

# Certifikačný poriadok Prvej slovenskej certifikačnej autority.

**Verzia dokumentu:** 1.1  
**Dátum:** 22. 4. 2003

© 2003 Viasec, s.r.o.

Všetky práva vyhradené

Vytlačené v Bratislave, Slovenská republika

Tento dokument neprešiel jazykovou úpravou.

# Obsah

---

1	Úvod.....	7
1.1	Prehľad.....	7
1.2	Identifikácia.....	7
1.3	Komunita a použiteľnosť.....	8
1.3.1	Autory.....	8
1.3.2	Koncové entity.....	9
1.3.2.1	Žiadatelia o certifikát PSCA a majitelia certifikátov PSCA.....	9
1.3.2.2	Strany spoliehajúce sa na certifikáty.....	9
1.3.3	Použiteľnosť.....	9
1.4	Kontaktné detaily.....	11
2	Všeobecné ustanovenia.....	12
2.1	Povinnosti.....	12
2.1.1	Povinnosti CA.....	12
2.1.2	Povinnosti RA.....	12
2.1.3	Povinnosti majiteľa certifikátu.....	13
2.1.4	Povinnosti strán spoliehajúcich sa na certifikáty.....	13
2.1.5	Povinnosti správy repozitára.....	14
2.2	Právne záruky.....	14
2.3	Finančná zodpovednosť.....	14
2.4	Rozhodcovské konanie a riešenie sporov.....	15
2.5	Poplatky.....	15
2.6	Zverejňovanie informácií a repozitár.....	16
2.6.1	Zverejňovanie informácií o CA.....	16
2.6.2	Frekvencia zverejňovania informácií.....	16
2.6.3	Kontroly prístupu.....	16
2.6.4	Repozitáre.....	16
2.7	Audit zhody.....	17
2.7.1	Frekvencia auditu zhody pre danú entitu.....	17
2.7.2	Identita audítora a kvalifikačné požiadavky na neho.....	17
2.7.3	Témy pokrývané auditom zhody.....	17
2.7.4	Akcie vykonané na odstránenie nedostatkov.....	17
2.7.5	Zaobchádzanie s výsledkami auditu.....	17
2.8	Dôvernosť.....	18
2.8.1	Typy informácií, ktoré sa majú chrániť.....	18
2.8.2	Okolnosti uvoľnenia dôverných informácií.....	18
2.9	Práva vyplývajúce z intelektuálneho vlastníctva.....	19
3	Identifikácia a autentizácia.....	20
3.1	Prvotná registrácia.....	20
3.1.1	Typy mien.....	20
3.1.2	Potreba zmysluplnosti mien.....	20
3.1.2.1	Osobný certifikát.....	21
3.1.2.2	Certifikát pre server.....	21
3.1.3	Jedinečnosť mien.....	22
3.1.4	Procedúra riešenia sporov pri kolízii mien.....	22
3.1.5	Rozpoznanie, autentizácia a rola obchodných značiek.....	22

3.1.6	Preukazovanie vlastníctva privátneho kľúča.....	23
3.1.7	Autentizácia identity organizácie.....	23
3.1.8	Autentizácia identity fyzickej osoby.....	24
3.1.9	Autentizácia identity komponentu.....	25
3.1.10	Predkladané doklady.....	26
3.1.11	Kontrola údajov na predložených dokladoch.....	26
3.2	Vydanie následného certifikátu.....	27
3.3	Vydanie následného certifikátu po zrušení starého.....	28
3.4	Žiadosť o zrušenie certifikátu.....	28
4	Prevádzkové požiadavky.....	29
4.1	Žiadanie o certifikát.....	29
4.1.1	Doručenie verejného kľúča žiadateľa o certifikát vydavateľovi certifikátu.....	29
4.2	Vydanie certifikátu.....	29
4.2.1	Doručenie privátneho kľúča majiteľovi certifikátu.....	30
4.2.2	Doručenie verejného kľúča CA používateľom.....	30
4.3	Prevzatie certifikátu.....	30
4.4	Suspendovanie certifikátu a zrušenie certifikátu.....	31
4.4.1	Zrušenie certifikátu.....	31
4.4.1.1	Okolnosti zrušenia certifikátu.....	31
4.4.1.2	Kto môže žiadať o zrušenie certifikátu.....	31
4.4.1.3	Procedúra žiadosti o zrušenie certifikátu.....	32
4.4.1.4	Čas na zrušenie certifikátu.....	33
4.4.2	Suspendovanie certifikátov.....	33
4.4.3	Zoznamy zrušených certifikátov.....	33
4.4.3.1	Frekvencia vydávania CRL.....	33
4.4.3.2	Požiadavky na overovanie CRL.....	34
4.4.4	Overenie aktuálneho stavu certifikátu.....	34
4.4.5	Iné použiteľné spôsoby oznamovania o zrušení certifikátu.....	34
4.5	Audit bezpečnosti.....	34
4.5.1	Typy zaznamenávaných udalostí.....	34
4.6	Archívne záznamy.....	35
4.7	Zmena kľúča CA.....	35
4.8	Havarijný plán pre mimoriadne udalosti.....	35
4.9	Ukončenie činnosti CA.....	36
5	Fyzické, procedurálne a personálne bezpečnostné opatrenia.....	37
6	Technické bezpečnostné opatrenia.....	38
6.1	Generovanie páru kľúčov a inštalácia.....	38
6.1.1	Generovanie páru kľúčov.....	38
6.1.2	Doručenie privátneho kľúča majiteľovi certifikátu.....	38
6.1.3	Dĺžky kľúčov.....	38
6.2	Ochrana kľúčov.....	38
6.2.1	Ochrana privátneho kľúča CA.....	38
6.2.2	Ochrana ostatných privátnych kľúčov.....	39
6.3	Manažment páru kľúčov.....	39
6.4	Počítačové bezpečnostné opatrenia.....	39
7	Profily certifikátov a zoznamov zrušených certifikátov.....	40
7.1	Profily certifikátov.....	40
7.1.1	Certifikát CA PSCA.....	40

7.1.2	Certifikáty PSCA.....	41
7.2	Profily zoznamov zrušených certifikátov.....	41
8	Administrácia špecifikácií.....	42
8.1	Procedúry na zmenu špecifikácie.....	42
8.2	Publikačná a oznamovacia politika.....	42
8.3	Procedúry schvaľovania CPS a externej politiky.....	42
8.4	Úľavy.....	42

## Zoznam použitých skratiek

---

<b>CA</b>	Certification Authority - Certifikačná autorita
<b>CP</b>	Certificate Policy - Certifikačný poriadok
<b>CPS</b>	Certificate Practice Statement - Vykonávacie smernice certifikačnej autority
<b>CRL</b>	Certification Revocation List - Zoznam zneplatnených certifikátov
<b>HSM</b>	Hardware Security Modul
<b>PMA</b>	Policy Management Authority - Vydavateľ certifikačných politík
<b>ACA</b>	Administrátor certifikačnej autority
<b>NBÚ</b>	Národný bezpečnostný úrad
<b>RA</b>	Registration Authority - Registračná autorita

# 1 Úvod

Tento dokument definuje certifikačnú politiku, ktorú uplatňuje Prvá slovenská certifikačná autorita (ďalej ako PSCA) pri implementovaní infraštruktúry verejných kľúčov (ďalej ako PKI) pozostávajúcej z produktov a služieb, ktoré poskytujú a spravujú certifikáty podľa štandardu X.509 pre kryptografiu verejných kľúčov. Certifikáty identifikujú meno nachádzajúce sa v certifikáte a zväzujú toto meno s príslušným párom kľúčov.

Pri aplikovaní tejto politiky na konkrétne aplikácie sa môže vyžadovať vyššia úroveň zabezpečenia ako je uvedená v tejto certifikačnej politike (ďalej CP).

## 1.1 Prehľad

Táto CP je politikou, na základe ktorých je zriadená a prevádzkovaná certifikačná autorita (ďalej ako CA) podliehajúca Prvej slovenskej certifikačnej autorite, ktorú prevádzkuje spoločnosť Viasec, s.r.o., ktorá je dcérskou spoločnosťou spoločnosti Slovanet, a.s. – súčasťou skupiny SlovaNet Holding B.V.

CP bola vytvorená 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 (RFC2527) a Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile (RFC3280).

Tento dokument definuje vytváranie a správu certifikátov s verejnými kľúčmi podľa štandardu X.509 verzie 3 pre ich použitie v aplikáciách vyžadujúcich si bezpečnú komunikáciu medzi počítačovými systémami pripojenými na počítačovú sieť.

Kostrová časť takejto počítačovej siete môže byť pritom nechránenou sieťou ako napr. Internet.

## 1.2 Identifikácia

Názov: Certifikačný poriadok Prvej slovenskej certifikačnej autority  
Skratka názvu: CP PSCA  
Verzia: apríl 2003

Tomuto dokumentu je priradený identifikátor objektu (OID) 1.3.6.1.4.1.16043.2.1.1.

Tento poriadok sa týka všetkých certifikátov vydávaných certifikačnou autoritou s názvom „Prvá slovenská certifikačná autorita“.

## 1.3 Komunita a použiteľnosť

### 1.3.1 Authority

**Autorita pre správu politiky** (Policy Management Authority (ďalej ako PMA) je zložka PSCA ustanovená za účelom:

- dohľadu na vytváranie a aktualizáciu certifikačných politík, vrátane vyhodnocovania zmien a plánov na implementovanie ľubovoľných prijatých zmien
- revízie CPS PSCA, aby sa zaručilo, že prax CA vyhovuje príslušnej certifikačnej politike
- revízie výsledkov auditov zhody, aby sa určilo, či CA adekvátne dodržiava ustanovenia schváleného dokumentu CPS, ďalej potom dávanie odporúčaní pre CA ohľadne nápravných akcií a iných vhodných opatrení
- riadenia a usmerňovania činnosti certifikačnej autority a registračných autorít
- na požiadanie robí výklad ustanovení CPS a svojich pokynov pre RA a CA
- vykonáva funkciu audítora, prípadne touto činnosťou poverí samostatného pracovníka
- vykonávania revízie CPS certifikačnej autority prostredníctvom analýzy CPS, aby sa zaručilo, že prax CA vyhovuje príslušnej certifikačnej politike

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

**Certifikačná autorita (CA)** je entita autorizovaná PMA na vytváranie, podpisovanie a vydávanie certifikátov s verejným kľúčom.

Pod pojmom certifikačná autorita resp. CA sa ďalej v tomto dokumente myslí certifikačná autorita PSCA.

CA je zodpovedná za všetky aspekty vydávania a správy certifikátov, vrátane kontroly nad procesom registrácie, procesom identifikácie a autentizácie, procesom vytvárania certifikátov, publikácie certifikátov, zrušenia certifikátov. CA zaručuje, že všetky aspekty jej služieb a operácií a infraštruktúry zviazanej s certifikátmi vydanými podľa tohoto CPS sa vykonávajú v súlade s požiadavkami a ustanoveniami jej pravidiel na výkon certifikačných činností.

V prípade hierarchickej architektúry, CA musia byť podriadené koreňovej CA, pričom medzi danou CA a koreňovou CA môže byť najviac jedna prostredná CA. Charakter podriadenosti bude popísaný v jednom alebo viacerých dokumentoch CPS, ktoré boli vytvorené pre túto hierarchiu a bude implementovaný prostredníctvom rozšírení certifikátov.

**Registračná autorita (RA)** je entita, ktorá na základe rozhodnutia CA zbiera a verifikuje identity žiadateľov o certifikát a iné informácie, ktoré sa dostanú do certifikátov. RA musí vykonávať svoje aktivity v súlade s CPS schválenou PMA.

Spoločný termín pre CA a RA je tzv. **authority na správu certifikátov** (Certificate Management Authority, ďalej ako CMA). Termín CMA sa bude používať, keď funkciu

možno priradiť buď CA alebo RA alebo keď sa požiadavka týka súčasne CA aj RA. Rozdelenie zodpovednosti pri registrácii žiadateľa o certifikát medzi CA a RA sa môže líšiť pri viacerých implementáciách tejto certifikačnej politiky. Toto rozdelenie zodpovednosti bude popísané v CPS pre danú CA.

## **1.3.2 Koncové entity**

### **1.3.2.1 Žiadatelia o certifikát PSCA a majitelia certifikátov PSCA**

Žiadateľ o certifikát PSCA je entita, ktorej meno sa objaví ako subjekt v certifikáte a ktorá sa zaviazne, že bude používať svoj kľúč a certifikát v súlade s touto politikou.

Žiadateľ o certifikát sa prevzatím svojho certifikátu stáva majiteľom daného certifikátu.

Môžu nimi byť nasledovné kategórie, ktoré môžu potrebovať bezpečnú komunikáciu:

- zákazníci PSCA – zákazníkom PSCA sa môže stať každá svojprávná plnoletá fyzická osoba alebo právnická osoba, ktorá splní podmienky pre registráciu zákazníka uvedené v tomto dokumente.
- pracovné stanice, firewally, routery, servery a iné komponenty infraštruktúry. Tieto komponenty musia byť pod právomocou (správou) konkrétnych osôb, ktoré preberajú certifikáty a zodpovedajú za správnu ochranu a používanie príslušných privátnych kľúčov.

Podmienky, ktoré musí žiadateľ o certifikát PSCA splniť, aby mu bol vydaný certifikát PSCA, definuje tento dokument.

### **1.3.2.2 Strany spoliehajúce sa na certifikáty**

Stranou spoliehajúcou sa na certifikát je entita, ktorá tým, že používa cudzí certifikát na overenie integrity digitálne podpísanej správy alebo na ustanovenie bezpečnej komunikácie s majiteľom certifikátu, sa spolieha na platnosť väzby majiteľa certifikátu s daným verejným kľúčom. Strana spoliehajúca sa na certifikát môže použiť informáciu z certifikátu na určenie vhodnosti certifikátu na dané použitie.

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

## **1.3.3 Použiteľnosť**

Certifikáty PSCA sú vo všeobecnosti určené na zabezpečenie komunikácie pomocou softvéru resp. hardvéru, ktorý podporuje využitie certifikátov vyhovujúcich špecifikácii X.509 verzie 3.

Účelom vydávania certifikátov PSCA je vo všeobecnosti poskytnúť používateľovi certifikátu také prostriedky na zabezpečenie komunikácie (ktorými sú certifikáty), aby mohol využívať výhody bezpečnej komunikácie s minimálnymi nákladmi, napr. vhodným používaním bežne dostupného softvéru ako je napr. prehliadač Microsoft Explorer, poštoví klienti Microsoft Outlook Express, Microsoft Outlook, softvér na strane servera typu Apache, Microsoft IIS a podobne.

Certifikáty PSCA môžu byť vo všeobecnosti použité:

- pre potreby zabezpečenia elektronickej pošty (podpisovanie a/alebo šifrovanie správ posielaných elektronicou, neodmietnuteľnosť zodpovednosti za odoslanú správu elektronickej pošty)
- pre potreby zabezpečenia WWW komunikácie (dôveryhodná identifikácia webovského servera resp.klienta)
- pre potreby zabezpečovacích mechanizmov pracovných staníc používateľov
- pre potreby interných procesov PKI (bezpečná komunikácia medzi komponentami PKI a pod.)

PSCA vydáva zákazníkom tieto typy certifikátov:

- osobné certifikáty – určené v prvom rade pre potreby zabezpečenia elektronickej pošty
- certifikáty pre server – určené v prvom rade pre potreby zabezpečenia WWW komunikácie
- testovacie certifikáty – určené na oboznámenie sa s problematikou a technológiou používania certifikátov. Doba ich platnosti je obmedzená (spravidla na 30 dní). Údaje v nich uvedené PSCA neoveruje a nenesie žiadnu zodpovednosť za ich pravdivosť a ani za používanie týchto certifikátov a jeho prípadné dôsledky. Testovacie certifikáty sa nedajú zrušiť a ani sa nevytvárajú pre ne zoznamy zrušených certifikátov.

Tento dokument taxatívne nevymedzuje aplikácie, s ktorými môžu byť používané certifikáty PSCA – čo znamená, že rozhodnutie, s akým softvérom (aplikáciou) resp. s akou verziou softvéru (aplikácie) budú používať certifikáty je úplne v kompetencii majiteľov certifikátov resp. strán spoliehajúcich sa na certifikáty.

PSCA v tomto smere môže vydávať používateľom certifikátov len odporúčania, ktoré nie sú pre nich záväzné.

Certifikáty PSCA, ktoré boli vydané pre zložky PMA, sa môžu používať výlučne na výkon činností týchto zložiek a to len na ich pracoviskách.

Dokument CPS môže presnejšie vymedziť:

- zoznam aplikácií, pre ktoré sú vydávané certifikáty vhodné
- zoznam aplikácií, pre ktoré je použitie vydávaných certifikátov obmedzené
- zoznam aplikácií, pre ktoré je použitie vydávaných certifikátov zakázané

## 1.4 Kontaktné detaily

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

Adresa: Viasec, s.r.o.  
Prvá slovenská certifikačná autorita  
Záhradnícka 151  
821 08 Bratislava 2

Adresa elektronickej pošty: [oper@psca.sk](mailto:oper@psca.sk)  
www adresa: <http://www.pzca.sk>

Telefón a fax: +421 2 5020 2214

## 2 Všeobecné ustanovenia

### 2.1 Povinnosti

#### 2.1.1 Povinnosti CA

CA, ktorá vydáva certifikáty založené na tejto politike, musí vyhovovať ustanoveniam tohto dokumentu vrátane nasledujúcich ustanovení:

- konať v súlade s ustanoveniami schváleného dokumentu CPS
- zaručiť, že sa akceptujú registračné informácie jedine od RA, ktoré rozumejú tejto politike a sú zaviazané konať v súlade s ňou
- dávať do certifikátov len správne a náležité informácie a archivovať doklady dokazujúce správnosť údajov dávaných do certifikátov
- garantovať, že majiteľ certifikátu je viazaný povinnosťami v súlade s časťou 2.1.3 tejto politiky a informovaný o následkoch neplnenia týchto povinností
- zrušiť certifikáty majiteľov, ak sa zistí, že títo konali v rozpore so svojimi povinnosťami
- prevádzkovať v režime on-line repozitár, ktorý vyhovuje ustanoveniam uvedeným v časti 2.1.5

Ak sa zistí, že CA nekoná v súlade s týmito povinnosťami, uplatnia sa na ňu opatrenia uvedené v časti 2.5.5.

#### 2.1.2 Povinnosti RA

RA, ktorá vykonáva registračné funkcie popísané v tejto politike, 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.

Rozdelenie zodpovednosti medzi CA a RA sa môže líšiť pri viacerých implementáciách tejto certifikačnej politiky. Toto rozdelenie zodpovednosti bude popísané v CPS pre danú CA a RA. Napr. RA môže len zhromažďovať informácie pre CA. CA má výlučnú zodpovednosť za garancie, že certifikáty, ktoré podpisuje, sa vytvárajú a spravujú v súlade s touto politikou a že procesy vytvárania, správy a zrušenia certifikátov sú vykonávané len takými osobami, ktoré rozumejú príslušným požiadavkám certifikačnej politiky a sú zaviazané ich dodržiavať.

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

Na RA sa realizuje priamy kontakt medzi zákazníkmi a PSCA.

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

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

RA je pri výkone svojich činností povinná riadiť sa príslušnými dokumentami, ako je CPS a vykonávacie smernice.

### **2.1.3 Povinnosti majiteľa certifikátu**

Povinnosťou majiteľa certifikátu je:

- neustále chrániť svoje privátne kľúče v súlade s touto politikou a tiež ako je stanovené v jeho zmluve o vydaní a používaní certifikátu PSCA
- bezodkladne upovedomiť CMA, ktorá vydala jeho certifikát, o podozrení, že jeho privátny kľúč bol kompromitovaný alebo stratený. Toto upovedomenie musí byť urobené prostredníctvom mechanizmu, ktorý je v súlade s dokumentom CPS danej CA
- dodržiavať všetky lehoty, podmienky a obmedzenia uložené na používanie svojich privátnych kľúčov a certifikátov
- precízne sa identifikovať a vyjadrovať pri ľubovolnej komunikácii s RA resp. CA
- používať poskytnuté certifikáty len na patričné účely

Povinnosti majiteľa certifikátu sa týkajú aj osoby, ktorá prevzala certifikáty pre ňou spravované komponenty. (pozri časť 5.2.1.4)

Majiteľ certifikátu, ktorý nedodržuje resp. nedodržiaval svoje povinnosti, nemá nárok na náhradu prípadnej škody.

### **2.1.4 Povinnosti strán spoliehajúcich sa na certifikáty**

Strany spoliehajúce sa na certifikáty vydané podľa tejto politiky sú povinné:

- používať certifikát na účel, pre ktorý bol vydaný, ako je to dané informáciami v certifikáte
- predtým, ako sa na certifikát spoľahnú, overovať každý certifikát na platnosť (tzn. overovať, že certifikát je v danom čase platný a že sa nenachádza na aktuálnom zozname zrušených certifikátov vydanom PSCA)
- vytvoriť vzťah dôvery k CA, ktorá vydala daný certifikát, verifikovaním certifikačnej cesty v súlade so štandardom X.509 verzie 3 (tzn. napr. zabezpečiť, aby používaný softvér resp. hardvér mal pre svoju správnu funkciu vhodným spôsobom k dispozícii certifikát CA PSCA, aby bolo možné overiť digitálny podpis CA na danom certifikáte)

- uchovávať originálne podpísané dáta, aplikácie potrebné na čítanie a spracovanie týchto dát a kryptografické aplikácie potrebné na overovanie digitálnych podpisov týchto dát, pokiaľ môže byť potrebné overovať podpis týchto dát

### **2.1.5 Povinnosti správy repozitára**

Správa repozitára, ktorý podporuje CA pri publikovaní informácií podľa tejto politiky, sú povinná:

- udržiavať prístupnosť informácií podľa ustanovení tejto politiky pre publikovanie informácií o certifikátoch
- poskytovať mechanizmus riadenia prístupu dostatočný na ochranu informácií uložených v repozitári podľa časti 2.4.3

Prevádzkovanie a spravovanie repozitára patrí medzi povinnosti CA.

## **2.2 Právne záruky**

Tento poriadok 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 (vyhlášky NBÚ č. 537/2002 Z.z., č. 538/2002 Z.z., č. 539/2002 Z.z., č. 540/2002 Z.z., č. 541/2002 Z.z., č. 542/2002 Z.z.).

CPS, na základe ktorej sa prevádzkuje CA, definuje právne záruky, ktoré obsahujú popis zodpovednosti každého subjektu, napr. záruky a obmedzenia poskytovaných záruk, ohraničenie možných strát a náhrad, ďalšie obmedzenia zodpovednosti.

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

PSCA poskytuje záruku, že ňou vydaný certifikát bude vyhovovať štandardu X.509 verzie 3 a bude v súlade s týmto dokumentom.

## **2.3 Finančná zodpovednosť**

CPS, na základe ktorej sa prevádzkuje CA, definuje limity finančnej zodpovednosti CA a podmienky, za akých môžu byť uplatnené finančné nároky voči CA.

CA PSCA poskytuje záruku na použitie ňou vydaných certifikátov pri transakciách, ktorých hodnota nepresahuje písomne dohodnutý limit záruky za predpokladu, že boli dodržané príslušné ustanovenia tohto dokumentu.

Hodnota limitu záruky môže byť dohodnutá v písomnej forme, implicitne je to suma 1 000 Sk, ak nebolo písomnou formou dohodnuté inak. Limit záruky definuje maximálnu

sumu, ktorú poskytne zriaďovateľ PSCA ako odškodnenie za škodu vzniklú v dôsledku použitia certifikátu PSCA.

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

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

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

Akákoľvek žiadosť o náhradu škody musí byť podaná písomne.

## **2.4 Rozhodcovské konanie a riešenie sporov**

Pre potreby interpretácie politiky alebo riešenia sporov sa možno písomne obrátiť na najbližšiu vyššiu inštanciu. Inštancie sú usporiadané vzostupne v poradí:

- RA
- CA

PMA rozhoduje s konečnou platnosťou v prípade akýchkoľvek sporov o interpretácii alebo použiteľnosti tejto politiky.

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.

## **2.5 Poplatky**

Povinnosťou CA je vhodným spôsobom zverejniť platný cenník svojich služieb.

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

CA bude vhodným spôsobom zverejňovať platný cenník svojich služieb.

Tento cenník bude v každom prípade zverejnený prostredníctvom webu PSCA (www.pzca.sk).

## **2.6 Zverejňovanie informácií a repozitár**

### **2.6.1 Zverejňovanie informácií o CA**

CA musí poskytovať v on-line režime repozitár, ktorý je prístupný majiteľom certifikátov a stranám spoliehajúcim sa na certifikáty a ktorý obsahuje:

1. certifikáty vydané v súlade s touto politikou
2. aktuálne CRL
3. certifikát certifikačnej authority (patriaci k jej podpisovaciemu kľúču)
4. kópiu tejto politiky vrátane prípadných úľav pre CA schválených PMA

### **2.6.2 Frekvencia zverejňovania informácií**

Certifikát sa publikuje čo najskôr po jeho vytvorení, akonáhle prevezme certifikát majiteľ certifikátu. Výnimkou sú certifikáty, pri žiadosti o ktoré zákazník výslovne uviedol, že si ich zverejnenie neželá

CRL sa publikuje ako je špecifikované v časti 4.4.3.1.

Všetky informácie, ktoré majú byť publikované v repozitári, musia byť publikované bezodkladne, hneď ako sa CA takúto informáciu dozvie. CA špecifikuje vo svojom dokumente CPS časové limity, v rámci ktorých bude publikovať rôzne typy informácií.

### **2.6.3 Kontroly prístupu**

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

### **2.6.4 Repozitáre**

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

Funkciu repozitára CA PSCA bude zastávať web PSCA, ktorého domovská stránka má URL [www.pzca.sk](http://www.pzca.sk) a ktorý je prostredníctvom Internetu verejne prístupný majiteľom certifikátov, stranám spoliehajúcim sa na certifikáty a verejnosti vôbec.

## **2.7 Audit zhody**

### **2.7.1 Frekvencia auditu zhody pre danú entitu**

CA sa musí podrobiť každoročnému auditu o zhode. Okrem toho každá CA má právo požadovať pravidelné a nepravidelné revízie činností jej podriadených CMA, aby sa potvrdilo, že podriadená CMA funguje v súlade s bezpečnostnými praktikami a procedúrami popísanými v príslušnom dokumente CPS.

### **2.7.2 Identita audítora a kvalifikačné požiadavky na neho**

Audítor musí byť kompetentný v oblasti auditov o zhode a musí byť dôkladne oboznámený s dokumentom CPS auditovanej CMA.

### **2.7.3 Témy pokrývané auditom zhody**

Účelom auditu o zhode má byť záruka, že CA má vyhovujúci systém práce, ktorý garantuje kvalitu služieb, ktoré CA poskytuje a ktorý garantuje, že CA koná v súlade so všetkými požiadavkami tejto politiky a svojho dokumentu CPS. Všetky aspekty prevádzky CA vzťahujúce sa k tejto politike majú byť predmetom auditov zhody.

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

Keď audítor zistí rozpor medzi prevádzkou CMA a ustanoveniami jej dokumentu CPS, musia sa uskutočniť nasledujúce akcie:

- audítor zaznamená rozpor
- audítor upovedomí o rozpore subjekty definované v časti 2.7.5
- CA navrhne PMA zodpovedajúce opatrenie na nápravu vrátane očakávaného času potrebného na jeho realizáciu

PMA určí vhodné opatrenie na nápravu a to prípadne až po zrušenie certifikátu CA. Po náprave nedostatkov PMA obnoví činnosť CA.

### **2.7.5 Zaobchádzanie s výsledkami auditu**

Audítor zhody urobí pre PMA zápis o výsledkoch auditu o zhode. Výsledky budú oznámené v súlade s časťou 2.6 auditovanej CA a jej nadradenej CA, ak táto existuje. Vykonanie opatrení na nápravu má byť dané na vedomie príslušnej autorite. Na potvrdenie vykonania a účinnosti opatrení na nápravu sa môže požadovať špeciálny audit zhody alebo čiastkový audit zhody zameraný na daný aspekt činnosti auditovaného subjektu.

## 2.8 Dôvernosť

### 2.8.1 Typy informácií, ktoré sa majú chrániť

Dôvernými informáciami podliehajúcimi zodpovedajúcej ochrane sú:

- privátny kľúč CA PSCA používaný na vytváranie elektronického podpisu pri vydávaní certifikátov PSCA
- privátne kľúče patriace zložkám PSCA
- infraštruktúra (napr. dokumenty, procedúry, postupy, súbory, skripty, heslá, pass frázy a pod.) slúžiaca na prevádzku CA PSCA, vrátane jej RA
- osobné údaje zákazníkov podliehajúce ochrane v zmysle zákona č. 428/2002 Z.z. o ochrane osobných údajov

Certifikát by mal obsahovať len také informácie, ktoré sú dôležité a nevyhnutné na vykonávanie bezpečných transakcií pomocou certifikátu.

Za účelom náležitej správy certifikátov CMA môže požadovať, aby sa pri správe certifikátov v rámci CA používali aj informácie, ktoré nie sú uvedené v certifikátoch (napr. identifikačné čísla dokladov, adresy, telefónne čísla). Lubovoľná takáto informácia má byť explicitne definovaná v dokumente CPS. So všetkými informáciami uloženými v rámci CA 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 certifikátu zákazníkovi je, aby v zmysle Zákona o ochrane osobných údajov dal písomný súhlas, že PSCA bude uschovávať jeho osobné údaje, ktoré získala pri jeho registrácii. PSCA bude tieto údaje archivovať a spracovávať v rozsahu požadovanom zákonmi a vyhláškami, ktoré platia pre činnosť certifikačných autorít.

Všetky informácie, ktoré sú uvedené v certifikáte a teda sú zverejňované prostredníctvom repozitára, nie sú klasifikované ako dôverné a považujú sa za verejné. Zoznam zrušených certifikátov (CRL) tiež nie je považovaný za dôverný.

### 2.8.2 Okolnosti uvolnenia dôverných informácií

CA nezverejní žiadne informácie týkajúce sa žiadateľa o certifikát alebo majiteľa certifikátu žiadnej tretej strane, kým to nie je povolené touto politikou, požadované zákonom alebo príkazom kompetentného súdu. Každá požiadavka na uvolnenie informácií má byť autentizovaná a zadokumentovaná.

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 PSCA a kompetentných štátnych orgánov ako sú polícia, súdy, prokuratúra.

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

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

## 3 Identifikácia a autentizácia

### 3.1 Prvotná registrácia

Prijímané žiadosti o certifikát PSCA musia vyhovovať štandardu PKCS #10 alebo SPKAC a musia byť vo formáte PEM, ak nebolo so zákazníkom vopred dohodnuté inak.

#### 3.1.1 Typy mien

Každá CA má byť schopná vytvárať certifikáty, ktoré obsahujú rozlišovacie mená v zmysle X.500 ( X.500 Distinguished Name, ďalej ako rozlišovacie meno ). Vo všeobecnosti CA nemá priradovať rozlišovacie mená. Žiadatelia o certifikát si sami zvolia rozlišovacie meno, ktoré má byť v ich certifikáte.

#### 3.1.2 Potreba zmyslupnosti mien

Používané mená majú čo najjednoduchšie identifikovať osoby alebo iné objekty, ktorým sú priradené. CMA má zaručovať, že existuje vzťah patričnosti (príslušnosti, členstva) medzi majiteľom certifikátu a ľubovoľnou organizáciou alebo organizačnou jednotkou, ktorá je identifikovaná ľubovoľnou časťou ľubovoľného mena v certifikáte daného majiteľa.

Keď sa používajú rozlišovacie mená, položka common name má reprezentovať majiteľa certifikátu spôsobom, ktorý je pre človeka ľahko pochopiteľný. V prípade osoby to bude typicky jej právoplatné meno a priezvisko. V prípade zariadenia to môže byť napr. názov modelu a sériové číslo alebo názov procesu a aplikácie, úplné doménové meno, registrovaná IP adresa a podobne.

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

Používanie pseudonymov, prezýviek, krycích mien, aliasov a podobne (tzv. nicknames) v certifikátoch sa nepovoľuje – CMA odmietne prijať žiadosť o certifikát, ktorá by obsahovala v rozlišovacom mene položku s takouto hodnotou.

CA má právo odmietnuť vydať certifikát, ktorý by obsahoval údaje porušujúce princíp zmyslupnosti mien, zvláštny dôraz sa pritom kladie na údaj v položke commonName.

Požiadavka na zmyslupnosť sa pritom vzťahuje na hodnotu ľubovoľnej položky v rozlišovacom mene. Porušenie tohto princípu môže byť príčinou odmietnutia vytvoriť certifikát z danej žiadosti o certifikát.

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

Rozlišovacie meno používané v certifikátoch PSCA pozostáva z nasledujúcich položiek s nižšie uvedeným významom:

### 3.1.2.1 Osobný certifikát

<i>Názov položky:</i>	<i>Skratka názvu položky:</i>	<i>Popis položky:</i>
Štát (countryName)	C	Dvojnaková skratka štátu, SK pre Slovenskú republiku, údaj je povinný
Mesto (localityName)	L	Názov lokality, údaj je nepovinný
Firma (organizationName)	O	Názov organizácie, údaj je nepovinný
Útvar vo firme (organizationUnitName)	OU	Názov útvaru vo firme, údaj je nepovinný
Meno a priezvisko (commonName)	CN	Meno a priezvisko, údaj je povinný
Email adresa (emailAddress)	Email, E	Email adresa, údaj je povinný

### 3.1.2.2 Certifikát pre server

<i>Názov položky:</i>	<i>Skratka názvu položky:</i>	<i>Popis položky:</i>
Štát (countryName)	C	Dvojnaková skratka štátu, SK pre Slovenskú republiku, údaj je povinný
Názov štátu (stateOrProvinceName)	ST	Názov štátu, napr. Slovenska republika, Slovakia a pod., údaj je nepovinný
Mesto (localityName)	L	Názov lokality, údaj je nepovinný
Firma (organizationName)	O	Názov organizácie, údaj je nepovinný
Útvar vo firme (organizationUnitName)	OU	Názov útvaru vo firme, údaj je nepovinný
Názov komponentu (commonName)	CN	Názov komponentu, údaj je povinný
Email adresa (emailAddress)	Email, E	Email adresa, údaj je nepovinný

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

Použitie špeciálnych znakov (napr. čiarka, pomlčka, =, / a iné) treba obmedziť na minimálnu nutnú mieru, odporúčame prípadne tieto znaky použiť až po dohode s PSCA, v opačnom prípade si PSCA vyhradzuje právo odmietnuť takúto žiadosť o certifikát.

### **3.1.3 Jedinečnosť mien**

Jedinečnosť mien v rámci celej komunity majiteľov certifikátov musí byť vynútená.

CA a RA musia presadiť jedinečnosť mien v rámci celého menného priestoru. Keď sa používajú zriedkavejšie formy mena, takéto mená sa musia tiež pridelovať tak, že sa vynúti jedinečnosť mien v rámci celej komunity.

CA má dokumentovať vo svojom CPS, aké formy mena budú používané a ako sa budú stanovovať mená v rámci komunity.

Musí byť tiež zaručená jedinečnosť mien aj medzi súčasnými a minulými majiteľmi certifikátov (t.j. ak napr. „Ján Kováč“ opustí komunitu a nový, iný „Ján Kováč“ príde do komunity).

V prípade testovacích certifikátov sa jedinečnosť mien nekontroluje.

### **3.1.4 Procedúra riešenia sporov pri kolízii mien**

CMA musí zabezpečiť, že nepríde k žiadnej kolízii mien. V prípade potreby môže odmietnuť vydanie certifikátu z dôvodu kolízie mien. V prípade sporov týkajúcich sa kolízie mien a mien vo všeobecnosti sa bude postupovať podľa ustanovení bodu 2.4.

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

Žiadnej entite sa negarantuje, že jej meno v certifikáte bude obsahovať jej obchodnú značku (trademark) a to ani na jej výslovnú žiadosť.

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

CMA nevydá vedome certifikát obsahujúci meno, o ktorom kompetentný súd rozhodol, že porušuje obchodnú značku iného. CMA nebude povinné skúmať obchodné značky ani riešiť spory týkajúce sa obchodných značiek.

### 3.1.6 Preukazovanie vlastníctva privátneho kľúča

CMA bude požadovať, aby žiadateľ o certifikát potvrdil, že vlastní privátny kľúč, ktorý zodpovedá verejnému kľúču nachádzajúcemu sa v žiadosti o certifikát tak, že žiadateľ vlastnoručne podpíše a odovzdá RA vytlačenú žiadosť o certifikát, z ktorej sa má vytvoriť certifikát.

Ak sa žiadateľ o certifikát dá zastupovať na RA iným subjektom (fyzickou alebo právnickou osobou), musí tento zastupujúci subjekt odovzdať na RA vytlačenú žiadosť o certifikát, z ktorej sa má vytvoriť certifikát. Táto vytlačená žiadosť o certifikát musí obsahovať úradne overený (notárom alebo matrikou) podpis zastupovaného žiadateľa o certifikát.

V prípade žiadosti o následný osobný certifikát je prípustné, aby žiadateľ o certifikát preukázal vlastníctvo svojho privátneho kľúča tým, že svoju žiadosť o certifikát zašle žiadateľ na CMA podpísaným mailom, pričom pri podpise tohto mailu musí žiadateľ použiť svoj platný certifikát PSCA.

V prípade, keď si sám žiadateľ o certifikát generuje kľúč priamo do tokenu, potom automaticky vlastní privátny kľúč v čase jeho generovania.

CMA negeneruje páry kľúčov pre cudzie subjekty. Žiadna zložka PSCA v nijakom prípade nearchivuje žiadne privátne kľúče patriace zákazníkom - cudzím subjektom.

### 3.1.7 Autentizácia identity organizácie

Žiadosť o certifikát 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).

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

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

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 získania certifikátu, 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 odstavec) 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).

### **3.1.8 Autentizácia identity fyzickej osoby**

CMA musí garantovať, že identita žiadateľa o certifikát a jeho verejný kľúč sú zodpovedajúco previazané. Každá CMA má špecifikovať vo svojom dokumente CPS procedúry na autentizáciu identity žiadateľa o certifikát. CMA bude zaznamenávať tento proces pre každý certifikát. Dokumentácia o identifikácii musí minimálne obsahovať:

- identita osoby, ktorá vykonáva identifikáciu
- vyhlásenie podpísané touto osobou, že overila identitu žiadateľa o certifikát tak, ako to požaduje táto certifikačný poriadok
- jednoznačné identifikačné čísla z predložených preukazov dokladujúcich identitu autentizovanej osoby
- dátum a čas vykonania identifikácie

Súčasťou dokumentácie o identifikácii musí byť vyhlásenie o identite, ktoré bude vlastnoručne podpísané žiadateľom o certifikát 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 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 odstavec) musí splnomocnená právnická osoba preukázať svoju totožnosť podľa časti 3.1.7.

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

### 3.1.9 Autentizácia identity komponentu

CMA musí garantovať aj v takomto prípade, že identita komponentu a jeho verejný kľúč sú zodpovedajúco previazané.

Hardvérový alebo softvérový komponent, ktorý bude používať certifikáty, bude predmetom certifikácie a je možné vytvoriť preň certifikát PSCA pre server (t.j. nie osobný certifikát). V takom prípade komponent musí byť priradený fyzickej alebo právnickej osobe (organizácii), ktorá ho spravuje (viď časť 5.2).

Táto osoba alebo organizácia je povinná poskytnúť CMA nasledujúce informácie, ako je to popísané v častiach 3.1.8 a 5.2:

- identifikáciu zariadenia
- verejné kľúče zariadenia (obsiahnuté v žiadosti o certifikát)
- autorizáciu zariadenia a jeho atribúty (ak nejaké majú byť uvedené v certifikáte)
- kontaktné údaje, aby CMA mohla v prípade potreby komunikovať s touto osobou

CMA bude autentizovať správnosť ľubovolnej autorizácie (hodnoty položky rozlišovacieho mena), ktorá má byť uvedená v certifikáte a bude overovať predložené údaje.

Metódy na vykonanie tejto autentizácie a kontroly údajov zahrňujú:

- overenie identity danej osoby v súlade s požiadavkami časti 3.1.8
- overenie identity organizácie, ktorej patrí daný komponent, v súlade s požiadavkami časti 3.1.7
- overenie oprávnenosti použitia údajov, ktoré majú byť uvedené v jednotlivých položkách certifikátu, s dôrazom na obsah položky commonName.

Typickou hodnotou tejto položky bude úplné doménové meno alebo registrovaná IP adresa.

V prípade použitia doménového mena je podmienkou, aby príslušná doména druhej úrovne patrila subjektu, ktorý je žiadateľom o daný certifikát pre server. V tomto prípade sa automaticky predpokladá, že tým, že subjekt – žiadateľ o certifikát pre server použil v žiadosti o certifikát dané doménové meno, dal PSCA čestné vyhlásenie, že je vlastníkom zodpovedajúcej domény druhej úrovne a že si je vedomý všetkých následkov a zodpovednosti za prípadné neoprávnené používanie daného doménového mena.

V prípade použitia registrovanej IP adresy RA nebude skúmať, či subjekt – žiadateľ o certifikát pre server používa danú registrovanú IP adresu oprávnene t.j. či daná registrovaná IP adresa je súčasťou adresného segmentu, ktorý je v organizácii RIPE registrovaný na daný subjekt – žiadateľa o certifikát pre server. V tomto prípade sa automaticky predpokladá, že tým, že subjekt – žiadateľ o certifikát pre server použil v žiadosti o certifikát registrovanú IP adresu, dal PSCA čestné vyhlásenie, že danú IP adresu používa oprávnene a že si je vedomý všetkých následkov a zodpovednosti za prípadné neoprávnené používanie danej IP adresy.

### **3.1.10 Predkladané doklady**

Všetky doklady, predkladané na CMA potenciálnymi zákazníkmi – žiadateľmi o certifikát, 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 predloženom 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 bodu 2.4.

### **3.1.11 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 nasledovné:

#### ***Osobné doklady fyzickej osoby:***

- a) platnosť predloženého dokladu – v prípade neplatného osobného dokladu sa postupuje ako pri chýbajúcom osobnom doklade – RA registráciu odmietne

- b) plnoletosť fyzickej osoby (t.j. vek 18 rokov) – RA odmietne registráciu neplnoletých osôb. Za neplnoleté osoby má právo konať ich zákonný zástupca (obvykle rodič).
- c) či nie je zjavný nesúlad medzi fotografiou v osobnom doklade a vzhľadom majiteľa osobného dokladu – ak áno, RA môže odmietnuť registráciu.
- d) bezrozpornosť 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
- b) 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)
- c) či je výpis úradne overený (notárom alebo matrikou), ak sa nejedná o originál

#### ***Plné moci:***

- a) či je plná moc úradne overená (notárom alebo matrikou)
- b) 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
- c) 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
- d) či plná moc nie je časovo obmedzená alebo ak obsahuje inú podmienku, či je táto splnená

## **3.2 Vydanie následného certifikátu**

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

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

Žiadateľ o následný certifikát sa musí podrobiť požiadavkám prvej registrácie (hlavne autentizácii jeho identity).

Jedinou výnimkou je možnosť, že požiada o vydanie následného certifikátu tak, že svoju žiadosť o certifikát zašle žiadateľ na CMA podpísaným mailom, pričom pri podpise tohto mailu musí žiadateľ použiť svoj platný certifikát PSCA.

Majiteľ platného certifikátu PSCA môže požiadať o vydanie následného certifikátu počas posledných 30 dní platnosti svojho certifikátu. Okrem tohto obdobia nemôžu existovať žiadne dva certifikáty so zhodným rozlišovacím menom, v prípade osobných certifikátov ani so zhodnou email adresou v rozlišovacom mene.

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

### **3.3 Vydanie následného certifikátu po zrušení starého**

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

### **3.4 Žiadosť o zrušenie certifikátu**

Žiadosť o zrušenie certifikátu musí byť autentizovaná, pozri časť 4.4.1.3. Žiadosť o zrušenie certifikátu môže byť autentizovaná použitím privátneho kľúča patriaceho k certifikátu bez ohľadu na to, či daný privátny kľúč bol alebo nebol kompromitovaný.

## 4 Prevádzkové požiadavky

### 4.1 Žiadanie o certifikát

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

Keď žiadateľ o certifikát požiada o certifikát, žiadateľ a RA musia vykonať nasledovné kroky:

- overiť a zaznamenať identitu žiadateľa (podľa časti 3.1)
- žiadateľ musí mať vygenerovaný pár kľúčov (verejný a privátny kľúč) pre každý ním požadovaný certifikát
- preukázať, že verejný kľúč tvorí pár kľúčov s privátnym kľúčom vlastneným žiadateľom o certifikát (podľa časti 3.1.6)
- poskytnúť dostatočné podklady na overenie ľubovoľných identifikačných údajov, ktoré sa majú dostať do certifikátu

#### 4.1.1 Doručenie verejného kľúča žiadateľa o certifikát vydavateľovi certifikátu

Verejné kľúče (obsiahnuté v žiadostiach o certifikát) sa musia doručiť CA prostredníctvom RA buď osobne žiadateľom o certifikát alebo subjektom, ktorým sa žiadateľ nechá zastupovať na RA, aby sa garantovala väzba overenej identity žiadateľa k verejnému kľúču, ktorý sa certifikuje. Jedinou výnimkou je v prípade následného certifikátu možnosť požiadať o vydanie následného certifikátu tak, že svoju žiadosť o certifikát zašle žiadateľ na CMA podpísaným mailom, pričom pri podpise tohto mailu musí žiadateľ použiť svoj platný certifikát PSCA (pozri časť 3.2).

### 4.2 Vydanie certifikátu

CA nevytvorí certifikát, kým sa k spokojnosti CA nedokončia všetky verifikácie a prípadné zmeny, ak sú potrebné. CA nezodpovedá za prípadné dodatočné náklady žiadateľa o certifikát, 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 certifikátu, na CMA zostáva zodpovednosť overiť, že informácie sú správne a presné.

Za preverenie údajov žiadateľa zodpovedá RA.

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

#### **4.2.1 Doručenie privátneho kľúča majiteľovi certifikátu**

PSCA neposkytuje službu generovania kľúčov pre žiadateľov o certifikát.

#### **4.2.2 Doručenie verejného kľúča CA používateľom**

CMA a strany spoliehajúce sa na certifikáty musia konať v súčinnosti, aby sa zaručilo autentizované a integrálne doručenie certifikátu CA PSCA.

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

- nahranie certifikátu z web servera PSCA zabezpečeného platným certifikátom PSCA
- pri použití tokenov CMA môže nahráť dôveryhodné certifikáty na doručované tokeny
- osobné prevzatie certifikátu PSCA na RA
- RA na požiadanie poskytne strane spoliehajúcej sa na certifikáty alebo inému ľubovoľnému záujemcovi fingerprint certifikátu CA 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 PSCA na Internete zverejňovať fingerprint certifikátu CA PSCA prostredníctvom svojho web servera.

Fingerprint (alebo hash) posielaný spolu s certifikátom nie je prijateľný ako autentizačný mechanizmus.

### **4.3 Prevzatie certifikátu**

Len čo CA vytvorí certifikát, RA vyzve žiadateľa o certifikát prostredníctvom email správy zaslanej na dohodnutú email adresu, aby sa dostavil na RA kvôli prevzatiu svojho certifikátu a podpísaniu potvrdenia o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát, ktoré tvorí prílohu zmluvy o vydaní a používaní certifikátu PSCA. Toto potvrdenie sa vyhotoví v troch exemplároch – jeden pre žiadateľa a dva zostanú na RA. Pokiaľ si žiadateľ o certifikát odmietne prevziať certifikát, bude certifikát zrušený a poplatok nebude žiadateľovi vrátený.

Žiadateľ o certifikát sa pri preberaní svojho certifikátu môže dať zastupovať na RA inou fyzickou alebo právnickou osobou za rovnakých podmienok ako pri podávaní žiadosti o certifikát (pozri časti 3.1.7 resp. 3.1.8).

Vytvorený certifikát bude odovzdaný na majiteľovu 3,5“ disketu spolu s certifikátom CA PSCA a certifikačným poriadkom PSCA.

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

## **4.4 Suspendovanie certifikátu a zrušenie certifikátu**

### **4.4.1 Zrušenie certifikátu**

#### **4.4.1.1 Okolnosti zrušenia certifikátu**

Certifikát sa má zrušiť, keď sa väzba medzi subjektom a jeho verejným kľúčom definovaným v certifikáte už nepovažuje za platnú. Príklady okolností, ktoré rušia túto väzbu, sú:

- identifikačné informácie alebo pričlenené prvky ľubovoľných mien v certifikáte sa stanú neplatnými
- ukázalo sa, že majiteľ certifikátu nedodržuje svoje povinnosti majiteľa certifikátu, ktoré ho zmluvne viažu
- došlo ku strate privátneho kľúča
- je podozrenie, že bol kompromitovaný privátny kľúč
- majiteľ certifikátu alebo iná oprávnená strana požiadala o zrušenie certifikátu
- smrť majiteľa certifikátu
- došlo ku kompromitácii privátneho kľúča CA PSCA
- rozsudok alebo predbežné opatrenie súdu

Vždy, keď sa CA dozvie o niektorej z vyššie uvedených okolností, daný certifikát sa zruší a dá sa na zoznam zrušených certifikátov (ďalej ako CRL).

Zrušené certifikáty sa budú vyskytovať na všetkých nových vydaniach CRL, minimálne dovtedy, kým dané certifikáty nestratia platnosť.

#### **4.4.1.2 Kto môže žiadať o zrušenie certifikátu**

Majiteľ certifikátu (alebo ním poverená fyzická alebo právnická osoba) môže hocikedy požiadať spôsobom stanoveným CPS o zrušenie svojho vlastného certifikátu a to aj bez udania dôvodu žiadosti o zrušenie certifikátu.

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

Ak bol certifikát vytvorený na základe špeciálnej zmluvy so zákazníkom, v tejto zmluve je možné dohodnúť, kto okrem majiteľa certifikátu má právo požiadať o zrušenie daného certifikátu, akým spôsobom a za akých okolností.

O zrušenie certifikátu môže tiež požiadať:

- CMA (daný pracovník je povinný písomne zdokumentovať túto skutočnosť vrátane dôvodu svojho konania)
- súd prostredníctvom svojho rozsudku alebo predbežného opatrenia (k dokumentom o zrušení certifikátu musí CMA priložiť kópiu príslušného súdneho rozhodnutia)
- subjekt (fyzická alebo právnická osoba) na základe dedičského konania (k dokumentom o zrušení certifikátu musí CMA priložiť kópiu dokladov, z ktorých vyplýva právo daného subjektu žiadať o zrušenie certifikátu)

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

#### 4.4.1.3 Procedúra žiadosti o zrušenie certifikátu

Žiadosť o zrušenie certifikátu podáva oprávnená osoba na RA prostredníctvom troch exemplárov vyplneného formulára „Žiadosť o zrušenie certifikátu“, ktorý je k dispozícii na webe PSCA alebo na RA – dva kusy zostávajú na RA, jeden kus pracovník RA potvrdí s uvedením aktuálneho dátumu a času a vráti žiadateľovi.

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

Ak sa majiteľ certifikátu nechá na RA zastupovať vo veci zrušenia certifikátu, zastupujúci subjekt sa musí preukázať overenou plnou mocou (notárom alebo matrikou), z textu ktorej je jednoznačne zrejmá vôľa majiteľa certifikátu zrušiť svoj certifikát. 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 certifikátu, 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 časti 3.1.7 resp. 3.1.8).

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

Majiteľ platného certifikátu PSCA môže požiadať o zrušenie svojho certifikátu tiež tak, že pošle na kontaktnú email adresu PSCA uvedenú v časti 1.4 mail podpísaný svojím osobným certifikátom PSCA, ktorý obsahuje správu s jednoznačne vyjadrenou vôľou zrušiť certifikát, konkrétne vetu “Žiadam týmto o zrušenie svojho certifikátu PSCA číslo nnn.”.

Takýmto spôsobom možno požiadať o zrušenie certifikátu aj z dôvodu kompromitácie privátneho kľúča, na podpis žiadosti o zrušenie certifikátu pritom možno použiť certifikát, ktorého zrušenie požaduje samotná žiadosť.

Majiteľ platného certifikátu PSCA môže požiadať o zrušenie svojho certifikátu tiež tak, že pošle na kontaktnú email adresu PSCA uvedenú v časti 1.4 obyčajný mail (t.j. nemusí byť podpísaný), ktorý obsahuje správu s jednoznačne vyjadrenou vôľou zrušiť certifikát, konkrétne vetu "Žiadam týmto o zrušenie svojho certifikátu PSCA číslo nnn." a dohodnuté heslo, ktoré žiadateľ o daný certifikát uviedol na formulári Žiadosť o vydanie certifikátu.

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

#### **4.4.1.4 Čas na zrušenie certifikátu**

Tento poriadok nestanovuje žiadny konkrétny čas na zrušenie. CA bude zrušovať certifikáty tak rýchlo ako je to len možné po prevzatí náležitej žiadosti o zrušenie a má vždy zrušiť certifikáty v rámci časových obmedzení popísaných v časti 4.4.3.1.

CA bude bezodkladne informovať (bezpečným mailom alebo písomne) majiteľa certifikátu o zrušení jeho certifikátu, pričom uvedie, kto a kedy o zrušenie daného certifikátu požiadal.

### **4.4.2 Suspendovanie certifikátov**

Pod termínom „suspendovanie certifikátov“ sa myslí dočasné pozastavenie ich platnosti. PSCA nepodporuje túto črtu.

Certifikáty vydané podľa tejto politiky, ktoré boli dané na CRL, sa za žiadnych okolností nebudú môcť považovať za platné (napr. prostredníctvom ich odstránenia z CRL v budúcnosti).

### **4.4.3 Zoznamy zrušených certifikátov**

#### **4.4.3.1 Frekvencia vydávania CRL**

CRL sa vydáva bez zbytočného odkladu po zrušení certifikátu.

CA zruší certifikát najneskôr do 25 hodín od momentu prijatia náležitej žiadosti o zrušenie certifikátu na RA.

Na žiadosti o zrušenie podané po 15.00 hod. sa pritom hľadá akoby boli podané v nasledujúci pracovný deň o 8.00 hod. Dni pracovného voľna (soboty, nedele, sviatky) sa do 25 hodinovej lehoty nepočítajú.

Aby sa zaručila aktuálnosť informácií, CRL sa vydáva minimálne raz za 30 dní a to aj vtedy, ak od vydania posledného CRL nedošlo k zrušeniu žiadneho certifikátu ani k žiadnej zmene v stave jednotlivých certifikátov.

CRL sa zverejňujú prostredníctvom repozitára. CA zverejňuje len aktuálne, najnovšie CRL. CA archivuje všetky CRL, ktoré vydala.

CMA na požiadanie cez email, telefón alebo fax zašle aktuálne CRL prostredníctvom zabezpečeného mailu na dohodnutú email adresu čo najskôr, vždy však do 25 hodín od požiadavky (v zmysle vyššie uvedenej 25 hodinovej lehoty).

#### **4.4.3.2 Požiadavky na overovanie CRL**

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

#### **4.4.4 Overenie aktuálneho stavu certifikátu**

Overenie aktuálneho stavu certifikátu sa robí prostredníctvom aktuálneho CRL publikovaného PSCA.

Softvér implementujúci CA a klientov – strany spoliehajúce sa na certifikáty môže voliteľne podporovať (automatizované) overovanie aktuálneho stavu certifikátu v režime on-line.

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

#### **4.4.5 Iné použiteľné spôsoby oznamovania o zrušení certifikátu**

CMA odpovie na dopyt týkajúci sa stavu konkrétneho certifikátu, ak bol tento dopyt urobený telefonicky, faxom alebo emailom.

### **4.5 Audit bezpečnosti**

#### **4.5.1 Typy zaznamenávaných udalostí**

Zaznamenávajú sa všetky udalosti CMA a tiež interakcie žiadateľov o certifikát a majiteľov certifikátov s CMA. Záznamy môžu byť buď v elektronickej alebo v písomnej forme a môžu byť vytvárané buď automatizovane alebo manuálne.

Prezeranie záznamov sa umožní jednotlivým zložkám CMA v rozsahu týkajúcom sa nimi vykonávaných činností, v celom rozsahu PMA a osobám vykonávajúcim audit zhody. Záznamy sa pravidelne archivujú.

## 4.6 Archívne záznamy

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

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

Modifikovanie alebo odstraňovanie archivovaných informácií nie je prípustné.

## 4.7 Zmena kľúča CA

CA používa svoj podpisovací (privátny) kľúč pri vytváraní certifikátov používateľov. Avšak strany spoliehajúce sa na certifikáty používajú certifikát CA počas celej doby platnosti ich certifikátov. Teda CA nesmie vydávať užívateľom certifikáty, ktorých doba platnosti presahuje dobu platnosti certifikátov CA (a verejných kľúčov CA) a doba platnosti certifikátu CA musí presahovať dobu platnosti všetkých vydaných užívateľských certifikátov.

Po vytvorení nového certifikátu CA sa tento zverejní na webe PSCA a musia sa nanovo vytvoriť certifikáty všetkých subjektov, ktoré majú v čase vytvorenia nového certifikátu CA platné certifikáty. Všetci majitelia platných certifikátov budú upovedomení o platnosti nového certifikátu CA.

Celý proces musí prebehnúť bez negatívneho vplyvu na úroveň zabezpečenia.

## 4.8 Havarijný plán pre mimoriadne udalosti

V prípade kompromitácie kľúča CA sa certifikát CA zruší. Informácia o jeho zrušení sa musí publikovať okamžite najrýchlejším možným spôsobom. Následne sa musí vykonať nová inštalácia CA.

CA upozorní majiteľov certifikátov, ktoré boli podpísané zrušeným certifikátom CA ako aj strany spoliehajúce sa na dané certifikáty, že zrušený certifikát CA sa má odstrániť z každej aplikácie, ktorú používajú strany spoliehajúce sa na certifikáty a má byť nahradený novým certifikátom CA. Tento sa musí distribuovať spoľahlivým spôsobom a v súlade s časťou 2.6.

V prípade havárie, pri ktorej je vybavenie CA poškodené a neschopné prevádzky ale nie je zničený jej podpisovací kľúč, fungovanie CA treba obnoviť podľa možnosti čo najrýchlejšie, pričom treba dať prioritu schopnosti zrušovať certifikáty a zverejňovať aktuálne CRL.

V prípade havárie, pri ktorej je inštalácia CA fyzicky poškodená a jej podpisovací kľúč je zničený, certifikát CA sa zruší. Potom sa kompletne zopakuje inštalácia CA obnovením vybavenia CA, vygenerovaním nových kľúčov CA, vytvorením nového certifikátu CA a

nových certifikátov RA. Nakoniec sa nanovo vydajú všetky užívateľské certifikáty za použitia nového certifikátu CA. Náklady na vytvorenie nových certifikátov subjektom, ktoré boli dotknuté vytvorením nového certifikátu CA, nesie v takomto prípade PSCA.

Strany spoliehajúce sa na certifikáty môžu na vlastné riziko urobiť rozhodnutie pokračovať v používaní certifikátov podpísaných použitím zničeného privátneho kľúča, aby sa splnili ich urgentné operačné požiadavky.

## **4.9 Ukončenie činnosti CA**

Pri ukončení činnosti CA z iných dôvodov ako sú udalosti spôsobené vyššou mocou (napr. prírodná katastrofa, vojnový stav, rozhodnutie štátnej moci a pod.) sa postupuje v súlade s časťou 4.8.

PSCA pritom vhodným spôsobom sprístupní informácie o ukončení svojej činnosti majiteľom všetkých ňou vydaných platných certifikátov a stranám spoliehajúcim sa na certifikáty.

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

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

Pred ukončením svojej činnosti RA poskytne archivované dáta zložke PSCA podľa pokynu PMA.

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

Na fyzické, procedurálne a personálne bezpečnostné opatrenia je kladený veľký dôraz. Opatrenia sú detailne rozpracované v CPS tak, aby zabezpečili dôveryhodnosť certifikačných služieb PSCA.

## **6 Technické bezpečnostné opatrenia**

### **6.1 Generovanie páru kľúčov a inštalácia**

#### **6.1.1 Generovanie páru kľúčov**

Tento poriadok nevyklučuje žiadny zdroj kľúčov, ktoré boli vygenerované v súlade s ustanoveniami tohto dokumentu a lokálnymi bezpečnostnými požiadavkami. Privátny kľúč bude vygenerovaný subjektom, ktorý sa stane jeho vlastníkom: napr. žiadateľom o certifikát alebo na zariadení (napr. počítač, čipová karta alebo iný token, HSM modul a pod.), ktoré je v počas generovania kľúča pod bezprostrednou kontrolou subjektu, ktorý sa stane vlastníkom generovaného kľúča.

#### **6.1.2 Doručenie privátneho kľúča majiteľovi certifikátu**

PSCA zásadne neposkytuje službu generovania páru kľúčov pre cudzí subjekt na zariadeniach patriacich PSCA.

#### **6.1.3 Dĺžky kľúčov**

CPS stanoví odporúčané dĺžky kľúčov resp. minimálne dĺžky kľúčov pre všetky typy entít a všetky používané algoritmy (napr. RSA).

V prípade použitia algoritmu RSA stanovená minimálna dĺžka kľúča musí byť aspoň 512 bitov, odporúčaná dĺžka kľúča aspoň 1 024 bitov.

### **6.2 Ochrana kľúčov**

#### **6.2.1 Ochrana privátneho kľúča CA**

Privátny kľúč CA PSCA je uložený v špeciálnom zariadení – HSM module, ktorý je certifikovaný podľa štandardu FIPS 140-2 level 3.

Pri operáciách správy privátneho kľúča CA PSCA (napr. generovanie, zálohovanie, zničenie) budú vždy prítomné aspoň dve určené oprávnené osoby. Používať privátny kľúč CA PSCA môžu len na to oprávnené osoby.

Privátny kľúč sa používa výlučne na podpisovanie certifikátov a CRL vydávaných CA PSCA.

Privátny kľúč CA je zálohovaný prostredníctvom softvéru na správu HSM modulu v zašifrovanej forme a tak, že k jeho dešifrovaniu je nevyhnutná autentizácia príslušného počtu oprávnených osôb (minimálne dve) na princípe „k“ z „n“.

HSM modul uschovávajúci privátny kľúč CA PSCA spolu s počítačom na vytváranie certifikátov PSCA (s výnimkou testovacích certifikátov) sa bude nachádzať na režimovom pracovisku v miestnosti, ktorá má objektívnu bezpečnosť minimálne na stupni „Dôverné“ v zmysle zákona 241/2001 Z.z. o ochrane utajovaných skutočností.

Vybavenie CA je neprestajne chránené pred neautorizovaným prístupom a to aj pred neautorizovaným fyzickým prístupom.

## **6.2.2 Ochrana ostatných privátnych kľúčov**

Nikto nemá mať prístup k privátnemu podpisovaciemu kľúču okrem jeho majiteľa.

Majiteľom kľúčov je dovolené zálohovať ich vlastné páry kľúčov. Počas zálohovania a prenosu majú byť kľúče zašifrované. Majiteľ kľúča zodpovedá za garanciu, že všetky kópie privátnych kľúčov sú chránené.

Aktivačné dáta pre privátne kľúče patriace k certifikátom potvrdzujúcim individuálnu identitu nemajú byť nikdy zdieľané.

Aktivačné dáta pre privátne kľúče patriace k certifikátom potvrdzujúcim identitu organizácie majú byť známe len tým, ktorí sú v organizácii autorizovaní na použitie daných privátnych kľúčov.

## **6.3 Manažment páru kľúčov**

Všetky certifikáty, ktoré vydá CA PSCA, budú archivované ďalších 20 rokov po ukončení ich platnosti resp. ukončení činnosti CA.

Certifikáty CA, ktoré sa používajú na vytváranie testovacích certifikátov sa po ukončení doby ich platnosti nearchivujú.

Archivovanie privátnych kľúčov je plne vecou majiteľov týchto kľúčov, PSCA ich nemôže archivovať, keďže ich nemá k dispozícii a ani ich negeneruje pre externé subjekty.

## **6.4 Počítačové bezpečnostné opatrenia**

Počítačové vybavenie CA je používané výhradne na účely výkonu činností CA. Bezpečnosť informačného systému je pravidelne podrobovaná kontrole na súlad noriem ISO 17799 a ISO 13335.

## 7 Profily certifikátov a zoznamov zrušených certifikátov

### 7.1 Profily certifikátov

Tento poriadok spravuje len certifikáty podľa štandardu X.509 verzie 3.

#### 7.1.1 Certifikát CA PSCA

*Algoritmy a dĺžky kľúčov uplatňované v certifikáte CA PSCA:*

Algoritmus podpisu (Signature Algorithm): sha1RSA

Verejný kľúč: RSA, dĺžka je 2048 bitov

Algoritmus fingerprintu (Thumbprint Algorithm): SHA1

Doba platnosti certifikátu CA je 10 rokov

*Obsah položiek v certifikáte CA PSCA:*

<i>Názov položky:</i>	<i>Skratka názvu položky:</i>	<i>Hodnota položky:</i>
Štát (countryName)	C	SK
Názov štátu (stateOrProvinceName)	ST	Položka sa nepoužije
Mesto (localityName)	L	Položka sa nepoužije
Firma (organizationName)	O	Viasec s.r.o.
Útvar vo firme (organizationUnitName)	OU	Položka sa nepoužije
Názov (commonName)	CN	Prva Slovenska Certifikačna Autorita
Email adresa (emailAddress)	Email, E	Položka sa nepoužije

**Nepoužitú, prázdne položky v certifikáte CA sa vôbec nebudú vyskytovať.**

### ***Použitá rozšírenia (certificate extensions) v certifikáte CA PSCA:***

kritické rozšírenie basicConstraints = CA:TRUE

kritické rozšírenie keyUsage = keyCertSign,cRLSign

nekritické rozšírenie subjectKeyIdentifier

nekritické rozšírenie subjectAltName = email:oper@psca.sk,URI:http://www.pzca.sk

nekritické rozšírenie crlDistributionPoints = URI:http://www.pzca.sk/crl.crl

nekritické rozšírenie certificatePolicies = 1.3.6.1.4.1.16043.2.1.1

## **7.1.2 Certifikáty PSCA**

Štruktúra certifikátov vydávaných CA PSCA (osobný certifikát PSCA a certifikát PSCA pre server) je detailne popísaná v dokumente CPS, vrátane používaných rozšírení certifikátov (certificate extensions).

Štruktúra certifikátov vydávaných CA PSCA sa môže meniť len na základe rozhodnutia PMA.

## **7.2 Profily zoznamov zrušených certifikátov**

CRL vydávané podľa tejto politiky sú CRL verzie 2.

## **8 Administrácia špecifikácií**

### **8.1 Procedúry na zmenu špecifikácie**

PMA má právo posúdiť a prípadne revidovať túto politiku.

Chyby, požiadavky na aktualizáciu alebo navrhované zmeny tohto dokumentu sa majú oznámiť kontaktu uvedenému v časti 1.4. Takáto komunikácia musí obsahovať popis zmeny, zdôvodnenie zmeny a kontaktné údaje osoby, ktorá zmenu požaduje.

Všetky zmeny politiky motivované PMA majú byť dané na vedomie subjektom, ktorých sa týkajú (viď časť 8.2) v perióde aspoň jedného mesiaca.

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

### **8.2 Publikačná a oznamovacia politika**

PMA má publikovať informácie týkajúce sa tejto politiky (vrátane tejto politiky) prostredníctvom webu a v súlade s pravidlami organizácie týkajúcimi sa obsahu webu.

PMA bude udržiavať zoznam CA, ktoré implementujú túto politiku. Navrhované zmeny politiky a aktualizácie politiky sa majú posielat' týmto CA. CMA má upovedomiť majiteľov certifikátov prostredníctvom mechanizmu popísaného v príslušnom dokumente CPS o každej zmene certifikačnej politiky.

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

PMA má urobiť rozhodnutie, či dokument CPS je v súlade s touto politikou. Ešte pred zahájením prevádzky má mať CMA 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 certifikáty.

### **8.4 Úpravy**

Za normálnych okolností PMA má rozhodnúť, či je odchýlka v praxi CMA podľa aktuálnej politiky prijateľná alebo či má CMA požiadať PMA o zmenu politiky.

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