První certifikační autorita, a.s.

Certifikační politika

vydávání kvalifikovaných mandátních certifikátů

verze 1.2

OBSAH

tab. 1 – Vývoj dokumentu

Verze	Datum vydání	Schválil	Pozn.
1.0	23.03.2015	Ředitel společnosti První certifikační autorita, a.s.	První vydání
1.1	21.09.2015	Ředitel společnosti První certifikační autorita, a.s.	Rozšíření položek certifikátu
1.2	9.11.2015	Ředitel společnosti První certifikační autorita, a.s.	Úprava naplnění položek v souvislosti se zákonem č. 273/2015 Z.z.

1 ÚVOD

Tento dokument definuje pravidla a postupy pro vydávání kvalifikovaných mandátních certifikátů společností První certifikační autorita, a.s., (dále též I.CA) fyzickým osobám, oprávněným ze zákona nebo na základě zákona jednat za jinou osobu nebo orgán veřejné moci nebo jejich jménem, nebo osobě, která vykonává činnost nebo funkci podle zvláštního předpisu.

1.1 Přehled

Dokument **Certifikační politika vydávání kvalifikovaných mandátních certifikátů** (dále též CP), vypracovaný společností První certifikační autorita, a.s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu kvalifikovaných certifikátů, a je v souladu:

- s dokumentem Směrnice 1999/93/ES Evropského parlamentu a Rady ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy,
- s aktuálním zněním zákona č. 227/2000 Sb., o elektronickém podpisu a s ním souvisejících předpisů a vyhlášek,
- s aktuálním zněním zákona č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok

a dodržuje strukturu standardu RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k němu irelevantní). Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem, obecně popisuje subjekty, které participují na poskytování této certifikační služby a definuje přípustné využívání vydávaných kvalifikovaných certifikátů (dále též certifikát).
- Kapitola 2 obsahuje problematiku odpovědností za zveřejňování a úložiště informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání certifikátu, resp. zneplatnění certifikátu, včetně definování typů a obsahů používaných jmen v žádostech, resp. vydávaných certifikátech.
- Kapitola 4 definuje procesy životního cyklu certifikátu, tzn. žádost o vydání certifikátu, zneplatnění certifikátu, služby související s ověřováním stavu certifikátu, ukončení poskytování certifikačních služeb atd.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí a jejich uchovávání, problematiku chování po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.
- Kapitola 7 definuje profil vydávaných certifikátů a seznamů zneplatněných certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytovaných certifikačních služeb.
- Kapitola 9 zahrnuje problematiku obchodní a právní.

Tento dokument může být mimo jiné využit nezávislými institucemi (např. auditorskými společnostmi) jako základ pro potvrzení toho, že certifikační služby v oblasti vydávaní kvalifikovaných certifikátů, poskytované společností První certifikační autorita, a.s., je možné považovat za důvěryhodné.

Bližší podrobnosti o naplnění položek certifikátů vydávaných podle této CP a o jejich správě jsou uvedeny v odpovídající Certifikační prováděcí směrnici.

1.2 Název a jednoznačné určení dokumentu

Název:	Certifikační politika vydávání kvalifikovaných mandátních certifikátů
OID:	1.3.6.1.4.1.23624.1.1.202.1.2
Platnost:	do odvolání nebo do dne ukončení služeb CA, vydávající kvalifikované mandátní certifikáty

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA")

Akreditovaná certifikační autorita společnosti První certifikační autorita, a.s., (dále též I.CA) vydávající certifikáty, splňující požadavky legislativ České republiky a Slovenské republiky.

1.3.2 Registrační autority (dále „RA")

Poskytování certifikačních služeb společnosti První certifikační autorita, a.s., v oblasti certifikátů se realizuje prostřednictvím vyhrazených registračních autorit, které:

- přijímají žádosti o kvalifikované certifikační služby uvedené v této CP, zejména přijímají žádosti o certifikáty, zprostředkovávají předání certifikátů a seznamů zneplatněných certifikátů, poskytují potřebné informace, vyřizují reklamace atd.,
- jsou oprávněny z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti - toto opatření jsou povinny neprodleně hlásit řediteli I.CA, který je potvrdí, zruší nebo změní,
- jsou zmocněny jménem I.CA uzavírat smlouvy o poskytování kvalifikované certifikační služby popsané v této CP,
- zajišťují zpoplatňování služeb I.CA, pokud není stanoveno smlouvou jinak.

Tyto registračních autority mohou být stacionární nebo mobilní.

1.3.3 Držitelé kvalifikovaných certifikátů a podepisující osoby nebo označující osoby, kteří požádali o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu a kterým byl certifikát vydán

Podepisující osobou je fyzická osoba (v případě této CP mandatář), která je držitelem bezpečného prostředku pro vytváření elektronických podpisů (SSCD) a jedná jménem jiné fyzické či právnické osoby (v případě této CP mandanta).

Držitelem certifikátu je fyzická osoba (v případě této CP mandatář) oprávněná ze zákona nebo na základě zákona jednat za jinou osobu nebo orgán veřejné moci (v případě této CP

mandanta), nebo osoba, která vykonává činnost podle zvláštního předpisu nebo vykonává funkci podle zvláštního předpisu (v případě této CP mandatář), které byl certifikát vydán.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na certifikát vydaný společností První certifikační autorita, a.s.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty mohou být subjekty, které může společnost První certifikační autorita, a.s., využívat pro zajištění certifikačních služeb, orgány dozoru, orgány činné v trestním řízení a další, kterým to ze zákona přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané společností První certifikační autorita, a.s., podle této certifikační politiky smějí být používány výhradně pro ověřování elektronického podpisu v souladu se ZoEP.

1.4.2 Omezení použití certifikátu

Certifikáty vydávané podle této certifikační politiky nesmějí být používány v rozporu s přípustným použitím popsaným v kapitole 1.4.1 a lze je využívat pouze pro legální účely a v souladu s platnými právními předpisy.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Tuto certifikační politiku nebo příslušnou certifikační prováděcí směrnici, spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Kontaktní osoba společnosti První certifikační autorita, a.s., odpovědná za správu této certifikační politiky nebo příslušné certifikační prováděcí směrnici, je uvedena na internetové adrese (viz kap. 2.2).

1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., s postupy jiných poskytovatelů certifikačních služeb, je ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování souladu podle bodu 1.5.3

V případě, že je potřebné provést změny v této politice a vytvořit její novou verzi, určuje ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze CP předchází její schválení ředitelem společnosti První certifikační autorita, a.s.

1.6 Přehled použitých pojmů a zkratek

tab. 2 – Pojmy a zkratky

Pojem	Vysvětlení
Bit	z anglického *binary digit* - číslice dvojkové soustavy - je základní a současně nejmenší jednotkou informace používanou především v číslicové technice
CA	certifikační autorita
certifikát na správu	certifikát, který slouží na ověření platnosti kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, kvalifikovaných časových razítek a certifikátů akreditovaných certifikačních autorit
CP	certifikační politika
CPS	certifikační prováděcí směrnice
CRL (Certificate Revocation List)	seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
data pro vytváření elektronické pečetě	jedinečná data, která původce pečetě používá k vytváření elektronické pečetě
data pro ověřování elektronické pečetě	jedinečná data, která se používají pro ověření elektronické pečetě
data pro vytváření elektronického podpisu	jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu
data pro ověřování elektronických podpisu	jedinečná data, která se používají pro ověření elektronického podpisu
data pro vytváření elektronické značky	jedinečná data, která označující osoba používá k vytváření elektronické značky
data pro ověřování elektronické značky	jedinečná data, která se používají pro ověření elektronické značky
elektronický dokument	číselně kódovaný dokument, uchovávaný na fyzickém nosiči, přenášený nebo zpracovávaný pomocí technických prostředků v elektronické, magnetické, optické nebo jiné

	formě
elektronická pečeť	informace, připojená nebo jinak logicky spojená s elektronickým dokumentem, která musí splňovat tyto požadavky: • není možné ji efektivně vytvořit bez znalosti soukromého klíče a elektronického dokumentu, • na základě znalosti této informace a veřejného klíče patřícího k soukromému klíči použitému při jejím vytvoření je možné ověřit, že elektronický dokument, ke kterému je připojená nebo s ním jinak logicky spojená, je shodný s elektronickým dokumentem, použitým na její vytvoření, • obsahuje údaj, který identifikuje původce pečetě
elektronický podpis	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě
elektronická značka	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: • jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, • byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, • jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat
hash (otisk, fingerprint, …)	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou
kvalifikovaný certifikát/kvalifikovaný systémový certifikát	certifikát, který má náležitosti podle platné české/slovenské legislativy, resp. platného standardu
Mandant	osoba nebo orgán veřejné moci, za které nebo jejichž jménem mandatář jedná
Mandatář	fyzická osoba, oprávněná ze zákona nebo na základě zákona jednat za jinou osobu nebo orgán veřejné moci nebo jejich jménem, nebo osoba, která vykonává činnost nebo funkci podle zvláštního předpisu
Mandát	potvrzení o platnosti práva jednat za jinou osobu nebo orgán veřejné moci nebo jejich jménem
mandátní certifikát	kvalifikovaný certifikát vydaný fyzické osobě oprávněné ze zákona nebo na základě zákona jednat za jinou osobu nebo

	orgán veřejné moci nebo jejich jménem, nebo osobě, která vykonává činnost nebo funkci podle zvláštního předpisu
následný certifikát	certifikát, který byl v souladu se smlouvou o poskytování kvalifikované certifikační služby, uzavřenou mezi žadatelem a I.CA, vydán žadateli na základě nové žádosti o certifikát v období platnosti certifikátu, ke kterému je tento následný certifikát vydáván
označující osoba	fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou
párová data	jedinečná data pro vytváření elektronického podpisu/elektronické značky/elektronické pečetě spolu s odpovídajícími daty pro ověřování elektronického podpisu/elektronické značky/elektronické pečetě
původce pečetě	právnická osoba nebo orgán veřejné moci, který je držitelem soukromého klíče a je schopný pomocí tohoto klíče vytvořit elektronickou pečeť elektronického dokumentu
RA	registrační autorita
smluvní partner	poskytovatel vybraných certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části - nejčastěji se jedná o smluvní RA
soukromý klíč	jedinečná data pro vytváření elektronického podpisu/ elektronické značky/elektronické pečetě
SSCD	Secure Signature Creation Device (bezpečné zařízení pro tvorbu elektronického podpisu)
spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát vydaný CA
veřejný klíč	jedinečná data pro ověřování elektronického podpisu/elektronické značky/elektronické pečetě
VoEP	• vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb) • sada vyhlášek Slovenské republiky, vztahujících se k problematice aktuálního znění zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov
zaručený elektronický podpis	elektronický podpis splňující požadavky české, resp. slovenské legislativy
ZoEP	• aktuální znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) • aktuální znění zákona Slovenské republiky č. 215/2002

	Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

Společnost První certifikační autorita, a.s., zřizuje a provozuje úložiště informací a dokumentace, za která taktéž jako poskytovatel certifikačních služeb odpovídá.

2.2 Zveřejňování informací a dokumentace

Základní adresy (dále též informační adresy), na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s., (certifikační politiky, zprávy pro uživatele, další informace dle ZoEP, ostatní veřejné a aktuální informace a dokumenty atd.), případně odkazy pro zjištění dalších informací, jsou:

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Česká republika
- internetová adresa http://www.ica.cz,
- sídla registračních autorit.

Adresy, které slouží pro kontakt veřejnosti s I.CA, jsou:

- sídlo registrační autority, která smluvní vztah s I.CA zprostředkovala,
- elektronická poštovní adresa info@ica.cz.

I.CA zveřejňuje výše uvedené kontaktní adresy na své internetové adrese a pracovištích RA. Pracovníci I.CA a smluvních partnerů jsou rovněž povinni tyto informace na vyžádání sdělit veřejnosti.

Na výše uvedené internetové adrese lze získat informace o:

- veřejných certifikátech (tzn. neobsahujících údaje, jejichž zveřejnění by bylo v rozporu s legislativou ČR/SK, např. zákon o ochraně osobních údajů, nebo u kterých si žadatel o certifikát vymínil, že nebude zveřejněn) - přímo se zveřejňují následující informace (ostatní informace lze získat z certifikátu):
  - číslo certifikátu,
  - obsah položky Obecné jméno (commonName),
  - údaj o počátku platnosti (s uvedením hodiny, minuty a sekundy),
  - odkazy na místo, kde lze certifikát získat v určených formátech (DER, PEM, TXT),
- seznamech zneplatněných certifikátů (CRL) - přímo se zveřejňují následující informace (ostatní informace lze získat ze samotného CRL):
  - datum vydání CRL,

- číslo CRL,
- odkazy na místo, kde lze CRL získat v určených formátech (DER, PEM, TXT).

Povolenými protokoly pro přístup k veřejným informacím jsou HTTP, HTTPS, FTP. Jiné protokoly povoleny nejsou. I.CA může bez udání důvodu přístup prostřednictvím některých z uvedených protokolů zrušit nebo pozastavit, přitom je povinna dodržet příslušná ustanovení ZoEP a VoEP. Tyto změny je I.CA povinna zveřejnit prostřednictvím svých informačních adres. Podrobnější informace o možnostech a příslušných parametrech uvedených protokolů I.CA zveřejňuje tamtéž.

V případech odejmutí akreditace, nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek/elektronických pečetí vydávaných certifikátů nebo seznamů zneplatněných certifikátů, oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes.

2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- certifikační politika, certifikační prováděcí směrnice - po schválení a vydání nové verze,
- seznam vydaných certifikátů – aktualizace při každém vydání nového certifikátu určeného ke zveřejnění,
- seznam zneplatněných certifikátů (CRL) - maximálně za 24 hodin od vydání předchozího CRL (zpravidla à 8 hodin),
- informace požadované ZoEP, VoEP (zejména získání nebo odejmutí akreditace, zneplatnění kvalifikovaného systémového certifikátu CA/certifikátu na správu s uvedením důvodu zneplatnění) – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných certifikačních služeb.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace (viz kapitoly 2.2 a 2.3) zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům I.CA, smluvním partnerům nebo subjektům definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Veškerá jména jsou konstruována v souladu se standardem X.501, resp. s navazujícím standardem X.520.

3.1.2 Požadavek na významovost jmen

Význam a obsah údajů vydávaného certifikátu je uveden v kapitole 7.

3.1.3 Anonymita a používání pseudonymu

Není podporováno.

3.1.4 Pravidla pro interpretaci různých forem jmen

Údaje uváděné v procesu žádosti o certifikát na RA se do certifikátů vydávaných CA přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech.

3.1.5 Jedinečnost jmen

Jedinečnost jmen je zajištěna identifikátorem, který je uložen v položce serialNumber pole Subject certifikátu.

3.1.6 Obchodní značky

Všechny položky certifikátu, které jsou v procesu vydání certifikátu ověřovány, mají předepsanou strukturu a musí být doloženy jejich správnost a úplnost.

Žadatel o certifikát je odpovědný za uvedení a použití obchodních značek nebo registrovaných ochranných známek v položkách certifikátu, které nejsou I.CA ověřovány.

3.2 Počáteční ověření identity

Certifikát spojuje identitu vlastníka dat pro vytváření elektronických podpisů s daty pro ověřování elektronických podpisů, přičemž všechny údaje obsažené v certifikátu musí být v době jeho vydání ověřeny jako platné.

3.2.1 Ověření souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek

Vlastnictví dat pro vytváření elektronických podpisů, odpovídajících datům pro ověřování elektronických podpisů, která daná žádost o certifikát (struktura PKCS#10, podpora hashovacích funkcí SHA-256 a SHA-512) obsahuje a která budou obsažena ve vydaném certifikátu, se prokazuje předložením této žádosti ověřujícímu subjektu. S ohledem na skutečnost, že žádost je elektronicky podepsána daty pro vytváření elektronických podpisů, odpovídajících datům pro ověřování elektronických podpisů obsažených v žádosti, dokazuje tímto způsobem žadatel o certifikát, že v době tvorby elektronického podpisu žádosti o certifikát vlastnil data pro tvorbu elektronických podpisů, odpovídající datům pro ověřování elektronických podpisů, která jsou v žádosti uvedena.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

I.CA vyžaduje originál, nebo úředně ověřenou kopii, výpisu z obchodního nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny, resp. jiného dokladu stejné právní váhy a který/která musí obsahovat úplné obchodní jméno, identifikační údaj, adresu sídla, jména statutárních zástupců (osoby/osob, oprávněné/oprávněných k zastupování) a způsob, jakým za právnickou osobu jednají a podepisují. Identifikačním údajem může být NTR (národní identifikační číslo právnické osoby), VAT (národní identifikační číslo právnické osoby pro DPH), popř. nebo SZ (údaj, definovaný platnou legislativou[1]).

3.2.3 Ověřování identity fyzické osoby

V případě žádosti o **prvotní certifikát** prokazuje mandatář, který musí být vždy fyzicky přítomen na RA, své identifikační údaje následujícími doklady:

- Originálem platného primárního osobního dokladu a originálem dalšího osobního dokladu (sekundárního). Primární osobní doklad pro občany České republiky nebo Slovenské republiky je občanský průkaz, platný cestovní pas, popř. obdobný doklad stejné právní váhy. Primární osobní doklad pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Sekundární osobní doklad (originál) musí být vydán orgánem veřejné moci nebo jinou organizací, jejíž existenci lze doložit a musí obsahovat celé občanské jméno fyzické osoby žadatele o certifikát a dále nejméně jeden z následujících údajů:
  - rodné číslo u občanů České republiky nebo Slovenské republiky, nebo datum narození žadatele (cizinec, jemuž rodné číslo nebylo orgánem veřejné moci České nebo Slovenské republiky přiděleno),
  - adresu trvalého bydliště žadatele,
  - fotografii obličeje žadatele.
- Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu. O shodnosti rozhoduje pracovník RA. Pokud žadatel nepředloží dva osobní doklady výše popsané kvality, nebude žádost přijata. Příkladem akceptovatelného sekundárního osobního dokladu jsou např. cestovní pas, řidičský

[1] v případě legislativy SK se jedná o identifikaci na základě souborů znaků přidělených podle § 27 odst. 4 zákona č. 540/2001 Z. z. o štátnej štatistike v znení zákona č. 55/2010 Z. z.

průkaz, služební průkazy státních úřadů, průkaz poslance, služební průkaz policie, zbrojní průkaz, vojenská knížka, průkaz zdravotního pojištění, průkazka hromadné dopravy, firemní průkazky, studentský průkaz atd.

- Primární osobní doklad musí obsahovat doplňující identifikátor/identifikátory (v souladu s legislativou Slovenské republiky).
- Dokumentem, prokazujícím název osoby nebo orgánu veřejné moci (včetně identifikačního údaje), u které mandatář vykonává činnost nebo funkci a potvrzením platnosti práva tuto činnost nebo funkci vykonávat. Potvrzení musí být opatřeno podpisem osoby s právem jednání za příslušnou organizaci. Pokud tato osoba není osobou oprávněnou k zastupování organizace, tj. není statutárním zástupcem (není uveden na výpisu z obchodního rejstříku nebo jiného zákonem určeného rejstříku nebo registru, v živnostenském listu, ve zřizovací listině, v zákoně, v případě organizační složky státu/orgánu veřejné moci ve zvláštním právním předpisu atd.), požaduje se navíc úředně ověřený doklad (plná moc, pověření, doklad o zákonném zastupování) podepsaný statutárním zástupcem organizace, potvrzující oprávněnost této osoby za organizaci jednat.

V případě žádosti o **prvotní certifikát** prokazuje mandant (prokazování mandátu), prostřednictvím mandatářem předkládané úředně ověřené plné moci (není-li určeno jinak), následující údaje:

- v případě fyzické osoby:
  - celé občanské jméno,
  - v případě zaměstnance název a identifikační údaj zaměstnavatele,
  - rodné číslo u občanů České republiky nebo Slovenské republiky nebo datum narození žadatele (cizinec, jemuž rodné číslo nebylo orgánem České nebo Slovenské republiky přiděleno),
  - číslo občanského průkazu nebo cestovního pasu,
- v případě právnické osoby nebo orgánu veřejné moci její název a identifikační údaj.

V případě žádosti o **následný certifikát** (výměna dat pro vytváření elektronických podpisů a jim odpovídajících dat pro ověřování elektronických podpisů) se ověří, že osobní údaje mandatáře a mandanta/mandátu uvedené v žádosti o vydání tohoto certifikátu souhlasí s údaji v dokumentech (předkládaných v procesu vydávání prvotního certifikátu) tohoto žadatele.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě

Není relevantní pro tento dokument.

3.2.5 Ověřování specifických práv

Mandatář prokazuje oprávnění jednat za mandanta nebo jeho jménem, jednat jako orgán veřejné moci nebo oprávnění vykonávat činnost podle zvláštního předpisu nebo vykonávat funkci podle zvláštního předpisu. Potvrzení musí být opatřeno podpisem osoby s právem jednání za mandanta nebo jeho jménem. Pokud tato podepisující osoba není statutárním zástupcem mandanta (není uvedena ve výpisu z obchodního rejstříku nebo v jiném zákonem určeném rejstříku nebo registru, v živnostenském listu, ve zřizovací listině, v zákoně, v případě organizační složky státu/orgánu veřejné moci ve zvláštním právním předpisu atd.),

požaduje se navíc úředně ověřený doklad (plná moc, pověření, doklad o zákonném zastupování) podepsaný statutárním zástupcem mandanta, potvrzující oprávněnost této osoby za mandanta jednat.

3.2.6 Kritéria pro interoperabilitu

Případná spolupráce společnosti První certifikační autorita, a.s., s jinými poskytovateli certifikačních služeb je vždy založena na písemné smlouvě s těmito poskytovateli.

3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a jim odpovídajících dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek (dále „párová data“)

Vlastnictví dat pro vytváření elektronických podpisů, odpovídajících datům pro ověřování elektronických podpisů, která daná žádost o certifikát (struktura PKCS#10) obsahuje a která budou obsažena ve vydaném certifikátu, se prokazuje způsobem, uvedeným v kapitole 3.2.1.

Pokud se jedná o vydání následného certifikátu a uvedená datová struktura byla podána v podobě elektronického dokumentu, musí být navíc podepsána zaručeným elektronickým podpisem, ověřitelným daty pro ověřování elektronických podpisů z platného certifikátu, ke kterému je vydáván tento následný certifikát.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

Služba výměny párových dat po zneplatnění certifikátu není podporována.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Údaje, které musí žádost o zneplatnění certifikátu obsahovat, jsou uvedeny v kapitole 4.9.3.

V případě **osobního předání žádosti o zneplatnění certifikátu na RA** musí držitel certifikátu prokázat, že mu byl certifikát vydán. Žádost o zneplatnění certifikátu musí být písemná a podepsaná držitelem certifikátu.

V případě **předání žádosti o zneplatnění certifikátu elektronickou cestou** jsou přípustné následující možnosti:

- elektronicky podepsaná elektronická zpráva - (revoke@ica.cz), elektronický podpis musí být realizován daty pro vytváření elektronického podpisu příslušnými k předmětnému certifikátu, jenž má být zneplatněn,
- elektronicky nepodepsaná elektronická zpráva, obsahující heslo pro zneplatnění certifikátu - (revoke@ica.cz),

- prostřednictvím formuláře na internetové informační adrese (http://www.ica.cz),
- prostřednictvím datové schránky.

V případě použití **listovní zásilky pro předání žádosti o zneplatnění certifikátu** musí být tato zaslána doporučeně na adresu sídla společnosti I.CA.

Údaje, které musí žádost o zneplatnění certifikátu obsahovat, jsou uvedeny v kapitole 4.9.3.

I.CA si vyhrazuje právo akceptování i jiných forem postupů při identifikaci a autentizaci zpracování požadavků na zneplatnění certifikátu, které však nesmí být v rozporu s platnou legislativou (ZoEP, VoEP).

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu dle této CP může podat mandatář (fyzická osoba, oprávněná ze zákona nebo na základě zákona jednat za jinou osobu nebo orgán veřejné moci nebo jejich jménem, nebo osoba, která vykonává činnost nebo funkci podle zvláštního předpisu).

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

4.1.2.1 Registrační proces

Registrační proces v případě prvotního certifikátu zahajuje mandatář dostavením se s potřebnými dokumenty na pracoviště RA, kde následně probíhá proces zpracování žádosti o certifikát.

4.1.2.2 Odpovědnosti žadatele

Mandatář je povinen zejména:

- poskytovat pravdivé a úplné informace při registraci žádosti o vydání prvotního a následného certifikátu,
- překontrolovat, zda údaje uvedené v žádosti o certifikát a certifikátu jsou správné a odpovídají požadovaným údajům,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle této CP, takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- užívat soukromý klíč a odpovídající certifikát vydaný podle této CP pouze pro účely stanovené v této CP,
- neprodleně uvědomit poskytovatele certifikačních služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče,
- zvolit vhodné heslo pro zneplatnění certifikátu (minimální/maximální délka hesla 4/32 znaků, povolené znaky 0..9, A..Z, a..z),
- seznámit se s CP, podle které mu byl vydán certifikát.

4.1.2.3 Odpovědnosti poskytovatele

Poskytovatel certifikačních služeb (I.CA) je zejména povinen:

- v procesu vydávání certifikátu na RA ověřit všechny požadované údaje podle předložených dokladů,
- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou poskytovateli certifikačních služeb k dispozici v době vydávání certifikátu,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,

- zveřejnit kvalifikované systémové certifikáty CA/certifikáty pro správu, využívané v procesu vydávání certifikátů koncovým uživatelům, aby se každý mohl ujistit o jeho identitě,
- činnosti, spojené s poskytováním certifikačních služeb, poskytovat v souladu s platnou legislativou, touto CP, příslušnou CPS, Systémovou bezpečnostní politikou CA a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

V případě vydávání **prvotního certifikátu** je prováděno:

- ověření vlastnictví dat pro vytváření elektronických podpisů (viz kapitola 3.2.1),
- ověření identity fyzické osoby mandatáře (viz kapitola 3.2.3),
- ověření identity právnické osoby, organizační složky státu nebo orgánu veřejné moci mandatáře, pokud pro některou z nich mandatář vykonává činnost nebo funkci (viz kapitola 3.2.2, 3.2.3),
- ověření specifických práv mandatáře a oprávnění pro přidělení mandátu (viz kapitola 3.2.5),
- ověření identity fyzické osoby mandanta – jedná-li se o fyzickou osobu (viz kapitola 3.2.3),
- ověřování identity právnické osoby, organizační složky státu nebo orgánu veřejné moci mandanta – nejedná-li se o fyzickou osobu (viz kapitola 3.2.2),
- kontrolování údajů obsažených v žádosti o certifikát s údaji obsaženými v předkládaných dokladech.

V případě vydávání **následného certifikátu** je prováděno:

- ověření vlastnictví dat pro vytváření elektronických podpisů mandatáře (viz kapitola 3.3.1),
- ověření skutečnosti, že osobní údaje mandatáře a mandanta uvedené v žádosti o vydání certifikátu souhlasí s údaji v dokumentech – postupy jsou uvedeny v příslušné CPS,
- ověření specifických práv mandatáře a oprávnění pro přidělení mandátu.

Pokud některá z výše uvedených ověření (pro prvotní, resp. následný certifikát) skončí negativně, proces vydání certifikátu je ukončen.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

V případě, že je výsledek kontrol procesu žádání o **prvotní certifikát** pozitivní, pracovník RA okopíruje předložené osobní doklady (není-li smluvně stanoveno jinak). Dokument „Protokol o podání žádosti o vydání kvalifikovaného mandátního certifikátu I.CA“, jehož součástí je věta „**Žadatel souhlasí s tím, aby společnost První certifikační autorita, a.s., skladovala pořízené kopie jeho osobních dokladů v souladu s platnou legislativou.**“ nechá žadateli o certifikát podepsat. Pokud žadatel o certifikát odmítne tento protokol podepsat, je

pracovník RA povinen proces vydávání certifikátu ukončit a kopie osobních dokladů zničit – skartovat (není-li smluvně stanoveno jinak).

V případě vyřizování žádosti o **následný certifikát** platí požadavky, uvedené v kapitole 4.2.1.

4.2.3 Doba zpracování žádosti o certifikát

Po kladném rozhodnutí o vydání certifikátu je I.CA povinna neprodleně certifikát vydat.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání certifikátu provádějí operátoři/operátorky provozního pracoviště CA kontroly na shodnost údajů, obsažených v žádosti o certifikát (struktura PKCS#10) a údajů, doplněných pracovníkem/pracovnicí RA. Kontroly na formální správnost údajů jsou taktéž prováděny programovým vybavením informačního systému CA.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující nebo označující osobě

O vydání certifikátu může být mandatář informován prostřednictvím pracovníka RA a v případě, že mandatář uvedl elektronickou poštovní adresu, je vydaný certifikát na tuto adresu taktéž zaslán.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání certifikátu, tzn.:

- splnění podmínek registrace,
- zaplacení určeného poplatku (není-li smluvně stanoveno jinak),
- prokázání vlastnictví dat pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů, která bude vydaný certifikát obsahovat,
- podepsání příslušné smlouvy,

je povinností mandatáře tento certifikát přijmout. Jediným způsobem, jakým může mandatář postupovat v případě, že tento certifikát nemá zájem převzít, je zažádat v souladu s touto CP o jeho zneplatnění.

I.CA může se smluvním partnerem sjednat postup odlišný od tohoto ustanovení CP. Tímto postupem však nesmí být dotčena příslušná ustanovení legislativních norem, které upravují oblast poskytování certifikačních služeb nebo obchodní činnosti s tímto spojené.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

I.CA je povinna zajistit neprodlené zveřejnění jí vydaných certifikátů, vyjma certifikátů:

- obsahujících údaje, jejichž zveřejnění by bylo v rozporu s legislativou ČR/SK (např. zákon o ochraně osobních údajů),
- u kterých si žadatel o certifikát vymínil, že nebudou zveřejněny.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

V případech vydání certifikátu při dostavení se mandatáře na RA, získá oznámení o vydaném certifikátu pracovník RA. Dále platí ustanovení kapitoly 4.4.2 a požadavky platné legislativy.

4.5 Použití párových dat a certifikátu

4.5.1 Použití dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a certifikátu držitelem certifikátu, podepisující nebo označující osobou

Povinností držitelů certifikátů a podepisujících osob je zejména:

- bez zbytečného odkladu podávat přesné, pravdivé a úplné informace I.CA ve vztahu k vydanému certifikátu,
- dodržovat veškerá relevantní ustanovení smlouvy o poskytování této kvalifikované certifikační služby,
- zacházet s prostředky, jakož i s daty, pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,
- uvědomit neprodleně poskytovatele certifikačních služeb, který vydal certifikát dle této CP o tom, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronického podpisu,
- využívat data pro vytváření elektronických podpisů související s vydaným certifikátem v souladu s ustanoveními této CP,
- při činnostech souvisejících s daty pro vytváření zaručeného elektronického podpisu dodržovat veškerá relevantní ustanovení ZoEP, VoEP a této CP.

4.5.2 Použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat kvalifikované systémové certifikáty CA/certifikáty na správu (související s kvalifikovaným mandátním certifikátem vydaným dle odpovídající CP) a ověřit hodnoty jejich otisků,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že elektronický podpis získaného elektronického dokumentu je platný a jemu odpovídající kvalifikovaný mandátní certifikát, včetně kvalifikovaných systémových certifikátů CA/certifikátů na správu (souvisejících s tímto elektronickým dokumentem) nebyly zneplatněny,
- dodržovat veškerá ustanovení této CP,

- při činnostech souvisejících s používáním vydaného kvalifikovaného mandátního certifikátu dodržovat veškerá relevantní ustanovení ZoEP, VoEP.

4.6 Obnovení certifikátu

Službou obnovení certifikátu je v kontextu tohoto dokumentu míněno obnovení již zneplatněného certifikátu nebo vydání následného certifikátu aniž by byla změněna data pro ověřování elektronických podpisů nebo jiné informace v certifikátu.

4.6.1 Podmínky pro obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.3 Zpracování požadavku na obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující nebo označující osobě

Služba obnovení certifikátu není poskytována.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Služba obnovení certifikátu není poskytována.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

Služba obnovení certifikátu není poskytována.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

Služba obnovení certifikátu není poskytována.

4.7 Výměna dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Službou výměny dat pro ověřování elektronických podpisů je v kontextu tohoto dokumentu míněno vydání následného certifikátu s novými daty pro ověřování elektronických podpisů, aniž by byly změněny jiné informace v certifikátu.

4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Žádost o vydání následného certifikátu (struktura PKCS#10) musí splňovat níže uvedené podmínky:

- položky pole Subject musí být totožné jako v certifikátu, ke kterému je tento následný certifikát požadován,
- data pro ověřování elektronických podpisů (veřejný klíč) musí být jiná než v původním certifikátu,
- ostatní položky žádosti zůstávají shodné s původními údaji v dokumentech předložených při prvotním vydání mandátního certifikátu.

4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Výměnu dat pro ověřování elektronických podpisů jsou oprávněni požadovat mandatáři.

4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Pokud jsou splněny podmínky pro výměnu dat pro ověřování elektronických podpisů (viz kapitola 4.7.1) je postupováno v souladu s kapitolou 4.2, v opačném případě je řízení k vydání certifikátu ukončeno.

4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek podepisující nebo označující osobě

Uvedeno v kapitole 4.3.2.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

Uvedeno v kapitole 4.4.1.

4.7.6 Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

Uvedeno v kapitole 4.4.2.

4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek jiným subjektům

Uvedeno v kapitole 4.4.3.

4.8 Změna údajů v certifikátu

Službou změny údajů v certifikátu je v kontextu tohoto dokumentu míněno vydání následného certifikátu se změněnými jinými informacemi v certifikátu, než data pro ověřování elektronických podpisů.

4.8.1 Podmínky pro změnu údajů v certifikátu

Služba změny údajů v certifikátu není poskytována.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Služba změny údajů v certifikátu není poskytována.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Služba změny údajů v certifikátu není poskytována.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující nebo označující osobě

Služba změny údajů v certifikátu není poskytována.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Služba změny údajů v certifikátu není poskytována.

4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji

Služba změny údajů v certifikátu není poskytována.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Služba změny údajů v certifikátu není poskytována.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádosti o zneplatnění certifikátu přijímá I.CA nepřetržitě pouze prostřednictvím předání žádosti elektronickou cestou a listovní zásilkou. Osobní předání na RA je možné pouze v pracovní době příslušné RA.

Zneplatnění certifikátu provede I.CA taktéž na základě podnětu subjektů oprávněných ze zákona.

Službu pozastavení platnosti certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických podpisů,
- je porušeno ustanovení smlouvy o poskytování kvalifikované certifikační služby ze strany držitele certifikátu, resp. podepisující osoby,
- nastanou-li skutečnosti uvedené v ZoEP a VoEP (např. neplatnost údajů v certifikátu).

I.CA si vyhrazuje právo akceptování i jiných podmínek na zneplatnění certifikátu, které však nesmí být v rozporu s ZoEP, VoEP.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Žádost o zneplatnění mohou podat:

- mandatář:
  - v případě, že hrozí nebezpečí zneužití jeho dat pro vytváření zaručeného elektronického podpisu,
  - poté, co se dozví, že mandant zemřel, byl právoplatně prohlášen za mrtvého, nebo zanikl,
  - poté, kdy zaniklo postavení orgánu veřejné moci,
- orgán veřejné moci nebo osoba, u které mandatář vykonával činnost nebo funkci podle zvláštního předpisu po tom, kdy mandatářovi zanikne nebo skončí výkon činnosti nebo funkce podle zvláštního předpisu,
- mandant - poté, kdy oprávnění mandatáře jednat za nebo jménem mandanta zaniklo,
- subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování kvalifikované certifikační služby v oblasti vydávání certifikátů,
- osoba oprávněná z pozůstalostního řízení mandatáře,
- poskytovatel certifikačních služeb (oprávněným žadatelem o zneplatnění certifikátu vydaného I.CA je v tomto případě ředitel I.CA):
  - v případě, že certifikát byl vydán na základě nepravdivých údajů,
  - pokud zjistí, že soukromý klíč, patřící k veřejnému klíči uvedenému v certifikátu, byl kompromitován,
  - pokud zjistí, že při vydání certifikátu nebyly splněny požadavky ZoEP,
  - dozví-li se prokazatelně, že podepisující osoba zemřela nebo zanikla nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil, nebo pokud údaje, na jejichž základě byl certifikát vydán, pozbyly pravdivosti,
- další subjekty, definované ZoEP.

4.9.3 Požadavek na zneplatnění certifikátu

V případě osobního předání žádosti o zneplatnění certifikátu na RA musí žádost obsahovat sériové číslo certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“), celé občanské jméno fyzické osoby, které byl certifikát vydán a heslo pro zneplatnění. Pokud si tato osoba heslo pro zneplatnění nepamatuje, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla primárního osobního dokladu předloženého při žádosti o vydání certifikátu. Tímto primárním osobním dokladem se musí pracovníkovi RA prokázat. Pracovník RA předá výše uvedenou žádost (dálkovým přístupem) na provozní pracoviště

certifikační autority. Odpovědný pracovník CA rozhodne, zda je žádost oprávněná a rozhodnutí sdělí prostřednictvím pracovníka RA. V případě, že je žádost oprávněná, je okamžik přijetí této žádosti na provozní pracoviště certifikační autority zároveň datem a časem zneplatnění tohoto certifikátu. V případě, že žádost nelze akceptovat (nesprávné heslo pro zneplatnění, neprokazatelná identita fyzické osoby), pokusí se pracovník RA v součinnosti s touto fyzickou osobou tyto skutečnosti napravit a pokud to z libovolného důvodu nebude možné, žádost o zneplatnění certifikátu bude zamítnuta.

V případě předání žádosti o zneplatnění certifikátu elektronickou cestou jsou přípustné následující možnosti:

- Elektronicky podepsaná elektronická zpráva - tělo zprávy musí být následujícího tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  nebo

  Žádám o zneplatnění certifikátu číslo = xxxxxxx

  kde „xxxxxxx“ je sériové číslo certifikátu a musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

- Elektronicky nepodepsaná elektronická zpráva - tělo zprávy musí být následujícího tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  Heslo pro zneplatneni = yyyyyy

  nebo

  Žádám o zneplatnění certifikátu číslo = xxxxxxx

  Heslo pro zneplatnění = yyyyyy

  kde „xxxxxxx“ je sériové číslo certifikátu a „yyyyyy“ je heslo pro zneplatnění. Sériové číslo musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

  Pokud žádost splňuje požadavky výše uvedených dvou možností, odpovědný pracovník CA neprodleně certifikát zneplatní.

- Prostřednictvím formuláře na k tomuto účelu vyhrazené internetové informační adrese http://www.ica.cz/.

Datum a čas zneplatnění certifikátu ve třech výše uvedených možnostech je určen okamžikem přijetí platné žádosti o zneplatnění certifikátu informačním systémem CA. V případě, že žádost nesplňuje požadavky, je zamítnuta a žadatel je elektronickou cestou o této skutečnosti informován. O kladném vyřízení není žadatel explicitně informován a tuto skutečnost zjistí v nejbližším vydaném seznamu zneplatněných certifikátů.

V případě **použití listovní zásilky žádosti o zneplatnění certifikátu** musí být v zásilce uvedena žádost v následujícím tvaru (v českém nebo slovenském jazyce):

Žádám o zneplatnění certifikátu číslo = xxxxxxx

Heslo pro zneplatnění = yyyyyy

kde „xxxxxxx“ je sériové číslo certifikátu a „yyyyyy“ je heslo pro zneplatnění.

Sériové číslo je buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“). Pokud si žadatel heslo pro zneplatnění nepamatuje, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla primárního osobního dokladu předloženého při žádosti o vydání certifikátu a žádost vlastnoručně podepsat.

V případě, že žádost uvedené požadavky splňuje, odpovědný pracovník CA certifikát v informačním systému CA zneplatní - datum a čas zneplatnění certifikátu je určen přijetím tohoto požadavku informačním systémem CA. V případě, že žádost nelze akceptovat (nesprávné heslo pro zneplatnění) bude žádost o zneplatnění certifikátu zamítnuta.

O vyřízení žádosti je žadatel informován doporučeným dopisem na poštovní adresu uvedenou jako adresa odesilatele.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Služba odkladu požadavku na zneplatnění certifikátu není poskytována.

4.9.5 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu

Reakcí I.CA na přijetí platné žádosti o zneplatnění certifikátu je jeho neprodlené zneplatnění. Do doby zveřejnění seznamu zneplatněných certifikátů je dotyčný certifikát zablokován[2]. Maximální prodlení mezi zneplatněním certifikátu a zveřejněním seznamu zneplatněných certifikátů, na kterém je tento certifikát poprvé uveden, je nejvýše 24 hodin.

Odblokování certifikátu, který byl zablokován na základě platné žádosti o jeho zneplatnění, I.CA nepovoluje.

4.9.6 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn

Spoléhající se strany jsou povinny provádět veškeré úkony, uvedené v kapitole 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je společností První certifikační autorita, a.s., vydáván v pravidelných intervalech, nejvýše 24 hodin od vydání předchozího CRL (zpravidla v osmihodinových intervalech).

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

V procesu vydávání CRL je s ohledem na platnou legislativu vždy dodrženo ustanovení kapitoly 4.9.5.

4.9.9 Možnost ověřování statutu certifikátu on-line („dále OCSP“)

Služba může být poskytována smluvním partnerům za specifických podmínek.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

Viz kapitola 4.9.9.

[2] Stav, ve kterém se certifikát nachází od doby, kdy jej I.CA zneplatnila, do doby, kdy I.CA zveřejnila CRL, ve kterém je tento certifikát poprvé zařazen.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Jiné než výše uvedené způsoby oznamování zneplatnění certifikátu nejsou podporovány.

4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Postup pro zneplatnění certifikátu v případě kompromitace dat pro vytváření elektronických podpisů není odlišný od výše popsaného postupu pro zneplatnění certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Služba pozastavení platnosti certifikátu není poskytována.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Služba pozastavení platnosti certifikátu není poskytována.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Služba pozastavení platnosti certifikátu není poskytována.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Služba pozastavení platnosti certifikátu není poskytována.

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaném certifikátu.

4.10.2 Dostupnost služeb

I.CA garantuje zajištění nepřetržité dostupnosti (7 dní v týdnu, 24 hodin denně) a integrity seznamu zneplatněných certifikátů.

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb stavu certifikátu nejsou stanoveny. I.CA může bez udání důvodu poskytování charakteristik služeb stavu certifikátu rozšířit, přitom je povinna dodržet příslušná ustanovení ZoEP a VoEP.

4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo označující osobu

I.CA ukončí poskytování služeb držiteli certifikátu, resp. podepisující osobě, ve chvíli, kdy:

- skončila platnost certifikátu, aniž by bylo v souladu s touto CP požádáno o vydání následného certifikátu,
- dojde k ukončení smlouvy o poskytování kvalifikovaných certifikačních služeb mezi držitelem certifikátu a I.CA s výjimkou služby zneplatnění certifikátu, která je poskytována po celou dobu platnosti tohoto certifikátu.

4.12 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek u důvěryhodné třetí strany a jejich obnova

Služba úschovy dat pro vytváření elektronických podpisů není poskytována.

4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Služba úschovy dat pro vytváření elektronických podpisů není poskytována.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci

Služba zapouzdřování a obnovování šifrovacího klíče pro relaci není poskytována.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Oblasti managementu provozní a fyzické bezpečnosti jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, Systémová bezpečnostní politika CA, Certifikační prováděcí směrnice, Plán pro zvládání krizových situací a plán obnovy, tak v upřesňujících bezpečnostních normách a směrnicích. Uvedené dokumenty reflektují výsledky periodicky provedené analýzy rizik.

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Objekty provozního pracoviště jsou umístěny v geograficky odlišných lokalitách, které jsou dále jiné, než ředitelství společnosti, obchodní a vývojová pracoviště, pracoviště registračních autorit a obchodních míst.

Zařízení určená k výkonu hlavních certifikačních služeb jsou umístěna ve vyhrazených prostorách provozních pracovišť. Tyto prostory jsou zabezpečené obdobně jako zabezpečené oblasti kategorie „Důvěrné“ podle zákona ČR o ochraně utajovaných informací.

5.1.2 Fyzický přístup

Požadavky na fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozních pracovišť jsou uvedeny v interní dokumentaci společnosti. Ochrana objektů je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a případně speciálním systémem pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků.

5.1.3 Elektřina a klimatizace

V prostorách určených k výkonu hlavních certifikačních služeb je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20°C ± 5°C. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply), resp. diesel agregátu.

5.1.4 Vlivy vody

Všechny kritické systémy provozních pracovišť jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště jsou dle potřeby vybavena čidly.

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení, určená k výkonu hlavních certifikačních služeb, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

5.1.6 Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v kovových skříních, popř. trezorech. Kopie jsou ukládány v jiné geografické lokalitě, než kde je umístěno provozní pracoviště.

Papírová média, která je nutno, mj. dle ZoEP a VoEP, ukládat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

Veškerý papírový kancelářský odpad je před opuštěním pracovišť CA znehodnocen skartováním.

5.1.8 Zálohy mimo budovu

Kopie provozních záloh jsou uloženy na místě určeném ředitelem I.CA a popsaném v interní dokumentaci.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou ve společnosti I.CA definovány důvěryhodné role, které jsou spolu s odpovídajícími činnostmi a odpovědnostmi popsány v interní dokumentaci.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Ve společnosti První certifikační autorita, a.s., jsou pro procesy poskytování kvalifikovaných certifikačních služeb definovány činnosti, které se musí vykonávat jedině za účasti více než jediné osoby. Jedná se zejména o:

- generování párových dat pro vytváření/ověřování elektronické značky/elektronické pečetě vydávaných certifikátů a seznamů zneplatněných certifikátů,
- ničení dat pro vytváření elektronické značky/elektronické pečetě vydávaných certifikátů a seznamů zneplatněných certifikátů,
- aktivace kryptografického modulu, obsahujícího data pro vytváření elektronické značky/elektronické pečetě vydávaných certifikátů a seznamů zneplatněných certifikátů.

Pro provádění ostatních úloh není počet přítomných osob určen, musí však jít výhradně o pověřené pracovníky.

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci (jméno, certifikát) a autentizaci (heslo, soukromý klíč) k těm komponentám, které jsou pro jejich činnost nezbytné.

5.2.4 Role vyžadující rozdělení povinností

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou definované v interní dokumentaci.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Pracovníci I.CA v důvěryhodných rolích jsou vybíráni a přijímáni na základě dále popsaných personálních kritérií:

- naprostá občanská bezúhonnost - prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z rejstříku trestů nebo čestné prohlášení),
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně 3 roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně 5 let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně 1 rok v oblasti poskytování certifikačních služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti,
- v jednotlivých případech lze zkrátit délku uvedené praxe až o jednu třetinu stanovené délky na základě přezkoušení, při němž pracovník prokáže dostatečné znalosti k výkonu své funkce.

Ostatní pracovníci I.CA, podílející se přímo na poskytování certifikačních služeb, jsou přijímáni na základě následujících kritérií:

- vysokoškolské vzdělání v rámci akreditovaného bakalářského, resp. magisterského studijního programu, nebo středoškolské vzdělání,
- základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací všech kmenových pracovníků I.CA v důvěryhodných rolích jsou:

- sami tito pracovníci,
- osoby, které tyto pracovníky znají,
- veřejné zdroje informací.

Pracovníci při přijímání do pracovního poměru poskytují osobním pohovorem prvotní informace, které jsou aktualizovány při periodických pohovorech s nadřízeným pracovníkem v průběhu pracovního poměru.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Pracovníci I.CA jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samopřípravy a metodickým vedením již zaškoleným pracovníkem. Běžná doba na zaškolení je jeden měsíc.

5.3.4 Požadavky a periodicita školení

Pro kmenové pracovníky v důvěryhodných rolích pořádá vedení I.CA minimálně jedenkrát ročně interní výukový seminář, zaměřený na problematiku bezpečnosti informací.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti v mimořádných případech jsou pracovníci I.CA motivováni k získávání znalostí potřebných pro zastávání jiné role v I.CA.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Při zjištění neautorizované činnosti je s dotyčným pracovníkem postupováno způsobem uvedeným v interních dokumentech společnosti a řídícím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

I.CA může nebo musí některé činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými certifikačními politikami, relevantními částmi interní dokumentace I.CA, které jim budou poskytnuty, a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci I.CA mají k dispozici kromě certifikační politiky, certifikační prováděcí směrnice, bezpečnostní a provozní dokumentace veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

5.4 Auditní záznamy (logy)

5.4.1 Typy zaznamenávaných událostí

S ohledem na skutečnost, že I.CA je akreditovaným poskytovatelem certifikačních služeb, jsou v procesu poskytování těchto služeb zaznamenávány veškeré události požadované ZoEP a VoEP.

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní bezpečnostní dokumentaci, v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány v souladu s požadavky ZoEP.

5.4.4 Ochrana auditních záznamů

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem, zajišťujícím ochranu před jejich změnami, krádeží a zničením (ať již úmyslným, tak neúmyslným).

Elektronické auditní záznamy jsou ukládány ve dvou kopiích, každá kopie je umístěna v jiné místnosti provozních prostor I.CA. Minimálně jedenkrát měsíčně se provádí uložení těchto auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

Auditní záznamy v papírové formě jsou umístěny mimo provozních prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je definována v interní bezpečnostní dokumentaci.

5.4.5 Postupy pro zálohování auditních záznamů

Zálohování elektronických auditních záznamů probíhá obdobným způsobem jako zálohování ostatních elektronických informací. Zálohování auditních záznamů v papírové formě prováděno není.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Auditní záznamy jsou shromažďovány v rámci jednotlivých subsystémů.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s., prováděno v periodických intervalech, v případě incidentu, majícího vliv na bezpečnost poskytovaných služeb, okamžitě.

5.5 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je u I.CA prováděno dle požadavků ZoEP a VoEP a dle interní dokumentace, která je s těmito legislativními normami v souladu.

5.5.1 Typy informací a dokumentace, které se uchovávají

I.CA uchovává níže uvedené typy informací a dokumentaci (v elektronické nebo listinné podobě), které souvisejí s poskytovanými certifikačními službami v oblasti vydávání certifikátů, zejména:

- smlouvy o poskytování kvalifikované certifikační služby, včetně žádosti o poskytování služby,
- kopie dokladů, předkládaných při uzavření smlouvy o poskytování kvalifikované certifikační služby,
- potvrzení o převzetí certifikátu, případně souhlas s jeho zveřejněním v seznamu vydaných certifikátů,
- prohlášení držitele certifikátu o tom, že mu byly před uzavřením smlouvy o poskytování kvalifikované certifikační služby poskytnuty písemné informace o přesných podmínkách pro využívání této služby, o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je či není poskytovatel kvalifikovaných certifikačních služeb akreditován,
- dokumenty a záznamy související s životním cyklem vydaného certifikátu včetně tohoto certifikátu,
- další záznamy požadované ZoEP a VoEP,
- aplikační programové vybavení a veškerá dokumentace společnosti, která je nutná pro provádění kontrol,
- identifikace místa, kde jsou uloženy informace a dokumentace, jejichž uchování je vyžadováno ZoEP a VoEP,
- veškeré seznamy zneplatněných certifikátů,
- identifikační údaje osoby, která provedla ověření totožnosti žadatele o certifikát, popř. zmocnitele včetně obchodního názvu případného smluvního partnera, který tuto činnost pro I.CA zajišťuje,
- záznam o manipulaci (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby) s informacemi,
- provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování uchovávaných informací a dokumentace

I.CA zajišťuje uchovávání informací a dokumentace dle kapitoly 5.5.1 v souladu s požadavky ZoEP.

Po celou dobu existence I.CA jsou uchovávány informace, vztahující se ke kvalifikovaným systémovým certifikátům CA/certifikátům na správu, využívaným v procesech vydávání certifikátů koncovým uživatelům a seznamů zneplatněných certifikátů s výjimkou příslušných dat pro vytváření elektronické značky/elektronické pečetě.

Postupy při uchovávání informací a dokumentace jsou upraveny interní dokumentací I.CA.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Uchovávané informace a dokumentace obsahují i osobní data klientů, proto je vzhledem k platné legislativě dbáno zvýšené ochrany těchto dat. Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny formou opatření vycházejících z požadavků objektové a fyzické bezpečnosti.

Postupy při ochraně úložiště uchovávaných informací a dokumentace jsou upraveny interní dokumentací I.CA.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací I.CA.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V případě, že jsou využívána časová razítka, jedná se o kvalifikovaná časová razítka, vydávaná I.CA.

5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)

Informace a dokumentace jsou ukládány na místo určené ředitelem I.CA. Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směrnicemi. Shromažďování uchovávaných informací je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Uchovávané informace a dokumentace jsou umístěny v určených lokalitách a jsou přístupné:

- zaměstnancům I.CA, pokud je to k jejich činnosti vyžadováno,
- oprávněným kontrolním subjektům, orgánům činných v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna dat pro ověřování elektronických značek v nadřízeném kvalifikovaném systémovém certifikátu poskytovatele

Výměna dat pro ověřování elektronických značek/elektronických pečetí v nadřízeném kvalifikovaném systémovém certifikátu CA/certifikátu na správu je v případě standardních situací (uplynutí platnosti certifikátu) s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) prováděna formou vydání nového nadřízeného kvalifikovaného systémového certifikátu CA/certifikátu na správu, obsahujícího nová data pro ověřování elektronických značek/elektronických pečetí poskytovatele.

V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu tvorby elektronických značek/elektronických pečetí, tzn. změny kryptografických algoritmů, délky klíčů atd.) je tato činnost prováděna v adekvátním časovém období.

Jak v případě standardních situací, tak nestandardních situací, je výměna dat pro ověřování elektronických značek/elektronických pečetí v nadřízeném kvalifikovaném systémovém certifikátu CA/certifikátu na správu držitelům certifikátů a veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

V případě výskytu uvedených událostí postupuje I.CA v souladu s interními dokumenty, obsahujícími plány pro zvládání krizových situací a plán obnovy.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

V případě poškození výpočetních prostředků, softwaru nebo dat postupuje I.CA v souladu s interními dokumenty, obsahujícími plány pro zvládání krizových situací a plán obnovy.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek poskytovatele

V případě vzniku důvodné obavy z kompromitace dat pro vytváření elektronických značek/elektronických pečetí pro elektronické označování/elektronické podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů I.CA:

- ukončí jejich používání,
- okamžitě a trvale zneplatní příslušný kvalifikovaný systémový certifikát CA/certifikát na správu a zničí jemu odpovídající data pro vytváření elektronických značek/elektronických pečetí,
- oznámí příslušnému úřadu informaci o zneplatnění příslušného kvalifikovaného systémového certifikátu CA/certifikátu na správu s uvedením důvodu zneplatnění,
- zneplatní všechny platné certifikáty, které byly výše uvedenými daty elektronicky označeny/elektronicky podepsány,
- pokud je to možné, informuje držitele platných certifikátů o zneplatnění těchto certifikátů, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, kterou tyto osoby uvedly v žádosti o vydání certifikátu; součástí této informace je důvod ukončení platnosti příslušného kvalifikovaného systémového certifikátu CA/certifikátu na správu,
- bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese a v nejméně jednom celostátně distribuovaném deníku (viz kapitola 2.2); pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,

Obdobný postup bude uplatněn i v případě, že dojde k takovému vývoji kryptoanalytických metod (např. změny kryptografických algoritmů, délky klíčů atd.), že by mohla být bezprostředně ohrožena bezpečnost procesu vydávání certifikátů a seznamu zneplatněných certifikátů.

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interními dokumenty, obsahujícími plány pro zvládání krizových situací a plán obnovy.

5.8 Ukončení činnosti CA nebo RA

V případě plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů, tzn. z jiných důvodů, než jsou mimořádné události, jakými jsou stávky, občanské nepokoje, válečný stav, přírodní katastrofy celostátního rozsahu nebo jiné výsledky působení vyšší moci, zajistí I.CA provedení následujících činností:

- Certifikáty vydané v souladu s legislativou České republiky:
  - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 3 měsíce před plánovaným ukončením činnosti,
  - vynaloží veškeré možné úsilí pro to, aby evidence vedená dle platné legislativy byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání certifikátů; v případě, že se jí nepodařilo tuto evidenci předat jinému kvalifikovanému poskytovateli certifikačních služeb v oblasti vydávání certifikátů, ohlásí nejpozději 30 dnů před plánovaným datem ukončení činnosti tuto skutečnost příslušnému úřadu a zajistí předání této evidence příslušnému úřadu - tuto informaci zahrne do zprávy odeslané všem svým klientům, kteří jsou držiteli platných smluv o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů, pokud toto bude známo nejméně 2 měsíce před plánovaným ukončením činnosti,
  - zpřístupní informaci o ukončení činnosti I.CA v oblasti vydávání certifikátů na své internetové informační adrese nejméně 2 měsíce před plánovaným ukončením činnosti,
  - ukončí poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů,
  - prokazatelné zničí svá data pro vytváření elektronických značek vydávaných certifikátů a seznamů zneplatněných certifikátů.
- Certifikáty vydané v souladu s legislativou Slovenské republiky:
  - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 6 měsíců před plánovaným ukončením činnosti,
  - ohlásí každému držiteli platného certifikátu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 6 měsíců před plánovaným ukončením činnosti,
  - může se dohodnout s jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání certifikátů o převzetí záznamů o vydaných a zrušených certifikátech a provozní dokumentaci – pokud žádný kvalifikovaný poskytovatel certifikačních služeb v oblasti vydávání certifikátů tyto záznamy nepřevezme:
    - zaniká platnost všech jí vydaných certifikátů ode dne zániku jako akreditovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů,
    - převezme tyto záznamy úřad.

V případě ukončení činnosti konkrétního pracoviště RA je tato skutečnost oznámena na internetové adrese http://www.ica.cz, případně formou vývěsky (je-li to možné) na pracovišti této RA.

V případě odnětí akreditace I.CA bez prodlení informuje o této skutečnosti nejen subjekty, kterým poskytuje své kvalifikované certifikační služby, ale i další dotčené osoby způsobem uvedeným v kapitolách 2.2 a 2.3.

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat CA (soukromý klíč, kterým CA elektronicky označuje/elektronicky podepisuje vydávané certifikáty a seznamy zneplatněných certifikátů a veřejný klíč sloužící pro ověřování těchto elektronických značek/elektronických pečetí), které probíhá v zabezpečené zóně v souladu s dokumentem Systémová bezpečnostní politika CA a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 úroveň 3 a mj. tedy splňuje požadavky ZoEP a VoEP. Veškeré požadavky na proces generování párových dat CA jsou definovány v interní bezpečnostní dokumentaci.

I.CA z principiálních bezpečnostních důvodů neposkytuje službu generování párových dat žadatele o certifikát na svých zařízeních.

6.1.2 Předání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek podepisující nebo označující osobě

Služba generování párových dat žadatele o certifikát a tedy předání dat pro vytváření elektronických podpisů podepisující osobě není neposkytována.

6.1.3 Předání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek poskytovateli certifikačních služeb

Veřejný klíč žadatele o certifikát je poskytovateli certifikačních služeb doručen v elektronické podobě - v žádosti o certifikát ve formátu PKCS#10.

6.1.4 Poskytování dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek certifikační autoritou spoléhajícím se stranám

Data pro ověřování elektronických značek/elektronických pečetí vydaných certifikátů a seznamů zneplatněných certifikátů, jsou obsažena v kvalifikovaném systémovém certifikátu CA/certifikát na správu, jehož získání je garantováno následujícími způsoby:

- obdržením na RA (osobní návštěva),
- prostřednictvím internetových informačních adres I.CA a příslušného akreditačního úřadu, případně prostřednictvím věstníku tohoto úřadu.

Získání dat pro ověřování elektronických podpisů koncových uživatelů formou certifikátů veřejných klíčů je popsáno v kapitole 2.2.

6.1.5 Délky párových dat

V procesu poskytování kvalifikovaných certifikačních služeb využívá I.CA výhradně nejprověřenější klasický asymetrický algoritmus RSA. Mohutnost klíčů (resp. parametrů

daného algoritmu) použitých pro elektronické označování/elektronické podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je 2048 bitů, mohutnost klíčů (resp. parametrů daného algoritmu) na straně klienta je 2048 bitů.

6.1.6 Generování parametrů dat pro ověřování elektronických podpisů nebo dat pro vytváření elektronických značek a kontrola jejich kvality

Algoritmy použité pro generování celočíselných hodnot nutných pro fungování elektronického podpisu (např. testy prvočíselnosti atd.), mají parametry uvedené v platné legislativě (ZoEP, VoEP), resp. v ní odkazovaných technických standardech nebo normách.

I.CA kontroluje povolenou délku dat pro ověřování elektronických podpisů a možný dvojí výskyt stejných dat pro ověření elektronických podpisů ve vydávaných certifikátech. V případě duplicitního výskytu dat pro ověření elektronických podpisů je žadatel o certifikát požádán o vygenerování nových párových dat. Již vydaný certifikát je neprodleně zneplatněn, držitel takového certifikátu je o tomto neprodleně a vhodným způsobem informován a vyzván ke generování nových párových dat.

6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů nebo dat pro vytváření elektronických značek

Uvedeno v kapitole 1.4.

6.2 Ochrana dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a bezpečnost kryptografických modulů

6.2.1 Standardy a podmínky používání kryptografických modulů

Generování párových dat I.CA a uložení soukromého klíče I.CA, sloužícího pro vytváření elektronických značek/elektronických pečetí vydávaných certifikátů a seznamů zneplatněných certifikátů, probíhá v kryptografickém modulu, který splňuje požadavky platné legislativy vztahující se k problematice elektronického podpisu, tedy standardu FIPS PUB 140-2 úroveň 3.

6.2.2 Sdílení tajemství

Při provádění citlivých činností (viz kapitoly 6.1.1 a 6.2.10) je nezbytná přítomnost tří pracovníků I.CA v důvěryhodných rolích, z nichž dva znají část kódu k provedení těchto činností.

6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Služba úschovy dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek není poskytována.

6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Kryptografický modul použitý pro správu párových dat I.CA, umožňuje zálohování soukromého klíče sloužícího pro vytváření elektronických značek/elektronických pečetí vydávaných certifikátů a seznamů zneplatněných certifikátů. Soukromý klíč je zálohován s využitím nativních prostředků konkrétního kryptografického modulu v zašifrované podobě.

6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Po uplynutí doby platnosti soukromého klíče určeného k vytváření elektronických značek/elektronických pečetí vydávaných certifikátů a seznamů zneplatněných certifikátů je tento (včetně záloh) zničen a jeho další zálohování se neprovádí. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, proto je u I.CA zakázáno.

6.2.6 Transfer dat pro vytváření elektronických značek do kryptografického modulu nebo z kryptografického modulu

Soukromý klíč sloužící pro vytváření elektronických značek/elektronických pečetí vydávaných certifikátů a seznamů zneplatněných certifikátů, je generován přímo v kryptografickém modulu.

Vkládání soukromého klíče do kryptografického modulu v případě, že se jedná o jeho obnovení ze šifrované zálohy, probíhá za přímé osobní účasti nejméně dvou určených pracovníků I.CA. V okamžiku jeho vkládání musí být vyhrazená stanice a kryptografický modul odpojeny od počítačové sítě. O vložení soukromého klíče je pořízen písemný záznam.

6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

Soukromý klíč, sloužící k vytváření elektronických značek/elektronických pečetí, je uložen bezpečným způsobem v kryptografickém modulu, splňujícím požadavky platné legislativy.

6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Aktivaci soukromého klíče sloužícího pro vytváření elektronických značek/elektronických pečetí vydávaných certifikátů a seznamů zneplatněných certifikátů, vygenerovaného v kryptografickém modulu, provádí určení pracovníci I.CA prostřednictvím vlastní aktivace kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. Po aktivaci je systém připraven k elektronickému označování/elektronickému podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a aktivační čipová karta se vyjme. Po aktivaci je zařízení přístupné pouze určeným odpovědným pracovníkům I.CA.

6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Deaktivaci soukromého klíče sloužícího pro vytváření elektronických značek/elektronických pečetí vydávaných certifikátů a seznamů zneplatněných certifikátů, provádí určení pracovníci I.CA prostřednictvím kryptografického modulu a aktivační čipové karty podle přesně

určeného postupu, který je upraven interní dokumentací. O provedené deaktivaci je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Soukromý klíč sloužící k elektronickému označování/elektronickému podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je uložen v kryptografickém modulu. Ničení soukromého klíče je realizováno prostředky kryptografického modulu. Zálohy soukromých klíčů uložených v zašifrované podobě na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů. Veškeré požadavky na proces ničení soukromého klíče, sloužícího k elektronickému označování/elektronickému podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, jsou definovány v interní bezpečnostní dokumentaci.

6.2.11 Hodnocení kryptografických modulů

Nástroj elektronického podpisu pro elektronické označování/elektronické podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, byl certifikován na shodu s požadavky standardu FIPS PUB 140-2 úroveň 3.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Problematika uchovávání dat pro ověřování elektronických značek/elektronických pečetí je řešena v souladu s ZoEP a VoEP.

6.3.2 Maximální doba platnosti certifikátu vydaného podepisující nebo označující osobě a párových dat

Maximální doba platnosti každého vydaného certifikátu je uvedena v těle tohoto certifikátu.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou vytvářena v průběhu procesu instalace, kdy jsou generována párová data I.CA sloužící pro vytváření a ověřování elektronických značek/elektronických pečetí vydávaných certifikátů a seznamů zneplatněných certifikátů.

6.4.2 Ochrana aktivačních dat

Výše uvedená aktivační data jsou pracovníky I.CA chráněna způsobem uvedeným v interní bezpečnostní dokumentaci.

6.4.3 Ostatní aspekty aktivačních dat

Výše uvedená aktivační data jsou určena výhradně pro procesy poskytování kvalifikovaných certifikačních služeb a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů je definována ZoEP a VoEP.

Detailní řešení specifických technických požadavků počítačové bezpečnosti je popsáno v interní dokumentaci.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení bezpečnosti I.CA je založeno na mezinárodních a národních standardech, zejména:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements/Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis – část 1: Požadavky na bezpečnost systémů, resp. CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements / Bezpečnostné požiadavky na dôveryhodné systémy spravujúce certifikáty pre elektronický podpis – časť 1: Požiadavky na bezpečnosť systémov.
- ČSN ETSI TS 101 456 V1.4.3 - Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty, resp. ETSI TS 101 456 V1.4.3 – Electronic Signatures and Infrastructures; Policy Requirements for Certification Authorities Issuing Qualified Certificates / Elektronické podpisy a infraštruktúry; Požiadavky na postupy certifikačnej autority vydávajúcej kvalifikované certifikáty.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky, resp. STN ISO/IEC 27001 Information Technology. Security Techniques. Information Security Management Systems. Requirements / Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací, resp. STN ISO/IEC 27002 Information Technology. Security Techniques. Code of Practice for Information Security Controls / Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.
- ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací, resp. STN ISO/IEC 27005 Information Technology. Security Techniques. Information Security Risk Management / Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.6.2 Kontroly řízení bezpečnosti

Soulad se standardy (viz kapitola 6.5.2), ZoEP a VoEP je ověřován pravidelnými audity systému managementu bezpečnosti informací, prováděnými pracovníky nezávislých auditorských firem, a kontrolami bezpečnostní shody, prováděnými pracovníky I.CA. Tato problematika je popsána v interní dokumentaci. I.CA si vyhrazuje právo provádění i jiných typů kontrol, resp. auditů.

6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je v I.CA je vytvářeno procesním přístupem typu „Plánování-Zavedení-Kontrola-Využití“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování – definování bezpečnostní politiky, plánů, cílů, procesů a postupů s ohledem na řízení rizik a bezpečnost informací tak, aby byly v souladu s celkovou bezpečnostní politikou,
- implementace a provoz - bezpečnostní politiky, plánů, cílů, procesů a postupů,
- monitorování a přehodnocování – posouzení procesu s ohledem na bezpečnostní politiku a předání poznatků vedení společnosti k posouzení,
- využití – na základě rozhodnutí vedení organizace provedení nápravných opatření.

6.7 Síťová bezpečnost

V prostředí I.CA nejsou prostředky provádějící vlastní kvalifikované certifikační služby přímo dostupné z veřejné sítě Internet. Informační systém je mimo jiné chráněn komerčním produktem typu firewall. Veškerá komunikace mezi RA a provozním pracovištěm certifikační autority je vedena šifrovaně. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci.

6.8 Časová razítka

Řešení je uvedeno v kapitole 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

tab. 3 – Profil certifikátu

Položka	Obsah	Pozn.
Version	v3 (0x2)	
serialNumber	jedinečné sériové číslo vydávaného certifikátu	
SignatureAlgorithm	identifikátor algoritmu, použitého pro elektronickou značku/pečeť tohoto certifikátu	
Issuer	informace o vydavateli certifikátu	
Validity	1 rok	
Subject	informace o mandatáři a mandantovi/ mandátu	viz tab. 4
subjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	veřejný klíč podepisující osoby	
Extensions	rozšiřující položky certifikátu	viz tab. 5
Signature	elektronická značka/elektronická pečeť vydavatele certifikátu	

tab. 4 - Subject

	Položka	Obsah
Mandatář	commonName	povinná položka: složená z položek givenName a surName, doplněných dle požadavků příslušné CPS, např. givenName surName OPRÁVNENIE x N kde: x – konkrétní číslo oprávnění N – konkrétní název oprávnění
	givenName	povinná položka: křestní jméno/jména
	surName	povinná položka: příjmení
	title	nepovinná položka: pozice ve firmě, identifikátor
	serialNumber	povinná položka: ICA – číslo (generuje I.CA)
	serialNumber	povinná položka: rodné číslo ve tvaru PNOSK-

		rodné_číslo, nebo číslo identifikačního průkazu nebo cestovního pasu (v případě občanů ČR/SK se jedná o občanský průkaz) ve tvaru IDCxx-číslo_dokladu resp. PASxx-číslo_dokladu, kde xx je kód státu
	serialNumber	povinná položka v případě, že je současně uveden serialNumber=PNOSK-rodné číslo, pokud není uveden, položka je nepovinná: může obsahovat číslo cestovního pasu nebo identifikačního průkazu (v případě občanů ČR/SK se jedná o občanský průkaz) ve tvaru PASxx-číslo_dokladu, resp. IDCxx-číslo_dokladu, kde xx je kód státu
	organizationName	povinná položka: zaměstnavatel mandatáře (resp. mandatář u této organizace vykonává činnost nebo funkci podle zvláštního předpisu) v případě, že mandatář poskytuje služby jako fyzická osoba, uvede se jméno a příjmení tak, jak je uvedeno v registru
	organizationalUnitName	nepovinná položka: může obsahovat název dílčího organizačního členění
	serialNumber	povinná položka: identifikační údaj zaměstnavatele mandatáře (resp. mandatář u této organizace vykonává činnost nebo funkci podle zvláštního předpisu) v jednom z tvarů: VATxx-id nebo SZ:xx-id nebo NTRxx-id kde: xx - kód státu id – viz 3.2.2
	countryName	povinná položka: kód státu trvalého pobytu mandatáře
	localityName	nepovinná položka: adresa mandatáře
	stateOrProvinceName	nepovinná položka: nižší územní správní celek mandatáře
Mandant	givenName	povinná položka v případě fyzické osoby: křestní jméno/jména
	surName	povinná položka v případě fyzické osoby: příjmení
	serialNumber	povinná položka v případě fyzické osoby - občana SK: rodné číslo ve tvaru PNOSK-rodné_číslo
	serialNumber	povinná položka v případě fyzické osoby: číslo cestovního pasu nebo identifikačního průkazu (v případě občanů ČR/SK se jedná o občanský průkaz) ve tvaru PASxx-číslo_dokladu, resp. IDCxx-číslo_dokladu, kde xx je kód státu
	organizationName	povinná položka v případě fyzické osoby – zaměstnance nebo právnické osoby/orgánu

		veřejné moci: MANDANT zaměstnavatel mandanta
	serialNumber	povinná položka v případě fyzické osoby – zaměstnance nebo právnické osoby/orgánu veřejné moci: identifikační údaj zaměstnavatele mandanta v jednom z tvarů: VATxx-id nebo SZ:xx-id nebo NTRxx-id kde: xx - kód státu id – viz 3.2.2

7.1.1 Číslo verze

Všechny vydávané certifikáty jsou v souladu s X.509 ve verzi 3.

7.1.2 Rozšiřující položky v certifikátu

tab. 5 - Rozšiřující položky certifikátu

Položka	Obsah/Kritičnost	Pozn.
AuthorityKeyIdentifier.Key Identifier	hash veřejného klíče vydavatele certifikátu	nekritická, povinná
SubjectKeyIdentifier	hash veřejného klíče ve vydávaném certifikátu	nekritická, povinná
KeyUsage	digitalSignature, nonRepudiation	kritická, povinná
CertificatePolicies.		nekritická, povinná
.PolicyInformation(1)		
policyIdentifier	1.3.6.1.4.1.23624.1.1.202.1.2	politika, dle které I.CA vydá tento mandátní certifikát
[1.1]policyQualifiers .PolicyQualifierInfo(1) userNotice	Tento kvalifikovany certifikat je vydan podle zakona Ceske republiky c. 227/2000 Sb. v platnem zneni/This is qualified certificate according to Czech Act No. 227/2000 Coll.	
.PolicyInformation(2)		
policyIdentifier	1.3.158.36061701.0.0.0.1.2.2	
[2.1]policyQualifiers .PolicyQualifierInfo(1) userNotice	EN: Qualified certificate of mandate pursuant to Act No. 215/2002 Coll. and Decree No. 131/2009 Coll. SK: Kvalifikovany mandatny certifikat podla zakona c. 215/2002 Z.z. a vyhlasky c. 131/2009 Z.z.	
.PolicyInformation(3)		
policyIdentifier	1.3.158.36061701.1.1.x	x – konkrétní číslo oprávnění

[3.1]policyQualifiers .PolicyQualifierInfo(1) *cPSuri*	http://www.ica.cz	
[3.2]policyQualifiers .PolicyQualifierInfo(2) *userNotice*	EN: Authorization x N, SK: Opravnenie x N	x – konkrétní číslo oprávnění N – konkrétní název oprávnění
SAN.rfc822Name	e-mail adresa	nekritická, nepovinná
BasicConstraints cA	 False	nekritická, povinná
CRL Distribution Points	odkazy na soubor (HTTP URI), kde lze získat CRL	nekritická, povinná
AuthorityInfoAccess	odkaz na soubor (HTTP URI), ve kterém bude uložen certifikát vydávající CA	nekritická, povinná
QCStatements	esi4-qcStatement-1(id-etsi-qcs-QcCompliance)	nekritická, povinná
	esi4-qcStatement-4(id-etsi-qcs-QcSSCD)	
nsComment	číslo čipové karty	nekritická položka a povinná položka pouze v případě vydání certifikátu na čipovou kartu, generuje I.CA

I.CA si vyhrazuje právo výše uvedenou množinu rozšiřujících položek rozšířit, nebo omezit.

7.1.3 Objektové identifikátory (dále „OID") algoritmů

V procesu poskytování certifikačních služeb jsou využívány algoritmy, uvedené v platné legislativě, resp. v příslušných technických standardech, na které je touto legislativou odkazováno.

7.1.4 Způsoby zápisu jmen a názvů

Uvedeno v kapitole 3.1.

7.1.5 Omezení jmen a názvů

Jména a názvy uvedené v certifikátu musí, je-li to možné, přesně odpovídat údajům v dokladech, kterými žadatel o certifikát nebo podepisující osoba prokazují svoji totožnost, popř. v plné moci.

V případě nutnosti krácení textů z důvodů překročení povolené délky (uvedena v příslušném technickém standardu, např. RFC 5280) je postupováno v souladu s příslušnou legislativou ČR/SK.

7.1.6 OID certifikační politiky

Viz tabulka 5.

7.1.7 Rozšiřující položka „Policy Constrainsts“

Není aplikováno.

7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“

Viz tabulka 5.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz tabulka 5.

7.2 Profil seznamu zneplatněných certifikátů

tab. 6 - Profil CRL

Položka	Obsah
Version	v2
SignatureAlgorithm	identifikátor a parametry algoritmu, použitého I.CA pro elektronickou značku/elektronickou pečeť vydávaného CRL
Issuer	označení vydavatele CRL
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	jedinečné sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
reasonCode	důvod zneplatnění certifikátu
crlExtensions	rozšiřující položky CRL (viz tab. 7)

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X.509 verze 2.

7.2.2 Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů

tab. 7 - Rozšiřující položky CRL

Položka	Obsah	Kritická
AutorityKeyIdentifier.KeyIdentifier	hash veřejného klíče vydavatele CRL	NE
CRL Number	Číslo CRL	NE

7.3 Profil OCSP

Viz kapitola 4.9.9.

7.3.1 Číslo verze

Viz kapitola 4.9.9.

7.3.2 Rozšiřující položky OCSP

Viz kapitola 4.9.9.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

S ohledem na skutečnost, že společnost První certifikační autorita, a.s., je akreditovaným poskytovatel certifikačních služeb, jsou periodicity hodnocení, včetně okolností pro provádění hodnocení, striktně dány požadavky ZoEP a VoEP, jedná se zejména o audit systému řízení bezpečnosti informací, kontroly bezpečnostní shody a audit bezpečnosti poskytování certifikačních činností.

Společnost První certifikační autorita, a.s., si vyhrazuje právo provádění i jiných forem hodnocení.

8.2 Identita a kvalifikace hodnotitele

Hodnocení vyžadované ZoEP a VoEP provádějí hodnotitelé splňující požadavky těchto legislativních norem.

8.3 Vztah hodnotitele k hodnocenému subjektu

V případě hodnocení požadovaného ZoEP a VoEP je vztah hodnotitele k poskytovateli certifikačních služeb dán danou legislativou.

V ostatních případech je vztah hodnotitele k hodnocenému subjektu definován příslušným standardem.

8.4 Hodnocené oblasti

V případě hodnocení požadovaného ZoEP a VoEP jsou hodnocené oblasti konkretizovány touto legislativou, v ostatních případech jsou hodnocené oblasti dány standardy, dle kterých je hodnocení prováděno.

8.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manažer I.CA, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat certifikační služby v souladu s ZoEP, VoEP, přeruší I.CA vydávání certifikátů do doby, než budou nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána řediteli, resp. bezpečnostnímu manažerovi I.CA.

V nejbližším možném termínu svolá bezpečnostní manažer I.CA schůzi bezpečnostního výboru, na které musí být přítomni členové vedení společnosti, které s obsahem závěrečné zprávy seznámí.

Sdělování výsledků hodnocení taktéž podléhá požadavkům ZoEP a VoEP.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za vydání certifikátu jsou uvedeny v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA. Služba obnovení certifikátu není poskytována.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup k vydaným veřejným certifikátům elektronickou cestou I.CA nezpoplatňuje.

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Přístup k informacím o zneplatněných certifikátech (aktuální CRL) elektronickou cestou I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Zneplatnění certifikátu a stažení elektronické verze této CP (ve všeobecně používaném formátu PDF) je poskytováno zdarma.

Poplatky za nadstandardní služby jsou stanovovány smluvně.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

I.CA si vyhrazuje právo změny výše poplatku za vydání prvotního, popř. následného certifikátu. I.CA je rovněž oprávněna stanovit pro individuálně uzavřené smlouvy odlišnou výši těchto poplatků.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

Společnost První certifikační autorita, a.s., prohlašuje, že má uzavřené pojištění podnikatelských rizik takovým způsobem, aby byly pokryty případné finanční škody.

9.2.2 Další aktiva a záruky

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiné zajištění na provoz v souladu s požadavky uvedenými v ZoEP a s ohledem na riziko vzniku odpovědnosti za škodu.

Podrobné informace o aktivech společnosti První certifikační autorita, a.s., je možno získat z Výroční zprávy I.CA.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Služba není poskytována.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

Citlivými a důvěrnými informacemi I.CA jsou veškeré informace, které nejsou zveřejňovány způsobem uvedeným v kapitole 2.2, zejména:

- data pro vytváření elektronických značek/elektronických pečetí (soukromý klíč) příslušná k datům pro ověřování elektronických značek/elektronických pečetí, obsaženým v kvalifikovaných systémových certifikátech CA/certifikátech na správu,
- data pro vytváření elektronických značek/podpisů (soukromý klíč), příslušná k datům pro ověřování elektronických podpisů/značek obsaženým v účelových certifikátech I.CA (např. klíče pro komunikaci s RA),
- ostatní kryptograficky podstatné informace sloužící k provozu CA a RA,
- vybrané obchodní informace I.CA,
- veškeré interní informace a dokumentace stýkající se poskytování kvalifikovaných certifikačních služeb dle ZoEP,
- veškeré osobní údaje.

9.3.2 Informace mimo rámec citlivých informací

Za veřejné se považují typy informací, které nepatří do žádné z uvedených skupin v kapitole 9.3.1.

9.3.3 Odpovědnost za ochranu citlivých informací

Žádný zaměstnanec I.CA, který přijde do styku s informacemi uvedenými v kapitole 9.3.1, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

Zaměstnanci I.CA, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení příslušných prací.

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

9.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje klientů, uživatelů či pracovníků podléhající ochraně ve smyslu příslušných zákonných norem.

9.4.3 Údaje, které nejsou považovány za citlivé

Informace, které nejsou považovány za důvěrné, jsou obecně údaje zveřejňované způsobem, uvedeným v kapitole 2.2.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů a dalších neveřejných informací odpovídá ředitel I.CA.

9.4.5 Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací

Problematika oznamování o používání důvěrných informací a souhlasu s používáním citlivých informací (viz relevantní části kapitol 3 a 4) je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

9.4.6 Poskytování citlivých informací pro soudní či správní účely

Poskytování citlivých informací pro soudní, resp. správní, účely je v I.CA řešeno v souladu s požadavky příslušných zákonných norem.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně dle požadavků příslušných zákonných norem.

9.5 Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek, certifikáty CA, párová data CA a procedury, zajišťující provoz systému poskytujícího kvalifikované certifikační služby v oblasti certifikátů, jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče příslušné certifikátům CA pouze k elektronickému označování/elektronickému podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů,
- vydávané certifikáty splňují náležitosti požadované ZoEP a VoEP,

- zneplatní certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud:

- klient neporušil povinnosti plynoucí mu ze smlouvy o poskytování kvalifikované certifikační služby a této CP,
- spoléhající se strana neporušila povinnosti této CP.

Klient uplatňuje záruku vždy u RA, která zpracovala jeho prvotní žádost. Pokud RA není schopna vyřídit záruční nároky ve své pravomoci, postoupí je k řízení I.CA a o této skutečnosti klienta vyrozumí. Na používání certifikátu, který I.CA nevydala, se záruky nevztahují.

9.6.2 Zastupování a záruky RA

RA přejímá závazek za správné poskytování služeb uvedených v kapitole 1.3.2. RA nevyřídí kladně žádost, pokud žadatel hodnověrným způsobem neprokázal svoji identitu, nedoložil údaje uvedené v žádosti o službu, odmítá potřebné údaje sdělit nebo odmítne podepsat příslušné dokumenty (viz příslušné kapitoly této CP). RA dále zodpovídá:

- za včasné předání žádostí o zneplatnění vydaných certifikátů k vyřízení na pracoviště CA,
- za vyřizování připomínek a stížností klientů.

9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Držitel certifikátu nebo podepisující osoba postupují v souladu s ZoEP a VoEP a ručí za správnost jimi uváděných informací v celém životním cyklu využívání poskytované certifikační služby.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s ZoEP a VoEP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., se především striktně řídí ZoEP a nemůže se zříci záruk v něm určených.

9.8 Omezení odpovědnosti

Hranice odpovědnosti společnosti První certifikační autorita, a.s., se v oblasti poskytování kvalifikovaných certifikačních služeb řídí platnou legislativou.

9.9 Odpovědnost za škodu, náhrada škody

V procesu poskytování certifikačních služeb platí vždy takové záruky, které byly sjednány mezi společností První certifikační autorita, a.s., a žadatelem o konkrétní certifikační službu. Smlouva nesmí být v rozporu s platnou legislativou a musí být vždy v písemné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak příslušnými právními předpisy, tak příslušnými certifikačními politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb uzavřené se zákazníkem,
- jiné záruky, než výše uvedené, neposkytuje.

Další možné náhrady škody vycházejí z ustanovení příslušných zákonů a o jejich výši může rozhodnout soud.

Společnost První certifikační autorita, a.s., neodpovídá:

- za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb držitelem, zejména za provozování v rozporu s podmínkami uvedenými v certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.,
- za škodu vyplývající z použití certifikátu v období po podání žádosti o jeho zneplatnění, pokud společnost První certifikační autorita, a.s., dodrží definovanou lhůtu pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL).

Oprávněnou reklamaci je možné podat těmito způsoby:

- e-mailem na adresu reklamace@ica.cz,
- doporučenou poštovní zásilkou na adresu sídla společnosti,
- osobně v sídle společnosti.

Reklamující osoba (držitel certifikátu) je povinna uvést:

- číslo smlouvy,
- číslo příjmového dokladu,
- co nejvýstižnější popis závad a jejich projevů.

Povinnost I.CA:

O reklamaci rozhodne I.CA nejpozději do tří pracovních dnů od doručení reklamace a vyrozumí o tom reklamujícího (formou elektronické pošty, nebo doporučenou zásilkou), pokud se strany nedohodnou jinak.

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do jednoho měsíce ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

Nový certifikát bude držiteli poskytnut zdarma v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek/elektronických pečetí, kterými CA elektronicky označuje/elektronicky podepisuje vydávané certifikáty a seznamy zneplatněných certifikátů, nabídne I.CA držitelům bezplatné vydání nového certifikátu - případné náklady na vydání nových certifikátů hradí I.CA, která po dobu zablokování certifikátů

nese veškerou odpovědnost za případné škody vzniklé v souvislosti se zneužitím těchto certifikátů,

- v případě, že I.CA při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát se stejným veřejným klíčem, je žadatel o certifikát vyzván k vygenerování nové žádosti a tedy i nových párových dat - držitel již existujícího certifikátu, který vlastní veřejný klíč stejný jako žadatel o vydání certifikátu, je vyzván k vygenerování nových párových dat, jeho původní certifikát je okamžitě zneplatněn a držitel je o této skutečnosti informován.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato CP nabývá platnosti dnem uvedeným v kapitole 10 a platí minimálně po dobu platnosti posledního podle ní vydaného certifikátu.

9.10.2 Ukončení platnosti

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CP, je ředitel společnosti První certifikační autorita, a.s.

9.10.3 Důsledky ukončení a přetrvání závazků

Platnost CP může být bez náhrady ukončena až po skončení platnosti posledního certifikátu, který byl podle této CP vydán.

9.11 Komunikace mezi zúčastněnými subjekty

Pro individuální oznámení a komunikaci se zúčastněnými subjekty může I.CA využít jimi dodané e-mailové adresy, poštovní adresy, telefonní čísla, osobní jednání atd.

Komunikovat s I.CA lze taktéž způsoby uvedenými na adrese http://www.ica.cz/.

9.12 Změny

9.12.1 Postup při změnách

Postup je realizován řízeným procesem popsaným v interním dokumentu.

9.12.2 Postup při oznamování změn

Postup je realizován řízeným procesem popsaným v interním dokumentu. Vydání nové certifikační politiky se změněným OID bude oznámeno v aktualitách na webových stránkách I.CA.

9.12.3 Okolnosti, při kterých musí být změněn OID

V případě vydání nové verze tohoto dokumentu je pro tento dokument přiděleno nové OID.

9.13 Řešení sporů

Tato CP a příslušná CPS, jejich výklad a aplikace se řídí ZoEP a VoEP.

V případě, že držitel certifikátu, podepisující osoba, spoléhající se strana nebo smluvní partner nesouhlasí s předloženým výkladem, mohou použít následující stupně odvolání:

- odpovědný pracovník RA,
- odpovědný pracovník I.CA (nutné písemné podání),
- ředitel I.CA (nutné písemné podání a složení finanční jistiny, která je vrácena v případě kladného vyřízení stížnosti).

Uvedený postup dává nesouhlasící straně možnost prosazovat svůj názor rychlejším způsobem, než soudní cestou.

9.14 Rozhodné právo

Obchodní činnost společnosti První certifikační autorita, a.s., se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

Systém poskytování certifikačních služeb je provozován ve shodě s legislativní požadavky ZoEP a VoEP a dále s relevantními mezinárodními standardy.

9.16 Další opatření

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost ustanovení

Není relevantní pro tento dokument.

9.16.4 Zřeknutí se práv

Není relevantní pro tento dokument.

9.16.5 Vyšší moc

I.CA nenese odpovědnost za porušení svých povinností způsobené zásahy vyšší moci, jako jsou například přírodní katastrofy velkého rozsahu, stávky, občanské nepokoje nebo válečný stav.

9.17 Další opatření

Tato CP a příslušná CPS zohledňují požadavky technických norem a standardů, uvedených v kapitole 6.5.2 a dále:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační politika vydaná společností První certifikační autorita, a.s. nabývá platnosti a účinnosti dnem 09.11.2015.