První certifikační autorita, a.s.

CERTIFIKAČNÍ POLITIKA

VYDÁVÁNÍ CERTIFIKÁTŮ CA/TSS

Verze 2.4

Tabulka 1 - Identifikace

Název	Certifikační politika certifikátů CA/TSS
Společnost	První certifikační autorita, a.s.
Schválil	Ředitel společnosti První certifikační autorita, a.s.

Tabulka 2 – Vývoj dokumentu

Verze	**Datum vydání**	**Shrnutí změn**
1.00	18.12.2001	První verze dokumentu
2.0	30.05.2005	• Aktualizace podle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb., aktualizace norem, procedur auditu • Vytvoření struktury striktně dle RFC 3647
2.1	09.12.2005	Přidání TSA
2.2	01.10.2007	Použití více vyhrazených serverů pro vydávání kvalifikovaných časových razítek
2.3	01.02.2008	Zařazení certifikátu do Microsoft root certificate program
2.4	22.09.2015	Aktualizace a revize dokumentu

Obsah

1 Úvod

Tento dokument, **Certifikační politika vydávání certifikátů CA/TSS** (dále též CP), vypracovaný společností První certifikační autorita, a. s. (dále též I.CA):

- se zabývá skutečnostmi, které se vztahují na I.CA a které souvisejí s vydáváním certifikátů CA a TSS, jejich další správou, použitím, akceptací, ukončením platnosti, zneplatněním a všemi aspekty souvisejícími s nakládáním s párovými daty,
- striktně dodržuje členění dokumentu navržené v RFC 3647, s přihlédnutím k doporučením orgánů EU a k právu ČR v dané oblasti. Jednotlivé kapitoly jsou proto v této CP zachovány i v případě, že jsou ve vztahu k ní irelevantní.

1.1 Přehled

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

V procesu poskytování kvalifikovaných certifikačních služeb v oblasti vydávaných kvalifikovaných certifikátů a/nebo kvalifikovaných systémových certifikátů provozuje společnost První certifikační autorita, a.s jedinou certifikační autoritu – viz kapitola 1.3.1.

Informace o dalších poskytovaných certifikačních službách je možno získat na internetové informační adrese, uvedené v kapitole 2 .

Není-li uvedeno jinak, je dále v tomto dokumentu pod pojmy:

- **certifikát** míněn kvalifikovaný certifikát a/nebo kvalifikovaný systémový certifikát
- **časové razítko** míněno kvalifikované časové razítko
- **certifikát CA** míněn nadřízený kvalifikovaný systémový certifikát, resp. kvalifikovaný certifikát I.CA - (poskytovatele certifikačních služeb v oblasti certifikát)
- **certifikát TSS** míněn nadřízený kvalifikovaný systémový certifikát, resp. kvalifikovaný certifikát serveru, generujícího kvalifikovaná časová razítka

Vydávané certifikáty CA jsou kořenové, „self-signed“ certifikáty I.CA. Data pro ověřování elektronických značek, resp. elektronických podpisů, které mj. tyto certifikáty obsahují, jsou spojena s daty pro vytváření elektronických značek, resp. elektronických podpisů, kterými I.CA elektronicky označuje, resp. elektronicky podepisuje vydávané certifikáty a seznamy zneplatněných certifikátů v souladu s platnou legislativou.

Vydávané certifikáty TSS jsou nadřízené kvalifikované systémové certifikáty, vydané I.CA. Data pro ověřování elektronických značek, resp. elektronických podpisů, které mj. tyto certifikáty obsahují, jsou spojena s daty pro vytváření elektronických značek, resp. elektronických podpisů, kterými konkrétní TSS systému TSA elektronicky označuje, resp. elektronicky podepisuje vydávaná časová razítka v souladu s platnou.

1.2 Název a identifikace dokumentu

Název tohoto dokumentu	:	Certifikační politika vydávání certifikátů CA/TSS
OID	:	1.3.6.1.4.1.23624.1.4.0.1

1.3 Participující subjekty

1.3.1 Certifikační autority (dále "CA")

Společnost První certifikační autorita, a. s., (dále též I.CA) je akreditovaným poskytovatelem certifikačních služeb v souladu s legislativou České republika a Slovenské republiky, vztahující se k problematice elektronického podpisu.

1.3.2 Registrační autority (dále "RA")

Pro potřeby této CP irelevantní.

1.3.3 Držitelé kvalifikovaných systémových certifikátů a označující osoby, kteří požádali o vydání kvalifikovaného certifikátu a/nebo kvalifikovaného systémového certifikátu (dále certifikátu) a kterým byl certifikát vydán

Držitelem certifikátů CA/TSS je I.CA. Oprávněným žadatelem a následně držitelem certifikátů je I.CA jako právnická osoba.

1.3.4 Spoléhající se strany

Spoléhající se stranou mohou být fyzické osoby, právnické osoby nebo organizační složky státu, spoléhající se na vydaný certifikát dle této CP.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány dozoru dle aktuálního znění ZoEP, orgány činné v trestním řízení a další, kterým to ze zákona přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty CA, resp. TSS mohou být používány v aplikacích pouze pro ověřování elektronické značky/elektronického podpisu vydaných certifikátů, seznamu zneplatněných certifikátů, resp. časových razítek.

1.4.2 Omezení použití certifikátu

Certifikáty CA/TSS nesmí být využívány v rozporu s vydávaným účelem nebo s platnou legislativou.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Praha 9
Česká republika

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Touto osobou je pracovník I.CA, jmenovaný ředitelem společnosti První certifikační autorita, a.s. do role bezpečnostního managera.

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 I.CA s postupy jiných poskytovatelů certifikačních služeb, je ředitel společnosti První certifikační autorita, a.s. Déle platí ustanovení kapitoly 3.2.6.

1.5.4 Postupy při schvalování souladu s bodem 1.5.3

V případě, že je potřebné s ohledem na kapitolu 1.5.3 provést změny v odpovídající CPS a této CP, určuje ředitel I.CA osobu, která je oprávněna změny provádět. Touto osobou je pracovník I.CA, jmenovaný do role bezpečnostního managera.

1.6 Přehled použitých pojmů a zkratek

Tabulka 3a – Pojmy

Pojem	Vysvětlení
Certifikát	datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu
Čas	světový čas UTC
Držitel certifikátu	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující osobu nebo pro označující osobu a které byl kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydán
Elektronický podpis	údaje, resp. informace, které splňují požadavky platné legislativy
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
Kvalifikovaný certifikát (QC)	certifikát, který má náležitosti podle platné legislativy a byl vydán kvalifikovaným poskytovatelem certifikačních služeb
Nadřízený kvalifikovaný systémový certifikát	kvalifikovaný certifikát poskytovatele certifikačních služeb, který se řídí speciálními dokumenty vydanými I.CA
Následný kvalifikovaný certifikát	kvalifikovaný certifikát, který byl v souladu se smlouvou o poskytování kvalifikované certifikační služby, uzavřenou mezi koncovým uživatelem a I.CA, vydán koncovému uživateli na základě nové žádosti o kvalifikovaný certifikát elektronicky podepsané platnými daty pro vytváření elektronických podpisů souvisejícími s již vydaným kvalifikovaným certifikátem, ke kterému je vydáván tento následný

	kvalifikovaný certifikát ať již z důvodu výměny dat pro ověřování elektronických podpisů (kapitola 4.7) nebo změny údajů v certifikátu (kapitola 4.8)
Párová data (dvojice soukromý a veřejný klíč)	jedinečná data pro vytváření elektronického podpisu, resp. elektronické značky spolu s odpovídajícími daty pro ověřování elektronického podpisu, resp. elektronické značky
Podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby
Smluvní partner	poskytovatel certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části
Soukromý klíč	jedinečná data pro vytváření elektronického podpisu nebo elektronické značky
Statut kvalifikovaného certifikátu	stav, ve kterém se kvalifikovaný certifikát nachází, tzn. ve stavech platnosti, neplatnosti, zneplatnění, zablokování
Spoléhající se strana	subjekt, spoléhající se při své činnosti na certifikát, vydaný I.CA
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu nebo elektronické značky
Zablokování	stav, ve kterém se kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nachází od doby, kdy jej I.CA zneplatnila, do doby, kdy I.CA zveřejnila CRL, ve kterém je tento kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát poprvé zařazen.
Zaručený elektronický podpis	elektronický podpis, splňující požadavky české legislativy
Zneplatnění	stav kvalifikovaného certifikátu, který byl I.CA zneplatněn – tomuto certifikátu nelze již platnost obnovit
Žádost o službu (Žádost)	Formální dokument žádosti o některou ze služeb poskytovaných I.CA např. žádost o vydání kvalifikovaného certifikátu, žádost o zneplatnění kvalifikovaného certifikátu atd.
Žádost o vydání kvalifikovaného certifikátu	formální, standardní dokument elektronické žádosti o vydání kvalifikovaného certifikátu dle přípustných norem a směrnic definovaných v této CP

Tabulka 3b – Zkratky

Zkratka	**Vysvětlení**
CA	centrální pracoviště certifikační autority společnost První certifikační autorita, a.s.
CP	certifikační politika (veřejný dokument)
CPS	certifikační prováděcí směrnice (neveřejný dokument)
CRL	**C**ertificate **R**evocation **L**ist (seznam zneplatněných certifikátů)
CZ	mezinárodní kód pro Českou republiku
DS/NTP	**D**atum **S**ecure**/N**etwork **T**ime **P**rotocol - zabezpečená varianta NTP protokolu
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
I.CA	První certifikační autorita, a.s. – akreditovaný poskytovatel certifikačních služeb
IETF	**I**nternet **E**ngineering **T**ask **F**orce
EPS	**E**lektrická **p**ožární **s**ignalizace
HSM	**H**ardware **S**ecurity **M**odul (bezpečné úložiště privátního klíče)
IETF	**I**nternet **E**ngineering **T**ask **F**orce
MV ČR	**M**inisterstvo **V**nitra **Č**eské **r**epubliky
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
NMI	**N**ational **M**easurement **I**nstitute (Národní úřad pro míry a váhy (v USA))
NTMS	**N**etwork **T**ime **M**anagement **System** (Systém správy času prostřednictvím sítě)
NTP	**N**etwork **T**ime **P**rotocol

Zkratka	Vysvětlení
OID	(Object Identifier) číselná identifikace objektu v rámci jednotné klasifikace objektů podle ISO/ITU
PKI	**P**ublic **K**ey **I**nfrastructure
TMC	**T**rusted **M**aster **C**lock (Hodiny v kořeni služby distribuce TT)
TS	**T**ime **S**tamp (Časové razítko)
TSA	**T**ime **S**tamping **A**uthority (Autorita časových razítek)
TSQ	**Time S**tamp **Q**uery (Žádost o časové razítko)
TSR	**Time S**tamp **R**esponse (Odpověď na žádost o časové razítko)
TSS	**T**ime **S**tamp **S**erver (Server, vydávající časová razítka)
TT	**T**rusted **T**ime (Důvěryhodný čas)
TTDS	**T**rusted **T**ime **D**istribution **S**ystem
TTI	**T**rusted **T**ime **I**nfrastructure (Infrastruktura důvěryhodného času)
TST	**T**ime **S**tamp **T**oken (část časového razítka obsahující jméno TSS, UTC čas, přesnost, sériové číslo,verze, hash algoritmus, nonce)
UPS	Uninterruptible Power Supply
UTC	**U**niversal **C**o-ordinated **T**ime, Standard přijatý 1.1.1972 pro světový koordinovaný čas (Coordinated Universal Time – UTC). Funkci "oficiálního časoměřiče" atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
VoEP	vyhláška České republiky 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)
ZoEP	aktuální znění zákona České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb.

2 Odpovědnosti za zveřejňování a úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

S ohledem na požadavky ZoEP zřizuje I.CA úložiště informací a dokumentace.

2.2 Zveřejňování informací a dokumentace

Základní adresy, na nichž lze nalézt veřejné informace o I.CA s ohledem na problematiku nadřízených kvalifikovaných systémových certifikátů (tzn. certifikátů CA a TSS) jsou:

a) První certifikační autorita, a.s.

Podvinný mlýn 2178/6, 190 00 Praha 9, Česká republika

b) URL: http://www.ica.cz (dále též internetová informační adresa)

c) sídla registračních autorit

Kontaktní adresy, které slouží pro kontakt veřejnosti s I.CA (dále též kontaktní adresy), jsou:

a) sídlo registrační autority, která smluvní vztah s I.CA zprostředkovala

b) elektronická poštovní adresa info@ica.cz

Výše uvedené informační a kontaktní adresy I.CA zveřejňuje na své internetové informační adrese, pracovištích SRA a VSRA. Pracovníci I.CA a smluvních partnerů (SRA) jsou rovněž povinni tyto informace na vyžádání sdělit všem uživatelům. Totéž platí i v případě, že dojde ke změně kontaktních adres.

Certifikáty CA a TSS lze získat na adrese http://www.ica.cz/.

V případech odejmutí akreditace nebo zneužití, popř. vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů vydávaných certifikátů nebo seznamů zneplatněných certifikátů, oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Mladá fronta Dnes (ČR).

2.3 Periodicita zveřejňování informací

S ohledem na problematiku certifikátů CA/TSS, zveřejňuje I.CA informace s následující periodicitou:

- Získání nebo odejmutí akreditace dle ZoEP – okamžitě.
- Certifikáty CA/TSS včetně hashe – před jejich využíváním.
- Informace o zneplatnění certifikátů CA/TSS s uvedením důvodu zneplatnění (v případě zneužití nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů, určených pro označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů, časových razítek) – bezodkladně.

2.4 Řízení přístupu k jednotlivým typům úložišť

Přístup ke konkrétním typům úložišť pověřenými pracovníky I.CA je definován interní dokumentací.

3 Identifikace a autentizace

3.1 Pojmenovávání

3.1.1 Typy jmen

Tabulka 4a – certifikát CA: Subject a Issuer

Položka	Hodnota
Organization (O)	První certifikační autorita, a.s.
CommonName (CN)	I.CA – Qualified root certificate
Country (C)	CZ

Tabulka 4b – certifikát TSS: Issuer

Položka	Hodnota
Organization (O)	První certifikační autorita, a.s.
CommonName (CN)	I.CA – Qualified root certificate
Country (C)	CZ

Tabulka 4c – certifikát TSS: Subject

Položka	Hodnota
Organization (O)	První certifikační autorita, a.s.
OrganizationUnit (OU)	Time Stamp Server X
CommonName (CN)	Time Stamping Authority
Country (C)	CZ

Pozn. X – číslo TSS (1, 2, 3, ….)

3.1.2 Požadavek na významovost jmen

Ve výše uvedených atributech se především kontroluje přítomnost nepovolených znaků. V případě výskytu nepovolených znaků se žádost nepřijme.

Dále se kontroluje přítomnost všech povinných atributů. Pokud některý z povinných atributů není vyplněn, žádost se nepřijme.

Odstraňují se úvodní a koncové mezery (0x20) a skupiny mezer uprostřed položky se redukují na jedinou mezeru, toto platí i pro „whitespaces“ (ASCII, Unicode : 0x09 – 0x0D, 0x20)

3.1.3 Anonymita a používání pseudonymu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

3.1.4 Pravidla pro interpretaci různých forem jmen

Pokud se jedná o jména nebo jiné skutečnosti, které jsou uvedeny v předkládaných dokumentech, přenášejí se tato jména v té podobě, v jaké jsou v dokumentu uvedena. Vlastní transkripce se neprovádí.

3.1.5 Jedinečnost jmen

Jedinečnost jména Subject a Issuer je zaručena.

3.1.6 Obchodní značky

Ve vydaném certifikátu CA/TSS se musí ověřitelné údaje vztahovat k I.CA.

3.2 Počáteční ověření identity

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

Vlastnictví dat pro vytváření elektronických značek, resp. elektronických podpisů, odpovídající datům pro ověřování elektronických značek, resp. elektronických podpisů, která bude daný certifikát CA/TSS obsahovat, se prokazuje předložením žádosti o vydání certifikátu CA/TSS, elektronicky označené, resp. elektronicky podepsané těmito daty. Toto je kontrolováno tím, že je pomocí dat pro ověřování elektronických značek, resp. elektronických podpisů, uvedených v žádosti o certifikát CA/TSS, ověřena platnost elektronické značky, resp. elektronického podpisu na této žádosti.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Jediná fyzická osoba, která může rozhodnout o vydání certifikátu CA/TSS, je ředitel I.CA, který před zahájením vlastního generování párových dat CA/TSS:

- se identifikuje platným občanským průkazem a sekundárním osobním průkazem (viz kapitola 3.2.3),
- komisi, která provádí generaci párových dat CA/TSS, předloží listinné dokumenty, které dokládají jeho jmenování do funkce ředitele I.CA a originál nebo notářsky ověřenou kopii výpisu z obchodního rejstříku, na jejichž základě byla I.CA vytvořena a která musí obsahovat úplné obchodní jméno, identifikační číslo (IČO), statutární orgán a sídlo. Identifikace ostatních členů této komise se provádí v souladu s vnitřními směrnicemi.

3.2.3 Ověřování identity fyzické osoby

Ředitel I.CA předloží své následující údaje:

- celé občanské jméno,
- datum narození,
- číslo předloženého primárního osobního dokladu.

Vyžaduje se předložení originálu platného primárního osobního dokladu a originálu dalšího osobního dokladu (sekundárního). Primární osobní doklad pro občany ČR musí být občanský průkaz, popř. obdobný doklad stejné právní váhy. Primární osobní doklad pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Sekundární osobní doklad musí být vydán orgánem veřejné moci nebo jinou organizací, jejíž existenci lze doložit. Sekundární osobní doklad musí obsahovat celé občanské jméno fyzické osoby, vyřizující žádost a dále nejméně jeden z následujících údajů:

- datum narození (nebo rodné číslo u občanů ČR),
- adresu trvalého bydliště žadatele,
- fotografii obličeje.

Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo označující osobě

Všechny informace musí být ověřeny.

3.2.5 Ověřování specifických práv

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

3.2.6 Kritéria pro interoperabilitu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

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

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

Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky, jako v případě počátečního ověření identity.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky, jako v případě počátečního ověření identity.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Je možné pouze osobní jednání, kdy musí žadatel o zneplatnění certifikátu prokázat, že je ředitelem I.CA. Žádost o zneplatnění certifikátu musí být písemná a podepsaná žadatelem.

Po identifikaci a autentizaci postupuje žadatel o zneplatnění certifikátu způsobem, uvedeným v kapitole 4.9.3.

4 Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Viz kapitola 3.2.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Viz kapitola 3.2.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Viz kapitola 3.2.

4.2.2 Přijetí nebo odmítnutí žádosti o certifikát

Viz kapitola 4.3.

4.2.3 Doba zpracování žádosti o certifikát

Při dodržení všech potřebných podmínek řádově minuty.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydání certifikátu

V procesu vydávání certifikátu jsou prováděny nezbytné kontroly a další činnosti, popsané v interní dokumentaci.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu nebo označující osobě

V procesu vydávání certifikátu CA/TSS je ředitel I.CA informován prostřednictvím člena komise.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání certifikátu CA/TSS, tzn. splněny podmínky identifikace a prokázání vlastnictví dat pro vytváření elektronických značek, resp. elektronických podpisů odpovídajících datům pro ověřování elektronických značek, resp. elektronických podpisů, která bude vydaný certifikát CA/TSS obsahovat, je povinností ředitele I.CA tento certifikát přijmout.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

I.CA je povinna zajistit zveřejnění certifikátu CA/TSS.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

V případech vydání certifikátu CA/TSS získají oznámení o jeho vydání pracovníci komise.

4.5 Použití párových dat a certifikátu

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

Viz kapitola 1.4..

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

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje příslušný certifikát a ověřit kontrolní součet tohoto certifikátu,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že tento certifikát nebyl zneplatněn

4.6 Obnovení certifikátu

Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu nebo označující osobě

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejnění vydaných obnovených certifikátů poskytovatelem

Viz kapitola 4.6.

4.6.7 Oznámení o vydání obnoveného certifikátu ostatním subjektům

Viz kapitola 4.6.

4.7 Výměna dat pro ověřování elektronických značek v certifikátu

Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

4.7.1 Podmínky pro výměnu dat pro ověřování elektronických značek v certifikátu

Viz kapitola 4.7.

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

Viz kapitola 4.7.

4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických značek

Viz kapitola 4.7.

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

Viz kapitola 4.7.

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

Viz kapitola 4.7.

4.7.6 Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických značek

Viz kapitola 4.7.

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

Viz kapitola 4.7.

4.8 Změna údajů v certifikátu

Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji označující osobě

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát CA/TSS může být zneplatněn na základě následujících okolností:

- došlo nebo existuje důvodné podezření, že došlo ke kompromitaci soukromého CA/TSS
- nastanou-li skutečnosti uvedené v platné legislativě

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Žádost o zneplatnění mohou podat subjekty oprávněné dle platné legislativy nebo ředitel I.CA.

4.9.3 Požadavek na zneplatnění certifikátu

Po splnění podmínek na identifikaci a autentizaci je postupováno následujícím způsobem. Žádost musí obsahovat sériové číslo certifikátu buď v dekadickém tvaru nebo hexadecimální (uvozeno řetězcem „0x“), celé občanské jméno ředitele I.CA, kterému byl certifikát vydán a heslo pro zneplatnění. Pokud žádost splňuje výše uvedené požadavky, odpovědný pracovník CA neprodleně certifikát zneplatní. Datum a čas zneplatnění je určen okamžikem přijetí platné žádosti o zneplatnění certifikátu serverem I.CA.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

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

Reakcí I.CA na přijetí platné žádosti o zneplatnění certifikátu CA/TSS, vydaného I.CA, je jeho okamžité zneplatnění a zveřejnění této informace (viz kapitola 2.2). CRL obsahující sériové číslo zneplatněného certifikátu musí být vydán neprodleně po zneplatnění tohoto certifikátu.

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

Viz kapitola 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů, které byly vydány I,CA, je společností První certifikační autorita, a.s. vydáván v pravidelných intervalech, maximálně jedenkrát za 24 hodin (zpravidla po 8 hodinách), v případě nutnosti bezodkladně.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Viz kapitola 4.9.7.

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

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

4.9.10 Požadavky při ověřování statutu certifikátu na on-line

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

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

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

Služby související s ověřováním statutu certifikátu CA jsou poskytovány I.CA, resp. MV ČR formou zveřejňování informací:

- prostřednictvím internetových informačních adres I.CA (viz kapitola 2.2),
- prostřednictvím internetových informačních MV ČR (viz http://www.mvcr.cz/) a jeho příslušného věstníku,
- o zneplatněných certifikátech:
  - prostřednictvím internetových informačních adres I.CA (viz kapitola 2.2),
  - prostřednictvím internetových informačních MV ČR (viz http://www.mvcr.cz/).

Služby související s ověřováním statutu certifikátu TSS, vydaného v souladu s legislativou CZ, jsou poskytovány I.CA, resp. MV ČR formou zveřejňování informací:

- prostřednictvím internetových informačních adres I.CA (viz kapitola 2.2),
- prostřednictvím internetových informačních MV ČR (viz http://www.mvcr.cz/) a jeho příslušného věstníku,
- o zneplatněných certifikátech:
  - na adresách, uvedených v certifikátu relevantního TSS,
  - prostřednictvím internetových informačních adres I.CA (viz kapitola 2.2),
  - prostřednictvím internetových informačních MV ČR (viz http://www.mvcr.cz/).

4.10.2 Dostupnost služeb

I.CA zajišťuje nepřetržitou dostupnost služeb (7 dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných certifikátů a seznamu zneplatněných certifikátů (platné CRL).

4.10.3 Další charakteristiky služeb statutu certifikátu

Další služby, kromě těch, které jsou uvedené v kapitole 4.10.1, nejsou poskytovány.

4.11 Ukončení poskytování služeb pro držitele certifikátu označující osobou

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

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

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

4.12.1 Politika a postupy při úschově a obnovování dat pro elektronických značek

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

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

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

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, Systémová bezpečnostní politika TSA, Certifikační prováděcí směrnice vydávání CA/TSS, Plán pro zvládání krizových situací a plán obnovy, tak v upřesňujících interních bezpečnostních normách a směrnicích. Uvedené dokumenty reflektují výsledky 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 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 sledování 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) a diesel agregátu.

5.1.4 Vliv vody

Všechny kritické systémy provozních pracovišť jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště jsou dle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací 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. podle platné legislativy týkající se elektronického podpisu, archivovat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu provozního pracoviště

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Pro činnosti, odpovídajícím rolím podle bezpečnostních požadavků standardu pro důvěryhodné systémy (viz vyhláška České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb), jsou ve společnosti I.CA definovány důvěryhodné role. Základní činnosti a odpovědnosti osob v důvěryhodných rolí je definován v interní dokumentaci.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Ve společnosti První certifikační autorita, a.s. jsou pro procesy poskytování 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 elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- ničení dat pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- zálohování/obnovu dat pro vytváření elektronického podpisu I.CA vydávaných certifikátů a seznamů zneplatněných certifikátů,
- aktivace kryptografického modulu, obsahujícího data pro vytváření elektronického podpisu I.CA 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 jsou přiděleny prostředky pro řádnou autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné.

5.2.4 Role vyžadující rozdělení povinností

V procesu poskytování certifikačních služeb v oblasti kvalifikovaných certifikátů je minimálně zaručeno, že nelze spojit role, definované bezpečnostním standardem pro důvěryhodné systémy (viz vyhláška České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb).

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenost a bezúhonnost

Pracovníci v rolích podle bezpečnostních požadavků standardu pro důvěryhodné systémy (viz vyhláška České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb) a dále v rolích ředitel společnosti, bezpečnostní manager, manager pro zvládání krizových situací a plánu obnovy, bezpečnostní auditor jsou přijímáni na základě dále popsaných personálních kriterií:

- naprostá občanská bezúhonnost - prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z registru 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 důvěryhodné funkce.

Ostatní pracovníci jsou přijímáni na základě následujících kriterií:

- 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 jsou:

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

Pracovníci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, které aktualizují 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 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 na získávání znalostí potřebných na zastávání jiné role v I.CA. Změna role je možná pouze v mimořádných

případech (epidemické onemocnění, atp.) jako dočasné opatření. Pro trvalé vykonávání jiné důvěryhodné role je potřeba jmenování ředitelem 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 řídí 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 (dle ZoEP, VoEP) 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 těchto povinností jsou vyžadovány smluvní pokuty, případně je s nimi okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

Kmenoví zaměstnanci I.CA mají k dispozici kromě CP i příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

5.4 Auditní záznamy (logy)

5.4.1 Typy zaznamenávaných událostí

V důvěryhodných systémech I.CA jsou do elektronického auditního logu zaznamenávány události, požadované:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements ,
- ETSI TS 101 456 - Electronic Signatures and Infrastructures: Policy requirements for certification authorities issuing qualified certificates,
- ZoEP.

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 auditní 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 jednou týdně, v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchovávání auditních záznamů

Doba, po kterou se uchovávají auditní záznamy, je stanovena na minimálně 10 let od jejich vzniku.

5.4.4 Ochrana auditních záznamů

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

5.4.5 Postupy pro zálohování auditních záznamů

Zálohování auditních záznamů probíhá obdobným způsobem jako zálohovaní ostatních elektronických informací.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je ve vztahu k I.CA interní, ve vztahu k smluvním partnerům externí. Shromažďování auditních záznamů je evidováno.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

V případě neoprávněných pokusů není subjekt informován o zapsání události do auditního záznamu.

5.4.8 Hodnocení zranitelnosti

V I.CA byly provedeny následující činnosti:

- stanovení aktiv (programové vybavení, technické vybavení, data) a jejich vazeb,
- hodnocení aktiv informačního systému,
- stanovení relevantních hrozeb a zranitelností,
- hodnocení hrozeb a zranitelností,
- určení míry rizika pro každou kombinaci aktiva (skupiny aktiv), hrozby a zranitelnosti.

5.5 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je u I.CA prováděno dle požadavků ZoEP a dalších právních norem (aktuální znění zákona ČR č.499/2004 o archivnictví a spisové službě a o změně některých zákonů.

5.5.1 Typy informací a dokumentace, které se uchovávají

I.CA uchovává následující typy informací a dokumentace, které související s problematikou certifikátu CA/TSS:

- elektronické nebo písemné informace dle platné legislativy:
    - certifikát CA/TSS,

  - kopie předložených osobních dokladů žadatele o certifikát CA/TSS, na jejichž základě byla ověřena jeho identita,
  - dokumenty a záznamy související s životním cyklem vydaného certifikátu CA/TSS,

- auditní záznamy definované v kapitole 5.4.1 tohoto dokumentu, aplikační programové vybavení a veškerou dokumentaci společnosti, která je nutná pro provádění informačních auditů a kontrol bezpečnostní shody,
- identifikace místa, kde jsou uloženy informace a dokumentace, jejichž uchování je vyžadováno ZoEP,
- veškeré seznamy zneplatněných certifikátů,
- identifikační údaje osoby, která provedla ověření totožnosti žadatele o certifikát CA/TSS,
- záznam o manipulaci (tj. např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atp.) s informacemi,
- provozní a bezpečnostní dokumentaci.

5.5.2 Doba uchovávání uchovávaných informací a dokumentace

I.CA zajišťuje uchovávání informací a dokumentace dle kapitoly 5.5.1 po dobu nejméně 10 od jejich vzniku.

Po celou dobu existence I.CA jsou uchovávány informace, vztahující se k certifikátům CA/TSS, s výjimkou příslušných dat pro vytváření elektronické značky, resp. elektronického podpisu.

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 a proto je vzhledem k zákonům ČR č. 101/2000 Sb. v aktuálních zněních, 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.

Uchovávané informace a dokumentace jsou určeny výhradně pro interní potřebu I.CA a jsou přístupné:

- pracovníkům I.CA v důvěryhodných rolích,
- 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.

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 (viz kapitola 0) jsou upraveny interní dokumentací I.CA.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V případě, že budou využívána časová razítka, musí se jednat o kvalifikovaná časová razítka vydána I.CA.

5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní, 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 (viz kapitola 5.5.4). Shromažďování archivních záznamů je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Pracoviště, kde jsou informace a dokumentace uchovávány, obsahuje jejich seznam včetně data uložení.

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

Výměna dat pro ověřování elektronických podpisů v v nadřízeném kvalifikovaném systémovém certifikátu I.CA je v případě standardních situací (vypršení platnosti certifikátu) s dostatečným časovým předstihem před vypršením doby platnosti tohoto certifikátu prováděna formou vydání nového kořenového certifikátu I.CA. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu tvorby elektronických značek, 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 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

Postupy jsou uvedeny v interním dokumentu Plán pro zvládání krizových situací a plán obnovy.

5.7.2 Poškození výpočetních prostředků, software nebo dat

V případě poškození výpočetních prostředků, softwaru nebo dat postupuje I.CA v souladu s interním dokumentem Plán pro zvládání krizových situací a plán obnovy takovým způsobem, aby byl provoz obnoven v požadovaných termínech.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek /podpisů poskytovatele

V případě kompromitace nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů pro označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů I.CA:

- ukončí jejich používání,
- okamžitě a trvale zneplatní vlastní certifikát CA a jemu odpovídající data pro vytváření elektronických značek, resp. elektronických podpisů,
- zneplatní všechny certifikáty, které byly těmito daty označeny, resp. podepsány,
- bezodkladně:

- o této skutečnosti, včetně důvodu informuje:
  - na své internetové informační adrese,
  - v jednom celostátně distribuovaném deníku – viz kapitola 2.2 ,
- pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů, čímž je zajištěna dostupnost této informace minimálně dvěma na sobě nezávislými způsoby, umožňujícími dálkový přístup a jsou nepřetržitě dostupné,

- 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 certifikátu CA,
- oznámí příslušnému úřadu informaci o zneplatnění vlastního certifikátu CA s uvedením důvodu zneplatnění,
- v případě vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů pro označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů nabídne I.CA výše uvedeným držitelům bezplatné vydání nového certifikátu s tím, že případné náklady na vydání nových certifikátů sama hradí. Postup je stejný jako při vydání prvotního certifikátu.

V případě kompromitace nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů pro označování, resp. podepisování vydávaných kvalifikovaných časových razítek I.CA:

- ukončí jejich používání,
- okamžitě a trvale zneplatní vlastní příslušný nadřízený kvalifikovaný systémový certifikát, resp. kvalifikovaný certifikát serveru vydávajícího kvalifikovaná časová razítka,
- bezodkladně:
  - o této skutečnosti, včetně důvodu informuje:
    - na své internetové informační adrese,
    - v jednom celostátně distribuovaném deníku – viz kapitola 2.2,
  - pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů, čímž je zajištěna dostupnost této informace minimálně dvěma na sobě nezávislými způsoby, umožňujícími dálkový přístup a jsou nepřetržitě dostupné,
- pokud je to možné, informuje držitele platných kvalifikovaných časových razítek o zneplatnění certifikátu TSS, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, kterou tyto osoby uvedly v žádosti o vydání kvalifikovaných časových razítek - součástí této informace je důvod ukončení platnosti certifikátu TSS,
- oznámí MV ČR informaci o zneplatnění vlastního certifikátu TSS s uvedením důvodu zneplatnění,
- vydá nový certifikátu TSS - postup je stejný jako při vydání prvotního certifikátu TSS.

5.7.4 Schopnosti obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interním dokumentem Plán pro zvládání krizových situací a plán obnovy.

5.8 Ukončení činnosti CA

V případě plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů, tzn. z jiných důvodů, než-li 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:

- CZ:

- 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,
- zpřístupnění informaci o ukončení činnosti I.CA v oblasti vydávání certifikátů na své internetové informační adrese nejméně 2 měsíce před plánovaným ukončením činnosti,
- ukončí kvalifikované poskytování certifikačních služeb v oblasti vydávání certifikátů,
- prokazatelné zničí svá data pro vytváření elektronických značek, sloužící k označování vydávaných certifikátů a seznamu zneplatněných certifikátů.

- SK:
  - 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 kvalifikovaného 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 jím vydaných kvalifikovaných certifikátů ode dne zániku tohoto kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů,
    - převezme tyto záznamy úřad.

Problematika plánovaného ukončení činnosti I.CA, případně RA je detailně uvedena v interní dokumentaci.

6 Technická bezpečnost

6.1 Generování a instalace párových dat

Detailní popis generování a instalace párových dat je uveden v interních bezpečnostních směrnicích, zahrnujících problematiku, uvedenou v podkapitolách 6.1.1 až 6.1.7.

6.1.1 Generování párových dat

Generování párových dat I.CA (CA/TSS), 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 splňuje požadavky české, resp. slovenské legislativy, vztahující se k problematice elektronického podpisu. Použitý modul svými vlastnostmi odpovídá požadavkům vyžadovaným aktuálními verzemi ZoEP a VoEP. I.CA používá pro párová data, sloužící k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů délku rovnou 2048 bitů.

V průběhu procesu generování párových dat CA/TSS, sloužících k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek, musí být fyzicky přítomni:

- ředitel I.CA nebo jím jmenovaný člen vedení I.CA,
- bezpečnostní manager nebo bezpečnostní administrátor (konkrétně určí ředitel I.CA),
- administrátor systému, nebo jiný pověřený technicky proškolený pracovník I.CA.

Konkrétní technický postup generace párových dat CA/TSS, sloužících k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek a následné vyhotovení certifikátu CA/TSS, příslušného k těmto párovým datům, je popsán v interní dokumentaci I.CA.

O průběhu generování párových dat CA/TSS, sloužících k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek je vyhotoven písemný protokol obsahující:

- jmenný seznam přítomných pracovníků s uvedením: jména, příjmení, titulu,
- datum a čas zahájení a ukončení generace párových dat s přesností minimálně na minuty
- místo, kde ke generaci párových dat došlo,
- popis zařízení, na kterém byla generace prováděna, umožňující jednoznačnou identifikaci tohoto zařízení,
- kompletní výpis certifikátu CA/TSS, obsahující data pro ověřování elektronických značek, resp. elektronických podpisů vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek, obsažená v právě vygenerovaných párových datech,
- datum vyhotovení protokolu,
- vlastnoruční podpisy všech pracovníků, kteří generaci párových dat prováděli.

V případě generování párových dat, používaných v procesech správy systémových komponent I.CA, komunikaci s RA na vlastních zařízeních, jsou pracovníci I.CA a RA povinni využívat certifikáty, vydané I.CA.

6.1.2 Předání dat pro vytváření elektronických značek označující osobě

Generování párových dat CA/TSS je prováděno na zařízení a v prostředí, která jsou v okamžiku jejich generování pod výhradní kontrolou I.CA, a proto jsou tyto skutečnosti pro aplikaci tohoto vydání této CP irelevantní.

6.1.3 Předání dat pro ověřování elektronických značek poskytovateli certifikačních služeb

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

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

Data pro ověřování elektronických značek, resp. elektronických podpisů CA/TSS jsou obsažena v jeho certifikátu. Možnost získání certifikátu CA/TSS je garantována následujícími způsoby:

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

6.1.5 Délky párových dat

I.CA používá nejprověřenější klasický asymetrický šifrový algoritmus – RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) použitých pro označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek je 2048 bitů.

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

Algoritmy, použité pro generování celočíselných hodnot nutných pro fungování elektronického podpisu/značky (např. testy prvočíselnosti atd.) musí mít parametry uvedené v relevantních technických standardech nebo normách.

6.1.7 Omezení pro použití dat pro ověřování elektronických značek

Uvedeno v kapitole 7.1.2.

6.2 Ochrana dat pro vytváření elektronických značek a bezpečnost kryptografických modulů

Detailní popis je uveden v interních bezpečnostních směrnicích, zahrnujících problematiku, uvedenou v podkapitolách 6.2.1 až 6.2.10.

6.2.1 Standardy a podmínky používání kryptografických modulů

V kryptografických modulech (viz kapitola 6.1.1):

- jsou generována párová data CA/TSS,
- je uložen soukromý klíč CA/TSS pro označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek.

6.2.2 Sdílení tajemství

Ochrana sdílením tajemství je realizována prostředky kryptografického modulu. Při provádění citlivých činností, které souvisejí se zásadními činnostmi I.CA (viz. kapitoly 6.1.1 a 6.2.10), je nezbytná přítomnost tří pověřených pracovníků I.CA, z nichž dva znají část kódu k provedení těchto činností.

6.2.3 Úschova dat pro vytváření elektronických značek

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CP irelevantní.

6.2.4 Zálohování dat pro vytváření elektronických značek

Kryptografické moduly, použité pro správu certifikátů CA/TSS, umožňují zálohování dat pro vytváření elektronických značek, resp. elektronických podpisů. Data v zašifrované podobě jsou zálohována prostřednictvím čipových karet.

6.2.5 Uchovávání dat pro vytváření elektronických značek

Po uplynutí doby platnosti dat určených k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek jsou tato data, včetně jejich záloh zničena a jejich další zálohování se neprovádí. Uchovávání dat, určených k označování, resp. podepisování certifikátů, seznamů zneplatněných certifikátů a časových razítek představuje bezpečnostní riziko, a proto je u I.CA zakázáno.

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

Data pro vytváření elektronických značek, resp. elektronických podpisů příslušná k certifikátu CA/TSS jsou generována přímo v kryptografickém modulu.

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

6.2.7 Uložení dat pro vytváření elektronických značek v kryptografickém modulu

Data pro vytváření elektronických značek, resp. elektronických podpisů příslušná k certifikátu CA/TSS jsou v kryptografickém modulu uložena v šifrovaném tvaru.

6.2.8 Postup při aktivaci dat pro vytváření elektronických značek

Aktivaci dat pro vytváření elektronických značek, resp. elektronických podpisů I.CA v oblasti vydávání certifikátů a časových razítek, vygenerovaných v kryptografického 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 označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů, časových

razítek 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 značek

Deaktivaci dat pro vytváření elektronických značek, resp. elektronických podpisů I.CA v oblasti vydávání certifikátů a časových razítek po jejich vložení do kryptografického modulu provádí určení pracovníci I.CA prostřednictvím kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací.

O provedení deaktivace dat pro vytváření elektronických značek, resp. elektronických podpisů je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

6.2.10 Postup při zničení dat pro vytváření elektronických značek

Data pro vytváření elektronických značek, resp. elektronických podpisů, sloužící k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek, jsou uložena v kryptografickém modulu. Ničení je realizováno prostředky kryptografického modulu. Zálohy těchto dat uložené v zašifrované podobě na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů.

Při ničení dat pro vytváření elektronických značek, resp. elektronických podpisů, sloužících k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek musí být fyzicky přítomni:

- ředitel I.CA nebo jím jmenovaný člen vedení I.CA,
- bezpečnostní manažer nebo bezpečnostní administrátor (konkrétně určí ředitel I.CA),
- administrátor systému, nebo jiný pověřený technicky proškolený pracovník I.CA.

O průběhu ničení dat elektronických značek, resp. elektronických podpisů, sloužící k označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek je sepsán protokol.

6.2.11 Hodnocení kryptografického modulu

Nástroj elektronického podpisu pro elektronické podepisování vydávaných kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, splňuje požadavky na kryptografické moduly dle dokumentu „Standard pro hodnocení bezpečnosti kryptografických modulů vydaný NIST v USA – FIPS PUB 140-2 úroveň 3“.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických značek

Tato data jsou obsažena v certifikátech CA/TSS. Na rozdíl od jim příslušných dat pro vytváření elektronických značek, resp. elektronických podpisů, je důležité tato data uchovávat pro případ následné kontroly pravosti vydaných certifikátů, seznamů zneplatněných certifikátů a časových razítek. Se všemi certifikáty CA/TSS je nakládáno způsobem, uvedeným v kapitolách 5.4 a 5.5.

6.3.2 Maximální doba platnosti certifikátu označující osoby a párových dat

Platnost dat určených k ověřování vydaných certifikátů a seznamů zneplatněných certifikátů je dána platností vydaných certifikátů CA/TSS. Pokud dojde k neočekávanému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost použití párových dat, bude jejich životnost zkrácena. V takovém případě se postupuje analogicky postupům uvedených v kapitole 0.

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 pro označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů a časových razítek.

6.4.2 Ochrana aktivačních dat

Povinností pověřených pracovníků I.CA je chránit aktivační data.

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data jsou určena výhradně pro aktivaci soukromého klíče 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:

- 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.
- ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.
- ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.

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.

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 chráněn přístupovým routerem a produktem typu firewall. 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

Profily certifikátů CA/TSS odpovídají doporučením RFC 3280, resp. RFC 5280. Délka klíče certifikační autority, označujícího vydávané kvalifikované systémové certifikáty a seznamy zneplatněných certifikátů je 2048 bitů. Základní atributy jsou uvedeny v Tabulce 7.

Tabulka 7 – Profil certifikátu CA/TSS

Atribut	Hodnota
Version	verze 3
Serial Number	jedinečné číslo vydaného certifikátu CA/TSS
SignatureAlgorithm	algoritmus pro elektronickou značku, resp. elektronický podpis vydávaného certifikátu CA/TSS (sha1WithRSAEncryption)
Issuer	vydavatel certifikátu CA/TSS (viz kapitola 3.1.1)
NotBefore	datum a UTC čas počátku platnosti certifikátu CA/TSS
NotAfter	datum a UTC čas konce platnosti certifikátu CA/TSS
Subject	viz Issuer
SubjectPublicKeyInfo • algorithm • SubjectPublicKey	 rsaEncryption veřejný klíč certifikátu CA/TSS (2048 bit)
extensions	rozšíření certifikátu CA/TSS (viz tabulka 8/8a)
signatureValue	elektronický podpis vydávaného certifikátu CA/TSS

7.1.1 Čísla verzí

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

7.1.2 Rozšiřující položky v certifikátu

Tabulka 8 – Rozšiřující atributy certifikátu CA

Atribut	Hodnota
SubjectKeyIdentifier	SHA1 hash veřejného klíče certifikátu CA
BasicConstraints.cA	True
KeyUsage	keyCertSign, cRLSign
Certificate Policy • Policy • Explicit Text	 viz kapitola 7.1.6 viz kapitola 7.1.8

Tabulka 8a – Rozšiřující atributy certifikátu TSS

Atribut	Hodnota
AuthorityKeyIdentifier.KeyIdentifier	SHA1 hash veřejného klíče certifikátu CA
SubjectKeyIdentifier	SHA1 hash veřejného klíče certifikátu TSS
KeyUsage	Digital Sign, Non Repudation
ExtendedKeyUsage	id-kp-timeStamping
Certificate Policy • Policy • Explicit Text	 viz kapitola 7.1.6 viz kapitola 7.1.8

7.1.3 Objektové identifikátory (dále OID) algoritmů

Jsou využívány algoritmy, které v souladu s příslušnými technickými standardy.

7.1.4 Způsoby zápisu jmen a názvů

Uvedeno v kapitole 3.1.

7.1.5 Omezení jmen a názvů

Atribut nameConstraints není použit. Pro jméno subjektu (Subject) není žádné omezení s výjimkou omezení vyplývajících z kapitoly 3.1.2.

7.1.6 OID certifikační politiky

Tato CP je určena pro vydávání a správu certifikátů CA/TSS. Přidělené OID certifikační politiky, obsažené ve vydávaném certifikátu CA je uvedené v kapitole 1.2. OID politiky, obsaženém vydávaných certifikátech časovým serverům (TSS), je 1.3.6.1.4.1.23624.1.4.13.2.

7.1.7 Rozšiřující položka „Policy Constrainsts“

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

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

CA:

[1]CertificatePolicies:
Policy Identifier = viz kapitola 1.2
[1,1]Policy Qualifier Info:
Policy Qualifier Info=Uživatelské oznámení
Qualifier:
Text oznámení= Tento certifikat je vydan jako kvalifikovany systemovy certifikat v souladu se zakonem 227/2000 Sb. v platnem zneni.

TSS:

[1]CertificatePolicies:
Policy Identifier = viz kapitola 1.2
[1,1]Policy Qualifier Info:
Policy Qualifier Info=Uživatelské oznámení
Qualifier:
Text oznámení= Tento kvalifikovany systemovy certifikat TSA je vydan v souladu se zakonem 227/2000 Sb. v platnem zneni.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Položka je nekritická.

7.2 Profil seznamu zneplatněných certifikátů

Tabulka 9 – Profil CRL

Položka	Obsah
Version	Verze v2
SignatureAlgorithm	algoritmus pro elektronický podpis vydávaného CRL (sha1WithRSAEncryption)
Issuer	vydavatel CRL
thisUpdate	datum a UTC čas vydání CRL
nextUpdate	datum a předpokládaný UTC čas vydání následujícího CRL
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtension.CRL.Reason	důvod zneplatnění certifikátu
crlExtensions	rozšíření CRL - viz tab.10
signatureValue	elektronický podpis vydaného CRL

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

Tabulka 10 – Rozšiřující atributy CRL

Položka	Obsah
AuthorityKeyIdentifier.KeyIdentifier	hash veřejného klíče vydavatele CRL
CRLNumber	jedinečné číslo vydávaného CRL

7.3 Profil OCSP

Tyto skutečnosti jsou pro aplikaci vydání této CP irelevantní.

7.3.1 Číslo verze

Tyto skutečnosti jsou pro aplikaci vydání této CP irelevantní.

7.3.2 Rozšiřující položky OCSP

Tyto skutečnosti jsou pro aplikaci vydání této CP irelevantní.

8 Hodnocení shody a jiná hodnocení

V I.CA jsou prováděna hodnocení bezpečnosti v oblastech, uvedených v kapitole 8.4. Součástí těchto hodnocení je mimo jiné sledování, zda jsou plně dodržovány standardy, uvedené v kapitole.

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Celková kontrola bezpečnostní shody je prováděna po 4 letech od předchozí celkové kontroly bezpečnostní shody. Během těchto 4 let mohou být prováděny roční částečné kontroly bezpečnostní shody.

Audit systému bezpečnosti informací je prováděn po 2 letech od předchozího auditu systému bezpečnosti informací a je prováděn podle požadavků normy ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.

8.2 Identita a kvalifikace hodnotitele

Identita a kvalifikace hodnotitele je upravena interní směrnicí I.CA.

8.3 Vztah hodnotitele k hodnocené entitě

V případě auditu systému managementu bezpečnosti informací je hodnotitelem externí, nezávislá auditující organizace.

V případě celkové kontroly bezpečnostní shody nebo částečné kontroly bezpečnostní shody je hodnotitelem fyzická/právnická osoba, pověřená ředitelem společnosti První certifikační autorita, a.s.

8.4 Hodnocené oblasti

Cílem kontroly bezpečnostní shody je ověření, že společnost První certifikační autorita, a.s.:

- provozuje důvěryhodné systémy v souladu se ZoEP a VoEP,
- provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací, a to jejími částmi upravujícími řízení změn.

Předmětem kontroly bezpečnostní shody:

- jsou všechny důvěryhodné systémy I.CA (celková kontrola bezpečnostní shody), nebo,
- jsou všechny změny, které I.CA provedla od provedení předchozí kontroly bezpečnostní shody, a jejich vliv na důvěryhodné systémy I.CA (částečná kontrola bezpečnostní shody), nebo
- je v případě, že v důvěryhodných systémech I.CA nenastaly od předchozí částečné kontroly bezpečnostní shody žádné změny, ověření této skutečnosti.

Cílem auditu systému managementu bezpečnosti informací je objektivní a na I.CA nezávislé ověření, že je v důvěryhodných systémech I.CA v oblasti vydávání certifikátů zaveden a uplatňován systém managementu bezpečnosti informací.

S ohledem na uvedené, poskytne I.CA subjektu, který audit systému managementu bezpečnosti informací provádí zprávu o naposledy provedené kontrole bezpečnostní shody a bezpečnostní dokumentaci (v aktuálních verzích).

8.5 Postup v případě zjištěných nedostatků

V případě nedostatků, zjištěných na základě zprávy o celkové nebo částečné kontrole bezpečnostní shody (viz kapitoly 8.1, 8.4, 8.6) je bezpečnostní manager povinen do 15 dnů po obdržení zprávy určit, jaká opatření k odstranění nedostatků je I.CA povinna přijmout.

Zjistí-li příslušný úřad, že I.CA porušuje povinnosti stanovené ZoEP, VoEP uloží jí, aby ve stanovené lhůtě zjednala nápravu a případně určí, jaká opatření k odstranění nedostatků je I.CA povinna přijmout.

8.6 Sdělování výsledků hodnocení

I.CA zajistí zpracování zprávy o kontrole bezpečnostní shody, jejímž obsahem je:

- vymezení předmětu kontroly bezpečnostní shody:
  - celková kontrola bezpečnostní shody - vymezení všech důvěryhodných systémů podle s uvedením kvalifikovaných certifikačních služeb, které jsou prostřednictvím těchto systémů zajišťovány,
  - částečná kontrola bezpečnostní shody - vymezení změn, které I.CA provedla od provedení předchozí kontroly bezpečnostní shody a vymezení kvalifikovaných certifikačních služeb, které jsou zajišťovány prostřednictvím důvěryhodných systémů, těmito změnami ovlivněných,
- identifikace dokumentace, která byla předmětem kontroly bezpečnostní shody ,
- popis postupu, jakým byla kontrola bezpečnostní shody prováděna,
- jméno, popřípadě jména a příjmení osoby, která kontrolu bezpečnostní shody provedla,
- prohlášení subjektu, který kontrolu bezpečnostní shody provedl, o výsledku kontroly bezpečnostní shody, jehož součástí je prohlášení o tom, že I.CA provozuje důvěryhodné systémy v souladu se ZoEP, VoEP a provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací, a to jejími částmi upravujícími řízení změn.

Zpráva o kontrole bezpečnostní shody:

- je předána bezpečnostnímu managerovi do 10 dnů od ukončení kontroly, který s jejím obsahem seznámí ředitele I.CA a bezpečnostní výbor,
- je předána příslušnému úřadu do 30 dnů od ukončení kontroly.

I.CA zajistí:

- že zpráva o auditu systému managementu bezpečnosti informací obsahuje:
  - vymezení předmětu auditu systému managementu bezpečnosti informací, přičemž vymezením předmětu auditu se rozumí vymezení kvalifikovaných certifikačních služeb, které jsou zajišťovány prostřednictvím důvěryhodných systémů,
  - identifikace dokumentace, která byla předmětem auditu systému managementu bezpečnosti informací a kterou I.CA poskytla subjektu, který audit systému managementu bezpečnosti informací provádí,
  - prohlášení subjektu, který audit systému managementu bezpečnosti informací provedl, o výsledku auditu systému managementu bezpečnosti informací, jehož součástí je prohlášení o tom, že je v I.CA uplatňován systém managementu bezpečnosti informací,
- zveřejnění prohlášení o výsledku auditu systému managementu bezpečnosti informací ve zprávě pro uživatele.

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

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 a o zneplatnění certifikátu

Přístup k informacím o zneplatněných certifikátech elektronickou cestou I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Předání certifikátu CA/TSS je poskytováno zdarma.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

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 finanční 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

Viz kapitoly 9.2.1 a 9.2.2.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

Citlivými informacemi I.CA jsou:

- data pro vytváření elektronických značek, resp. elektronických podpisů příslušná k datům pro ověřování elektronických značek, resp. elektronických podpisů obsažených v certifikátech CA/TSS,
- data pro vytváření elektronických podpisů, resp. elektronických značek příslušná k datům pro ověřování elektronických podpisů, resp. elektronických značek obsažených v účelových certifikátech I.CA (např. klíče pro komunikaci s RA),
- ostatní kryptograficky podstatné informace sloužící k provozu I.CA,
- vybrané obchodní informace I.CA,
- veškeré informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb dle ZoEP.

Chráněnými obchodními informacemi jednotlivých RA jsou:

- data pro vytváření elektronických podpisů, resp. elektronických značek příslušná k datům pro ověřování elektronických podpisů, resp. elektronických značek obsažených v účelových certifikátech RA,
- ostatní kryptograficky podstatné informace sloužící k provozu RA,
- veškeré informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb dle ZoEP.

Za chráněné informace se rovněž považují veškeré další informace označené některým ze subjektů jako citlivé.

S chráněnými informacemi, bez ohledu na typ nosiče, je zacházeno tak, aby byla zajištěna jejich důvěrnost a integrita.

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

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

9.4 Ochrana osobních údajů

Problematika ochrany osobních údajů (kapitoly 9.4.1 až 9.4.7) je řešena interní dokumentací.

9.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů je v I.CA řešena v souladu s požadavky zákona ČR č. 101/2000 Sb. v aktuálním znění

9.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje klientů, uživatelů či pracovníků, podléhající ochraně ve smyslu příslušné zákonné normy (zákon č. 101/2000 Sb. v aktuálním znění).

9.4.3 Údaje, které nejsou považovány za důvěrné

Informace, které nejsou považovány za důvěrné jsou takové údaje, které nepodléhající ochraně ve smyslu příslušné zákonné normy (zákon č. 101/2000 Sb. v aktuálním znění).

9.4.4 Odpovědnost za ochranu osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákona č. 101/2000 Sb. v aktuálním znění.

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

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákona č. 101/2000 Sb. v aktuálním znění.

9.4.6 Poskytování citlivých informací pro soudní či správní účely

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákona č. 101/2000 Sb. v aktuálním znění.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákona č. 101/2000 Sb. v aktuálním znění.

9.5 Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek, certifikáty/klíče CA/TSS 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/TSS pouze k označování, resp. podepisování vydávaných certifikátů, seznamu zneplatněných certifikátů a časových razítek,
- vydávané certifikáty splňují náležitosti, uvedené v ZoEP,
- zneplatní certifikáty pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v odpovídající CP.

9.6.2 Zastupování a záruky RA

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

9.6.3 Zastupování a záruky držitele certifikátu a podepisující osoby

Držitel certifikátu postupuje v souladu s touto CP a ručí za informace, uvedené ve vydaném certifikátu.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu se ZoEP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

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

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované certifikační politikou, dle které byl certifikát vydán.

9.9 Odpovědnost za škodu, náhrada škody

Není relevantní pro tento dokument, je řešeno v politikách pro vydávání certifikátů koncovým klientům.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato CP 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

Uvedeno v kapitole 9.10.1.

9.11 Komunikace mezi zúčastněnými subjekty

Všechny zúčastněné subjekty jsou organizačnímu částmi I.CA a komunikace mezi nimi se řídí interními pravidly I.CA.

9.12 Změny

9.12.1 Postup při změnách

Postup je realizován řízeným procesem, uvedeném v interním dokumentu.

9.12.2 Postup při oznamování změn

Vydání nové verze certifikační politiky je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněno OID

V případě změn, majících vliv na obsah vydávaného certifikátu, je vždy změněn i její OID.

9.13 Řešení sporů

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

9.14 Rozhodné právo

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

9.15 Shoda s právními předpisy

Systém poskytování kvalifikovaných certifikačních služeb je provozován ve shodě s požadavky ZoEP.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

9.16.2 Postoupení práv

V případě ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb postupuje společnost První certifikační autorita, a.s., v souladu se ZoEP.

9.16.3 Oddělitelnost ustanovení

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

9.16.4 Zřeknutí se práv

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

9.16.5 Vyšší moc

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývající ze zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu.

9.17 Další opatření

Tyto skutečnosti jsou pro aplikaci tohoto vydání CP irelevantní.

10 Závěrečná ustanovení

Tato CP vydaná, společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 22.09.2015.