

# ViaSec

## PRVÁ SLOVENSKÁ CERTIFIKAČNÁ AUTORITA (PSCA)

Certifikačný poriadok akreditovanej certifikačnej autority PSCA

Typ dokumentu:

Skratka: **07**

Verzia dokumentu: 1.2

Dátum vydania: 1.9.2011

Počet strán dokumentu: 54

Vypracoval: Peter Novota

.....

Preskúmal: **Vladimír Hašík**

.....

Schválil: Patrik Krauspe

.....

Výtlačok

Riadená dokumentácia číslo:

Označenie dôvernosti:

**RD PSCA 006**

## Obsah

Obsah.....	2
Skratky a definície.....	5
Odkazy.....	7
Úvod.....	8
Prehľad.....	8
Identifikácia.....	8
Komunita a použiteľnosť.....	9
Autority.....	9
Autorita pre správu poriadkov (Policy Management Authority) (ďalej len PMA) je zložka ACA PSCA ustanovená za účelom:.....	9
Vlastná certifikačná autorita .....	9
Registračná autorita (RA) .....	9
Koncové entity.....	10
Subjekty, žiadatelia a majitelia KC PSCA.....	10
Strany spoliehajúce sa na KC.....	10
Typy KC .....	10
Použiteľnosť KC .....	11
Kontaktné detaily.....	12
Všeobecne.....	13
Povinnosti.....	13
Povinnosti ACA PSCA.....	13
Povinnosti RA.....	13
Povinnosti žiadateľa o KC.....	14
Povinnosti majiteľa KC.....	14
Povinnosti strán spoliehajúcich sa na KC.....	15
Povinnosti správy repozitára.....	15
Právne záruky.....	16
Finančná zodpovednosť .....	17
Rozhodcovské konanie a riešenie sporov.....	17
Poplatky .....	18
Zverejňovanie informácií a repozitár.....	18
Zverejňovanie informácií o ACA PSCA.....	18
Frekvencia zverejňovania informácií.....	18
Kontroly prístupu.....	19
Repozitáre.....	19
Audit zhody.....	19
Frekvencia auditu zhody pre danú entitu.....	19
Identita audítora a kvalifikačné požiadavky na neho.....	19
Témy pokrývané auditom zhody.....	19
Akcie vykonané na odstránenie nedostatkov.....	20
Zaobchádzanie s výsledkami auditu.....	20

Dôvernosť.....	20
Typy informácií, ktoré sa majú chrániť.....	20
Okolnosti uvoľnenia dôverných informácií.....	21
Práva vyplývajúce z intelektuálneho vlastníctva.....	21
Identifikácia a autentizácia.....	22
Prvotná registrácia.....	22
Typy mien.....	22
Potreba zmysluplnosti mien.....	22
Jednoznačnosť mien .....	24
Procedúra riešenia sporov pri kolízii mien .....	24
Rozpoznanie, autentizácia a rola obchodných značiek .....	25
Preukazovanie vlastníctva privátneho kľúča .....	25
Autentizácia identity organizácie.....	26
Autentizácia identity fyzickej osoby .....	27
Predkladané doklady.....	28
Kontrola údajov na predložených dokladoch .....	28
Osobné doklady fyzickej osoby.....	28
Výpisy z obchodného registra.....	29
Plné moci.....	29
Prvotná registrácia pracovníka ACA PSCA .....	29
Vydanie následného KC .....	29
Vydanie následného KC po zrušení starého .....	30
Žiadosť o zrušenie KC .....	30
Prevádzkové požiadavky.....	31
Žiadanie o KC .....	31
Detailný postup na získanie KC .....	31
Zákazník v dohodnutom termíne príde na RA, pričom vezme so sebou a predloží: .....	32
Postup pri registrácii zákazníka na RA.....	32
Doručenie verejného kľúča žiadateľa o KC vydavateľovi KC .....	34
Vydanie KC .....	35
Doručenie privátneho kľúča majiteľovi KC .....	35
Doručenie verejného kľúča ACA PSCA používateľom .....	35
Prevzatie KC .....	36
Zrušenie a suspendovanie KC.....	36
Zrušenie KC .....	36
Okolnosti zrušenia KC.....	36
Kto môže žiadať o zrušenie KC.....	37
Procedúra žiadosti o zrušenie KC.....	38
Suspendovanie KC.....	39
Zoznamy zrušených KC.....	40
Frekvencia vydávania CRL .....	40
Požiadavky na overovanie CRL .....	40
Overenie aktuálneho stavu KC.....	40

Iné použiteľné spôsoby oznamovania o zrušení KC.....	41
Audit bezpečnosti.....	41
Archívne záznamy .....	42
Zmena kľúča ACA PSCA .....	42
Havarijný plán pre mimoriadne udalosti .....	43
Ukončenie činnosti ACA PSCA .....	43
Fyzické, procedurálne a personálne bezpečnostné opatrenia.....	44
Fyzické bezpečnostné opatrenia.....	44
Procedurálne bezpečnostné opatrenia .....	44
Personálne bezpečnostné opatrenia .....	45
Technické bezpečnostné opatrenia .....	47
Profily KC a zoznamov zrušených KC.....	48
Profily KC .....	48
Vlastný certifikát ACA PSCA.....	48
KC .....	48
Profily zoznamov zrušených KC.....	52
Administrácia špecifikácií .....	53
Procedúry na zmenu špecifikácie .....	53
Publikačná a oznamovacia politika .....	53
Procedúry schvaľovania CPS a externej politiky .....	53
Úľavy .....	54

## Skratky a definície

<b>ACA</b>	– Akreditovaná certifikačná autorita (Accredited Certification Authority)
<b>CA</b>	– Certifikačná autorita (Certification Authority)
<b>CP</b>	– Certifikačný poriadok (Certificate Policy)
<b>CPS</b>	– Pravidlá na výkon certifikačných činností (Certificate Practice Statement)
<b>CRL</b>	– Zoznam zrušených certifikátov (Certification Revocation List)
<b>HSM</b>	– Hardware Security Modul
<b>PMA</b>	– Autorita pre správu poriadkov (Policy Management Authority)
<b>NBÚ</b>	– Národný bezpečnostný úrad
<b>KC</b>	– Kvalifikovaný certifikát
<b>RA</b>	– Registračná autorita (Registration Authority)
<b>PKI</b>	– Infraštruktúra verejných kľúčov (Public Key Infrastructure)
<b>PSCA</b>	– Prvá Slovenská Certifikačná Autorita

Pre účely tohto dokumentu sú použité nasledovné definície a pojmy:

**Akreditovaná certifikačná autorita** - certifikačná autorita, ktorá poskytuje akreditované certifikačné služby podľa Zákona č. 215/2002 Z. z. o elektronickom podpise, a ktorá má na poskytovanie týchto služieb akreditáciu Národného bezpečnostného úradu

**Certifikát** – elektronický dokument, ktorým vydavateľ certifikátu (certifikačná autorita) potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný.

**Certifikačná autorita** – autorita s dôverou jedného alebo viacerých používateľov (t.j. žiadateľov ako aj používateľov certifikátu) vytvárať certifikáty na základe overenia identity osoby, ktorej bol vydaný certifikát .

**Elektronický podpis** – informácia v elektronickej forme, ktorá je pripojená alebo logicky inak spojená s elektronickým dokumentom, ktorá slúži ako metóda autentizácie tohto dokumentu.

**Kvalifikovaný certifikát** – je certifikát fyzickej osoby, certifikát akreditovanej certifikačnej autority, krížový certifikát akreditovanej certifikačnej autority a certifikát

úradu, ktorý spĺňa podmienky podľa odsekov 2 až 5 a § 6 Zákona č. 215/2002 Z. z. o elektronickom podpise

**Podpisová politika** – súbor pravidiel, ktoré vyjadrujú použiteľnosť certifikátu v rámci určitej komunity a/alebo triedy aplikácií so spoločnými bezpečnostnými požiadavkami.

**Používateľ certifikátu** – entita, ktorá koná na báze dôvery v daný certifikát a/alebo na základe elektronického podpisu overeného daným certifikátom. Synonymom pojmu používateľ certifikátu je pojem strana spoliehajúca sa na certifikát.

**Pravidlá na výkon certifikačných činností** – postupy, ktoré certifikačná autorita používa pri vydávaní certifikátov.

**Subjekt** – entita identifikovaná v certifikáte ako majiteľ súkromného kľúča prislúchajúceho k verejnému kľúču obsiahnutému v certifikáte.

**Vlastná CA** – časť infraštruktúry certifikačnej autority (obsahujúca napr. HSM modul), ktorá spolu s registračnou autoritou vydáva certifikáty

**Zaručený elektronický podpis** – je elektronický podpis, ktorý musí spĺňať podmienky podľa § 3 a § 4 Zákona č. 215/2002 Z. z. o elektronickom podpise

**Žiadateľ** – entita, ktorá certifikačnej autorite predkladá žiadosť v mene jedného alebo viacerých subjektov.

**Token** – zariadenie určené na bezpečné generovanie, uloženie a použitie páru kľúčov tvoreného privátnym a verejným kľúčom, ktoré NBÚ certifikovalo ako produkt pre zaručený elektronický podpis, token môže byť napr. vo forme čipovej karty, USB kľúča, HSM modulu.

## Odkazy

Zákon č. 215/2002 Z. z. o elektronickom podpise a súvisiace vyhlášky v aktuálnom znení

Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (RFC3647)

Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC3280)

ETSI TS 101 456 V1.2.1 – Policy requirements for certification authorities issuing qualified certificates.

Zákon č. 428/2002 Z. z. o ochrane osobných údajov

## Úvod

Tento dokument definuje certifikačný poriadok (ďalej len CP), ktorú uplatňuje akreditovaná certifikačná autorita Prvá Slovenská Certifikačná Autorita (ďalej len ACA PSCA) pri implementovaní infraštruktúry verejných kľúčov (ďalej len PKI) pozostávajúcej z produktov a služieb, ktoré poskytujú a spravujú kvalifikované certifikáty (ďalej len KC) podľa štandardu X.509 pre kryptografiu verejných kľúčov v súlade so zákonom č. 215/2002 Z.z. o elektronickom podpise. KC identifikujú subjekt nachádzajúci sa v KC a zväzujú tento subjekt s príslušným párom kľúčov.

## Prehľad

Tento poriadok je politikou, na základe ktorej je zriadená a prevádzkovaná akreditovaná certifikačná autorita s názvom Prvá Slovenská Certifikačná Autorita, ktorú prevádzkuje spoločnosť Viasec, s.r.o.

CP bol vytvorený v súlade s vyhláškou NBÚ č. 541/2002 Z.z. a na základe materiálov Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (RFC3647), Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC3280) a ETSI TS 101 456 V1.2.1 – Policy requirements for certification authorities issuing qualified certificates.

Tento dokument definuje vytváranie a správu KC s verejnými kľúčmi podľa štandardu X.509 verzie 3 pre ich použitie v aplikáciách vyžadujúcich si KC.

## Identifikácia

Názov:	Certifikačný poriadok akreditovanej certifikačnej autority PSCA
Skratka názvu:	<b>CP ACA PSCA</b>
Verzia:	<b>September 2011</b>
Tomuto dokumentu je priradený identifikátor objektu (OID):	1.3.6.1.4.1.27626.3.1.1

Tento poriadok sa týka všetkých KC vydávaných ACA PSCA.

Pojmom KC resp. KC ACA PSCA sa v tomto dokumente označuje kvalifikovaný certifikát vydaný akreditovanou certifikačnou autoritou PSCA.

## Komunita a použiteľnosť

### Autority

Autorita pre správu poriadkov (Policy Management Authority) (ďalej len PMA) je zložka ACA PSCA ustanovená za účelom:

dohľadu na vytváranie a aktualizáciu certifikačných poriadkov, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien, revízie CP ACA PSCA, aby sa zaručilo, že prax ACA PSCA vyhovuje príslušnému certifikačnému poriadku,

revízie výsledkov auditov, aby sa určilo, či ACA PSCA adekvátne dodržiava ustanovenia schváleného dokumentu CP, ďalej potom dávanie odporúčaní pre ACA PSCA ohľadne nápravných akcií a iných vhodných opatrení,

riadenia a usmerňovania činnosti vlastnej certifikačnej autority a registračných autorít,

vykonávania revízie CP certifikačnej autority prostredníctvom analýzy CP, aby sa zaručilo, že prax ACA PSCA vyhovuje príslušnému certifikačnému poriadku.

PMA predstavuje zastrešujúcu zložku, ktorá rozhoduje s konečnou platnosťou vo všetkých záležitostiach a aspektoch týkajúcich sa ACA PSCA a jej činnosti.

#### Vlastná certifikačná autorita

Je entita autorizovaná PMA na vytváranie, podpisovanie a vydávanie KC s verejným kľúčom.

Zodpovedá za všetky aspekty vydávania a správy KC, vrátane kontroly nad procesom registrácie, procesom identifikácie a autentizácie, procesom vytvárania KC, publikácie KC, zrušovania KC.

Zaručuje, že všetky aspekty jej služieb a operácií a infraštruktúry zviazanej s KC vydanými podľa tejto politiky sa vykonávajú v súlade s požiadavkami a ustanoveniami tohto poriadku a jeho pravidiel na výkon akreditovaných certifikačných činností.

ACA PSCA je súčasťou hierarchickej PKI, sama však nemá podriadené certifikačné autority, ale je podriadená koreňovej CA NBÚ. Charakter tejto podriadenosti a spôsob jej implementácie určuje NBÚ.

#### Registračná autorita (RA)

Je entita, ktorá na základe rozhodnutia PMA zbiera a verifikuje identity subjektov, žiadateľov o KC a iné informácie, ktoré sa dostanú do KC.

RA musí vykonávať svoje aktivity v súlade so schváleným CP.

## Koncové entity

### Subjekty, žiadatelia a majitelia KC PSCA

Subjekt je entita, ktorej meno sa objaví ako subjekt KC a ktorá sa zaviazá, že bude používať svoj kľúč a KC v súlade s týmto certifikačným poriadkom.

Subjekt sa prevzatím svojho KC stáva majiteľom daného KC.

V zmysle platnej legislatívy subjektom KC môže byť len fyzická osoba, ktorá splní podmienky pre registráciu (samozrejme daná fyzická osoba pritom môže byť súčasne napr. živnostníkom alebo štatutárom, zamestnancom, členom a pod. právnickej osoby, ktorej niektoré údaje (napr. názov) sú súčasťou subjektu daného certifikátu).

Fyzická osoba môže na základe úradne overenej plnej moci, ktorá ju splnomocňuje zastupovať daný subjekt pri konaní na registračnej autorite, konať ako žiadateľ o akreditovanú certifikačnú službu (napr. vydanie KC, zrušenie KC), t.j. zastupovať na RA jednu alebo viacero osôb – subjektov KC.

Pri žiadaní o KC táto splnomocnená osoba uzatvára zmluvu s ACA PSCA v mene subjektu, ktorému je KC priradený a ktorý sa stáva jeho vlastníkom, avšak entitou, ktorá je autentifikovaná súkromným kľúčom prislúchajúcim k danému KC, je vždy osoba – subjekt KC.

Podmienky, ktoré musia subjekt a žiadateľ o KC splniť, aby subjektu bol vydaný KC, definuje tento dokument.

### Strany spoliehajúce sa na KC

Stranou spoliehajúcou sa na KC je entita, ktorá tým, že používa cudzí KC na overenie zaručeného elektronického podpisu, sa spolieha na platnosť väzby subjektu (t.j. majiteľa) KC s verejným kľúčom nachádzajúcim sa v danom KC. Strana spoliehajúca sa na KC môže použiť informáciu z KC na určenie vhodnosti KC na dané použitie.

Synonymom pojmu strana spoliehajúca sa na KC je pojem používateľ KC. Tento koná na báze dôvery v daný KC a/alebo na základe zaručeného elektronického podpisu overeného daným KC.

### Typy KC

ACA PSCA vydáva KC v súlade so zákonom č. 215/2002 Z.z. o elektronickom podpise a súvisiacimi vyhláškami NBÚ podľa štandardu X.509 verzia 3. Platnosť KC je jeden rok, ak sa zmluvne nedohodne kratšia doba.

V zmysle platnej legislatívy subjektom KC môže byť len fyzická osoba.

Podmienkou na vydanie KC je, aby pár kľúčov tvorený privátnym kľúčom a k nemu prislúchajúcim a vo vydávanom KC nachádzajúcim sa verejným kľúčom bol

bezpečným spôsobom vygenerovaný a uschovaný na bezpečnom zariadení (tokene), ktoré NBU certifikoval ako bezpečný produkt na vyhotovovanie zaručeného elektronického podpisu.

ACA PSCA uplatňujúca tento poriadok nevydáva žiadne certifikáty certifikačných autorít, t.j. nemá podriadené CA.

ACA PSCA uplatňujúca tento poriadok tiež nevydáva žiadne krížové certifikáty.

### **Použiteľnosť KC**

KC sú určené výlučne na vytváranie a overovanie zaručeného elektronického podpisu použitím bezpečného zariadenia na vyhotovovanie zaručeného elektronického podpisu a programovej aplikácie pre vyhotovovanie a overovanie zaručeného elektronického podpisu, ktoré boli certifikované Národným bezpečnostným úradom v zmysle ustanovení č. 215/2002 Z.z. o elektronickom podpise.

KC sú určené výlučne na účel, na ktorý tieto programové aplikácie KC využívajú.

Použiteľnosť vydávaných KC bude regulovaná a implementovaná prostredníctvom rozšírení KC.

Dokument „Pravidlá na výkon certifikačných činností ACA PSCA“ (ďalej len CPS, CPS ACA, CPS ACA PSCA) môže presnejšie vymedziť:

zoznam aplikácií, pre ktoré sú vydávané KC vhodné  
zoznam aplikácií, pre ktoré je použitie vydávaných KC obmedzené  
zoznam aplikácií, pre ktoré je použitie vydávaných KC zakázané

## Kontaktné detaily

Zriaďovateľom a majiteľom ACA PSCA je spoločnosť Viasec, s.r.o.

Adresa: **Viasec, s.r.o.**  
**Prvá Slovenská Certifikačná Autorita (PSCA)**  
**Borská 6**  
**841 04 Bratislava 4**

e-mail: [oper@psca.sk](mailto:oper@psca.sk)  
www: <http://www.pzca.sk>  
telefón **+421 2 35035030**  
fax: **+421 2 35035039**

## Všeobecne

### Povinnosti

Do procesov súvisiacich s poskytovaním a využívaním akreditovaných certifikačných služieb vstupujú nasledovné entity:

vlastná certifikačná autorita – je tvorená viacerými rolami, ktoré sa spoločne označujú ako služobné alebo dôveryhodné role ACA PSCA. Tieto role definuje dokument CPS. Ich kompetenciu, povinnosti a zodpovednosť vymedzí dokument CPS,  
registračná autorita (RA),  
subjekt (majiteľ KC),  
strana spoliehajúca sa na KC (používateľ KC).

### Povinnosti ACA PSCA

ACA PSCA, ktorá vydáva KC založené na tomto poriadku, musí vyhovovať ustanoveniam tohto dokumentu vrátane nasledujúcich ustanovení:

konať v súlade s ustanoveniami schváleného dokumentu CPS a tohto poriadku,  
zaručiť, že sa akceptujú registračné informácie jedine od RA, ktoré rozumejú tomuto poriadku a sú zviazané konať v súlade s ním,  
dávať do KC len správne a náležité informácie a archivovať doklady dokazujúce správnosť údajov dávaných do KC,  
garantovať, že majiteľ KC je viazaný povinnosťami v súlade s časťou tohto poriadku a informovaný o následkoch neplnenia týchto povinností,  
zrušiť KC majiteľov, ak sa zistí, že títo konali v rozpore so svojimi povinnosťami,  
prevádzkovať v režime on-line repozitár, ktorý vyhovuje ustanoveniam uvedeným v časti ,  
zachovávať mlčanlivosť o všetkých informáciách, najmä osobných údajoch, ktoré získa v rámci výkonu svojich povinností.

Ak sa zistí, že ACA PSCA nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu príslušné opatrenia.

### Povinnosti RA

RA, ktorá vykonáva registračné funkcie popísané v tomto poriadku, musí vyhovovať ustanoveniam tohto dokumentu a konať podľa príslušného schváleného dokumentu CPS. Ak sa zistí, že RA nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu príslušné opatrenia vrátane zastavenia jej činnosti ako RA.

Registračná autorita ACA PSCA (ďalej len RA) zabezpečuje funkciu podateľne pre ACA PSCA – konkrétne najmä zhromažďovanie a overovanie informácií od zákazníkov – žiadateľov o KC, ktoré majú byť uvedené v KC.

Na RA sa realizuje priamy kontakt medzi zákazníkmi a ACA PSCA.

RA prijíma žiadosti o KC, preveruje totožnosť žiadateľov o KC, sprostredkuje odovzdávanie KC a zoznamu zrušených KC zákazníkovi, prijíma a vybavuje ich reklamácie a sťažnosti, vyberá od zákazníkov stanovené poplatky za služby ACA PSCA.

RA zodpovedá za to, že ňou zbierané informácie RA overila a teda, že tieto informácie sú v danom čase pravdivé.

Pracovníci RA sú povinní zachovávať mlčanlivosť o všetkých informáciách, najmä osobných údajoch, ktoré získajú v rámci výkonu svojej roly pre ACA PSCA.

### **Povinnosti žiadateľa o KC**

Povinnosťou žiadateľa o KC je:

- a) predložiť RA presné, pravdivé a úplné informácie v súlade s požiadavkami tohto dokumentu,  
predložiť RA všetky požadované dokumenty,  
zabezpečiť, aby pri generovaní kľúčov boli použité vhodná dĺžka kľúča a vhodné algoritmy, ktoré sú v súlade s predpísanou podpisovou politikou,  
predložiť RA vygenerovanú žiadosť o KC, na základe ktorej sa má vydať KC, táto žiadosť o KC musí obsahovať údaje, ktoré sú v súlade s údajmi na predkladaných dokumentoch a formulároch,  
zaplatiť za KC sumu stanovenú platným cenníkom,  
prevziať KC vydaný na základe jeho žiadosti.

### **Povinnosti majiteľa KC**

Povinnosťou majiteľa KC (subjektu KC) je:

- a) zabezpečiť, aby pri generovaní kľúčov boli použité vhodná dĺžka kľúča a vhodné algoritmy, ktoré sú v súlade s predpísanou podpisovou politikou,  
generovať svoj pár kľúčov priamo v bezpečnom zariadení pre zaručený elektronický podpis,  
neustále chrániť svoje privátne kľúče a tokeny, v ktorých sú uložené, heslá na prístup k privátnym kľúčom v súlade s touto CP a tiež ako je stanovené v jeho zmluve o vydaní a používaní KC ACA PSCA,  
používať len kvalitné, silné heslá na prístup k privátnym kľúčom,  
v prípade straty tokenu, straty, zneužitia alebo kompromitácie privátneho kľúča, zabudnutia hesla na prístup k privátnemu kľúčovi, alebo, ak nastali zmeny, alebo sa

vyskytli nepresnosti v údajoch uvedených v danom KC, bezodkladne požiadať o zrušenie daného KC. Toto musí byť urobené prostredníctvom mechanizmu, ktorý je v súlade s týmto dokumentom,

po kompromitácii okamžite a natrvalo zastaviť používanie daného privátneho kľúča, dodržiavať všetky lehoty, podmienky a obmedzenia uložené na používanie svojich privátnych kľúčov, KC a tokenov,

precízne sa identifikovať a vyjadrovať pri ľubovoľnej komunikácii s RA resp. ACA PSCA,

používať poskytnuté KC len s aplikáciami, ktoré boli certifikované NBÚ ako produkty pre zaručený elektronický podpis,

používať svoj KC výlučne na vytváranie a overovanie zaručeného elektronického podpisu,

Majiteľ KC, ktorý nedodržiava resp. nedodržiaval svoje povinnosti, nemá nárok na náhradu prípadnej škody.

### **Povinnosti strán spoliehajúcich sa na KC**

Strany spoliehajúce sa na KC vydané podľa tohto poriadku sú povinné:

a) používať KC len s aplikáciami, ktoré boli certifikované NBÚ ako produkty pre zaručený elektronický podpis,

používať KC len na účel, pre ktorý bol vydaný, ako je to dané informáciami v KC, predtým, ako sa na daný zaručený elektronický podpis spoľahnú, overiť KC patriaci k danému zaručenému elektronickému podpisu na jeho platnosť (tzn. overovať, že KC bol v danom čase platný a že sa nenachádzal na aktuálnom zozname zrušených KC vydanom ACA PSCA),

uchovávať originálne podpísané dáta, aplikácie potrebné na čítanie a spracovanie týchto dát a kryptografické aplikácie potrebné na overovanie zaručených elektronických podpisov týchto dát, pokiaľ môže byť potrebné overovať zaručený elektronický podpis týchto dát.

### **Povinnosti správy repozitára**

Správa repozitára, ktorý podporuje ACA PSCA pri publikovaní informácií podľa tohoto CP, je povinná

a) udržiavať prístupnosť informácií podľa ustanovení tohto poriadku pre publikovanie informácií o KC,

poskytovať mechanizmus riadenia prístupu dostatočný na ochranu informácií uložených v repozitári podľa časti .

Prevádzkovanie a spravovanie repozitára patrí medzi povinnosti ACA PSCA.

## Právne záruky

Tento CP sa riadi platnými zákonmi Slovenskej republiky, najmä zákonom o elektronickom podpise a o zmene a doplnení niektorých zákonov (zákon č. 215/2002 Z.z.) a súvisiacimi vyhláškami Národného bezpečnostného úradu.

ACA PSCA garantuje jednoznačnosť čísla (*Serial Number*) každého ňou vydaného KC, tzn. garantuje, že neexistujú a nikdy nebudú existovať žiadne dva KC, ktoré by mali rovnaké číslo.

ACA PSCA zaručuje výkon akreditovaných certifikačných služieb v súlade so svojim certifikačným poriadkom a pravidlami na výkon akreditovaných certifikačných činností.

ACA PSCA ručí za to, že pri podpisovaní ňou vydávaných KC a CRL použije vlastný privátny kľúč uložený v HSM module patriaci k jej vlastnému certifikátu ACA PSCA.

ACA PSCA poskytuje záruku, že ňou vydaný KC bude vyhovovať štandardu X.509 verzie 3.

ACA PSCA v žiadnom prípade nezodpovedá za škody spôsobené neoprávneným alebo neopatrným použitím KC, použitím KC mimo rámec definovaný KC a certifikačným poriadkom, neoprávneným alebo neopatrným použitím CRL, použitím neplatného KC (exspirovaného alebo zrušeného), zneužitím súkromného kľúča klienta, treťou osobou, vyššou mocou (živelná pohroma, vojna prípadne iné nekontrolovateľné udalosti alebo sily).

ACA PSCA ani jej RA nie je zodpovedná za nesprávne údaje predložené žiadateľom o KC, ktoré sa pri registrácii nedajú overiť.

ACA PSCA nevykonáva funkciu prostredníka medzi majiteľmi a používateľmi KC.

ACA PSCA je zodpovedná výlučne za škody spôsobené spoliehaním sa na informácie, ktoré obsahujú KC ňou vydané. ACA PSCA si vyhradzuje právo každý takýto prípad najskôr prešetriť a posúdiť. V prípade, keď ACA PSCA nespôsobila chybu v informáciách uvedených v KC, za prípadné vzniknuté škody ACA PSCA nezodpovedá.

ACA PSCA nie je zodpovedná za nepriame, následné alebo náhodné škody, stratu zisku, stratu dát alebo iné škody vzniknuté v súvislosti s používaním alebo nefunkčnosťou KC, zaručeného elektronického podpisu alebo aplikácií, ktoré KC používajú.

ACA PSCA nie je zodpovedná za škody vzniknuté v čase od podania žiadosti o zrušenie KC do okamžiku zverejnenia daného KC v novom CRL, ak bol daný KC zverejnený v novom CRL do doby stanovenej týmto dokumentom.

Rozsah právnych záruk ACA PSCA ako poskytovateľa akreditovaných certifikačných služieb je definovaný v Zmluve o vydaní a používaní KC.

## Finančná zodpovednosť

ACA PSCA poskytuje záruku na použitie ňou vydaných KC v zmysle platnej legislatívy.

Záruku a z nej vyplývajúce plnenie je možné uznať len za predpokladov, že subjekt neporušil svoje povinnosti (hlavne ochranu svojho privátneho kľúča), a že každý kto sa v danom prípade spoliehal na KC vydaný ACA PSCA urobil všetko, aby prípadnej škode zabránil, najmä že si overil aktuálny stav predmetného KC (t.j. či daný KC nebol v rozhodujúcom čase, keď sa na neho spoliehalo, na zozname zrušených KC).

Neoverenie stavu KC pomocou zoznamu zrušených KC sa kvalifikuje ako hrubé porušenie povinností vyplývajúcich z tohto dokumentu, dôsledkom čoho zanikajú akékoľvek nároky na prípadné uplatňovanie si záruky voči ACA PSCA.

ACA PSCA a ani zriaďovateľ ACA PSCA nemajú žiadnu finančnú zodpovednosť za prípadné škody, ktoré by vznikli majiteľovi KC alebo strane spoliehajúcej sa na KC v súvislosti s používaním KC s nejakou konkrétnou aplikáciou resp. hardvérom, alebo v súvislosti s tým, že KC nie je možné používať s nejakou konkrétnou aplikáciou resp. hardvérom.

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

## Rozhodcovské konanie a riešenie sporov

Pre potreby interpretácie ustanovení tohto poriadku alebo riešenia sporov sa možno obrátiť na RA a v prípade nesúhlasu s jej rozhodnutím na najbližšiu vyššiu inštanciu. Inštancie sú usporiadané vzostupne v poradí:

RA

ACA PSCA (vybavuje len písomne podané žiadosti a podnety)

ACA PSCA si vyhradzuje právo každý sporný prípad najprv preskúmať. Prednostne bude snahou riešiť spory dohodou.

PMA rozhoduje s konečnou platnosťou v prípade akýchkoľvek sporov o interpretácii ustanovení tohto dokumentu alebo jeho použiteľnosti.

Povinnosťou každej inštancie je prípad zaprotokolovať a dať žiadateľovi resp. sťažovateľovi vysvetlenie resp. návrh na riešenie sporu a v prípade jeho nesúhlasu prípad postúpiť na vyššiu inštanciu.

Žiadnym rozhodnutím niektorej z tu definovaných inšancií nie je dotknuté právo sťažovateľa postúpiť sťažnosť nezávislému súdu.

## Poplatky

Povinnosťou ACA je vhodným spôsobom zverejniť platný cenník svojich služieb.

Poplatky za KC sa platia na RA spravidla v hotovosti, ak nie je dohodnuté so zákazníkom inak.

ACA PSCA bude vhodným spôsobom zverejňovať platný cenník svojich služieb.

Tento cenník bude v každom prípade zverejnený prostredníctvom webu ACA PSCA (<http://www.psc.sk>).

## Zverejňovanie informácií a repozitár

### Zverejňovanie informácií o ACA PSCA

ACA PSCA bude zverejňovať na Internete v on-line režime prostredníctvom svojho webu repozitár, ktorý je prístupný majiteľom KC a stranám spoliehajúcim sa na CK a ktorý obsahuje najmä:

KC, ktoré ACA PSCA vydala - KC sa budú zverejňovať prostredníctvom služby na vyhľadávanie KC.

aktuálne CRL a všetky predchádzajúce CRL

vlastný certifikát ACA PSCA (patriaci k jej podpisovému kľúču)

ACA PSCA bude zverejňovať na Internete v on-line režime prostredníctvom svojho webu CP ACA PSCA a ďalšie zákonom požadované dokumenty.

Verejne prístupné sú len aktuálne dokumenty. Dokumenty neaktuálne sú uložené v archíve a sprístupnené môžu byť len po dohode s poskytovateľom akreditovaných certifikačných služieb.

### Frekvencia zverejňovania informácií

Ak sa KC publikuje, tak čo najskôr po jeho vytvorení, ako náhle je možné prevzatie KC jeho majiteľom.

CRL sa publikuje, tak ako je špecifikované v ods. .

Všetky informácie, ktoré majú byť publikované v repozitári, majú byť publikované podľa možnosti čo najskôr.

## Kontroly prístupu

ACA PSCA musí chrániť ľubovoľnú informáciu uloženú v repozitári, ktorá nie je určená na verejné rozšírenie.

## Repozitáre

Repozitáre musia byť lokalizované tak, aby boli prístupné majiteľom KC a stranám spoliehajúcim sa na KC a v súlade s celkovými bezpečnostnými požiadavkami.

Funkciu repozitára ACA PSCA bude zastávať web ACA PSCA, ktorého domovská stránka má URL <http://www.psc.sk/> a ktorý je prostredníctvom internetu verejne prístupný majiteľom KC, stranám spoliehajúcim sa na KC a verejnosti vôbec.

## Audit zhody

### Frekvencia auditu zhody pre danú entitu

ACA PSCA sa podrobí každoročnému externému auditu bezpečnosti poskytovania akreditovaných certifikačných činností v súlade s požiadavkami platnej legislatívy.

Okrem toho ACA PSCA má právo požadovať pravidelné a nepravidelné revízie činností jej RA, aby sa potvrdilo, že RA funguje v súlade s bezpečnostnými praktikami a procedúrami popísanými v tejto politike a v príslušnom dokumente CPS.

### Identita audítora a kvalifikačné požiadavky na neho

Audítor musí byť v zmysle platnej legislatívy oprávnený na výkon auditu bezpečnosti akreditovaných certifikačných činností, musí byť kompetentný v oblasti auditov zhody a musí byť dôkladne oboznámený s týmto dokumentom a dokumentom CPS.

Osoba audítora musí byť nezávislá na ACA PSCA a zriaďovateľovi ACA PSCA, aby bola zaručená nestrannosť a objektívnosť auditu.

Audítora menuje PMA.

### Témy pokrývané auditom zhody

Témy pokrývané auditom definuje platná legislatíva.

Účelom auditu má byť záruka, že ACA PSCA má vyhovujúci systém práce, ktorý garantuje kvalitu služieb, ktoré ACA PSCA poskytuje a ktorý garantuje, že ACA PSCA koná v súlade s platnou legislatívou a so všetkými požiadavkami tohto dokumentu.

Predmetom auditu majú byť všetky aspekty prevádzky ACA PSCA vzťahujúce sa k tomuto dokumentu.

### **Akcie vykonané na odstránenie nedostatkov**

Keď audítor zistí rozpor medzi prevádzkou ACA PSCA a platnou legislatívou alebo ustanoveniami tohto dokumentu, musia sa uskutočniť nasledujúce akcie:

audítor zaznamená rozpor,  
audítor upovedomí o rozpore subjekty definované v časti ,  
PMA určí vhodné opatrenie na nápravu a to prípadne až po zrušenie vlastného certifikátu ACA PSCA. Po náprave nedostatkov PMA obnoví činnosť ACA PSCA resp. RA.

### **Zaobchádzanie s výsledkami auditu**

Audítor odovzdá PMA v zmysle platnej legislatívy záverečnú správu o výsledkoch auditu. Výsledky budú oznámené auditovanému subjektu a v prípade RA aj jej nadriadenej ACA PSCA.

Vykonanie opatrení na nápravu má byť dané na vedomie príslušnej autorite. Na potvrdenie vykonania a účinnosti opatrení na nápravu sa môže požadovať špeciálny audit alebo čiastkový audit zameraný na daný aspekt činnosti auditovaného subjektu.

## **Dôvernosť**

### **Typy informácií, ktoré sa majú chrániť**

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

privátny kľúč ACA PSCA používaný na vytváranie zaručeného elektronického podpisu pri vydávaní KC ACA PSCA  
privátne kľúče patriace k služobným certifikátom (napr. certifikáty patriace RA a pod.)  
infraštruktúra (napr. dokumenty, procedúry, postupy, súbory, skripty, heslá, pass frázy a pod.) slúžiaca na prevádzku ACA PSCA, vrátane jej RA  
osobné údaje subjektov a žiadateľov podliehajúce ochrane v zmysle zákona 428/2002 Z.z. o ochrane osobných údajov

Za účelom náležitej správy KC sa môže požadovať, aby sa pri správe KC v rámci ACA PSCA používali aj informácie, ktoré nie sú uvedené v KC (napr. identifikačné čísla dokladov, adresy, telefónne čísla).

Ľubovoľná takáto informácia sa explicitne definuje v časti tohto dokumentu. So všetkými informáciami uloženými v rámci ACA PSCA a nie v repozitári sa má zaobchádzať ako s citlivými informáciami a prístup k nim má byť obmedzený len na

osoby, ktoré tieto informácie nevyhnutne potrebujú na výkon svojich oficiálnych povinností.

Podmienkou na vydanie KC zákazníkovi je, aby v zmysle Zákona č. 428/2002 Z. z. o ochrane osobných údajov dal písomný súhlas, že ACA PSCA bude uschovávať jeho osobné údaje, ktoré získala pri jeho registrácii. ACA PSCA bude tieto údaje archivovať a spracovávať v rozsahu požadovanom zákonmi a vyhláškami, ktoré platia pre činnosť akreditovaných certifikačných autorít.

Všetky informácie, ktoré sú uvedené v KC a teda sú zverejňované prostredníctvom repozitára, nie sú klasifikované ako dôverné a považujú sa za verejné.

Zoznam zrušených KC (CRL) tiež nie je považovaný za dôverný.

### **Okolnosti uvoľnenia dôverných informácií**

ACA PSCA nezverejní žiadne informácie týkajúce sa žiadateľa o KC alebo subjektu KC žiadnej tretej strane, ak dané informácie nie sú považované za verejné, alebo ak to nie je požadované zákonom alebo príkazom kompetentného štátneho orgánu, ako je polícia, súd, prokuratúra.

Každá požiadavka na uvoľnenie informácií, ktoré nie sú považované za verejné, má byť autentizovaná a dokumentovaná.

ACA PSCA musí s osobnými údajmi zákazníka zaobchádzať v súlade s platnými zákonmi a nesmie ich poskytnúť žiadnej tretej strane s výnimkou subjektov, ktoré zo zákona majú právo kontrolovať činnosť ACA PSCA, a kompetentných štátnych orgánov ako sú polícia, súdy, prokuratúra.

### **Práva vyplývajúce z intelektuálneho vlastníctva**

Vlastník ACA PSCA je vlastníkom všetkých autorských práv na všetky dokumenty, dáta, procedúry, postupy, politiky, poriadky, certifikáty, KC a privátne kľúče, ktoré sú súčasťou infraštruktúry ACA PSCA a ktoré boli ním vytvorené.

## Identifikácia a autentizácia

### Prvotná registrácia

Prijímané žiadosti o KC a k nim patriace páry kľúčov sa musia generovať a uschovávať priamo na bezpečnom tokene a musia vyhovovať štandardu PKCS #10.

Bezpečný token musí byť certifikovaný na NBÚ ako HW produkt na vyhotovovanie zaručeného elektronického podpisu (SSCD).

Spôsob správneho generovania kľúčov preukazuje žiadateľ o KC čestným vyhlásením.

### Typy mien

ACA PSCA vydáva KC, ktoré obsahujú rozlišovacie mená v zmysle X.500 (X.500 Distinguished Name, ďalej ako rozlišovacie meno). Požiadavky na rozlišovacie mená sú uvedené nižšie.

ACA PSCA nepriraduje pre KC zákazníkov rozlišovacie mená.

Subjekty si sami zvolia rozlišovacie meno, ktoré má byť v ich KC.

### Potreba zmyslupnosti mien

Pojem „zmyslupnosť“ znamená, že forma mena má bežne používanú sémantiku na určenie identity osoby, organizácie alebo jej časti a podobne.

Používané mená majú spoľahlivo identifikovať osoby, ktorým sú priradené. ACA PSCA iba zaručuje, že existuje vzťah patričnosti (príslušnosti, členstva) medzi majiteľom KC a ľubovoľnou organizáciou alebo organizačnou jednotkou, ktorá je identifikovaná ľubovoľnou časťou mena v KC daného majiteľa. Dôraz sa pritom kladie na položku *commonName*, ktorá má jednoznačne reprezentovať majiteľa KC spôsobom, ktorý je pre človeka ľahko pochopiteľný. V prípade osoby to bude jej právoplatné meno a priezvisko v totožnej podobe, aká je uvedená v predložených dokladoch totožnosti ale bez použitia diakritiky (mäkčene, dĺžne).

Namiesto mena a priezviska je možné použiť pseudonym, avšak v tomto prípade poslednou časťou hodnoty tejto položky bezpodmienečne musí byť reťazec PSEUDONYM, aby bolo jednoznačné a jasné, že namiesto mena a priezviska je uvedený pseudonym a tak aby strana spoliehajúca sa na KC nemohla byť použitím pseudonymu uvedená do omylu. Neuvedenie reťazca PSEUDONYM za pseudonymom bude dôvodom na odmietnutie danej žiadosti o KC. Pseudonym nemusí byť zmyslupný, avšak RA má právo zamietnuť žiadosť obsahujúcu pseudonym, ktorý je z etického, rasového, náboženského alebo iného dôvodu nevhodný. Pseudonym tiež nesmie obsahovať výraz, ktorým by mohli byť poškodené

práva iného subjektu (napr. neoprávnené použitie registrovanej obchodnej značky ako pseudonymu). Použitie pseudonymu v žiadnom prípade nezabavuje subjekt povinnosti preukázať svoju totožnosť na RA.

ACA PSCA má právo odmietnuť vydať KC, ktorý by obsahoval údaje porušujúce princíp zmysluplnosti mien, zvláštny dôraz sa pritom kladie na údaj v položke *commonName*. Požiadavka na zmysluplnosť sa pritom vzťahuje na hodnotu ľubovoľnej položky v rozlišovacom mene. Porušenie tohto princípu môže byť príčinou odmietnutia vytvoriť KC z danej žiadosti o KC.

Pri zadávaní hodnôt do položiek žiadosti KC by mal subjekt resp. žiadateľ o KC mať na zreteli, že na RA bude musieť uspokojivým spôsobom preukázať oprávnenosť všetkých údajov, ktoré zadal do jednotlivých položiek žiadosti o KC.

Rozlišovacie meno používané v KC pozostáva z nasledujúcich položiek s nižším uvedeným významom:

### Položky rozlišovacieho mena KC

Názov položky:	Skratka názvu položky:	Popis položky:	Príklad hodnoty položky:	Typ a max. dĺžka položky:
countryName (Štát)	C	Dvojnaková skratka štátu – dvojmiestny kód podľa ISO 3166 definujúci štátnu príslušnosť subjektu, údaj je povinný	SK	PrintableString 2 znaky
stateOrProvinceName	ST	Názov kraja resp. provincie, údaj je nepovinný	Bratislavský kraj	UTF8String 128 znakov
localityName (Mesto)	L	Názov lokality, údaj je nepovinný	Bratislava	UTF8String 128 znakov
organizationName (Firma)	O	Názov organizácie, údaj je nepovinný	Info Servis a.s.	UTF8String 64 znakov
organizationUnitName (Útvár vo firme)	OU	Názov útvaru vo firme, údaj je nepovinný	Ekonomické oddelenie	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno a priezvisko alebo pseudonym, za ktorým je uvedený reťazec PSEUDONYM, údaj je povinný	Eva Maria Cibulova alebo napr. Udatný kojot PSEUDONYM	UTF8String 64 znakov
SERIALNUMBER	SERIALNUMBER	Odkaz na identitu fyzickej osoby	PNOSK 9959199999	UTF8String 64 znakov
givenName ((dané) mená)	GN	Všetky mená použité v položke CN okrem priezviska,	Eva Maria	UTF8String 64 znakov

		údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený		
Surname (Priezvisko)	SN	Priezvisko z položky CN, údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený	Cibulova	UTF8String 64 znakov
serialNumber		Položka slúži na zabezpečenie jednoznačnosti rozlišovacieho mena (pozri časť 3.1.3)	Položka nebude súčasťou žiadosti o KC – jej hodnotu určí ACA PSCA	

Okrem položiek uvedených v tejto tabuľke môže žiadosť o KC obsahovať ako nepovinný údaj email adresu, táto položka však nebude súčasťou rozlišovacieho mena ale zadaná email adresa bude uvedená v KC v jeho rozšírení *SubjectAltName*. Hodnota email adresy sa zadáva obvyklým spôsobom (t.j. ako rfc822Name).

Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.).

### Jednoznačnosť mien

ACA PSCA zodpovedá za jednoznačnosť mien v rámci celej komunity subjektov KC.

ACA PSCA prostredníctvom RA musí presadzovať jednoznačnosť mien v rámci celého menného priestoru, aby nedošlo k neprijateľným menným duplicitám. Musí byť pritom tiež zaručená jednoznačnosť mien aj medzi súčasnými a minulými majiteľmi KC (t.j. ak napr. „Ján Kováč“ opustí komunitu majiteľov KC a nový, iný „Ján Kováč“ pribudne do tejto komunity).

ACA PSCA dokumentuje vo svojom CPS, akým spôsobom bude zabezpečená jednoznačnosť mien v rámci komunity subjektov KC.

### Procedúra riešenia sporov pri kolízii mien

ACA PSCA prostredníctvom RA musí zabezpečiť, že nepríde k žiadnej kolízii mien. V prípade potreby môže odmietnuť vydanie KC z dôvodu kolízie mien. V prípade

sporov týkajúcich sa kolízie mien a mien vo všeobecnosti sa bude postupovať podľa ustanovení bodu .

Ak bol spor spôsobený chybou ACA PSCA, tá zjedná bezplatne a čo najrýchlejšie nápravu.

ACA PSCA si vyhradzuje právo v prípade nevyhnutnosti zrušiť KC subjektu, ktorý spor spôsobil.

### **Rozpoznanie, autentizácia a rola obchodných značiek**

Žiadnemu subjektu sa negarantuje, že jeho meno v KC bude obsahovať jeho obchodnú značku (trademark) a to ani na jeho výslovnú žiadosť.

V KC môžu byť použité len tie obchodné značky, ktorých vlastníctvo alebo prenájom žiadateľ o KC uspokojivo doložil. Žiadnu inú autentizáciu obchodných značiek ACA PSCA nevykonáva.

RA má právo odmietnuť žiadosť o KC, ak má podozrenie, že táto žiadosť obsahuje obchodnú značku, ktorej vlastníctvo alebo prenájom žiadateľ KC uspokojivo nedoložil.

ACA PSCA nevydá vedome KC obsahujúci meno, o ktorom kompetentný súd rozhodol, že porušuje obchodnú značku iného.

ACA PSCA nie je povinné skúmať obchodné značky ani riešiť spory týkajúce sa obchodných značiek.

### **Preukazovanie vlastníctva privátneho kľúča**

Všetky žiadosti o KC musia byť vo formáte PKCS#10, čo znamená, že žiadosť o KC bude podpísaná privátnym kľúčom patriacim k verejnému kľúču nachádzajúcemu sa v danej žiadosti o KC.

Všetky páry kľúčov a im zodpovedajúce žiadosti o KC sa musia generovať priamo v bezpečnom zariadení pre zaručený elektronický podpis, ktoré je certifikované NBÚ a to pod dohľadom RA.

Keď subjekt sám generuje kľúče priamo v svojom tokene, potom automaticky vlastní vygenerovaný privátny kľúč uložený v tokene v čase jeho generovania.

Žiadateľ o KC preukáže na RA vlastníctvo svojho privátneho kľúča tým, že na RA vygeneruje žiadosť o KC zodpovedajúcu svojmu privátnemu kľúču buď osobne alebo prostredníctvom osoby, ktorá sa preukáže úradnou plnou mocou.

V prípade žiadosti o následný KC je prípustné, aby žiadateľ preukázal vlastníctvo svojho privátneho kľúča tým, že svoju žiadosť o KC doručí na RA podpísanú svojím zaručeným elektronickým podpisom vytvoreným použitím svojho platného KC a aplikácie schválenej ACA PSCA a NBÚ.

ACA PSCA negeneruje páry kľúčov pre cudzie subjekty.

Žiadna zložka ACA PSCA v nijakom prípade nearchivuje žiadne privátne kľúče patriace zákazníkovi – cudzím subjektom.

### **Autentizácia identity organizácie**

Žiadosť o akreditovanú certifikačnú službu podávaná v mene právnickej osoby musí obsahovať meno právnickej osoby, iný identifikačný údaj, ak taký existuje (spravidla je to napr. IČO), adresu a dôkaz existencie danej právnickej osoby (spravidla výpisom z obchodného registra).

Právnická osoba musí byť registrovaná na území Slovenskej republiky a musí preukázať svoju totožnosť výpisom z obchodného registra nie starším ako tri mesiace.

RA bude overovať tieto údaje a okrem autentičnosti žiadajúcej osoby sa bude overovať, že daná osoba má právo konať v mene danej právnickej osoby vo veci príslušného KC.

Fyzické osoby (jedna alebo viac, podľa predloženého výpisu z obchodného registra), ktoré na základe predloženého výpisu z obchodného registra konajú na RA za danú právnickú osobu vo veci akreditovanej certifikačnej služby, musia preukázať svoju totožnosť podľa časti 3.1.8.

V mene právnickej osoby môže na RA konať len osoba, ktorá je jej štatutárom (alebo viac takýchto osôb súčasne, ak to vyžaduje predložený výpis z obchodného registra), prípadne sa právnická osoba môže nechať zastupovať fyzickou alebo inou právnickou osobou.

Ak sa právnická osoba nechá zastupovať na RA, zastupujúca fyzická alebo právnická osoba musí vždy predložiť výpis z obchodného registra zastupovanej právnickej osoby nie starší ako tri mesiace.

Ak sa právnická osoba nechá zastupovať na RA fyzickou osobou, táto zastupujúca fyzická osoba musí preukázať svoju totožnosť podľa časti 3.1.8 a navyše sa musí preukázať úradne overenou (notárom alebo matrikou) plnou mocou, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou právnickou osobou konať v danej veci v jej mene.

Ak sa právnická osoba nechá zastupovať na RA inou právnickou osobou, táto zastupujúca právnická osoba okrem príslušnej plnej moci (viď predošlý odsek) musí preukázať svoju totožnosť rovnakým spôsobom ako zastupovaná právnická osoba, ako je to požadované vyššie.

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje právnickú osobu, sa vo veci právnickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

V prípade, že právnická osoba nemôže preukázať svoju totožnosť výpisom z obchodného registra (platí pre nepodnikateľské subjekty ako sú napr. obec, cirkev, občianske združenie, nadácia, štátny orgán a podobne), musí takáto právnická osoba písomne preukázať okrem svojej totožnosti aj legálnosť (resp. „dôvod“) svojej existencie (s využitím a poukázaním na zákon alebo iný predpis, ktorý o subjekte daného typu pojednáva).

### **Autentizácia identity fyzickej osoby**

ACA PSCA garantuje, že identita subjektu KC a jeho verejný kľúč sú zodpovedajúco previazané.

ACA PSCA špecifikuje vo svojom dokumente CPS procedúry na autentizáciu identity subjektu resp. žiadateľa o KC. ACA PSCA zverejňuje požiadavky na identifikáciu fyzickej osoby prostredníctvom svojho webu a svojich RA.

ACA PSCA bude zaznamenávať tento proces pre každý KC. Dokumentácia o identifikácii musí minimálne obsahovať:

identita osoby, ktorá vykonáva identifikáciu,  
vyhlásenie podpísané touto osobou, že overila identitu subjektu resp. žiadateľa o KC tak, ako to požaduje táto certifikačná politika,  
jednoznačné identifikačné čísla z predložených osobných dokladov dokladujúcich identitu autentizovanej osoby,  
dátum a čas vykonania identifikácie.

Súčasťou dokumentácie o identifikácii musí byť vyplnený formulár obsahujúci zozbierané identifikačné údaje, ktorý bude vlastnoručne podpísaný identifikovanou osobou v prítomnosti osoby vykonávajúcej autentizáciu identity.

Fyzickou osobou môže byť plnoletý občan Slovenskej republiky alebo cudzí štátny príslušník.

Fyzická osoba musí preukázať svoju totožnosť dvomi z týchto osobných dokladov (minimálne jeden z nich musí obsahovať fotografiu fyzickej osoby):

občiansky preukaz,  
cestovný pas,  
vodičský preukaz,  
rodný list,  
osobný preukaz vojaka z povolania alebo vojenská knižka,  
povolenie na prechodný pobyt (resp. trvalý pobyt) v prípade cudzinca.

Ak fyzická osoba zastupuje na RA inú fyzickú osobu, musí sa navyše preukázať úradne overenou (notárom alebo matrikou) plnou mocou, z textu ktorej je jednoznačne jasné, že zastupujúca fyzická osoba bola splnomocnená splnomocňujúcou fyzickou osobou konať v danej veci v jej mene.

Ak právnická osoba zastupuje fyzickú osobu, okrem plnej moci (viď predošlý odsek) musí splnomocnená právnická osoba preukázať svoju totožnosť podľa časti .

Subjekt (fyzická alebo právnická osoba), ktorý zastupuje fyzickú osobu, sa vo veci fyzickej osoby, ktorú zastupuje, v žiadnom prípade nemôže nechať zastupovať iným subjektom.

### **Predkladané doklady**

Všetky doklady, predkladané potenciálnymi zákazníkmi – žiadateľmi o KC, musia byť buď originály alebo úradne overené kópie originálov. Nesmie v nich byť žiaden údaj doplňovaný, pozmeňovaný, prečiarknutý a podobne. Doklady, na ktorých je vyznačená doba ich platnosti, musia byť platné.

Ak má pracovník RA pochybnosti o totožnosti potenciálneho zákazníka (napr. zjavný nesúlad medzi fotografiou v predloženej osobnom doklade a vzhľadom zákazníka, rozpornosť dvoch predložených dokladov a podobne), môže odmietnuť jeho registráciu.

Prípadné predložené doklady v cudzom jazyku (okrem češtiny) musia byť preložené úradným prekladateľom – znalcom.

Na žiadosť potenciálneho zákazníka alebo RA sa prípadné sporné prípady pri preukazovaní totožnosti riešia postupom podľa ods. .

### **Kontrola údajov na predložených dokladoch**

V prípade ľubovoľných odôvodnených pochybností o totožnosti potenciálneho zákazníka môže RA jeho registráciu odmietnuť. Pracovník RA kontroluje na predložených dokladoch najmä skutočnosti podľa nasledovných odsekov.

Osobné doklady fyzickej osoby

a) platnosť predloženého dokladu

---

**Poznámka:** V prípade neplatného osobného dokladu sa postupuje ako pri chýbajúcom osobnom doklade – RA registráciu odmietne

---

plnoletosť fyzickej osoby (t.j. vek 18 rokov)

---

**Poznámka:** RA odmietne registráciu nepľnoletých osôb. Za nepľnoleté osoby má právo konať ich zákonný zástupca (obvykle rodič).

---

či nie je zjavný nesúlad medzi fotografiou v osobnom doklade a vzhľadom majiteľa osobného dokladu

---

**Poznámka:** Ak áno, RA môže odmietnuť registráciu.

---

integrita predložených dokladov, t.j. či údaje na jednom doklade neodporujú údajom na inom doklade

## Výpisy z obchodného registra

a) či výpis nie je starší ako 3 mesiace

či majú fyzické osoby (stačí jedna fyzická osoba, ak na výpise nie je uvedené inak), ktoré predložili daný výpis, právo konať (podpisovať) za danú právnickú osobu (t.j. či sú jej štatutárnymi zástupcami)

či je výpis úradne overený (notárom alebo matrikou), ak sa nejedná o originál

---

**Poznámka:** Výpis z obchodného registra získaný z internetu je pri konaní na RA nepoužiteľný.

---

## Plné moci

a) či je plná moc úradne overená (notárom alebo matrikou)

či sa údaje, uvedené v plnej moci, ktoré definujú zastupujúcu fyzickú resp. právnickú osobu, zhodujú s údajmi uvedenými na osobných dokladoch zastupujúcej fyzickej osoby resp. s údajmi uvedenými na výpise z obchodného registra zastupujúcej právnickej osoby

rozsah plnej moci - t.j. či plná moc oprávňuje splnomocnenú fyzickú alebo právnickú osobu k požadovanému úkonu na RA v mene splnomocňujúcej fyzickej alebo právnickej osoby

či plná moc nie je časovo obmedzená alebo ak obsahuje inú podmienku, či je táto splnená

## Prvotná registrácia pracovníka ACA PSCA

Prvotná registrácia osoby, zastávajúcej niektorú rolu v rámci ACA PSCA je popísaná v príslušných CPS.

## Vydanie následného KC

Čím dlhšie a častejšie sa kľúč používa, tým je náchylnejší na stratu alebo prezradenie. Toto zoslabuje záruku poskytovanú stranám spoliehajúcim sa na KC, že je v platnosti jednoznačná väzba medzi kľúčom a jeho majiteľom. Teda je dôležité, aby majiteľ KC periodicky dostával nové kľúče a opakovane potvrdzoval svoju identitu.

Vydanie následného KC znamená vlastne zmenu páru kľúčov KC – vytvorí sa nový KC, ktorý bude mať zhodné rozlišovacie meno ako starý KC až na to, že nový KC bude mať nový, odlišný verejný kľúč (zodpovedajúci novému, odlišnému privátnemu kľúču), odlišné číslo KC (*serial number*) a môže mať zmenenú dobu platnosti.

Žiadateľ o následný KC sa musí podrobiť požiadavkám prvotnej registrácie (hlavne autentizácii jeho identity). Jedinou výnimkou je možnosť, že požiada o vydanie následného KC tak, že svoju žiadosť o KC doručí na RA podpísanú svojim zaručeným elektronickým podpisom vytvoreným použitím svojho platného KC. Typ aplikácie, pomocou ktorej môže vytvoriť žiadosť určí ACA PSCA a NBÚ.

Majiteľ platného KC môže požiadať o vydanie následného KC počas posledných 30 dní platnosti svojho KC.

KC sa vydávajú s platnosťou maximálne na jeden rok, ak to nie je dohodnuté inak osobitnou písomnou zmluvou so zákazníkom.

Ustanovenia pre vydanie následného KC pre osoby v zastávajúcej služobnej roly ACA PSCA sú popísané v príslušných CPS.

## **Vydanie následného KC po zrušení starého**

V každom prípade žiadateľ o KC sa po zrušení KC musí podrobiť požiadavkám prvotnej registrácie.

## **Žiadosť o zrušenie KC**

Žiadosť o zrušenie KC musí byť autentizovaná, pozri časť .

Žiadosť o zrušenie KC môže byť autentizovaná použitím privátneho kľúča patriaceho k KC, ktorý sa má zrušiť, bez ohľadu na to, či daný privátny kľúč bol alebo nebol kompromitovaný.

## Prevádzkové požiadavky

### Žiadanie o KC

Účelom tejto politiky je identifikovať minimálne požiadavky a procedúry, ktoré sú nevyhnutné na podporu dôvery v KC. Účelom je tiež minimalizovať špecifické implementačné požiadavky na ACA PSCA, žiadateľov o KC, majiteľov KC a strany spoliehajúce sa na KC.

Keď žiadateľ o KC požiadava o KC, žiadateľ a RA musia vykonať nasledovné kroky:

Overiť a zaznamenať identitu subjektu a aj žiadateľa, ak to nie je tá istá osoba (podľa ods. )

Subjekt musí mať v svojom bezpečnom zariadení pre zaručený elektronický podpis vygenerovaný a uložený pár kľúčov (verejný a privátny kľúč) pre každý požadovaný KC

Preukázať, že verejný kľúč tvorí pár kľúčov s privátnym kľúčom vlastneným žiadateľom o KC (podľa časti )

Poskytnúť dostatočné podklady na overenie ľubovoľných identifikačných údajov, ktoré sa majú dostať do KC

Komunikácia medzi jednotlivými zložkami ACA PSCA týkajúca sa žiadosti o KC a procesu vydania KC má byť autentizovaná a chránená pred modifikáciou pomocou mechanizmov primeraných požiadavkám dát. Ľubovoľný elektronický prenos zdieľaných tajomstiev musí byť uskutočnený šifrovane. Tieto kroky možno vykonať v ľubovoľnom poradí, ktoré je vyhovujúce pre ACA PSCA aj žiadateľov a ktoré nie je v rozpore s bezpečnosťou.

Žiadosť ACA PSCA o vlastný certifikát bude predložená NBÚ spôsobom požadovaným NBÚ na základe platnej legislatívy.

### Detailný postup na získanie KC

Zákazník (žiadateľ o KC resp. subjekt – budúci majiteľ KC) vykoná nasledovné kroky ako prípravu na návštevu na RA:

a) oboznámi sa s týmto postupom, prípadne s princípmi a návodmi pre získanie KC, pripraví si hodnoty jednotlivých položiek žiadosti o KC tak, aby tieto hodnoty boli v súlade s týmto dokumentom s dôrazom na jeho časť ,

---

**Poznámka:** Pri zadávaní hodnôt do položiek žiadosti o KC by mal subjekt resp. žiadateľ o KC mať na zreteli, že na RA bude musieť uspokojivým spôsobom preukázať oprávnenosť všetkých údajov, ktoré zadal do jednotlivých položiek žiadosti o KC. Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.)

---

zákazník v súlade s hodnotami, ktoré mieni použiť pri generovaní žiadosti o KC, vyplní formulár "Žiadosť o vydanie KC" v dvoch exemplároch, pričom si formulár si skopíruje z webu <http://www.psc.sk> (je k dispozícii aj na RA).

zákazník si pripraví zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra (odporúčame overiť platnosť dokladov) podľa ustanovení časti .

---

**Poznámka:** Je potrebné, aby si zákazník pripravil kópie (nemusia byť overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré mieni predložiť na RA (napr. výpis z obchodného registra a iné doklady o právnickej osobe, plnomocenstvo, ak sa dá zastupovať na RA), aby ich mohol odovzdať na RA. Výpis z obchodného registra získaný z Internetu nie je postačujúci, nakoľko má len informatívny charakter a nie je použiteľný na právne úkony

**Odporúčanie:** Odporúča sa, aby si zákazník ešte pred návštevou RA overil a vyjasnil prípadné pochybnosti a problémy, najmä tie, ktoré týkajú vhodnosti hodnôt jednotlivých položiek v žiadosti o KC.

---

Zákazník si dohodne termín návštevy RA (telefonicky, e-mailom)

Zákazník v dohodnutom termíne príde na RA, pričom vezme so sebou a predloží:

zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra, plná moc atď. podľa ustanovení časti ,

---

**Poznámka:** Zákazník odovzdá na RA kópie (nemusia byť overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré predkladá na RA pri registrácii (napr. výpis z obchodného registra a iné doklady o právnickej osobe, plnomocenstvo v prípade zastupovania iného subjektu),

---

vyplnený formulár "Žiadosť o vydanie KC" v dvoch exemplároch, príslušnú peňažnú čiastku, ak nebola vopred dohodnutá iná forma platby za KC.

Postup pri registrácii zákazníka na RA

a) Pracovník RA overí totožnosť subjektu resp. žiadateľa o KC, ktorý ho zastupuje, podľa ustanovení častí a .

V prípade úspešného overenia totožnosti pracovník RA vypíše pre každú overenú fyzickú osobu dvojmo formulár „Súhlas so spracovaním osobných údajov“, tento sám podpíše a dá ho podpísať žiadateľovi o KC resp. subjektu, ktorý ho zastupuje. Jeden vyplnený formulár zostáva na RA, jeden dostane žiadateľ

Zákazník priamo na RA pod dohľadom pracovníka RA pomocou definovaného softvéru vygeneruje novú žiadosť o KC priamo v svojom tokene a uloží ju na disk

---

**Upozornenie:** Žiadosť o KC resp. v nej sa nachádzajúci verejný kľúč, pre ktorý už bol vydaný KC, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného KC a bude na RA odmietnutá!

**Poznámka:** Žiadosť musí obsahovať vhodne vyplnené položky v súlade s tabuľkou "Položky rozlišovacieho mena KC" uvedenou v časti ,

---

zákazník v súlade s údajmi, ktoré zadal do prehliadača pri generovaní žiadosti o KC, vyplní formulár "Žiadosť o vydanie KC" v dvoch exemplároch, ak tak neurobil ešte

pred príchodom na RA, formulár je k dispozícii na RA alebo si ho môže skopírovať z webu <http://www.psc.sk/>.

Pracovník RA preberie od zákazníka súbor so žiadosťou o KC a vyplnený formulár "Žiadosť o vydanie KC".

Pracovník RA skontroluje, či sa údaje na vyplnenom formulári "Žiadosť o vydanie KC" zhodujú s údajmi na žiadosti o KC v súbore a či sú vyplnené všetky povinné položky.

Všetky položky musia byť vyplnené bez diakritiky. Malé a veľké písmená sa rozlišujú.

Položky ST (stateOrProvinceName (názov kraja)), L (localityName („Mesto")), O (organizationName ("Firma")), OU (organizationUnitName ("Útvar vo firme")) a Email adresa sú nepovinné.

Ostatné položky žiadosti o KC **musia byť povinne vyplnené** nasledovne:

Názov položky:	Spôsob vyplnenia položky:
<b>C (countryName (Štát) )</b>	Dvojnaková skratka štátu (dvojmiestny kód podľa ISO 3166, SK pre Slovenskú republiku) definujúci štátnu príslušnosť subjektu KC
<b>CN (commonName (Meno a priezvisko))</b>	Meno a priezvisko alebo pseudonym subjektu KC, ak bol použitý pseudonym, musí byť za ním uvedený reťazec PSEUDONYM (spolu max. 64 znakov)
<b>G (givenName („dané mená"))</b>	Všetky mená použité v položke CN okrem priezviska, údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený
<b>SN (Surname (Priezvisko))</b>	Priezvisko z položky CN, údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený

Prostredníctvom informačného systému ACA PSCA sa automatizovane overí, či pre verejný kľúč nachádzajúci sa v predloženej žiadosti o KC už nebol v minulosti vydaný KC. Ak bol, RA žiadosť o KC odmietne prijať z bezpečnostných dôvodov, lebo už raz certifikovaný verejný kľúč nemôže byť použitý v inom KC.

Zákazník a pracovník RA podpíšu dva exempláre zákazníkovi vyplneného formulára "Žiadosť o vydanie KC". Jedna kópia zostáva zákazníkovi.

**Upozornenie:** Údaje uvedené v položkách "Žiadosti o vydanie KC" by sa mali presne zhodovať s hodnotami uvedenými v elektronickej forme žiadosti v súbore. Všetky dôsledky za prípadné chyby a odlišnosti nesie zákazník.

Akýkoľvek rozdiel v hodnotách povinných položiek (pozri tabuľku vyššie) medzi "Žiadosťou o vydanie KC" a žiadosťou v súbore môže byť príčinou odmietnutia vydania KC alebo oneskorenia jeho vydania.

Pri posudzovaní hodnôt všetkých položiek berie pracovník RA do úvahy zmysluplnosť týchto hodnôt (bližšie pozri časť ) – porušenie princípu zmysluplnosti môže byť dôvodom na odmietnutie vydania KC.

Žiadateľ o KC musí na RA uspokojivým spôsobom preukázať všetky údaje, ktoré zadal do jednotlivých položiek žiadosti o KC.

Ak žiadateľ predloží aj iné doklady (okrem osobných dokladov fyzických osôb, napr. výpis z obchodného registra alebo iný doklad o právnickej osobe, plná moc v prípade zastupovania iného subjektu), pracovník RA prevezme a uschová kópie (nemusia byť overené) všetkých predložených dokladov, porovná ich s originálmi a na každú kópiu napíše text „Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis.

**Poznámka:** Výpis z obchodného registra získaný z Internetu nie je postačujúci, nakoľko má len informatívny charakter a nie je použiteľný na právne úkony.

---

Ak je v položke CN (commonName (Meno a priezvisko)) uvedený aj jeden alebo viacero titulov (napr. Ing., Mgr., CSc. a iné), použitie titulu v žiadosti o KC sa akceptuje, ak sa použité tituly nachádzajú v aspoň jednom z predložených osobných dokladov patriacich subjektu KC. V opačnom prípade je žiadateľ povinný RA preukázať oprávnenosť použitia každého uvedeného titulu predložením originálu alebo úradne overenej kópie diplomu alebo iného dokumentu, ktorý potvrdzuje, že daná osoba má právo používať daný titul.

RA odmietne žiadosť o KC, ktorá obsahuje uvedenie titulu, ktorý žiadateľ nevie dokladovať vyššie uvedeným spôsobom.

Pracovník RA predloží žiadateľovi o KC na podpis Zmluvu o vydaní a používaní KC ACA PSCA v dvoch exemplároch – jeden pre ACA PSCA a jeden pre zákazníka. Súhlas žiadateľa s textom tejto zmluvy je podmienkou na prijatie žiadosti o KC a vytvorenie KC.

Pracovník RA zinkasuje v hotovosti poplatky podľa „Cenníka služieb ACA PSCA“ a vydá zákazníkovi daňový doklad. Zákazník bude môcť dostať svoj KC až po zaplatení zaň. Zákazník môže platiť aj faktúrou, ak to s ním bolo dohodnuté.

Pracovník RA vloží do aplikácie RA a informačného systému ACA PSCA žiadosť o KC zo súboru a ostatné požadované údaje.

V prípade, že z danej žiadosti o KC z nejakého dôvodu nie je možné urobiť KC, Operátor CA o tom upovedomí príslušnú RA vrátane uvedenia dôvodu, ktorá potom vyrozumie žiadateľa o KC. Žiadateľ o KC môže v takom prípade buď podať novú žiadosť o KC alebo mu budú vrátené zaplatené peniaze.

Všetky doklady v tlačenej forme bude RA odosielať na CA stanoveným spôsobom v stanovených periódach.

### **Doručenie verejného kľúča žiadateľa o KC vydavateľovi KC**

Verejné kľúče (obsiahnuté v žiadostiach o KC) sa musia generovať v bezpečnom zariadení na RA buď osobne subjektom KC alebo žiadateľom o KC, ktorým sa subjekt nechá zastupovať na RA, aby sa garantovala väzba overenej identity žiadateľa k verejnému kľúču, ktorý sa certifikuje.

Jedinou výnimkou je v prípade následného KC možnosť požiadať o vydanie následného KC tak, že svoju žiadosť o KC doručí žiadateľ na RA podpísanú svojím zaručeným elektronickým podpisom vytvoreným použitím svojho platného KC v aplikácii, ktorú schváli ACA PSCA a NBÚ.

## Vydanie KC

ACA PSCA nevytvorí KC, kým sa k spokojnosti ACA PSCA nedokončia všetky verifikácie a prípadné zmeny, ak sú potrebné.

ACA PSCA nezodpovedá za prípadné dodatočné náklady žiadateľa o KC, ktoré vzniknú v priebehu registrácie, napr. kvôli potrebe opakovanej návštevy RA napr. v dôsledku neúplných alebo chýbajúcich dokladov alebo iných nedostatkov.

Hoci žiadateľ pripravuje väčšinu dátových položiek KC, na ACA PSCA zostáva zodpovednosť overiť, že informácie sú správne a presné.

Za preverenie údajov žiadateľa zodpovedá RA.

CA má právo nevytvoriť KC, hoci žiadateľ o KC úspešne prešiel procesom registrácie na RA, ak sa dodatočne zistí závažná skutočnosť, ktorá bráni vydaniu KC (napr. chyba vo formáte žiadosti o KC).

## Doručenie privátneho kľúča majiteľovi KC

Privátny kľúč bude spravidla generovať sám subjekt priamo vo svojom tokene, v ktorom vygenerovaný privátny kľúč zostane a teda nie je potrebné privátny kľúč doručiť. Iná osoba tak môže robiť len za podmienky osobného dohľadu majiteľa tokenu na proces generovania kľúčov.

## Doručenie verejného kľúča ACA PSCA používateľom

ACA PSCA a strany spoliehajúce sa na KC musia konať v súčinnosti, aby sa zaručilo autentizované a integrálne doručenie certifikátu ACA PSCA.

Prijateľné metódy na doručenie certifikátu ACA PSCA a jeho autentizovanie sú:

nahratie certifikátu z web servera ACA PSCA zabezpečeného platným certifikátom ACA PSCA,

osobné prevzatie certifikátu ACA PSCA na RA

RA na požiadanie poskytne strane spoliehajúcej sa na KC alebo inému ľubovoľnému záujemcovi fingerprint certifikátu ACA PSCA a to konkrétne telefonicky, zabezpečeným mailom alebo osobne pri návšteve záujemcu na RA. Konkrétna voľba spôsobu poskytnutia fingerprintu závisí na dohode so záujemcom. Okrem toho bude ACA PSCA na Internete zverejňovať fingerprint certifikátu ACA PSCA prostredníctvom svojho web servera. Fingerprint (alebo hash) posielaný spolu s certifikátom nie je prijateľný ako autentizačný mechanizmus.

## Prevzatie KC

ACA PSCA bude vydávať KC v režime on-line, tzn. žiadateľ spravidla bude môcť prevziať vydaný KC v rámci návštevy RA, pri ktorej sa uskutočnil proces registrácie a prijatia žiadosti o KC.

Pri preberaní KC žiadateľ podpíše „Potvrdenie o vydaní KC“ a jeho odovzdaní žiadateľovi o KC, ktoré tvorí prílohu zmluvy o vydaní a používaní KC. Toto potvrdenie sa vyhotoví v dvoch exemplároch – jeden pre žiadateľa a jeden pre RA.

Subjekt sa pri preberaní svojho KC môže dať zastupovať na RA inou fyzickou alebo právnickou osobou za rovnakých podmienok ako pri podávaní žiadosti o KC (pozri časti resp. ).

Vytvorený KC bude uložený v tokene a odovzdaný na 3,5“ diskete žiadateľa alebo subjektu, ktorý ho zastupuje, spolu s certifikátom ACA PSCA a certifikačným poriadkom ACA PSCA v elektronickej forme.

ACA PSCA môže osobitnou zmluvou so zákazníkom dohodnúť aj iný postup na prevzatie KC.

## Zrušenie a suspendovanie KC

### Zrušenie KC

Okolnosti zrušenia KC

KC sa má zrušiť, keď sa väzba medzi subjektom a jeho verejným kľúčom definovaným v KC už nepovažuje za platnú. ACA PSCA je zo zákona povinná zrušiť KC, ktorý spravuje, v nasledovných prípadoch:

zistí, že pri vydaní KC neboli splnené požiadavky zákona  
zistí, že KC bol vydaný na základe nepravdivých údajov  
o zrušenie KC požiada subjekt, ktorého údaje sú uvedené v KC  
zrušenie KC nariadi ACA PSCA svojím rozhodnutím súd  
dozvie sa, že subjekt KC zomrel

zistí, že došlo ku kompromitácii privátneho kľúča patriaceho k danému KC, napr. ak privátny kľúč patriaci k verejnému kľúču uvedenému v KC pozná iná osoba, než subjekt uvedený v KC

dozvie sa, že údaje uvedené v KC sa stali neaktuálnymi  
subjekt porušil svoje povinnosti stanovené certifikačným poriadkom a/alebo zmluvou medzi ním a CA

dozvie sa, že subjekt sa stal nesvojprávnym na základe rozhodnutia súdu  
došlo ku kompromitácii privátneho kľúča ACA PSCA

Vždy, keď sa ACA PSCA dozvie o niektorej z vyššie uvedených okolností, daný KC sa zruší a dá sa na zoznam zrušených KC (CRL).

Zrušené KC sa budú vyskytovať na všetkých nových vydaniach CRL.

Kto môže žiadať o zrušenie KC

Subjekt - majiteľ KC (alebo ním poverená fyzická alebo právnická osoba) môže hocikedy požiadať spôsobom stanoveným týmto dokumentom o zrušenie svojho vlastného KC a to aj bez udania dôvodu žiadosti o zrušenie KC.

RA dá CA návrh na zrušenie KC, ak sa dozvie, že nastala niektorá z okolností uvedených v časti 4.4.1.1.

O zrušenie KC môže tiež požiadať:

ACA PSCA (daný pracovník je povinný písomne zdokumentovať túto skutočnosť vrátane dôvodu svojho konania)

súd prostredníctvom svojho rozsudku alebo predbežného opatrenia (k dokumentom o zrušení KC musí ACA PSCA priložiť kópiu príslušného súdneho rozhodnutia)

subjekt (fyzická alebo právnická osoba) na základe dedičského konania (k dokumentom o zrušení KC musí ACA PSCA priložiť kópiu dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie KC)

súdom poverená osoba (napr. poručník subjektu KC, ktorý sa má zrušiť) (k dokumentom o zrušení KC musí ACA PSCA priložiť kópiu príslušného súdneho rozhodnutia)

V prípade služobného certifikátu pracovníka CA resp. RA môže o zrušenie služobného certifikátu okrem jeho majiteľa požiadať tiež PMA, ak sa zistí závažná okolnosť (pozri časť 4.4.1.1) na zrušenie daného služobného certifikátu.

#### Procedúra žiadosti o zrušenie KC

Žiadosť o zrušenie KC podáva oprávnená osoba na RA prostredníctvom dvoch exemplárov vyplneného formulára „Žiadosť o zrušenie KC“, ktorý je k dispozícii na webe ACA PSCA alebo na RA – jeden kus zostáva na RA, jeden kus pracovník RA potvrdí s uvedením aktuálneho dátumu a času (s uvedením hodín, minút a sekúnd) a vráti žiadateľovi o zrušenie.

RA poskytne v prípade potreby žiadateľovi o zrušenie pomoc pri zistení čísla (*Serial Number*) predmetného KC, aby bolo možné jednoznačne identifikovať KC, ktorý sa má zrušiť.

Osoba požadujúca zrušenie KC sa buď musí na RA podrobiť rovnakému procesu autentizácie, aký je požadovaný pri prvotnej registrácii žiadateľa o KC alebo sa musí preukázať dohodnutým heslom pre zrušenie daného KC, ktoré žiadateľ o daný KC uviedol na formulári Žiadosť o vydanie KC.

Autentizácia požiadavky na zrušenie KC je dôležitá, aby sa predišlo svojvoľnému zrušeniu KC neautorizovanou stranou.

Ak sa majiteľ KC nechá na RA zastupovať vo veci zrušenia KC, zastupujúci subjekt sa musí preukázať overenou plnou mocou (notárom alebo matrikou), z textu ktorej je jednoznačne zrejmé vôľa majiteľa KC zrušiť svoj KC. Zastupujúci subjekt je povinný nechať na RA doklad potvrdzujúci jeho plnú moc alebo jeho kópiu (nemusí byť overená). Pracovník RA prevezme a uschová tento doklad, v prípade neoverenej kópie túto porovná s originálom a napíše na ňu text „Potvrdzujem zhodu s originálom“ a doplní dátum a svoj podpis.

RA posúdi oprávnenosť žiadosti o zrušenie KC, v prípade, že je zrejmé, že žiadateľ o zrušenie nie je oprávnenou osobou, RA môže danú žiadosť o zrušenie odmietnuť.

RA tiež odmietne žiadosť, ak žiadateľ nesplní podmienky autentizácie svojej identity (pozri ods. resp. ).

Pracovník RA preverí na aktuálnom CRL platnosť KC, ktorý sa má zrušiť, v prípade KC, ktorý už nie je platný, žiadosť o jeho zrušenie odmietne ako bezpredmetnú – nie je možné zrušiť KC, ktorého platnosť už vypršala alebo ktorý už bol zrušený.

Na prijatie žiadosti o zrušenie KC, ktorú RA považuje za oprávnenú (t.j. ktorá vyhovuje príslušným ustanoveniam tohto dokumentu), RA bezodkladne reaguje tak, že danú žiadosť o zrušenie KC vloží do aplikácie RA resp. informačného systému CA, aby sa mohlo vykonať zrušenie KC, tzn. aby sa KC dostal na najbližšie CRL.

Majiteľ platného KC môže požiadať o zrušenie svojho KC tiež tak, že pošle na kontaktnú email adresu uvedenú v ods. mail, ktorý obsahuje žiadosť s jednoznačne vyjadrenou vôľou zrušiť KC, konkrétne vetu "Žiadam týmto o zrušenie svojho KC číslo nnn." podpísanú zaručeným elektronickým podpisom, ktorý bol vyhotovený použitím jeho KC. Takýmto spôsobom možno požiadať o zrušenie KC aj z dôvodu kompromitácie privátneho kľúča, na podpis žiadosti o zrušenie KC pritom možno použiť KC, ktorého zrušenie požaduje samotná žiadosť.

Majiteľ platného KC môže požiadať o zrušenie svojho KC tiež tak, že pošle na kontaktnú email adresu ACA PSCA uvedenú v časti obyčajný mail (t.j. mail nemusí obsahovať správu podpísanú (zaručeným) elektronickým podpisom), ktorý obsahuje správu s jednoznačne vyjadrenou vôľou zrušiť KC, konkrétne vetu "Žiadam týmto o zrušenie svojho KC číslo nnn." a dohodnuté heslo, ktoré žiadateľ o daný KC uviedol na formulári Žiadosť o vydanie KC.

Žiadosť o zrušenie KC je možné podať aj telefonicky, písomne alebo faxom. Žiadateľ sa pri tom autentizuje pomocou hesla dohodnutého na zrušenie KC.

Ak k zrušeniu KC nedôjde z vôle držiteľa KC, po vydaní nového CRL bude RA bezodkladne informovať (mailom alebo písomne) držiteľa KC o zrušení jeho KC, pričom uvedie, kto a kedy o zrušenie daného KC požiadal. Táto povinnosť je povinnosťou tej konkrétnej RA, ktorá danú žiadosť o zrušenie KC prijala. Ak nebola žiadosť o zrušenie KC prijatá na RA ale priamo na CA (napr. v prípade žiadosti o zrušenie KC na kontaktnú email adresu uvedenú v časti ), táto povinnosť patrí osobe, ktorá žiadosť o zrušenie KC vložila do aplikácie RA.

## **Suspendovanie KC**

Pod termínom „suspendovanie KC“ sa myslí dočasné pozastavenie jeho platnosti. ACA PSCA nepodporuje túto črtu.

KC nebudú môcť považovať za platné (napr. prostredníctvom ich odstránenia z CRL v budúcnosti).

## Zoznamy zrušených KC

### Frekvencia vydávania CRL

ACA PSCA zruší KC najneskôr do 24 hodín od momentu prijatia náležitej žiadosti o zrušenie KC na RA.

CRL sa vydáva s periódou maximálne 24 hodín a to aj vtedy, ak od vydania posledného CRL nedošlo k zrušeniu žiadneho KC ani k žiadnej zmene v stave jednotlivých KC.

ACA PSCA zverejňuje aktuálny zoznam zrušených KC a všetky predchádzajúce zoznamy zrušených KC na svojej internetovej stránke (webe).

ACA OSCA archivuje všetky CRL, ktoré vydala.

ACA PSCA na požiadanie cez email, telefón alebo fax zašle aktuálne CRL prostredníctvom mailu na dohodnutú email adresu podľa možnosti čo najskôr.

ACA PSCA zverejní popis ako získať informácie o zrušení KC, ktoré vydala a objasnenie dôsledkov použitia zastaranej informácie o zrušení KC.

### Požiadavky na overovanie CRL

Použitie zrušeného KC môže spôsobiť škodu alebo mať fatálne následky pre isté aplikácie. Odpoveď na otázku, ako často by sa mali získavať nové údaje o zrušených KC, má byť určená stranou spoliehajúcou sa na KC alebo správcom daného systému. Ak dočasne nie je možné získať informácie o zrušených KC, potom strana spoliehajúca sa na KC musí buď odmietnuť použitie KC alebo urobiť kvalifikované rozhodnutie, ktorým akceptuje riziko, zodpovednosť a dôsledky použitia KC, ktorého autenticita nemôže byť zaručená podľa štandardov tohto dokumentu. Takéto použitie KC môže byť príležitostne nevyhnutné, aby sa vyhovel urgntným operačným požiadavkám.

V čase medzi podaním oprávnenej žiadosti o zrušenie KC a zverejnením zrušeného KC na CRL nesie majiteľ KC všetku zodpovednosť za prípadné škody spôsobené zneužitím jeho KC. Po zverejnení KC v CRL nesie všetku zodpovednosť za prípadné škody spôsobené použitím zrušeného KC strana, ktorá sa na daný zrušený KC spoliehla.

## Overenie aktuálneho stavu KC

Overenie aktuálneho stavu KC sa robí primárne prostredníctvom aktuálneho CRL publikovaného ACA PSCA. Alternatívnou možnosťou na overenie aktuálneho stavu KC je využitie služieb OCSP servera

Softvér používaný klientmi – stranami spoliehajúcimi sa na KC môže voliteľne podporovať (automatizované) overovanie aktuálneho stavu KC v režime on-line. Pretože však táto on-line komunikácia sa vo všeobecnosti nemôže garantovať,

strana spoliehajúca sa na KC má byť pripravená na manuálne (neautomatizované) overovanie aktuálneho stavu KC, na ktoré sa spolieha.

Ak daný softvér nepodporuje overovanie aktuálneho stavu KC v režime on-line, strana spoliehajúca sa na KC je povinná manuálne (tzn. v režime off-line) overiť aktuálny stav KC, na ktorý sa spolieha.

### **Iné použiteľné spôsoby oznamovania o zrušení KC**

ACA PSCA odpovie na dopyt týkajúci sa stavu konkrétneho KC, ak bol tento dopyt urobený telefonicky, faxom alebo emailom.

### **Audit bezpečnosti**

Aby sa vytvorilo optimálne prostredie na výkon auditu, sú implementované mechanizmy zabezpečujúce nepretržité (v režime on-line) kontrolné zaznamenávanie (logovanie) činnosti technických a programových komponentov, ktorými je realizovaná CA resp. RA, čo umožňuje sledovať, dodatočne preskúmať činnosť komponentu a v prípade potreby určiť zodpovednosť konkrétnej osoby za ňou vykonané činnosti.

V rámci ACA PSCA sa uskutočňuje priebežná kontrola funkčnosti a bezpečnosti použitých komponentov a opatrení. Vykonáva sa pravidelná analýza kontrolných záznamov (logov) vytváraných jednotlivými technickými a programovými komponentmi s osobitným dôrazom na zistenie anomálnych udalostí, stavov, chýb funkčnosti a nepovolených aktivít, kontroluje sa dodržiavanie platných bezpečnostných opatrení pracovníkmi ACA PSCA a tiež v prípade potreby sa budú navrhovať vhodné nápravné opatrenia.

Softvér implementujúci ACA PSCA zaznamenáva udalosti týkajúce sa aplikácií vykonávajúcich certifikačné služby. Tieto záznamy budú pokiaľ možno elektronicky podpísané, budú fyzicky chránené a bude zabezpečená ich nedostupnosť zo siete mimo infraštruktúry ACA PSCA.

Zaznamenávajú sa všetky udalosti v rámci pracoviska ACA PSCA. Záznamy môžu byť buď v elektronickej alebo v písomnej forme a môžu byť vytvárané buď automatizovane alebo manuálne.

Bude sa uplatňovať kontrola prístupu k záznamom - prezeranie a spracovanie záznamov sa umožní jednotlivým pracovníkom ACA PSCA v rozsahu týkajúcom sa nimi vykonávaných činností, v celom rozsahu PMA a osobám vykonávajúcim audit.

## Archívne záznamy

Archivácia záznamov sa vykonáva vhodným spôsobom v pravidelných intervaloch, aby sa zabezpečilo dlhodobé uloženie záznamov v zmysle požiadaviek zákona č. 215/2002 Z.z.

Záznamy sa pravidelne archivujú a uchovávajú na bezpečnom mieste s porovnateľnou úrovňou bezpečnosti ako pracovisko ACA PSCA. Záznamy slúžiace na audit sa budú uchovávať minimálne 10 rokov.

Prezeranie archivovaných záznamov sa umožní v celom rozsahu PMA a osobám vykonávajúcim audit.

Modifikovanie alebo odstraňovanie archivovaných informácií nie je prípustné.

Bude zabezpečená utajenosť a integrita archivovaných záznamov a médií.

## Zmena kľúča ACA PSCA

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

K zmene kľúčov ACA PSCA môže dôjsť z dvoch príčin:

Blíži sa čas ukončenia platnosti (expirácie) aktuálne používaných kľúčov ACA PSCA. Toto je normálny stav - 14 dní pred uplynutím platnosti doteraz používaného páru kľúčov ACA PSCA sa na webe ACA PSCA zverejní oznam o blížiacej sa zmene kľúčov ACA PSCA. Po tom, čo sa vygeneruje nový kľúčový pár a NBÚ vydá nový vlastný certifikát ACA PSCA, sa zverejní nový vlastný certifikát ACA PSCA. Každý ďalší vydaný (nový) vlastný certifikát a CRL bude podpísaný novým súkromným kľúčom ACA PSCA.

Je nutné vymeniť aktuálne používané kľúče ACA PSCA z dôvodu ich kompromitácie. Toto je výnimočný, havarijný stav – ACA PSCA bezodkladne oznámi NBÚ, všetkým majiteľom vydaných KCv a verejnosti (NBÚ písomne, okrem toho prostredníctvom svojho webu, elektronickou poštou), že došlo ku kompromitácii kľúčov ACA PSCA. Bezodkladne tiež zruší svoj vlastný certifikát ACA PSCA ako aj všetky KC podpísané použitím kompromitovaného kľúča. ACA PSCA upozorní prostredníctvom svojho webu majiteľov KC, ktoré boli podpísané zrušeným certifikátom ACA PSCA ako aj strany spoliehajúce sa na dané KC, že zrušený certifikát ACA PSCA sa má odstrániť z každej aplikácie, ktorú používajú strany spoliehajúce sa na KC a má byť nahradený novým certifikátom ACA PSCA.

Zmena kľúčov osôb v dôveryhodných rolách ACA PSCA sa nevykonáva.

## Havarijný plán pre mimoriadne udalosti

V prípade kompromitácie kľúča ACA PSCA sa certifikát ACA PSCA zruší. Informácia o jeho zrušení sa musí publikovať okamžite najrýchlejším možným spôsobom. Ďalšie potrebné opatrenia sú uvedené v časti .

V prípade havárie, pri ktorej je vybavenie ACA PSCA poškodené a neschopné prevádzky, ale nie je zničený jej podpisovací kľúč, fungovanie ACA PSCA treba obnoviť podľa možnosti čo najrýchlejšie.

V prípade havárie, pri ktorej je inštalácia ACA PSCA fyzicky poškodená, jej podpisovací kľúč je v dôsledku toho zničený a nie je ho možné obnoviť zo zálohy, sa certifikát ACA PSCA zruší.

ACA PSCA bude mať vypracovaný dokument zaoberajúci sa mimoriadnymi udalosťami a postupmi pre zabezpečenie činnosti ACA PSCA v prípade mimoriadnych udalostí.

## Ukončenie činnosti ACA PSCA

Ešte pred ukončením poskytovania služieb sa vykoná:

ACA PSCA patričným spôsobom, minimálne 6 mesiacov vopred, oznámi informácie o plánovanom ukončení svojej činnosti NBÚ, majiteľom všetkých ňou vydaných platných KC, stranám spoliehajúcim sa na KC a verejnosti. Toto oznámenie sa vykoná prostredníctvom webu ACA PSCA, elektronickej pošty, obyčajnej pošty, registračných autorít, prípadne elektronických médií a tlače.

Ukončia sa všetky prípadné mandátne zmluvy, splnomocnenia a pod. konať v mene ACA PSCA (napr. poskytovať služby RA) s externými subjektmi.

ACA PSCA sa pokúsi uzavrieť zmluvu s inou akreditovanou ACA PSCA, ktorá by zabezpečila kontinuitu v poskytovaní akreditovaných certifikačných služieb.

Všetky dokumenty a archivované dáta od RA aj ostatných zložiek ACA PSCA sa sústredia a archivujú podľa pokynov PMA.

Vykonanie kontroly dodržania zákona o ochrane osobných údajov.

Po ukončení svojej činnosti ACA PSCA nevydá žiaden KC a zabezpečí preukázateľné zničenie podpisových dát (privátneho kľúča) ACA PSCA.

Ak je dôvodom ukončenia činnosti ACA PSCA nejaký dôvod bez vzťahu k bezpečnosti, potom ani certifikát ACA PSCA, ktorá končí činnosť, ani KC podpísané touto ACA PSCA nemusia byť zrušené.

## **Fyzické, procedurálne a personálne bezpečnostné opatrenia**

Bezpečnosť ACA PSCA je založená na súhrne bezpečnostných opatrení v oblasti fyzickej a objektovej, procedurálnej a personálnej bezpečnosti. Tieto bezpečnostné opatrenia sú navrhnuté, dokumentované a aplikované na základe bezpečnostných pravidiel.

### **Fyzické bezpečnostné opatrenia**

Pracovisko ACA PSCA sa nachádza v budove, ktorá je použitia bezpečnostnej techniky nepretržite strážená strážnou službou. Pracovisko ACA PSCA predstavuje režimové pracovisko – miestnosť, ktorá má objektívnu bezpečnosť minimálne na stupni „Dôverné“ v zmysle zákona o ochrane utajovaných skutočností.

Vybavenie ACA PSCA je neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom. Vybavenie pozostáva len z vybavenia vyhradeného na funkcie ACA PSCA, nesmie slúžiť na žiadne účely, ktoré sa netýkajú ACA PSCA.

Neautorizované používanie vybavenia ACA PSCA je zakázané. Sú implementované opatrenia na fyzickú bezpečnosť, ktoré ochránia hardvér a softvér pred neautorizovaným použitím. Kryptografické moduly sú chránené pred krádežou, stratou a neautorizovaným použitím.

Zariadenia a priestory, v ktorých je umiestnené vybavenie ACA PSCA, je postačujúco zásobované elektrickou energiou a klimatizované na vytvorenie spoľahlivého operačného prostredia.

Médiá sú uskladnené tak, aby boli chránené pred náhodným, neúmyselným poškodením (vodou, ohňom, elektromagneticky). Médiá, ktoré obsahujú informácie týkajúce sa bezpečnostného auditu, archív alebo zálohované informácie sú uložené v lokalite oddelenej od vybavenia ACA PSCA.

Zálohy a archivované dokumenty sú uložené na mieste s fyzickými a procedurálnymi opatreniami primeranými prevádzkovanej ACA PSCA a oddelene od priestorov ACA PSCA.

### **Procedurálne bezpečnostné opatrenia**

Dôležitým princípom procedurálnych bezpečnostných opatrení, ktorý podporuje celkovú bezpečnosť ACA PSCA, je princíp „need to know“. ACA PSCA pozostáva z organizačného hľadiska zo služobných rolí („funkcií“), ktoré sú zastávané navzájom disjunktnými skupinami osôb. Týmto sa oddelí prístup k citlivým informáciám, t.j.

každá osoba má prístup len k tým informáciám, ktoré potrebuje na výkon roly, ktorú zastáva.

Tento prístup poskytuje tiež možnosť, že pri niektorých zvlášť dôležitých činnostiach sa môže vyžadovať, aby pri ich vykonávaní bolo prítomných viacero osôb zastávajúcich danú rolu (tzv. princíp "k" z "n"). Dôvodom tu je bezpečnostné hľadisko – prítomné osoby sa navzájom kontrolujú – týmto sa minimalizuje tak možnosť úmyselného zneužitia právomoci nejakou osobou ako aj pravdepodobnosť neúmyselnej chyby alebo omylu.

Každá činnosť v ľubovoľnom systéme, ktorý je súčasťou ACA PSCA, je prístupná len predstaviteľovi tej služobnej roly, ktorá má na danú činnosť oprávnenie. Všetky činnosti sa pritom musia realizovať v súlade s príslušnými zavedenými procedúrami a postupmi.

Pre všetky služobné roly, ktoré kľúčovým spôsobom vplývajú na poskytovanie certifikačných služieb, sú zavedené dokumentované procedúry a postupy.

Zálohy systému postačujúce na obnovu v prípade zlyhania systému sa vykonávajú podľa periodického rozvrhu a použitím vopred definovaných a dokumentovaných postupov a procedúr.

## **Personálne bezpečnostné opatrenia**

Personálne bezpečnostné opatrenia sú zabezpečované internými mechanizmami subjektu – zriaďovateľa.

Prevádzku ACA PSCA zabezpečujú pracovníci s odbornou znalosťou problematiky elektronického podpisu, znalosťou bezpečnostných procedúr v prípade pracovníkov s bezpečnostnými povinnosťami, skúsenosťami s informačnou bezpečnosťou a s vedomosťami z oblasti legislatívy.

Všetky služobné roly sa personálne obsadzujú tak, aby sa vylúčil prípadný konflikt záujmov, ktorý by mohol vytvárať oprávnené pochybnosti o dôveryhodnosti ACA PSCA. Služobné roly, ktoré sú vo vzťahu vzájomnej podriadenosti, sa personálne obsadzujú tak, aby nemohla byť spochybnená nezávislosť a nestrannosť pri výkone kontrolných funkcií.

Osoby vybrané na zastávanie rolí, ktoré si vyžadujú dôveryhodnosť, musia byť zodpovedné a dôveryhodné. Funkcie vykonávané týmito rolami formujú základ dôvery v celú PKI. Aby sa zvýšila pravdepodobnosť, že tieto roly sa budú vykonávať úspešne, uplatňujú sa dva prístupy. Prvým prístupom je zabezpečenie, aby osoba vykonávajúca rolu bola dôveryhodná a náležite vyškolená a poučená. Druhým prístupom je rozdelenie funkcie s rolami medzi niekoľko ľudí tak, aby si ľubovoľná škodlivá činnosť vyžadovala dohodu s inou osobou.

Personál pre ľubovoľnú rolu sa vyberá na základe spoľahlivosti, lojality a dôveryhodnosti. Všetky osoby zastávajúce služobné roly musia byť občanmi

Slovenskej republiky.

Osoby vybrané na zastávanie služobných rolí musia mať odborné znalosti, patričné skúsenosti a kvalifikáciu potrebnú pre ponúkané služby a vykonávané roly.

Všetky osoby zastávajúce služobné roly musia byť náležite poučené a zaškolené.

## Technické bezpečnostné opatrenia

Technická časť infraštruktúry ACA PSCA (hardvér a softvér) bude pozostávať len z bezpečných systémov a oficiálneho softvéru od spoľahlivých producentov a dodávateľov. Architektúra infraštruktúry ACA PSCA je navrhnutá skúsenými odborníkmi použitím komponentov, ktoré spĺňajú štandardy na úrovni súčasných poznatkov.

Osobitná pozornosť musí byť venovaná kryptografickému modulu (HSM modulu), ktorý slúži na generovanie, úschovu a použitie privátneho kľúča ACA PSCA a ktorý patrí k najcitlivejším aktívam. Privátny kľúč ACA PSCA je uložený v HSM module, ktorý je certifikovaný minimálne podľa štandardu FIPS 140-2 level 3.

ACA PSCA používa na ochranu svojho privátneho kľúča kombináciu fyzických, logických a procedurálnych opatrení, ktoré zaručujú bezpečnosť privátneho kľúča. Tieto opatrenia sú popísané v dokumente CPS.

Súčasťou systému ACA PSCA sú zariadenia pre nepretržitú detekciu, monitorovanie a signalizáciu neautorizovaných a neobvyklých pokusov o prístup k jej prostriedkom.

Publikačné aplikácie zabezpečia kontrolu prístupu pred pokusmi o pridanie alebo zmazanie KC alebo modifikovaním iných združených údajov.

Aplikácie súvisiace s udávaním stavu zrušenia zabezpečia kontrolu prístupu pred pokusmi o modifikovanie informácií o stave zrušenia.

Všetky funkcie ACA PSCA, pri ktorých sa používa počítačová sieť, sú zabezpečené pred neautorizovaným prístupom a inými škodlivými činnosťami.

## Profily KC a zoznamov zrušených KC

Profily KC a zoznamov zrušených KC sú stanovené centrálné – ani osoby zastávajúce služobné roly nemôžu svojvoľne meniť štruktúru KC. Štruktúra KC vydávaných ACA PSCA sa môže meniť len na základe rozhodnutia PMA.

### Profily KC

Tento dokument pripúšťa len KC vyhovujúce štandardu X.509 verzie 3.

### Vlastný certifikát ACA PSCA

Algoritmy a dĺžky kľúčov uplatňované o vlastnom certifikáte ACA PSCA:

Algoritmus podpisu (Signature Algorithm):	<b>sha256WithRSAEncryption</b>
Verejný kľúč:	<b>RSA, dĺžka je 4 096 bitov</b>
Algoritmus fingerprintu (Thumbprint Algorithm):	<b>SHA1</b>

Doba platnosti certifikátu ACA PSCA: je stanovená NBÚ, ktorý certifikát vydáva

Obsah položiek vo vlastnom certifikáte ACA PSCA:

Názov položky	Skratka názvu položky	Hodnota položky
Štát (countryName)	C	SK
Mesto (localityName)	L	Bratislava
Firma (organizationName)	O	Viasec a.s.
Útvar vo firme (organizationUnitName)	OU	ACA
Názov (commonName)	CN	PSCA3

**Poznámka:** Použité rozšírenia (certificate extensions) a ich hodnoty vo vlastnom certifikáte ACA PSCA: stanoví NBÚ ako vydavateľ certifikátu

### KC

Štruktúra KC vydávaných ACA PSCA sa môže meniť len na základe rozhodnutia PMA.

Algoritmy a dĺžky kľúčov uplatňované v KC:

Algoritmus podpisu (Signature Algorithm): **Sha256RSA**  
 Verejný kľúč: **RSA, dĺžka je 2 048 bitov**  
 Algoritmus fingerprintu (Thumbprint Algorithm): **SHA1**

Doba platnosti KC je jeden rok (365 dní), ak nebola zmluvne dohodnutá iná doba platnosti.

Obsah položiek rozlišovacieho mena v KC:

Názov položky:	Skratka názvu položky:	Popis položky:	Príklad hodnoty položky:	Typ a max. dĺžka položky:
countryName (Štát)	C	Dvojnaková skratka štátu – dvojmiestny kód podľa ISO 3166 definujúci štátnu príslušnosť subjektu, údaj je povinný	SK	PrintableString 2 znaky
stateOrProvinceName	ST	Názov kraja resp. provincie, údaj je nepovinný	Bratislavsky kraj	UTF8String 128 znakov
localityName (Mesto)	L	Názov lokality, údaj je nepovinný	Bratislava	UTF8String 128 znakov
organizationName (Firma)	O	Názov organizácie, údaj je nepovinný	Info Servis a.s.	UTF8String 64 znakov
organizationUnitName (Útvar vo firme)	OU	Názov útvaru vo firme, údaj je nepovinný	Ekonomicke oddelenie	UTF8String 64 znakov
commonName (Meno a priezvisko)	CN	Meno a priezvisko alebo pseudonym, za ktorým je uvedený reťazec PSEUDONYM, údaj je povinný	Eva Maria Cibulova alebo napr. Udatny kojot PSEUDONYM	UTF8String 64 znakov

SERIALNUMBER	SERIAL NUMBER	Odkaz na identitu fyzickej osoby	PNOSK 9959199999	UTF8String 64 znakov
givenName ((dané mená)	GN	Všetky mená použité v položke CN okrem priezviska, údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený	Eva Maria	UTF8String 64 znakov
Surname (Priezvisko)	SN	Priezvisko z položky CN, údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený	Cibulova	UTF8String 64 znakov
serialNumber		Položka slúži na zabezpečenie jednoznačnosti rozlišovacieho mena (pozri časť 3.1.3)	Položka nebude súčasťou žiadosti o KC – jej hodnotu určí ACA PSCA	

Schematické znázornenie obsahu a nastavenie typických hodnôt jednotlivých položiek používateľského KC:

**Certificate:****Data:****Version: 3 (0x2)****Serial Number: 254 (0xfe)****Signature Algorithm: sha256WithRSAEncryption****Issuer: C=SK, L=Bratislava, O=Viasec s.r.o., OU=ACA, CN=PSCA3****Validity****Not Before: <datum a cas>****Not After : <datum a cas>****Subject: C=SK, L=xxx serialNumber=PNOSK xxxxxxxxxxxx, CN=meno a priezvisko, SN=priezvisko, GN=meno****Subject Public Key Info:****Public Key Algorithm: rsaEncryption****RSA Public Key: (2048 bit)****Modulus****hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:****....****hh:hh:hh:hh:hh:hh:hh:hh:hh****Exponent: 65537 (0x10001)****X509v3 extensions:****....****Signature Algorithm: sha256WithRSAEncryption****hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:hh:****....****hh:hh**

Použitá rozšírenia (certificate extensions) v KC ACA PSCA:

Názov rozšírenia	Hodnota rozšírenia	Kritičnosť
authorityKeyIdentifier	určí sa výpočtom	nekritické
subjectKeyIdentifier	určí sa výpočtom	nekritické
keyUsage	nonRepudiation	kritické
certificatePolicies	Policy:1.3.158.36061701.0.0.0.1.2.2 Policy:0.4.0.1456.1.1 Policy:1.3.6.1.4.1.16043.3.1.1 CPS= <a href="http://www.psc.sk/aca/pdf/cp_aca3q_1_1.pdf">http://www.psc.sk/aca/pdf/cp_aca3q_1_1.pdf</a> ,	nekritické
crlDistributionPoints	URI: <a href="http://www.psc.sk/aca/crl/aca3_psc.crl">http://www.psc.sk/aca/crl/aca3_psc.crl</a>	nekritické
AuthorityInfoAccess	URI: <a href="http://www.psc.sk/aca/certs/aca3q_psc.cer">http://www.psc.sk/aca/certs/aca3q_psc.cer</a>	nekritické
QCstatements	<i>esi4-qcStatement-1</i>	nekritické
SubjectAltNames	email adresa majiteľa KC (rfc822Name), ak bola zadaná v žiadosti o KC	nekritické

## Profily zoznamov zrušených KC

CRL vydávané ACA PSCA3 sú CRL verzie 2.

CRL budú vydávané tou istou ACA PSCA3 ako KC.

CRL obsahuje všetky zrušené KC vrátane tých, ktoré už v čase vydania daného CRL nie sú platné.

Použitá rozšírenia (CRL extensions) v kvalifikovanom CRL:

Názov rozšírenia	Hodnota rozšírenia	Kritičnosť
authorityKeyIdentifier	určí sa výpočtom	nekritické
CRLNumber	určuje sa automaticky	nekritické
issuingDistributionPoint	URI: <a href="http://www.psc.sk/aca/crl/aca3_psc.crl">http://www.psc.sk/aca/crl/aca3_psc.crl</a>	kritické

## **Administrácia špecifikácií**

### **Procedúry na zmenu špecifikácie**

ACA PSCA si vyhradzuje právo v prípade potreby tento dokument aktualizovať alebo zrušiť.

PMA je orgán, ktorý s konečnou platnosťou schvaľuje znenie tohto dokumentu a jeho prípadné zmeny.

Chyby, požiadavky na aktualizáciu alebo navrhované zmeny tohto dokumentu sa majú oznámiť kontaktu uvedenému v časti . Takáto komunikácia musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje resp. navrhuje.

Všetky zmeny motivované PMA majú byť dané na vedomie subjektom, ktorých sa týkajú v lehote aspoň jedného mesiaca.

Každá zmenená verzia tohto dokumentu má byť očíslovaná a evidovaná.

Oprava preklepov, gramatických a štylistických chýb, zmena kontaktných údajov sa nepovažujú za zmeny iniciujúce zmenu verzie tohto dokumentu.

Po uplynutí doby určenej na posúdenie návrhu na zmenu má PMA navrhovanú zmenu prijať, prijať s úpravou alebo odmietnuť.

### **Publikačná a oznamovacia politika**

ACA PSCA bude publikovať informácie týkajúce sa tejto politiky (vrátane tejto politiky ako celku) prostredníctvom webu a v súlade s pravidlami organizácie týkajúcimi sa obsahu webu. Tento dokument bude k dispozícii tiež na každej RA.

### **Procedúry schvaľovania CPS a externej politiky**

PMA urobí rozhodnutie, či dokument CPS je v súlade s touto politikou. Ešte pred zahájením svojej prevádzky má mať ACA PSCA schválený svoj dokument CPS a musí spĺňať všetky jeho požiadavky.

PMA je autorizovaná robiť rozhodnutia, či sú externé dokumenty CPS v súlade s touto politikou.

PMA má informovať o takýchto rozhodnutiach takým spôsobom, aby boli tieto informácie dobre prístupné stranám spoliehajúcim sa na KC.

## Úľavy

PMA má rozhodnúť, či je odchýlka v praxi ACA PSCA podľa aktuálnej politiky prijateľná alebo či je potrebné urobiť zmenu politiky.

PMA môže povoliť úľavu od niektorej požiadavky politiky, aby sa vyhovelo urgentným, nepredvídateľným prevádzkovým požiadavkám. Keď sa povolí úľava, PMA má toto zverejniť pomocou webu prístupného stranám spoliehajúcim sa na KC a má buď iniciovať trvalú zmenu do politiky alebo má pre danú úľavu stanoviť konkrétny časový limit.