491466A01345D7267817CC28BF138FDDB87

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

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

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

Tab. 7.5a Profil krížového certifikátu vydaného KCA2 pre KCA1

7.6 Profil certifikátu akreditovanej CA / uznanej zahraničnej CA vydávaného KCA

V nasledujúcej tabuľke je uvedený profil certifikátu pre akreditovanú CA / uznanú zahraničnú CA vydávaného KCA.

Pole	Kritickosť	Obsah
version		v3
serialNumber		jednoznačné sériové číslo pridelené KCA
signatureAlgorithm		sha256withRSAEncryption (1.2.840.113549.1.1.11)
issuer		CN=KCA NBU SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
validity		začiatok platnosti certifikátu (X) koniec platnosti certifikátu (X + 3 roky)
subject		Rozlišovacie meno (DN) akreditovanej CA / uznanej zahraničnej CA Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
subjectPublicKeyInfo		RSA (najmenej 2048 bits) verejný kľúč akreditovanej CA / uznanej zahraničnej CA
policyMappings		[1]Issuer Domain=1.3.158.36061701.0.0.0.1.2.2 Subject Domain=0.4.0.1456.1.1 [2]Issuer Domain=1.3.158.36061701.0.0.0.1.2.2 Subject Domain=1.3.158.36061701.0.0.0.1.2.2
authorityInfoAccess		[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ep.nbusr.sk/kca/certs/kca3/kcanbusr3_p7c.p7c [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary [3]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap:///cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary
authorityKeyIdentifier (SHA1)		KeyID=7f f1 3d 21 c2 97 5a 2e 97 07 0e b1 69 83 25 fd 21 86 3e 07
cRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name:

		URL=http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ep.nbusr.sk/cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList; [3]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap:///cn=KCA NBU SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;
subjectKeyIdentifier (SHA1)		haš verejného kľúča akreditovanej CA / uznanej zahraničnej CA
basicConstraints	**Critical**	Subject Type=CA Path Lenght Constraint=1
certificatePolicies	**Critical**	[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://ep.nbusr.sk/kca/doc/kca_cps.pdf
policyConstraints	**Critical**	Required Explicit Policy Skip Certs=0
keyUsage	**Critical**	keyCertSign, cRLSign

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

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

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

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

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

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

7.8 Profil zoznamu CRL vydávaného KCA

V nasledujúcej tabuľke je uvedený profil zoznamu CRL generovaného KCA.

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

7.8a Profil zoznamu CRL vydávaného KCA

8. Administrácia špecifikácií

8.1 Zmenové procedúry

Tieto CPS sú revidované ako celok raz za 12 mesiacov. Chyby, požiadavky na aktualizáciu alebo navrhované zmeny majú byť zaslané na kontaktnú adresu uvedenú v bode 1.7 týchto CPS. Tieto návrhy musia obsahovať popis navrhovanej zmeny, zdôvodnenie zmeny a kontaktnú informáciu o fyzickej alebo právnickej osobe, ktorá zmenu požaduje.

Všetky uvažované zmeny týchto CPS majú byť zaslané dotknutým stranám minimálne mesiac vopred. NBÚ môže akceptovať, akceptovať s modifikáciami alebo zamietnuť navrhované zmeny.

8.2 Identifikácia verzií

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

Verzia A.B

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

Podstatné zmeny CPS sa v čísle verzie odrážajú na pozícii A.

8.3 Procedúry na zverejnenie

NBÚ zverejní tieto CPS na internetovej stránke podľa bodu 2.6.1 týchto CPS. Aktuálne platné CPS musia byť v súlade s aktuálne platným CP.

8.4 Procedúry na schvaľovanie

Tieto CPS schvaľuje riaditeľ sekcie informačnej bezpečnosti a elektronického podpisu NBÚ.

9. Účinnosť

Pravidlá na výkon certifikačných činností koreňovej certifikačnej autority, verzia 3.0 nadobúdajú účinnosť dňa 17. 8. 2010.