

Národný bezpečnostný úrad  
sekcia ekonomiky a prevádzky



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

Verzia: 3.2

Dokument nadobúda účinnosť dňa 19.08.2015

# Obsah

Zoznam použitých pojmov .....	5
Skratky.....	7
1. Úvod .....	9
1.1 Účel certifikačného poriadku .....	9
1.2 Identifikácia CP.....	9
1.3 Charakteristika, použitie a subjekty pracujúce s certifikátmi .....	10
1.3.1 Charakteristika certifikátov .....	10
1.3.2 Kľúče KCA .....	10
1.3.3 Použitie certifikátov.....	10
1.3.4 Subjekty pracujúce s certifikátom KCA .....	11
1.4 Kontaktné informácie KCA .....	13
1.4.1 Špecifikácia administrátorskej organizácie.....	13
1.4.2 Kontaktná adresa .....	13
1.4.3 Kontaktná osoba.....	13
2. Všeobecné ustanovenia .....	14
2.1 Povinnosti jednotlivých subjektov .....	14
2.1.1 Povinnosti KCA.....	14
2.1.2 Povinnosti držiteľa certifikátu KCA .....	14
2.1.3 Povinnosti používateľa certifikátov .....	14
2.1.4 Povinnosti správcov adresárov.....	14
2.2 Právne záruky.....	15
2.3 Finančná zodpovednosť KCA.....	15
2.4 Rozhodcovské konanie a riešenie sporov .....	15
2.5 Zverejňovanie informácií KCA .....	15
2.5.1 Zverejňovanie dokumentácie KCA .....	15
2.5.2 Zverejňovanie certifikátov KCA .....	15
2.5.3 Zverejňovanie zoznamov zrušených certifikátov KCA .....	16
2.5.4 Periodicita publikovania informácií KCA.....	17
2.6 Audit zhody .....	17
2.7 Dôvernosť .....	17
2.8 Ochrana práv duševného vlastníctva .....	17
3. Identifikácia a autentifikácia .....	18
3.1 Menná konvencia.....	18
3.1.1 Certifikáty KCA .....	18
3.1.2 Certifikáty na správu.....	19

3.1.3	Kvalifikované certifikáty .....	20
3.2	Iniciálna registrácia .....	21
3.2.1	Koreňová certifikačná autorita KCA .....	21
3.2.2	Následník KCA .....	21
3.3	Spôsob preukázania vlastníctva súkromného kľúča KCA .....	21
3.4	Vydanie následného certifikátu KCA .....	21
3.5	Vydanie následného certifikátu po zrušení certifikátu KCA .....	21
3.6	Žiadosť o zrušenie certifikátu KCA .....	21
4.	Prevádzkové postupy .....	23
4.1	Generovanie kľúčov .....	23
4.1.1	Generovanie kľúčov KCA .....	23
4.1.2	Generovanie podpisových kľúčov pre kvalifikované certifikáty .....	23
4.2	Žiadosť o vydanie certifikátu KCA .....	24
4.3	Vydanie certifikátu KCA .....	24
4.4	Prevzatie certifikátu KCA .....	24
4.5	Zrušenie certifikátu KCA .....	24
4.5.1	Okolnosti na zrušenie .....	24
4.5.2	Oprávnení žiadateľa o zrušenie certifikátu .....	25
4.5.3	Postup pri zrušení certifikátu .....	25
4.5.4	Interval na zrušenie certifikátu .....	25
4.5.5	Periodicita publikovania zoznamu CRL .....	25
4.5.6	Zisťovanie stavu certifikátov .....	25
4.5.7	Iné možnosti informovania o zrušení certifikátov .....	25
4.6	Audit bezpečnosti poskytovania certifikačných činností KCA .....	25
4.7	Archivácia záznamov KCA .....	25
4.8	Výmena kľúčov KCA .....	26
4.9	Havarijný plán KCA .....	26
4.10	Ukončenie činnosti KCA .....	26
5.	Fyzické procedurálne a personálne bezpečnostné opatrenia KCA .....	27
5.1	Opatrenia na zaistenie fyzickej bezpečnosti .....	27
5.2	Opatrenia na zaistenie procedurálnej bezpečnosti .....	27
5.3	Opatrenia na zaistenie personálnej bezpečnosti .....	27
6.	Technické bezpečnostné opatrenia .....	28
6.1	Opatrenia na zaistenie bezpečnej prevádzky KCA .....	28
6.2	Kryptografické prostriedky ochrany kľúčov KCA .....	28
7.	Profily certifikátov a zoznamov zrušených certifikátov .....	29
7.1	Profil certifikátu KCA (KCA1) .....	29
7.2	Profil certifikátu následníka KCA (KCA2) .....	31

7.3	Profil certifikátu druhého následníka KCA (KCA3) .....	33
7.4	Profil krížového certifikátu vydaného KCA1 pre KCA2.....	35
7.5	Profil krížového certifikátu vydaného KCA2 pre KCA1.....	37
7.6	Profil certifikátu akreditovanej CA / uznanej zahraničnej CA .....	39
7.7	Profil certifikátu pre podpisovanie slovenského TSL a schválených podpisových politík vydávaného KCA 41	
7.8	Profil kvalifikovaného certifikátu fyzickej osoby .....	43
7.9	Profil kvalifikovaného systémového certifikátu .....	43
7.10	Profil zoznamu CRL vydávaného KCA.....	44
8.	Administrácia špecifikácií.....	45
8.1	Identifikácia verzií .....	45
8.2	Schvaľovanie verzií .....	45
9.	Účinnosť certifikačného poriadku.....	46

## Zoznam použitých pojmov

<b>adresárové služby</b>	Špecializovaná databáza, v ktorej sú zverejňované certifikáty a zoznamy zrušených certifikátov.
<b>certifikačná autorita</b>	Dôveryhodná autorita, ktorá generuje certifikáty a zoznamy zrušených certifikátov (komponent infraštruktúry PKI).
<b>certifikačné služby</b>	Služby, ktoré poskytuje certifikačná autorita (registrácia, certifikácia, overenie platnosti a funkčnosti certifikátu, zrušenie certifikátu, výmena kľúčov).
<b>certifikačný poriadok</b>	Pomenovaný zoznam pravidiel, ktoré označujú použiteľnosť certifikátu v príslušnej skupine alebo triede aplikácií zdieľajúcej spoločné bezpečnostné požiadavky.
<b>certifikácia</b>	Proces, počas ktorého certifikačná autorita na základe štandardizovanej žiadosti vydá k príslušnému verejnému kľúču certifikát.
<b>certifikát</b>	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.
<b>certifikát na správu</b>	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.
<b>elektronický podpis</b>	Jedinečná digitálna identifikácia entity, ktorá sa využíva na autentifikáciu zdroja, integrity dát a nepopierateľnosť. Elektronický podpis využíva princípy asymetrickej kryptografie a matematickú funkciu známu ako „message digest“.
<b>HSM</b>	Kryptografický modul hardvérovej ochrany kľúča umožňujúci vykonávať kryptografické operácie.
<b>infraštruktúra PKI</b>	Technické a programové vybavenie použité na zaistenie poskytovania certifikačných služieb.
<b>KCA</b>	Koreňová certifikačná autorita Národného bezpečnostného úradu.
<b>kľúčový pár</b>	Dvojica asymetrických kľúčov, ktorá pozostáva zo súkromného a verejného kľúča.
<b>kompromitácia súkromného kľúča</b>	Zneužitie, použitie alebo prístupenie 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.
<b>obnova kľúčov</b>	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.
<b>pravidlá na výkon certifikačných činností</b>	Zoznam predpisov a praktík, ktoré certifikačné autority používajú pri vydávaní certifikátov.
<b>registračná autorita</b>	Komponent infraštruktúry PKI používaný na posúvanie schválených žiadostí o vydanie certifikátu do certifikačnej autority.

<b>spoliehajúca strana</b>	Subjekt alebo komponent, ktorý požaduje od PKI infraštruktúry overenie stavu certifikátu.
<b>súkromný kľúč</b>	Súkromná časť dvojice asymetrických kľúčov, ktorá sa používa na podpisovanie a (alebo) dešifrovanie správ.
<b>verejný kľúč</b>	Verejná časť dvojice asymetrických kľúčov, ktorá sa používa na overovanie a (alebo)dešifrovanie správ.
<b>zrušenie certifikátu</b>	Predčasné ukončenie platnosti certifikátu. Platnosť certifikátu nie je možné obnoviť.
<b>zoznam zrušených certifikátov</b>	Zoznam všetkých zrušených neexpirovaných certifikátov vydaných CA.

## Skratky

<b>C</b>	krajina ( <i>Country</i> )
<b>CA</b>	certifikačná autorita ( <i>Certification Authority</i> )
<b>CMLC</b>	životný cyklus správy certifikátu ( <i>Certificate Management Life Cycle</i> )
<b>CN</b>	bežné meno ( <i>Common Name</i> )
<b>CP</b>	certifikačný poriadok ( <i>Certificate Policy</i> )
<b>CPS</b>	pravidlá na výkon certifikačných činností ( <i>Certification Practice Statement</i> )
<b>CRL</b>	zoznam zrušených certifikátov ( <i>Certificate Revocation List</i> )
<b>CSE</b>	Certificate Signing Event
<b>DN</b>	rozlišovacie meno ( <i>Distinguished Name</i> )
<b>eIDAS</b>	Electronic Identification and trust services
<b>ETSI</b>	European Telecommunications Standards Institute
<b>EÚ</b>	Európska únia ( <i>European Union</i> )
<b>FIPS</b>	Federal Information Processing Standards
<b>HSM</b>	kryptografický modul hardvérovej ochrany kľúča ( <i>Hardware Security Module</i> )
<b>HTTP</b>	Hypertext Transfer Protocol
<b>IČO</b>	identifikačné číslo organizácie
<b>IDC</b>	číslo identifikačnej karty
<b>IEC</b>	International Electrotechnical Commission
<b>ISO</b>	International Organization for Standardization
<b>KCA</b>	koreňová certifikačná autorita
<b>KCA1</b>	koreňová certifikačná autorita 1
<b>KCA2</b>	prvý následník koreňovej certifikačnej autority, druhá verzia koreňovej certifikačnej autority
<b>KCA3</b>	druhý následník koreňovej certifikačnej autority, tretia verzia koreňovej certifikačnej autority
<b>L</b>	lokalita ( <i>Locality</i> )
<b>LDAP</b>	protokol pre prístup k adresárovým službám ( <i>Lightweight Directory Access Protocol</i> )
<b>NBÚ</b>	Národný bezpečnostný úrad
<b>NTR</b>	Identifikačné číslo organizácie

<b>O</b>	organizácia ( <i>Organization</i> )
<b>OID</b>	objektový identifikátor ( <i>Object Identifier Descriptor</i> )
<b>OU</b>	organizačná jednotka ( <i>Organizational Unit</i> )
<b>PKCS</b>	Public Key Cryptography Standards
<b>PKI</b>	infraštruktúra verejného kľúča ( <i>Public Key Infrastructure</i> )
<b>PNO</b>	osobné číslo
<b>QCP</b>	kvalifikovaný certifikačný poriadok ( <i>Qualified Certificate Policy</i> )
<b>RFC</b>	Request for Comments
<b>RSA</b>	Rivest-Shamir-Adleman
<b>SHA</b>	Secure Hash Algorithm
<b>SK</b>	Slovensko ( <i>Slovakia</i> )
<b>SR</b>	Slovenská republika ( <i>Slovak Republic</i> )
<b>SSCD</b>	bezpečné zariadenie na vyhotovovanie elektronického podpisu ( <i>Secure Signature Creation Device</i> )
<b>SW TWS</b>	Software for Trustworthy System
<b>SZ</b>	identifikácia na základe súboru znakov
<b>TS</b>	technická špecifikácia ( <i>Technical Specification</i> )
<b>TSL</b>	dôveryhodný zoznam ( <i>Trusted List</i> )
<b>V</b>	verzia ( <i>Version</i> )
<b>VAT</b>	daňové identifikačné číslo
<b>Z. z.</b>	zbierka zákonov



# 1. Úvod

## 1.1 Účel certifikačného poriadku

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

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

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

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

## 1.2 Identifikácia CP

Certifikačný poriadok identifikujúci certifikáty KCA, certifikáty na správu a kvalifikované certifikáty (kvalifikované certifikáty fyzických osôb a kvalifikované systémové certifikáty) vydávané akreditovanými CA a uznanými zahraničnými CA, ktoré spĺňajú požiadavky platných právnych predpisov SR je identifikovaný pomocou OID odvodeného od OID NBÚ.

OID tohto CP má tvar:

**1.3.158.36061701.0.0.0.1.2.2**

kde jednotlivé zložky OID majú nasledovný význam:

<b>1</b>	ISO
<b>3</b>	ISO Identified Organization
<b>158</b>	Slovakia
<b>36061701</b>	jedinečný identifikátor NBÚ priradený organizáciou ISO (IČO)
<b>0</b>	riaditeľ NBÚ
<b>0</b>	útvár NBÚ
<b>0</b>	KCA
<b>1</b>	dokumentácia KCA
<b>2</b>	certifikačné poriadky
<b>2</b>	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

## 1.3 Charakteristika, použitie a subjekty pracujúce s certifikátmi

### 1.3.1 Charakteristika certifikátov

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

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

### 1.3.2 Kľúče KCA

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

### 1.3.3 Použitie certifikátov

Certifikáty KCA môžu byť použité na:

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

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

- a) overovanie platnosti kvalifikovaných certifikátov – kvalifikovaných certifikátov fyzických osôb a kvalifikovaných systémových certifikátov,
- b) overovanie certifikátov na správu,
- c) overenie platnosti zoznamov CRL vydávaných akreditovanými CA a uznanými zahraničnými CA,
- d) overovanie platnosti nepriamych zoznamov zrušených certifikátov (aj v on-line režime ),
- e) overenie platnosti certifikátov na správu autorít časových pečiatok.

Kvalifikované certifikáty fyzických osôb môžu byť použité na overovanie platnosti zaručených elektronických podpisov a kvalifikované systémové certifikáty môžu byť použité na overovanie platnosti zaručených elektronických pečatí.

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

### 1.3.3.1 Dôležité obmedzenia certifikátov požadované v tomto CP

- a) Certifikáty na správu a kvalifikované certifikáty, ktoré vytvárajú certifikačnú cestu v strome dôvery KCA, musia obsahovať v rozšírení certificatePolicies objektový identifikátor tohto CP (1.3.158.3606.1701.0.0.0.1.2.2).
- b) Žiadne certifikáty vytvárajúce certifikačnú cestu v strome dôvery KCA, nesmú okrem self-signed certifikátov obsahovať v rozšírení certificatePolicies objektový identifikátor anyPolicy (2.5.29.32.0).
- c) Certifikát sa nesmie nachádzať v stave pozastavenia platnosti, teda v stavoch certificateHold a removeFromCRL.
- d) Čas zrušenia certifikátu v zozname zrušených certifikátov nesmie byť pred časom, po ktorom bol vydaný iný zoznam zrušených certifikátov, podľa ktorého bol certifikát platný.
- e) Súkromný kľúč prislúchajúci k verejnému kľúču, na ktorý bol vydaný kvalifikovaný certifikát fyzickej osoby sa musí nachádzať na bezpečnom zariadení na vyhotovenie elektronického podpisu (SSCD), ktoré je certifikované NBÚ a nijakým spôsobom neumožňuje export súkromného kľúča zo SSCD. Za overenie SSCD zariadenia zodpovedá akreditovaná CA a uznaná zahraničná CA, a ak SSCD zariadenie fyzická osoba žiadajúca o kvalifikovaný certifikát nevlastní, tak aj za jeho dodanie žiadateľovi,
- f) Súkromný kľúč prislúchajúci k verejnému kľúču, na ktorý bol vydaný kvalifikovaný systémový certifikát sa musí nachádzať na bezpečnom zariadení na vyhotovenie elektronickej pečate, ktoré je certifikované NBÚ. Za overenie bezpečného zariadenia zodpovedá akreditovaná CA a uznaná zahraničná CA.

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

Certifikáty KCA, certifikáty na správu a kvalifikované certifikáty musia spĺňať požiadavky, ktoré definuje NBÚ v štandardoch zverejnených na vlastných internetových stránkach. Uvedené štandardy podrobne definujú požiadavky na formáty certifikátov KCA, certifikátov na správu, kvalifikovaných certifikátov a zoznamov CRL.

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

<http://www.nbusr.sk/sk/elektronicky-podpis/standardy-nbu/schvalene-formaty.html>

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

[http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/legislativa/kontrola\\_cert\\_cesty.pdf](http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/legislativa/kontrola_cert_cesty.pdf)

## 1.3.4 Subjekty pracujúce s certifikátom KCA

### 1.3.4.1 Koreňová certifikačná autorita (KCA)

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

### 1.3.4.2 Registračná autorita KCA

Služby registračnej autority KCA v zmysle tohto CP vykonáva NBÚ.

### 1.3.4.3 Správca adresárov KCA

Správcom adresárov KCA v zmysle tohto CP je NBÚ.

### 1.3.4.4 Držiteľ certifikátu KCA

Držiteľom certifikátu KCA je NBÚ.

### 1.3.4.5 Používatelia certifikátu KCA (Relying Party)

Používateľmi certifikátu KCA sú:

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

### 1.3.4.6 Druhy certifikátov vydávané KCA

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

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

---

## 1.4 Kontaktné informácie KCA

### 1.4.1 Špecifikácia administrátorskej organizácie

Tento CP je spravovaný NBÚ.

### 1.4.2 Kontaktná adresa

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

<http://www.nbusr.sk>

<http://ep.nbusr.sk>

### 1.4.3 Kontaktná osoba

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

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

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

Fax: +421 2/ 6869 1710

E-mail: [podatelna@nbusr.sk](mailto:podatelna@nbusr.sk)  
[secadmin@nbusr.sk](mailto:secadmin@nbusr.sk)

## 2. Všeobecné ustanovenia

### 2.1 Povinnosti jednotlivých subjektov

#### 2.1.1 Povinnosti KCA

KCA ako vydavateľ certifikátu vlastného verejného kľúča je povinná:

- a) zaistiť kontrolu vlastníctva a správneho priradenia súkromného kľúča z príslušného kľúčového páru k verejnému kľúču,
- b) zabezpečiť správnosť všetkých informácií v tele certifikátu a ich súlad s jeho certifikačným profilom,
- c) potvrdiť vlastníctvo a správne priradenie súkromného a verejného kľúča, ako aj správnosť informácií obsiahnutých v tele certifikátu vydaním certifikátu verejného kľúča,
- d) včas zverejniť informácie o novo vydanom certifikáte,
- e) včas informovať používateľov o pripravovanej zmene kľúčov a certifikátov,
- f) zverejnením certifikátu (resp. jeho charakteristik) viacerými prostriedkami vytvoriť podmienky na bezpečné overenie platnosti a správnosti certifikátu.

#### 2.1.2 Povinnosti držiteľa certifikátu KCA

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

- a) používať súkromný kľúč prislúchajúci k certifikátu KCA iba na účely, na ktoré bol určený,
- b) zaobchádzať so svojim súkromným kľúčom s náležitou starostlivosťou tak, aby nemohlo dôjsť k jeho zneužitiu,
- c) neodkladne zrušiť certifikát KCA ak zistí, že došlo k neoprávnenému použitiu jeho súkromného kľúča alebo ak hrozí neoprávnené použitie jeho súkromného kľúča,
- d) dodržiavať všetky podmienky a obmedzenia týkajúce sa používania súkromných kľúčov a certifikátov.

#### 2.1.3 Povinnosti používateľa certifikátov

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

#### 2.1.4 Povinnosti správcov adresárov

Správca adresárov je povinný zabezpečiť:

- a) včasné a presné publikovanie certifikátov,
- b) včasné a presné publikovanie zoznamov CRL.

---

## 2.2 Právne záruky

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

---

## 2.3 Finančná zodpovednosť KCA

V rámci tohto CP nie je stanovená žiadna finančná zodpovednosť.

---

## 2.4 Rozhodcovské konanie a riešenie sporov

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

---

## 2.5 Zverejňovanie informácií KCA

KCA zverejňuje:

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

### 2.5.1 Zverejňovanie dokumentácie KCA

Verejne prístupná dokumentácia KCA je zverejnená elektronicky na nasledujúcej internetovej stránke:

<http://ep.nbusr.sk/kca/index.html>

V listinnej podobe je dokumentácia k dispozícii na NBÚ.

### 2.5.2 Zverejňovanie certifikátov KCA

KCA zverejňuje nasledovné typy vydaných certifikátov:

- a) certifikát vlastného verejného kľúča KCA,
- b) certifikáty následníkov KCA,
- c) krížové certifikáty KCA a následníka KCA vydávané počas procesu výmeny kľúčov KCA (ak sú vydané),
- d) certifikáty vydané pre 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](http://ep.nbusr.sk/kca/zoznam_certifikatov.html)
- b) v listinnej podobe na NBÚ,
- c) v dennej tlači – platí pre certifikáty KCA a certifikáty následníkov KCA,
- d) certifikát vlastného verejného kľúča KCA (KCA1) je dostupný prostredníctvom adresárových služieb na adrese:  
[ldap://ep.nbusr.sk/cn=Korenova\\_CA\\_pre\\_kvalifikovane\\_certifikaty\\_1,l=Bratislava,ou=Sekcia\\_elektronickeho\\_podpisu,o=Narodny\\_bezpecnostny\\_urad,c=sk?caCertificate;binary](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](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](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 podliehajúceho zverejňovaniu.

### **2.5.3 Zverejňovanie zoznamov zrušených certifikátov KCA**

KCA publikuje zoznamy CRL nasledovne:

#### **KCA1**

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

Archív CRL (HTTP): <http://ep.nbusr.sk/kca/archive>

Archív CRL (LDAP): [ldap://ep.nbusr.sk/ou=crls,ou=Sekcia\\_elektronickeho\\_podpisu,o=Narodny\\_bezpecnostny\\_urad,c=sk?cRLDistributionPoint?sub?](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](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?](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?](ldap://ep.nbusr.sk/ou=arch_crls_KCA3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?cRLDistributionPoint?sub?)

## **2.5.4 Periodicita publikovania informácií KCA**

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

Zároveň musí byť zabezpečené, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, ktorý obsahuje 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 Audit zhody**

Tento CP sa riadi platnými právnymi predpismi SR.

---

## **2.7 Dôvernosť**

Tento CP sa riadi platnými právnymi predpismi SR.

---

## **2.8 Ochrana práv duševného vlastníctva**

Tento CP sa riadi platnými právnymi predpismi SR.

## 3. Identifikácia a autentifikácia

### 3.1 Menná konvencia

#### 3.1.1 Certifikáty KCA

##### 3.1.1.1 Menná konvencia pre KCA

###### **KCA1 (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 NBÚ SR  
Organizational Unit: Sekcia IBEP  
Organization: Narodny bezpecnostny urad  
Locality: Bratislava  
Country: SK

DN držiteľa certifikátu:

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

**KCA3 (self-signed)**

DN vydavateľa certifikátu:

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

DN držiteľa certifikátu:

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

**3.1.1.2 Pravidlá na zabezpečenie jednoznačnosti mien KCA**

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

**3.1.1.3 Riešenie sporov týkajúcich sa mien KCA**

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

**3.1.2 Certifikáty na správu**

Menná konvencia certifikátov na správu musí byť navrhovaná KCA, akreditovanými CA a uznanými zahraničnými CA tak, aby jednoznačne identifikovala držiteľa certifikátu.

Na základe § 3 ods. 8 vyhlášky NBÚ č. 131/2009 Z. z. musí byť v certifikátoch na správu uvedený identifikátor certifikačného poriadku akreditovaných certifikačných služieb OID s hodnotou QCP SK '1 3 158 36061701 0 0 0 1 2 2'. Tento identifikátor musí byť uvedený v rozšírení certifikačnej politiky certifikátu a je aj identifikátorom certifikačnej politiky, ktorá sa smie uviesť len v kvalifikovaných certifikátoch a certifikátoch na správu vydaných certifikačnými autoritami akreditovanými NBÚ. V certifikátoch koncového používateľa v rozšírení certifikačného poriadku, ktorého OID je '1 3 158 36061701 0 0 0 1 2 2', by mal byť uvedený v položke userNotice-explicitText (formát utf8String) text s informáciou o type certifikátu podľa slovenskej legislatívy uvádzaný v anglickom ako aj v slovenskom jazyku s úvodným textom „EN: “ a „SK: “, ktorý obsahuje najmä: „Certifikát je vydaný ako certifikát na správu podľa zákona č. 215/2002 Z. z. a vyhlášky NBÚ č. 131/2009 Z. z.“.

### 3.1.3 Kvalifikované certifikáty

#### 3.1.3.1 Kvalifikované certifikáty fyzických osôb

Pravidlá menšej konvencie kvalifikovaných certifikátov fyzických osôb sú uvedené v štandarde NBÚ „Formáty certifikátov a kvalifikovaných certifikátov“, ktorý je zverejnený na nasledujúcej internetovej stránke:

<http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/schvalene-formaty/formatycertqc4ts.pdf>

Na základe § 3 ods. 8 vyhlášky NBÚ č. 131/2009 Z. z. musí byť v kvalifikovaných certifikátoch fyzických osôb uvedený identifikátor certifikačného poriadku akreditovaných certifikačných služieb OID s hodnotou QCP SK '1 3 158 36061701 0 0 0 1 2 2'. Tento identifikátor musí byť uvedený v rozšírení certifikačnej politiky certifikátu a je aj identifikátorom certifikačnej politiky, ktorá sa smie uviesť len v kvalifikovaných certifikátoch a certifikátoch na správu vydanými certifikačnými autoritami akreditovanými NBÚ. V certifikátoch koncového používateľa v rozšírení certifikačného poriadku, ktorého OID je '1 3 158 36061701 0 0 0 1 2 2', by mal byť uvedený v položke userNotice-explicitText (formát utf8String) text s informáciou o type certifikátu podľa slovenskej legislatívy uvádzaný v anglickom ako aj v slovenskom jazyku s úvodným textom „EN: “ a „SK: “, ktorý obsahuje najmä: „Certifikát je vydaný ako kvalifikovaný certifikát podľa zákona č. 215/2002 Z. z. a vyhlášky NBÚ č. 131/2009 Z. z.“.

Kvalifikovaný certifikát fyzickej osoby spája identitu vlastníka súkromného kľúča s verejným kľúčom slúžiacim na overenie jeho podpisov, pričom všetky údaje obsiahnuté v kvalifikovanom certifikáte fyzickej osoby boli v čase jeho vydania poskytovateľom certifikačných služieb overené ako platné. Tieto údaje sú uložené najmä v položkách mena subjektu Certificate-tbsCertificate-subject-RelativeDistinguishedName.

Obsah položky commonName je informatívny a pre overovateľa a podpisovateľa poskytuje stručnú informáciu o mene a prípadne type certifikátu. Položka commonName musí byť uvedená a musí sa nachádzať iba raz.

Kvalifikovaný certifikát fyzickej osoby podľa § 3 ods. 4 vyhlášky NBÚ č. 131/2009 Z. z. musí obsahovať minimálne:

- a) krstné meno v givenName, priezvisko v surname alebo pseudonym v pseudonym,
- b) doplnujúci identifikátor zabezpečujúci jednoznačnosť identifikačných údajov držiteľa kvalifikovaného certifikátu v serialNumber vo forme „PNO“ (SK legislatíva) a môže obsahovať aj (legislatíva EÚ – eIDAS) „IDC“ a „PAS“.

#### 3.1.3.2 Kvalifikované systémové certifikáty

Pravidlá menšej konvencie kvalifikovaných systémových certifikátov sú uvedené v štandarde NBÚ „Formáty certifikátov a kvalifikovaných certifikátov“, ktorý je zverejnený na nasledujúcej internetovej stránke:

<http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/schvalene-formaty/formatycertqc4ts.pdf>

Na základe § 3 ods. 8 vyhlášky NBÚ č. 131/2009 Z. z. musí byť v kvalifikovaných systémových certifikátoch uvedený identifikátor certifikačného poriadku akreditovaných certifikačných služieb OID s hodnotou QCP SK '1 3 158 36061701 0 0 0 1 2 2'. Tento identifikátor musí byť uvedený v rozšírení certifikačnej politiky certifikátu a je aj identifikátorom certifikačnej politiky, ktorá sa smie uviesť len v kvalifikovaných certifikátoch a certifikátoch na správu vydanými certifikačnými autoritami akreditovanými NBÚ. V certifikátoch koncového používateľa v rozšírení certifikačného poriadku, ktorého OID je '1 3 158 36061701 0 0 0 1 2 2', by mal byť uvedený v položke userNotice-explicitText (formát utf8String) text s informáciou o type certifikátu podľa slovenskej legislatívy uvádzaný v anglickom ako aj v slovenskom jazyku s úvodným textom „EN: “ a „SK: “, ktorý obsahuje najmä: „Certifikát je vydaný ako kvalifikovaný systémový certifikát podľa zákona č. 215/2002 Z. z. a vyhlášky NBÚ č. 131/2009 Z. z.“.

Kvalifikovaný systémový certifikát spája identitu vlastníka súkromného kľúča s verejným kľúčom slúžiacim na overenie jeho pečatí, pričom všetky údaje obsiahnuté v kvalifikovanom systémovom certifikáte boli v čase jeho vydania poskytovateľom certifikačných služieb overené ako platné. Tieto údaje sú uložené najmä v položkách mena subjektu Certificate-tbsCertificate-subject-RelativeDistinguishedName.

Kvalifikovaný systémový certifikát podľa § 3 ods. 6 vyhlášky NBÚ č. 131/2009 Z. z. musí obsahovať minimálne meno v položke organizationName a minimálne v jednej položke serialNumber jeden identifikačný údaj typu „VAT“, „NTR“ alebo „SZ:“. Kvalifikovaný systémový certifikát nesmie obsahovať givenName, surname alebo pseudonym (čím sa jednoznačne odlišuje od kvalifikovaných certifikátov vydaných fyzickej osobe).

Obsah položky commonName je informatívny a pre overovateľa a podpisovateľa poskytuje stručnú informáciu o mene a prípadne type certifikátu. Položka commonName musí byť uvedená a musí sa nachádzať iba raz.

---

## 3.2 Iniciálna registrácia

### 3.2.1 Koreňová certifikačná autorita KCA

Iniciálna registrácia KCA sa vykonáva v procese formálneho založenia KCA v procedúre jej vytvárania. Na autentifikáciu KCA v procese iniciálnej registrácie slúži zákon č. 215/2002 Z. z. o elektronickom podpise a rozhodnutie riaditeľa príslušného útvaru NBÚ o zriadení KCA.

### 3.2.2 Následník KCA

Iniciálna registrácia následníka KCA sa vykonáva v procese formálneho zriadenia následníka KCA v procedúre jeho vytvárania. Na autentifikáciu následníka KCA v procese iniciálnej registrácie slúži zákon č. 215/2002 Z. z. o elektronickom podpise a rozhodnutie riaditeľa príslušného útvaru NBÚ o zriadení následníka KCA.

---

## 3.3 Spôsob preukázania vlastníctva súkromného kľúča KCA

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

---

## 3.4 Vydanie následného certifikátu KCA

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

---

## 3.5 Vydanie následného certifikátu po zrušení certifikátu KCA

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

---

## 3.6 Žiadosť o zrušenie certifikátu KCA

Žiadosť o zrušenie certifikátu vlastného verejného kľúča KCA môže podať KCA alebo oprávnená tretia strana. Formálna žiadosť musí byť podaná písomnou formou a musí byť podpísaná osobami

oprávnenými na podanie žiadosti o zrušenie, aby sa predišlo neautorizovanému zrušeniu certifikátu, a aby boli naplnené ustanovenia § 15 zákona č. 215/2002 Z. z. o elektronickom podpise.

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

## 4. Prevádzkové postupy

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 životného cyklu správy certifikátu je zrušenie certifikátu.

### 4.1 Generovanie kľúčov

#### 4.1.1 Generovanie kľúčov KCA

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

#### 4.1.2 Generovanie podpisových kľúčov pre kvalifikované certifikáty

Kľúčový pár prislúchajúci ku kvalifikovanému certifikátu musí byť generovaný výhradne na technickom zariadení označovanom ako bezpečné zariadenie na vyhotovovanie elektronického podpisu, resp. bezpečné zariadenie na vyhotovovanie elektronickej pečate, ktoré musí byť certifikované NBÚ v zmysle zákona č. 215/2002 Z. z. o elektronickom podpise. Bezpečný produkt nesmie umožňovať export súkromného kľúča alebo nekontrolované použitie súkromného kľúča. Operácie so súkromným kľúčom musia byť výhradne pod kontrolou vlastníka bezpečného produktu.

---

## 4.2 Žiadosť o vydanie certifikátu KCA

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

---

## 4.3 Vydanie certifikátu KCA

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

- a) bezpečnostný správca KCA,
- b) interný audítor KCA,
- c) jeden príslušník alebo zamestnanec NBÚ.

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

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

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

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

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

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

---

## 4.4 Prevzatie certifikátu KCA

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

---

## 4.5 Zrušenie certifikátu KCA

### 4.5.1 Okolnosti na zrušenie

KCA zruší certifikát vlastného verejného kľúča v prípade:

- a) ak súkromný kľúč patriaci k verejnému kľúču uvedenému v certifikáte bol ukradnutý, stratený, pozmenený alebo ináč kompromitovaný,
- b) úmyselného zneužitia kľúčov a certifikátov autorizovanou osobou,
- c) podstatného závažného porušenia prevádzkových požiadaviek identifikovaných v tomto CP a príslušnom CPS,
- d) ak zrušenie certifikátu nariadila oprávnená tretia strana (súd),
- e) ak KCA ukončila svoju činnosť.



### **4.5.2 Oprávnení žiadateľa o zrušenie certifikátu**

O zrušenie certifikátu KCA môže požiadať:

- a) KCA,
- b) oprávnená tretia strana (súd).

### **4.5.3 Postup pri zrušení certifikátu**

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

### **4.5.4 Interval na zrušenie certifikátu**

Interval na zrušenie certifikátu je maximálne 24 hodín.

### **4.5.5 Periodicita publikovania zoznamu CRL**

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

Zároveň musí byť zabezpečené, aby od prijatia žiadosti o zrušenie certifikátu do zverejnenia prvého zoznamu zrušených certifikátov, ktorý obsahuje jeho číslo neuplynulo viac ako 24 hodín – § 6 vyhlášky NBÚ č. 131/2009 Z. z.

### **4.5.6 Zisťovanie stavu certifikátov**

Stav certifikátov vydaných KCA je možné zisťovať:

- a) na základe zoznamov CRL (bod 2.5.3 tohto CP),
- b) z informácií uverejnených na internetovej stránke (bod 2.5.3 tohto CP).

### **4.5.7 Iné možnosti informovania o zrušení certifikátov**

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

---

## **4.6 Audit bezpečnosti poskytovania certifikačných činností KCA**

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

---

## **4.7 Archivácia záznamov KCA**

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

---

## 4.8 Výmena kľúčov KCA

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

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

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

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

---

## 4.9 Havarijný plán KCA

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

---

## 4.10 Ukončenie činnosti KCA

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

---

## 5. Fyzické procedurálne a personálne bezpečnostné opatrenia KCA

---

### 5.1 Opatrenia na zaistenie fyzickej bezpečnosti

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

---

### 5.2 Opatrenia na zaistenie procedurálnej bezpečnosti

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

---

### 5.3 Opatrenia na zaistenie personálnej bezpečnosti

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

Personál KCA má kvalifikáciu potrebnú na zabezpečovanie certifikačných činností KCA.

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

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

## 6. Technické bezpečnostné opatrenia

### 6.1 Opatrenia na zaistenie bezpečnej prevádzky KCA

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

Prvky oddelenia sieťovej komunikácie vymedzujú spôsob vzájomnej komunikácie komponentov systému.

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

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

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

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

### 6.2 Kryptografické prostriedky ochrany kľúčov KCA

Kľúče KCA sú generované a uchovávané v kryptografickom module hardvérovej ochrany kľúča (ďalej len „HSM“) certifikovanom NBÚ podľa zákona č. 215/2002 Z. z. o elektronickom podpise.

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

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

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

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

## 7. Profily certifikátov a zoznamov zrušených certifikátov

### 7.1 Profil certifikátu KCA (KCA1)

Haš certifikátu KCA (KCA1) je nasledovný:

**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)		<b>30 f4 a8 71 ce 72 9f 99 b4 29 ba f9 03 b1 41 10 5f 24 dc 99</b>
basicConstraints	<b>Critical</b>	Subject Type=CA  Path Length Constraint=3

certificatePolicies	<b>Critical</b>	<p>[1]Certificate Policy:</p> <p>Policy Identifier=1.3.158.36061701.0.0.0.1.2.1</p> <p>[1,1]Policy Qualifier Info:</p> <p>Policy Qualifier Id=User Notice</p> <p>Qualifier:</p> <p>Notice Text=Tento certifikat je vydany ako kvalifikovany certifikat "Korenovej CA pre kvalifikovane certifikaty 1" v sulade so zakonom c. 215/2002 Z. z..</p> <p>[1,2]Policy Qualifier Info:</p> <p>Policy Qualifier Id=CPS</p> <p>Qualifier:</p> <p><a href="http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_1.pdf">http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_1.pdf</a></p>
keyUsage	<b>Critical</b>	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: <a href="http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf">http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf</a> [2]Certificate Policy: Policy Identifier=0.4.0.1862.1.1
cRLDistributionPoints		[1]CRL Distribution Point Distribution Point Name: Full Name: URL= <a href="http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl">http://ep.nbusr.sk/kca/crls2/kcanbusr2.crl</a>
subjectKeyIdentifier (SHA1)		<b>06 da 89 e7 d3 8e 53 3a 79 77 e9 eb f9 a6 b6 32 65 3f 46 24</b>
basicConstraints	<b>Critical</b>	Subject Type=CA Path Length Constraint=None
keyUsage	<b>Critical</b>	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 NBÚ 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 NBÚ 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		<p>[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2</p> <p>[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://ep.nbusr.sk/kca/doc/kca_cps.pdf">http://ep.nbusr.sk/kca/doc/kca_cps.pdf</a></p>
cRLDistributionPoints		<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=<a href="http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl">http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl</a></p> <p>[2]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ep.nbusr.sk/cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;</p> <p>[3]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap:///cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;</p>
subjectInfoAccess		<p>URL=<a href="http://ep.nbusr.sk/kca/certs/kca3/kcanbusr3.p7c">http://ep.nbusr.sk/kca/certs/kca3/kcanbusr3.p7c</a> URL=ldap://ep.nbusr.sk/cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary URL=ldap:///cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary</p>
subjectKeyIdentifier (SHA1)		<b>7f f1 3d 21 c2 97 5a 2e 97 07 0e b1 69 83 25 fd 21 86 3e 07</b>
basicConstraints	<b>Critical</b>	Subject Type=CA Path Length Constraint=None
keyUsage	<b>Critical</b>	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.

		<p>[1,2]Policy Qualifier Info:  Policy Qualifier Id=CPS  Qualifier:  <a href="http://www.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf">http://www.nbusr.sk/kca/doc/kcaq_cp1_2_2.pdf</a>  [2]Certificate Policy:  Policy Identifier=0.4.0.1862.1.1</p>
authorityInfoAccess		<p>[1]Authority Info Access  Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)  Alternative Name:  URL=<a href="http://ep.nbusr.sk/kca/certs/kca/certifikat_der.cer">http://ep.nbusr.sk/kca/certs/kca/certifikat_der.cer</a></p>
authorityKeyIdentifier (SHA1)		KeyID=30 f4 a8 71 ce 72 9f 99 b4 29 ba f9 03 b1 41 10 5f 24 dc 99
cRLDistributionPoints		<p>[1]CRL Distribution Point  Distribution Point Name:  Full Name:  URL=<a href="http://ep.nbusr.sk/kca/crls/current_a.crl">http://ep.nbusr.sk/kca/crls/current_a.crl</a></p>
subjectKeyIdentifier (SHA1)		06 da 89 e7 d3 8e 53 3a 79 77 e9 eb f9 a6 b6 32 65 3f 46 24
basicConstraints	<b>Critical</b>	<p>Subject Type=CA  Path Length Constraint=None</p>
keyUsage	<b>Critical</b>	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:** FC06AEDA98C9A625720B3C1E7BF9491466A01345D7267817CC28BF138FDDB87

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 NBÚ SR v sulade s platnymi pravnymi predpismi SR.

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

Tab. 7.5a Profil krížového certifikátu vydaného KCA2 pre KCA1

## 7.6 Profil certifikátu akreditovanej CA / uznanej zahraničnej CA

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 NBÚ SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK  Atribút Country (C) je kódovaný v PrintableString, ostatné atribúty v UTF8String.
validity		začiatok platnosti certifikátu - (X)  koniec platnosti certifikátu (X) + (N) rokov – koniec platnosti certifikátu akreditovanej CA / uznanej zahraničnej CA nesmie presiahnuť koniec platnosti certifikátu KCA
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 NBÚ 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 NBÚ 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:

		<p>URL=<a href="http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl">http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl</a></p> <p>[2]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=ldap://ep.nbusr.sk/cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;</p> <p>[3]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=ldap:///cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;</p>
subjectKeyIdentifier (SHA1)		haš verejného kľúča akreditovanej CA / uznanej zahraničnej CA
basicConstraints	<b>Critical</b>	<p>Subject Type=CA</p> <p>Path Length Constraint=1</p>
certificatePolicies	<b>Critical</b>	<p>[1]Certificate Policy:</p> <p>Policy Identifier=1.3.158.36061701.0.0.0.1.2.2</p> <p>[1,1]Policy Qualifier Info:</p> <p>Policy Qualifier Id=CPS</p> <p>Qualifier:</p> <p><a href="http://ep.nbusr.sk/kca/doc/kca_cps.pdf">http://ep.nbusr.sk/kca/doc/kca_cps.pdf</a></p>
policyConstraints	<b>Critical</b>	Required Explicit Policy Skip Certs=0
keyUsage	<b>Critical</b>	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 NBÚ 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 Length Constraint=None
certificatePolicies		[1]Certificate Policy: Policy Identifier=1.3.158.36061701.0.0.0.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://ep.nbusr.sk/kca/doc/kca_cps.pdf">http://ep.nbusr.sk/kca/doc/kca_cps.pdf</a> [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= <a href="http://ep.nbusr.sk/kca/certs/kca3/kcanbusr3_p7c.p7c">http://ep.nbusr.sk/kca/certs/kca3/kcanbusr3_p7c.p7c</a> [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)

		<p>Alternative Name:</p> <p>URL=ldap://ep.nbusr.sk/cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary</p> <p>[3]Authority Info Access</p> <p>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)</p> <p>Alternative Name:</p> <p>URL=ldap:///cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=SK?caCertificate;binary</p>
subjectAltName		<p>RFC822 Name=<a href="mailto:podatelna@nbusr.sk">podatelna@nbusr.sk</a></p> <p>URL=<a href="http://www.nbusr.sk/en/electronic-signature/index.html">http://www.nbusr.sk/en/electronic-signature/index.html</a></p>
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		<p>[1]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=<a href="http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl">http://ep.nbusr.sk/kca/crls3/kcanbusr3.crl</a></p> <p>[2]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=ldap://ep.nbusr.sk/cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;</p> <p>[3]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=ldap:///cn=KCA NBÚ SR 3,ou=SIBEP,o=Narodny bezpecnostny urad,l=Bratislava,c=sk?certificateRevocationList;</p>
subjectKeyIdentifier (SHA1)		naš verejného kľúča podpisovateľa slovenského TSL a schválených podpisových politík
keyUsage	<b>Critical</b>	nonRepudiation

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

---

## 7.8 Profil kvalifikovaného certifikátu fyzickej osoby

Profil kvalifikovaného certifikátu fyzickej osoby je uvedený v dokumente NBÚ „Formáty certifikátov a kvalifikovaných certifikátov“, ktorý sa nachádza na nasledujúcej internetovej stránke:

<http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/schvalene-formaty/formatcertqc4ts.pdf>

Na základe § 3 ods. 8 vyhlášky NBÚ č. 131/2009 Z. z. musí byť v kvalifikovaných certifikátoch fyzických osôb uvedený identifikátor certifikačného poriadku akreditovaných certifikačných služieb OID s hodnotou QCP SK '1 3 158 36061701 0 0 0 1 2 2'. Tento identifikátor musí byť uvedený v rozšírení certifikačnej politiky certifikátu a je aj identifikátorom certifikačnej politiky, ktorá sa smie uviesť len v kvalifikovaných certifikátoch a certifikátoch na správu vydanými certifikačnými autoritami akreditovanými NBÚ. V certifikátoch koncového používateľa v rozšírení certifikačného poriadku, ktorého OID je '1 3 158 36061701 0 0 0 1 2 2', by mal byť uvedený v položke userNotice-explicitText (formát utf8String) text s informáciou o type certifikátu podľa slovenskej legislatívy uvádzaný v anglickom ako aj v slovenskom jazyku s úvodným textom „EN: “ a „SK: “, ktorý obsahuje najmä: „Certifikát je vydaný ako kvalifikovaný certifikát podľa zákona č. 215/2002 Z. z. a vyhlášky NBÚ č. 131/2009 Z. z.“.

Kvalifikovaný certifikát fyzickej osoby spája identitu vlastníka súkromného kľúča s verejným kľúčom slúžiacim na overenie jeho podpisov, pričom všetky údaje obsiahnuté v kvalifikovanom certifikáte fyzickej osoby boli v čase jeho vydania poskytovateľom certifikačných služieb overené ako platné. Tieto údaje sú uložené najmä v položkách mena subjektu Certificate-tbsCertificate-subject-RelativeDistinguishedName.

Obsah položky commonName je informatívny a pre overovateľa a podpisovateľa poskytuje stručnú informáciu o mene a prípadne type certifikátu. Položka commonName musí byť uvedená a musí sa nachádzať iba raz.

Kvalifikovaný certifikát fyzickej osoby podľa § 3 ods. 4 vyhlášky NBÚ č. 131/2009 Z. z. musí obsahovať minimálne:

- a) krstné meno v givenName, priezvisko v surname alebo pseudonym v pseudonym,
- b) doplňujúci identifikátor zabezpečujúci jednoznačnosť identifikačných údajov držiteľa kvalifikovaného certifikátu v serialNumber vo forme „PNO“ (SK legislatíva) a môže obsahovať aj (legislatíva EÚ – eIDAS) „IDC“ a „PAS“.

---

## 7.9 Profil kvalifikovaného systémového certifikátu

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

<http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/schvalene-formaty/formatcertqc4ts.pdf>

Na základe § 3 ods. 8 vyhlášky NBÚ č. 131/2009 Z. z. musí byť v kvalifikovaných systémových certifikátoch uvedený identifikátor certifikačného poriadku akreditovaných certifikačných služieb OID s hodnotou QCP SK '1 3 158 36061701 0 0 0 1 2 2'. Tento identifikátor musí byť uvedený v rozšírení certifikačnej politiky certifikátu a je aj identifikátorom certifikačnej politiky, ktorá sa smie uviesť len v kvalifikovaných certifikátoch a certifikátoch na správu vydanými certifikačnými autoritami akreditovanými NBÚ. V certifikátoch koncového používateľa v rozšírení certifikačného poriadku, ktorého OID je '1 3 158 36061701 0 0 0 1 2 2', by mal byť uvedený v položke userNotice-explicitText (formát utf8String) text s informáciou o type certifikátu podľa slovenskej legislatívy uvádzaný v anglickom ako aj v slovenskom jazyku s úvodným textom „EN: “ a „SK: “, ktorý obsahuje najmä: „Certifikát je vydaný ako kvalifikovaný systémový certifikát podľa zákona č. 215/2002 Z. z. a vyhlášky NBÚ č. 131/2009 Z. z.“.

Kvalifikovaný systémový certifikát spája identitu vlastníka súkromného kľúča s verejným kľúčom slúžiacim na overenie jeho pečatí, pričom všetky údaje obsiahnuté v kvalifikovanom systémovom certifikáte boli

v čase jeho vydania poskytovateľom certifikačných služieb overené ako platné. Tieto údaje sú uložené najmä v položkách mena subjektu Certificate-tbsCertificate-subject-RelativeDistinguishedName.

Kvalifikovaný systémový certifikát podľa § 3 ods. 6 vyhlášky NBÚ č. 131/2009 Z. z. musí obsahovať minimálne meno v položke organizationName a minimálne v jednej položke serialNumber jeden identifikačný údaj typu „VAT“, „NTR“ alebo „SZ:“. Kvalifikovaný systémový certifikát nesmie obsahovať givenName, surname alebo pseudonym (čím sa jednoznačne odlišuje od kvalifikovaných certifikátov vydaných fyzickej osobe).

Obsah položky commonName je informatívny a pre overovateľa a podpisovateľa poskytuje stručnú informáciu o mene a prípadne type certifikátu. Položka commonName musí byť uvedená a musí sa nachádzať iba raz.

## 7.10 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 NBÚ SR 3 OU=SIBEP O=Narodny bezpecnostny urad L=Bratislava C=SK
thisUpdate		(X)
nextUpdate		max. (X) + 4 hodiny + 72000 sekúnd
cRLNumber		jednoznačné číslo CRL pridelené KCA
authorityKeyIdentifier		KeyID=7f f1 3d 21 c2 97 5a 2e 97 07 0e b1 69 83 25 fd 21 86 3e 07

### 7.10a Profil zoznamu CRL vydávaného KCA

## 8. Administrácia špecifikácií

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

Pred schválením zmien v nasledujúcej verzii CP upozorní NBÚ všetky akreditované CA a uznané zahraničné CA, ktorým vydal certifikát.

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

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

---

### 8.1 Identifikácia verzií

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

Verzia A.B

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

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

---

### 8.2 Schvaľovanie verzií

Tento CP schvaľuje riaditeľ sekcie ekonomiky a prevádzky NBÚ.

## 9. Účinnosť certifikačného poriadku

Tento CP kľúča nadobúda účinnosť dňa 19.08.2015.