První certifikační autorita, a.s.

POLITIKA VYDÁVÁNÍ KVALIFIKOVANÝCH ČASOVÝCH RAZÍTEK

Stupeň důvěrnosti : veřejný dokument

Verze 2.0

Tabulka 1 - Identifikace

Název	Politika vydávání kvalifikovaných časových razítek
Společnost	První certifikační autorita, a.s.
Schválil	ředitel společnosti První certifikační autorita, a.s.

Tabulka 2 – Vývoj dokumentu

Verze	Datum vydání	Shrnutí změn
1.0	01.02.2006	první verze dokumentu
2.0	01.10.2007	použití více vyhrazených serverů pro vydávání kvalifikovaných časových razítek

Obsah

1 Úvod

Tento dokument, **Politika vydávání kvalifikovaných časových razítek,** vypracovaný společností První certifikační autorita, a. s. (dále též I.CA) :

- je v souladu se zákonem 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., a s ním souvisejících předpisů a vyhlášek
- je v souladu se zákonem Slovenské republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok
- se zabývá skutečnostmi, které se vztahují na :
    - I.CA, klienty, spoléhající se strany, smluvní partnery[1] a jiné účastníky PKI, a které souvisejí s vydávaným kvalifikovaným časovým razítkem - jeho další správou a používáním
    - aspekty, související se správou serveru, vydávajícího kvalifikovaná časová razítka
- je kompatibilní s doporučeními ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities a RFC 3647, s přihlédnutím k doporučením orgánů EU, právu ČR a SR v dané oblasti.

Přečtením tohoto dokumentu se ujistěte o tom, zda kvalifikovaná časová razítka, vydávaná I.CA, splňují Vaše požadavky.

[1] pojmy I.CA, klient, spoléhající se strany a smluvní partner jsou uvedeny v kapitole 3

2 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 časových razítek, poskytované společností První certifikační autorita, a.s., je možné považovat za důvěryhodné.

Společnost **První certifikační autorita, a.s., je od:**

- 18.03.2002 prvním akreditovaným poskytovatelem certifikačních služeb v ČR pro oblast vydávání **kvalifikovaných certifikátů** podle zákona ČR 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.,
- 01.02.2006 akreditovaným poskytovatelem certifikačních služeb v ČR pro oblast vydávání **kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek** podle zákona ČR 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.,
- 21.09.2006 prvním zahraničním kvalifikovaným poskytovatelem certifikačních služeb v SR, kterému byla udělena akreditace v oblasti poskytování **kvalifikovaných certifikátů a kvalifikovaných časových razítek** podle aktuálního znění zákona SR č. 215/2002 o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok

Podrobný popis autority časových razítek je uveden v dalších dokumentech, které jsou obecně neveřejné. Neveřejné dokumenty, včetně zpráv, výsledků testů a interních kontrol vytvářejí dokumentační sadu, dosažitelnou výhradně autorizovanému personálu a auditorům. V tabulce 3 jsou uvedeny významné bezpečnostní dokumenty, vztahující se k certifikačním službám v oblasti kvalifikovaných časových razítek.

Tab. 3 – Bezpečnostní dokumenty

Číslo	Název dokumentu	Status
1.	Politika vydávání kvalifikovaných časových razítek	Veřejný
2.	Prováděcí směrnice vydávání kvalifikovaných časových razítek	Neveřejný
3.	Zpráva a souhlas vedení I.CA o hodnocení rizik TSA (obsahující analýzu rizik)	Neveřejný
4.	Systémová bezpečnostní politika TSA	Neveřejný
5.	Plán pro zvládání krizových situací a plán obnovy	Neveřejný
6.	Zpráva pro uživatele TSA	Veřejný
7.	Sada bezpečnostních norem a směrnic	Neveřejný
8.	Celková bezpečnostní politika	Neveřejný
9.	Prohlášení o aplikovatelnosti	Neveřejný

Dokument Politika vydávání kvalifikovaných časových razítek je vypracován na obecné úrovni a nepopisuje technické detaily datového komunikačního systému, struktury společnosti, operačních procedur nebo technické ochrany. Také nijak nespecifikuje prostředí, ve kterém je TSA provozována. Technické a operační detaily jsou uvedeny v relevantních interních dokumentech.

Vydávání a správa nadřízeného kvalifikovaného systémového certifikátu, resp. certifikátu TSS se řídí speciálními dokumenty „Certifikační politika vydávání certifikátů CA/TSS“ a „Certifikační prováděcí směrnice vydávání certifikátů CA/TSS“

V procesu poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů provozuje společnost První certifikační autorita, a.s jedinou certifikační autoritu.

V procesu poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek provozuje společnost První certifikační autorita, a.s jedinou autoritu časových razítek, jejíž jádrem je sada kvalitativně totožných serverů, generujících tato časová razítka.

Informace o dalších poskytovaných certifikačních službách je možno získat na internetové informační adrese, uvedené v kapitole 7.4.13.3.2.

2.1 Název a identifikace dokumentu

Název tohoto dokumentu	:	Politika vydávání kvalifikovaných časových razítek
OID	:	1.3.6.1.4.1.23624.1.4.14.2

3 Přehled použitých pojmů a zkratek

Dále uvedený přehled pojmů a zkratky je platný pro tento dokument. V případě pojmu může být na pravé straně v závorkách uveden zdroj, v němž se nachází původní pojem včetně definice. Použité zkratky mají alternativní charakter, tzn. v textu může být použit jak plný text, tak i jeho zkratka, přičemž obojí má totožnou obsahovou hodnotu.

3.1 Použité pojmy

Tabulka 4 – 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	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného časového razítka a které bylo kvalifikované časové razítko vydáno
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	matematicky vypočtená jedinečná hodnota, představující zhuštěnou hodnotu dlouhé zprávy, ze které byla vypočtena
I.CA	První certifikační autorita, a.s. – akreditovaný poskytovatel certifikačních služeb
Klient	fyzická nebo právnická osoba, se kterou uzavřela I.CA smlouvu o vydávání kvalifikovných časových razítek
Kvalifikované časové razítko	datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem
Kvalifikovaný certifikát (QC)	certifikát, který má náležitosti podle platné legislativy a byl vydán kvalifikovaným poskytovatelem certifikačních služeb
Kvalifikovaný systémový certifikát (QSC)	certifikát, který má náležitosti podle § 12a ZoEP a byl vydán kvalifikovaným poskytovatelem certifikačních služeb (§ 2, písm. m ZoEP)
Nadřízený kvalifikovaný systémový certifikát, resp. certifikát I.CA nebo certifikát TSS	kvalifikovaný certifikát poskytovatele certifikačních služeb, který se řídí speciálními dokumenty vydanými I.CA • „Certifikační politika vydávání certifikátů CA/TSS“ • „Certifikační prováděcí směrnicí vydávání certifikátů CA/TSS“
Nonce	Náhodné číslo, o kterém se předpokládá, že jej klient vygeneruje pouze jednou (64 bit integer). V případě, že toto číslo žádost

Pojem	Vysvětlení
	obsahuje, pak toto číslo musí obsahovat i odpověď.
Otisk	viz hash
Párová data	jedinečná data pro vytváření elektronického podpisu nebo elektronické značky spolu s odpovídajícími daty pro ověřování elektronického podpisu nebo 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
ReqPolicy	Identifikátor politiky
Smluvní partner	poskytovatel 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 nebo elektronické značky
Statut kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu	stav, ve kterém se kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nachází, tzn. ve stavech platnosti, neplatnosti, zneplatnění, zablokování
Spoléhající se strana	subjekt spoléhající se při své činnosti na kvalifikovaný certifikát, kvalifikovaný systémový certifikát nebo kvalifikované časové razítko vydané I.CA
Uživatel	klient, držitel, spoléhající se strana, žadatel, popř. subjekt, rozhodující se o využívání poskytované certifikační služby v oblasti kvalifikovaných časových razítek
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, který splňuje následující požadavky : • je jednoznačně spojen s podepisující osobou • umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě • byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou • je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat
Zneplatnění	kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát, který byl I.CA zneplatněn bez možnosti obnovení této platnosti
Žadatel	fyzická osoba nebo oprávněný jednatel právnické osoby podávající na RA žádost o službu.
Žádost o službu (Žádost)	formální dokument žádosti o některou ze služeb poskytovaných I.CA
Žádost o vydání kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu nebo kvalifikovaného časového razítka	formální, standardní dokument elektronické žádosti o vydání kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu nebo kvalifikovaného časového razítka dle přípustných norem a směrnic definovaných v konktrétní politice

3.2 Zkratky

Tabulka 5 – Zkratky

Zkratka	Vysvětlení
CRL	**C**ertificate **R**evocation **L**ist (seznam zneplatněných certifikátů)
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
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**inistersvo **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
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, generující 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	**U**ninterruptible **P**ower **S**upply
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 (BIPM)
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) • vyhláška Slovenské republiky č. 540/2002 Z.z., o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov
ZoEP	• aktuální znění zákona České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některýchdalších 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. • aktuální znění zákona Slovenské republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov

4 Základní pojetí

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

- **certifikát** míněn kvalifikovaný certifikát, resp. kvalifikovaný systémový certifikát
- **časové razítko** míněno kvalifikované časové razítko
- **certifikát TSS** míněn certifikát konkrétního serveru generujícího kvalifikovaná časová razítka

4.1 Služby autority časových razítek (TSA)

Procesy, spojené s vydáváním kvalifikovaných časových razítek, jsou rozděleny do dvou oblastí :

- základní procesy - generování a vydávání kvalifikovaných časových razítek
- podpůrné procesy - monitorování a řízení operací spojených s procesem vydávání kvalifikovaných časových razítek, tzn. :
    - synchronizace časového údaje TSS s poskytovatelem důvěryhodných synchronizačních časových služeb, který zajišťuje tyto služby na základě písemné smlouvy pro I.CA
    - správa ostatních systémových komponent TSA.

4.2 Autorita časových razítek

TSA je z pohledu klientů a spoléhajících se stran důvěryhodná komunikační infrastruktura, vydávající kvalifikovaná časová razítka. Z titulu provozovatele nese celkovou zodpovědnost za poskytování certifikačních služeb v oblasti vydávání kvalifikovaných časových razítek společnost První certifikační autorita, a.s.

Pro základní procesy (kapitola 4.1) nejsou využívány smluvní partneři a generování kvalifikovaných časových razítek je prováděno serverem/servery (TSS), umístěným/umístěnými v provozním prostředí I.CA.

4.3 Žadatelé o kvalifikované časové razítko a držitelé kvalifikovaného časového razítka

Žadatelem nebo držitelem kvalifikovaného časového razítka může být na základě písemné smlouvy (viz kapitola 4.3) s I.CA individuální koncový uživatel (fyzická osoba), nebo právnická osoba, resp. organizační složka státu zahrnující několik koncových uživatelů.

V případě, že žadatelem nebo držitelem kvalifikovaného časového razítka je individuální koncový uživatel, je pak tento přímo zodpovědný za to, že splní závazky vůči I.CA.

V případě, že žadatelem nebo držitelem kvalifikovaného časového razítka je právnická osoba nebo organizační složka státu, pak její závazky vůči I.CA platí i pro její koncové uživatele a tato právnická osoba nebo organizační složka státu je vždy zodpovědná za to, že její koncoví uživatelé závazky vůči I.CA splní. Proto musí právnická osoba nebo organizační složka státu vhodným způsobem informovat vlastní koncové uživatele.

4.4 Spoléhající se strana

Spoléhající se stranou je individuální fyzická osoba (koncový uživatel), právnická osoba nebo organizační složka státu, spoléhající se při své činnosti na vydaná kvalifikovaná časová razítka.

5 Politika TSA

5.1 Použití kvalifikovaných časových razítek

Politika vydávání kvalifikovaných časových razítek nedefinuje žádná omezení použitelnosti kvalifikovaného časového razítka, vydaného v souladu s jejím obsahem[2]. Kvalifikovaná časová razítka je možné použít např. v oblastech :

- elektronických podpisů, resp. elektronických značek, kdy je třeba ověřit, že byly vytvořeny v době, kdy certifikát veřejného klíče podepisující, resp. označující entity byl platný. Tato kontrola je nezbytná z následujících dvou důvodů :
    - zda nebyl během platnosti certifikátu elektronicky podepisující, resp. označující entity odpovídající soukromý klíč kompromitován
    - zda nebyl elektronický podpis, resp. značka vytvořen po ukončení doby platnosti příslušného certifikátu
- ochraně spustitelného kódu
- transakcí prováděných na síti

5.2 Hodnocení shody a jiná hodnocení

V I.CA jsou prováděna hodnocení bezpečnosti v oblastech, uvedených v kapitole 5.2.4. Součástí těchto hodnocení je mimo jiné sledování, zda jsou plně dodržovány standardy, uvedené v kapitole 7.4.7.2. Oblast hodnocení shody a jiných hodnocení (kapitoly 5.2.1 až 5.2.6) je upravena interní směrnicí I.CA.

S ohledem na skutečnost, že I.CA je aktreditovaným poskytovatelem certifikačních služeb (viz kapitola 2), je dále dle příslušných legislativ vykonáván dozor nad její činností akreditačními úřady, konkrétně Ministerstvem vnitra České republiky a Národním bezpečnostním úřadem Slovenské republiky.

5.2.1 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 jsou prováděny roční částečné kontroly bezpečnostní shody. Kontrola bezpečnostní shody je prováděna podle požadavků technické normy ČSN ISO/IEC TR 13335 - Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3.

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

5.2.2 Identita a kvalifikace hodnotitele

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

[2] kvalifikovaná časová razítka vydaná podle této politiky lze využívat jak v otevřených systémech veřejných služeb (např. státní správy), tak v uzavřených systémech soukromých společností.

5.2.3 Vztah hodnotitele k hodnocené entitě

V případě auditu systému řízení bezpečnosti informací je hodnotitelem externí, nezávislý auditující subjekt.

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

5.2.4 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 řízení bezpečnosti informací je objektivní a na I.CA nezávislé ověření, že je v důvěryhodných systémech I.CA v oblasti vydávání kvalifikovaných časových razítek zaveden a uplatňován systém řízení bezpečnosti informací.

S ohledem na uvedené, poskytne I.CA subjektu, který audit systému řízení bezpečnosti informací provádí :

- zprávu o naposledy provedené kontrole bezpečnostní shody
- bezpečnostní dokumentaci (v aktuálních verzích)

5.2.5 Postupy v případě zjištěných nedostatků

V případě nedostatků, zjištěných na základě zprávy o kontrole bezpečnostní shody, resp. zprávy o auditu systému řízení bezpečnosti informací, je bezpečnostní manager povinnen do 15 dnů po obdržení zprávy určit, jaká opatření k odstranění nedostatků je I.CA povinna přijmout.

Zjistí-li příslušný akreditační úřad (viz kapitola 5.2), že I.CA porušuje povinnosti stanovené ZoEP, VoEP (viz kapitoly 5.2.4 a 5.2.6) uloží jí, aby ve stanovené lhůtě zjednala nápravu a případně určí, jaká opatření k odstranění nedostatků je I.CA povinna přijmout.

5.2.6 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 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 řízení bezpečnosti informací obsahuje :
    - vymezení předmětu auditu systému řízení 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 řízení bezpečnosti informací a kterou I.CA poskytla subjektu, který audit systému řízení bezpečnosti informací provádí,
    - prohlášení subjektu, který audit systému řízení bezpečnosti informací provedl, o výsledku auditu systému řízení bezpečnosti informací, jehož součástí je prohlášení o tom, že je v I.CA uplatňován systém řízení bezpečnosti informací
- zveřejnění prohlášení o výsledku auditu systému řízení bezpečnosti informací ve zprávě pro uživatele.

6 Závazky a odpovědnosti

6.1 Závazky TSA

6.1.1 Obecné závazky TSA

Společnost První certifikační autorita a.s. zaručuje :

- nepřetržitý přístup ke službám TSA, s výjímkou plánovaných (předem ohlášených), popř. neplánovaných časových přerušení (tyto okolnosti jsou uvedeny v interní dokumentaci) spojených s technickými zásahy
- autentizovaný přístup ke službám vydávání kvalifikovaných časových razítek na základě písemné smlouvy (viz kapitola 4.3)
- striktní dodržování platné legislativy
- soulad se zákony a neporušování autorských ani licenčních práv aktivitami společnosti
- ochranu veškerých osobních údajů dle platné legislativy
- že se kdokoli může ujistit o její identitě a jejím certifikátu/certifikátech TSS
- poskytování kvalifikovaných certifikačních služeb osobami s odbornými znalostmi a kvalifikací nezbytnou pro poskytování kvalifikované certifikační služby a obeznámenými s příslušnými bezpečnostními postupy
- používání bezpečných systémů a bezpečných nástrojů - zajišťuje dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují včetně dostatečné kryptografické bezpečnosti těchto nástrojů
- používání bezpečných systémů pro uchovávání kvalifikovaných časových razítek
- dostatečnost finančních zdrojů nebo jiných finančních zajištění na provoz v souladu s požadavky uvedenými ZoEP a s ohledem na riziko vzniku odpovědnosti za škodu po celou dobu své činnosti
- že před uzavřením smlouvy (viz kapitola 4.3) s klientem o vydávání kvalifikovaných časových razítek jej písemně informuje o přesných podmínkách pro využívání této služby, včetně případných omezení pro její použití, a o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je či není akreditována
- že v případě odnětí akreditace bez prodlení informuje o této skutečnosti klienty a další dotčené osoby
- uchovávání informací a dokumentace souvisejících s poskytovanou službou vydávání kvalifikovaných časových razítek dle požadavků ZoEP
- že její kmenoví zaměstnanci, 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)

6.1.2 Závazky TSA ve vztahu k žadatelům o kvalifikované časové razítko a držitelům kvalifikovaných časových razítek

Společnost První certifikační autorita a.s. zajišťuje a zaručuje, že :

- jí vydávaná kvalifikovaná časová razítka obsahují všechny náležitosti stanovené ZoEP, VoEP
- použije soukromé klíče příslušné certifikátům TSS pouze k označování vydávaných kvalifikovaných časových razítek
- data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídají datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku
- implementovala odpovídající opatření proti padělání kvalifikovaných časových razítek
- vydá kvalifikované časové razítko neprodleně po obdržení platného požadavku
- žádným způsobem neověřuje otisk (hash), kterému má být kvalifikované časové razítko přiřazeno (s výjimkou jeho délky)

- využívá důvěryhodnou časovou synchronizaci
- jí vydané kvalifikované časové razítko obsahuje minimálně :

    - unikátní číslo kvalifikovaného časového razítka
    - označení pravidel, podle kterých bylo kvalifikované časové razítko vydáno
    - její název a stát, ve kterém má sídlo
    - časový údaj, jehož odchylka nepřesáhne 1 sekundu od UTC
    - data v elektronické podobě - otisk (hash), pro která bylo kvalifikované časové razítko vydáno
    - elektronickou značku, resp. elektronický podpis TSS

6.2 Závazky žadatelů o kvalifikované časové razítko a držitelů kvalifikovaného časového razítka

Žadatelé jsou vždy po obdržení odpovědi na žádost o kvalifikované časové razítko povinni zjistit chybový status. V případě chyby není kvalifikované časové razítko v odpovědi obsaženo a žadatel je povinen překontrolovat odpovídající chybovou hlášku. V opačném případě je žadatel povinen :

- ověřit elektronickou značku, resp. elektronický podpis TST a zkontrolovat, zda certifikát relevantního TSS nebyl odvolán - CRL je přístupné na elektronické informační adrese (kapitola 7.4.13.3.2)
- ověřit, zda vrácený otisk (hash) je totožný s odeslaným
- v případě, že žádost obsahovala položku „nonce“ ověřit, že její hodnota v odpovědi je totožná
- v případě, že žádost obsahovala položku „reqPolicy“ ověřit, že její hodnota v odpovědi je totožná

6.3 Závazky spoléhajících se stran

Obecným závazkem spoléhajících se stran je ověření elektronické značky, resp. elektronického podpisu TST. Spoléhající se strana je povinna :

- ověřit platnost certifikátu relevantního TSS
- překontrolovat, zda politika, pod kterou bylo kvalifikované časové razítko vydáno, je akceptovatelná jejím potřebám, popř. potřebám jí provozované aplikace

V případě ověřování kvalifikovaného časového razítka po ukončení platnosti certifikátu relevantního TSS, jsou spoléhající se strany povinny :

- ověřit, zda certifikát relevantního TSS nebyl v době vydání kvalifikovaného časového razítka odvolán - CRL je přístupné na elektronické informační adrese (kapitola 7.4.13.3.2)
- ověřit, zda kryptografická funkce pro tvorbu otisku (hash) v kvalifikovaném časovém razítku je stále bezpečná – uvedeno na elektronické informační adrese (kapitola 7.4.13.3.2)
- ujistit se, zda délka kryptografického klíče a algoritmus jsou stále považovány za bezpečné - uvedeno na elektronické informační adrese (kapitola 7.4.13.3.2)

6.4 Odpovědnost

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud klient nebo spoléhající se strana neporušili povinnosti, plynoucí jim z této politiky. Na kvalifikovaná časová razítka, která I.CA nevydala, se záruky nevztahují.

7 Požadavky na postupy TSA

7.1 Správa politiky

7.1.1 Organizace spravující politiku TSA nebo prováděcí směrnici TSA

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

7.1.2 Kontaktní osoba organizace spravující politiku TSA nebo prováděcí směrnici TSA

Ředitel I.CA určuje kontaktní osobu, jejíž e-mail, telefonní číslo a fax jsou uvedeny na internetové informační adrese (kapitola 7.4.13.3.2).

7.1.3 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.

7.1.4 Postupy při schvalování souladu s bodem 7.1.3

V případě, že je potřebné s ohledem na kapitolu 7.1.3 provést změny v tomto dokumentu a odpovídající prováděcí směrnici, určuje ředitel I.CA osobu, která je oprávněna změny provádět. Dále platí ustanovení, uvedené v kapitole 7.1.3.

7.2 Požadavky na životní cyklus párových dat TSA

Párová data TSA jsou používána pro zajištění integrity, důvěrnosti, autentizace a zajištění neodmítnutelnosti odpovědnosti. S ohledem na různé úrovně hrozeb, které závisí na způsobu využívání párových dat, lze tato data rozdělit do následujících kategorií :

- párová data (relevantního TSS) vyhrazená pro elektronické označování, resp. elektronické podepisování vydávaných kvalifikovaných časových razítek a ověřování elektronické značky, resp. elektronického podpisu vydaných kvalifikovaných časových razítek
- párová data vyhrazená pro infrastrukturu důvěryhodného času, využívaná v procesech kontroly a synchronizaci měřidla času relevantního TSS
- párová data využívaná v procesu správy TSA

Následující kapitoly (7.2.1 až 7.2.10), včetně jejich podkapitol, řeší problematiku serverů generujících kvalifikovaná časová razítka (TSS). Konkrétní technický postup generace párových dat TSS a následné vyhotovení certifikátu TSS je popsán v interní dokumentaci I.CA.

7.2.1 Generování a instalace párových dat

7.2.1.1 Generování párových dat

Generování párových dat, které probíhá v zabezpečené zóně v souladu s dokumentem „***Systémová bezpečnostní politika TSA***“ a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu, který splňuje požadavky na kryptografické funkce a je uveden v seznamu nástrojů, u nichž byla příslušným úřadem vyslovena shoda. Použitý modul svými vlastnostmi odpovídá požadavkům vyžadovaným aktuálními verzemi ZoEP a VoEP. I.CA používá pro párová data, sloužící k označování, resp. podepisování vydávaných kvalifikovaných časových razítek, délku rovnou 2048 bitů.

V průběhu procesu generování párových dat, sloužících k elektronickému označování, resp. podepisování, vydávaných kvalifikovaných 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, sloužících k elektronickému označování, resp. podepisování vydávaných kvalifikovaných časových razítek a následné vyhotovení certifikátu TSS, příslušného k těmto párovým datům, je popsán v interní dokumentaci I.CA.

O průběhu generování párových dat, sloužících k elektronickému označování, resp. podepisování vydávaných kvalifikovaných 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 TSS, obsahující data pro ověřování elektronických značek, resp. elektronických podpisů vydávaných kvalifikovaných časových razítek, obsažená v právě vygenerovaných párových datech
- datum vyhotovení protokolu
- vlastnoruční podpisy všech pracovníků, kteří generaci párových dat prováděli

7.2.1.2 Předání veřejných klíčů

Způsob předání veřejných klíčů TSS je uveden v interní dokumentaci I.CA.

7.2.1.3 Poskytování veřejných klíčů

Data pro ověřování elektronických značek, resp. elektronických podpisů relevantního TSS jsou obsažena v jeho certifikátu, který je možno získat nejméně dvěma nezávislými kanály :

- prostřednictvím internetových informačních adres I.CA a příslušného úřadu
- prostřednictvím věstníku příslušného úřadu

7.2.1.4 Délky párových dat

I.CA používá nejprověřenější klasický asymetrický šifrový algoritmus – RSA. Mohutnost směnných prvků (klíčů - modulus) použitých pro označování, resp. podepisování vydávaných kvalifikovaných časových razítek je 2048 bitů.

7.2.2 Ochrana soukromého klíče (dat pro vytváření elektronických značek)

7.2.2.1 Standardy a podmínky používání kryptografických modulů

Generování párových dat relevantního TSS a uložení jeho soukromého klíče (sloužícího pro elektronické označování, resp. podepisování vydávaných kvalifikovaných časových razítek) jsou realizovány jeho kryptografickým modulem, který je uveden v seznamu nástrojů, u nichž byla vyslovena shoda.

7.2.2.2 Sdílení tajemství

Ochrana sdílením tajemství je realizována prostředky kryptografického modulu. Při provádění citlivých činností, které souvisejí se zásadními činnostmi (viz. kapitoly 7.2.1.1 a 7.2.2.10), je nezbytná přítomnost tří pověřených pracovníků I.CA, z nichž dva znají část kódu k provedení těchto činností.

7.2.2.3 Úschova soukromých klíčů (dat pro vytváření elektronických značek, resp. elektronických podpisů)

Služba není poskytována.

7.2.2.4 Zálohování soukromých klíčů (dat pro vytváření elektronických značek resp. elektronických podpisů)

Kryptografický modul, použitý pro účely vydávání a spravování certifikátů relevantního TSS, umožňuje zálohování dat pro vytváření elektronických značek, resp. elektronických podpisů. Konkrétní technický postup je popsán v interní dokumentaci I.CA.

7.2.2.5 Uchovávání soukromých klíčů

Po uplynutí doby platnosti dat určených k elektronickému označování, resp. elektronickému podepisování vydávaných kvalifikovaných časových razítek, jsou tato data včetně jejich záloh zničena. Uchovávání dat, určených k elektronickému označování, resp. elektronickému podepisování kvalifikovaných časových razítek, představuje bezpečnostní riziko, a proto je u I.CA zakázáno.

7.2.2.6 Transfer soukromých klíčů

Data pro vytváření elektronických značek, resp. elektronických podpisů, příslušná k datům pro ověřování elektronických značek, resp. elektronických podpisů jsou generována přímo v kryptografickém modulu relevantního TSS.

Vkládání dat pro vytváření elektronických značek, resp. elektronických podpisů do kryptografického modulu konkrétního TSS 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 TSS odpojen od počítačové sítě.

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

7.2.2.7 Uložení soukromých klíčů v kryptografickém modulu

Data pro vytváření elektronických značek, resp. elektronických podpisů, příslušná k datům pro ověřování elektronických značek, resp. elektronických podpisů, jsou v kryptografickém modulu relevantního TSS uložena v šifrovaném tvaru.

7.2.2.8 Postup při aktivaci soukromých klíčů

Aktivaci dat pro vytváření elektronických značek, resp. elektronických podpisů, vygenerovaných v kryptografického modulu relevantního TSS, provádí určení pracovníci I.CA prostřednictvím vlastní aktivace daného kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní směrnicí.

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

7.2.2.9 Postup při deaktivaci soukromých klíčů

Deaktivaci dat pro vytváření elektronických značek, resp. elektronických podpisů po jejich vložení do kryptografického modulu relevantního TSS provádí určení pracovníci I.CA prostřednictvím kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní směrnicí.

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

7.2.2.10 Postup při zničení soukromých klíčů (dat pro vytváření elektronických značek, resp. elektronických podpisů)

Data pro vytváření elektronických značek, resp. elektronických podpisů, sloužící k označování, resp. podepisování vydávaných kvalifikovaných časových razítek, jsou uložena v kryptografickém modulu relevantního TSS. 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 poskytovatele, sloužících k označování, resp. podepisování vydávaných kvalifikovaných 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 a sítě nebo jiný pověřený technicky proškolený pracovník I.CA

O průběhu ničení dat pro vytváření elektronických značek, resp. elektronických podpisů poskytovatele sloužících k označování vydávaných kvalifikovaných časových razítek je sepsán protokol.

7.2.3 Uchovávání veřejných klíčů

Data pro ověřování elektronických značek, resp. elektronických podpisů jsou nezbytná pro důvěryhodnost a ověřování platnosti vydaných kvalifikovaných časových razítek. Tato data jsou obsažena v certifikátech relevantních TSS. Oproti jim příslušných dat pro vytváření elektronických značek, resp. elektronických podpisů, je důležité tato data uchovávat pro případ následné kontroly pravosti vydaných kvalifikovaných časových razítek a proto je se všemi certifikáty TSS zacházeno způsobem, uvedeným v kapitolách 7.4.13.1 a 7.4.13.2.

7.2.4 Profil certifikátů

Profil certifikátů TSS obsahuje veškeré náležitosti ZoEP a jeho základní vlastnosti jsou uvedeny v tabulce 6.

Tabulka 6 – certifikát TSS

Atribut	Hodnota	Příklad
Version	verze 3	2
Serial Numer	jedinečné číslo vydaného certifikátu TSS	10100629
Signature • algorithm • parameters	 algoritmus pro tvorbu elektronické značky, resp. elektronického podpisu vydávaného certifikátu TSS volitelné parametry	 sha1withRSAEncryption
Issuer	označení vydavatele certifikátu Country (C) Organization (O) CommonName (CN)	 CZ První certifikační autorita, a.s. I.CA - Qualified root certificate
NotBefore	datum a UTC čas počátku platnosti certifikátu TSS	01/02/2006 00:00:00
NotAfter	datum a UTC čas konce platnosti certifikátu TSS	01/02/2011 00:00:00
Subject	označení držitele certifikátu TSS Country (C) Organization (O) Organization Unit (OU) CommonName (CN)	 CZ První certifikační autorita, a.s. Time Stamp Server X[3] Time Stamping Authority
SubjectPublicKeyInfo • algorithm • SubjectPublicKey	 identifikátor algoritmu veřejného klíče certifikátu TSS veřejný klíč držitele certifikátu	 rsaEncryption RSA (2048)
Signature algorithm • algorithm • parameters	 algoritmus pro tvorbu elektronické značky, resp. elektronického podpisu vydávaného certifikátu TSS volitelné parametry	 sha1withRSAEncryption
signatureValue	elektronická značka, resp. elektronický podpis vydaného certifikátu TSS	RSA (2048)

Každé vydané kvalifikované časové razítko zahrnuje identifikátor politiky, pod kterou bylo vydáno.

7.2.5 Aktivační data

7.2.5.1 Generování a instalace aktivačních dat

Aktivační data jsou vytvářena v průběhu procesu instalace, kdy jsou generována párová data relevantního TSS.

7.2.5.2 Ochrana aktivačních dat

Povinností pověřených pracovníků I.CA je chránit aktivační data.

[3] kde X je číslo TSS (tzn. 1,2,3,.....)

7.2.5.3 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.

7.2.6 Výměna párových dat

Procesy výměny dat pro ověřování dat elektronických značek, resp. elektronických podpisů v certifikátu relevantního TSS jsou popsány v interní dokumentaci I.CA

7.2.7 Ukončení životního cyklu párových dat

Platnost párových dat (s mohutností klíče 2048 bitů), určených k označování, resp. podepisování generovaných kvalifikovaných časových razítek, je stanovena na 5 let.

Platnost dat, určených k ověřování označených, resp. podepsaných kvalifikovaných časových razítek je dána platností vydaných certifikátů relevantních TSS. Po této době lze data pro ověřování elektronických značek, resp. elektronických podpisů použít bez záruky. 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 7.4.10.

Pro kontrolu vydaných kvalifikovaných časových razítek je každý expirovaný veřejný klíč relevantního TSS dále archivován po celou dobu činnosti TSA.

7.2.8 Zneplatnění a pozastavení platnosti certifikátu

7.2.8.1 Profil seznamu zneplatněných certifikátů

Tabulka 7 – Profil CRL

Položka	Obsah	Příklad
Version	Verze v2	1
Signature • algorithm • parameters	 algoritmus pro tvorbu elektronické značky, resp. elektronického podpisu vydávaného CRL volitelné parametry	 sha1withRSAEncryption
Issuer	označení vydavatele CRL Country (C) Organization (O) CommonName (CN)	 CZ První certifikační autorita, a.s. I.CA - Qualified root certificate
thisUpdate	datum a UTC čas vydání CRL	Nov 30 04:51:30 2005
nextUpdate	datum a předpokládaný UTC čas vydání následujícího CRL	Nov 30 16:51:30 2005
Signature algorithm • Algorithm • parameters	 algoritmus pro tvorbu elektronické značky, resp. elektronického podpisu vydávaného CRL volitelné parametry	 sha1withRSAEncryption

signatureValue	Eeektronická značka, resp. elektronický podpis vydaného CRL	RSA (2048)
CRL Number	Číslo CRL	456

Tabulka 8 – Rozšiřující položky CRL

Položka	Obsah	Příklad
revokedCertificates • userCertificate • revocationDate	jedinečné číslo vydaného certifikátu datum a UTC čas zneplatnění certifikátu	10100629 Jan 30 04:51:30 2005

7.2.8.2 Podmínky pro zneplatnění certifikátu

Certifikát relevantního TSS může být zneplatněn pouze na základě následujících okolností :

- nastanou-li skutečnosti uvedené v ZoEP
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek, resp. elektronických podpisů používaných k označování, resp. podepisování kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek, resp. elektronických podpisů tohoto TSS

Zneplatnění certifikátu relevantního TSS, provede I.CA na základě podnětu :

- subjektů oprávněných ze zákona
- ředitele I.CA

7.2.9 Služby související s ověřováním statutu certifikátu

7.2.9.1 Funkční charakteristiky

Služby související s ověřováním statutu certifikátu relevantního TSS jsou poskytovány formou zveřejňování informací :

- o veřejných certifikátech na adrese http://www.ica.cz/
- o zneplatněných certifikátech na adresách :
  - http://www.ica.cz/
  - http://qcrldp1.ica.cz/qica05.crl
  - http://qcrldp2.ica.cz/qica05.crl
  - http://qcrldp3.ica.cz/qica05.crl

Podrobné informace jsou uvedeny v kapitole 7.4.13.3.2.

7.2.9.2 Dostupnost služeb

I.CA zajišťuje nepřetržitou dostupnost služeb, uvedených v kapitole 7.2.9.1. Postup je uveden v interních dokumentech I.CA. Případná omezení jsou uvedena v písemné smlouvě (viz kapitola 4.3).

7.2.9.3 Další charakteristiky služeb statutu certifikátu

Další služby, kromě těch, které jsou uvedené v kapitole 7.2.9.1, nejsou poskytovány.

7.2.10 Správa kryptografického modulu používaného při vytváření kvalifikovaných časových razítek

Hardware relevantního TSS, který je připojen do infrastruktury důvěryhodného synchronizačního času, obsahuje hardware HSM (FIPS 140-2 level 3) je výrobcem doručen (s využitím důvěryhodných přepravců) do sídla společnosti První certifikační autorita, a.s. V procesu příjmu zásilky jsou kontrolovány správnost a neporušenost pečetí obalu zásilky od výrobce. Po převzetí zásilky je tato následně přemístěna na provozní pracoviště, na kterém je provedena další kontrola pečetí obalu zásilky, včetně pečetí samotného hardware. TSS je uložen na bezpečném místě s řízeným přístupem a je provedena základní instalace včetně testů, synchronizace a kontroly. Každá výše uvedená činnost je písemně zaznamenávána. Instalace, inicializace, kontrola a synchronizace TSS jsou prováděny osobami v důvěryhodných rolích a v přítomnosti svědků. V případu předání hardware TSS do servisu, ukončení poskytování kvalifikovaných certifikačních služeb v oblasti kvalifikovaných časových razítek nebo ukončení činnosti I.CA, jsou data pro vytváření elektronických značek, resp. elektronických podpisů generovaných kvalifikovaných časových razítek zničena dle doporučení výrobce. Konkrétní postupy správy TSS jsou popsány v interní dokumentaci I.CA.

7.2.10.1 Hodnocení kryptografického modulu

Kryptografický modul pro označování generovaných kvalifikovaných časových razítek, je uveden v seznamu nástrojů, u nichž byla příslušným úřadem vyslovena shoda, neboť odpovídá požadavkům na kryptografické moduly dle dokumentu „Standard pro hodnocení bezpečnosti kryptografických modulů vydaný NIST v USA – FIPS PUB 140-2 úroveň 3“.

7.3 Vydávání kvalifikovaných časových razítek

7.3.1 Žádost o kvalifikované časové razítko

7.3.1.1 Subjekty oprávněné podat žádost o kvalifikované časové razítko

Vydávání kvalifikovaných časových razítek je I.CA komerčně nabízenou službou fyzické osobě, právnické osobě nebo organizační složce státu, která se smluvně (viz kapitola 4.3) zaváže jednat podle této politiky.

Pro žadatele, který podepisuje s I.CA smlouvu (viz kapitola 4.3) je požadován minimální věk 15 let. Osoby od 15 do 18 let musí mít svého zákonného zástupce.

V případě fyzické osoby může být osobou, podepisující smlouvu (viz kapitola 4.3) pouze ta, která je způsobilá k právním úkonům dle příslušné právní normy. Pokud osoba, podepisující smlouvu (viz kapitola 4.3) nepožaduje služby přímo pro sebe, ale zastupuje jinou osobu, musí mít oprávnění tuto osobu zastupovat.

7.3.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Při registraci nového žadatele o službu poskytování kvalifikovaných časových razítek je dle předložených dokladů ověřena jeho identita a případně jeho oprávnění k zastupování. Při registraci nového žadatele se vyžaduje :

a) předložení platného osobního dokladu žadatele

b) způsobilost žadatele k právním úkonům

c) doklady, prokazující právo žadatele jednat za jinou fyzickou nebo právnickou osobu, organizační složku státu jako zástupce na základě plné moci s úředně ověřeným podpisem zastupovaného subjektu.

7.3.1.3 Počáteční ověření identity

7.3.1.3.1 Ověřování identity právnické osoby nebo organizační složky státu

V případě, kdy žadatel vystupuje jako zástupce právnické osoby nebo organizační složky státu, vyžaduje I.CA při uzavírání smlouvy (viz kapitola 4.3) o vydání jednoho nebo více kvalifikovaných časových razítek :

- originál nebo notářsky ověřenou kopii výpisu z obchodního rejstříku, živnostenského listu nebo jiného dokumentu, na jejichž základě byla právnická osoba nebo organizační složka státu vytvořena a které musí obsahovat úplné obchodní jméno, identifikační číslo (IČO), statutární orgán a sídlo
- doklad opravňující žadatele jednat jménem této právnické osoby nebo organizační složky státu – viz kapitola 7.3.1.2, odstavec c)

7.3.1.3.2 Ověřování fyzické osoby

V případě, kdy žadatel vystupuje jako fyzická osoba, vyžaduje I.CA při uzavírání smlouvy (viz kapitola 4.3) o vydání jednoho nebo více kvalifikovaných časových razítek :

- celé občanské jméno žadatele
- datum narození žadatele
- číslo předloženého osobního dokladu
- adresa trvalého bydliště žadatele

Pokud dojde během trvání smluvního vztahu k I.CA ke změnám ve výše uvedených vyžadovaných osobních údajích, je žadatel povinen tyto změny ohlásit I.CA. Žadatel se musí prokázat způsobem, uvedeným v kapitole 7.3.1.2.

7.3.2 Zpracování žádosti o kvalifikované časové razítko

7.3.2.1 Identifikace a autentizace

S ohledem na komerční bázi a nadstandardní služby v procesu vydávání kvalifikovaných časových razítek vytvoří žadatel bezpečné autentizované spojení s TSA (s využitím komerčních certifikátů vydaných I.CA). V případě neúspěšného spojení je transakce ukončena a klient vhodným způsobem informován.

7.3.2.2 Přijetí nebo zamítnutí žádosti o kvalifikované časové razítko

- Klientská aplikace vytvoří pro jakákoli elektronická data (zpráva, dokument, transakce, atd.) jejich otisk (hash), který je následně v uložen v žádosti na vytvoření kvalifikovaného časového razítka (v normovaném formátu dle RFC 3161). Takto vytvořená datová struktura je s využitím Internetu (jako přenosového média - protokol TCP/IP) předána TSA.

- V rámci TSA je žádost předána archivačnímu serveru a následně zaslána jednomu ze serverů TSS. Vzhledem ke skutečnosti, že je zasílán pouze otisk (hash), je obsah elektronických dat (zpráva, dokument, transakce, atd.) pro TSS naprosto neznámý (včetně identity klienta).

7.3.2.3 Doba zpracování žádosti o kvalifikované časové razítko

I.CA nestanovuje, není-li v písemné smlouvě (viz kapitola 4.3), pevný časový limit, ve kterém dojde ke zpracování žádosti o kvalifikované časové razítko, neboť se jedná časový sled následujících činností, z nichž některé záleží pouze na elektronickém přenosu žádosti k TSA. Časové údaje jsou uvedeny v následujícím seznamu :

- vytvoření žádosti o vydání kvalifikovaného časového razítka – řádově sekundy (záleží na typu aplikace)
- vygenerování kvalifikovaného časového razítka – řádově ms

7.3.3 Vydání kvalifikovaného časového razítka

7.3.3.1 Úkony TSA v průběhu vydávání kvalifikovaného časového razítka

V následujícím seznamu jsou v časovém sledu uvedeny činnosti TSA :

- relevantní TSS provede veškeré kontroly formální správnosti žádosti a následně vytvoří novou datovou strukturu v normovaném formátu dle RFC 3161, obsahující odpovídající chybový status
- v případě kladného výsledku kontrol žádosti je k otisku (hash), obsaženém v žádosti, přidán časový údaj, který je získán z měřidla důvěryhodného času, včetně informace o tomto měřidlu a takto vytvořená data jsou do výše nové datové struktury uložena
- nově vytvořená datová struktura je následně elektronicky označena, resp. elektronicky podepsána daty pro vytváření elektronické značky, resp. elektronického podpisu relevantního TSS - tím se tento server nezpochybnitelným způsobem zaručuje za správnost informací uvedených ve vygenerovaném kvalifikovaném časovém razítku
- tato datová struktura – odpověď na žádost o kvalifikované časové razítko, je odeslána archivačnímu serveru TSA

7.3.3.2 Oznámení o vydání kvalifikovaného časového razítka držiteli vydávání kvalifikovaného časového razítka

Poté, co jsou provedeny činnosti, uvedené v kapitole 7.3.3.1, odešle TSA odpověď klientovi.

7.3.4 Převzetí kvalifikovaného časového razítka

7.3.4.1 Klient

Po obdržení odpovědi na žádost o kvalifikované časové razítko je klient povinen zjistit status. V případě chyby není kvalifikované časové razítko v odpovědi obsaženo a klient by měl překontrolovat status a odpovídající chybovou hlášku. V opačném případě je klient povinen postupovat v souladu s kapitolou 6.2.

7.3.4.2 Spoléhající se strana

Ověřování kvalifikovaného časového razítka spoléhající se stranou probíhá v následujících krocích :

- vytvoření hodnoty otisk_1 (hash_1) z elektronických dat (zpráva, dokument, transakce, atd.), která bude porovnávána proti hodnotě otisk_2 (hash_2), obsažené v kvalifikovaném časovém razítku
- vybrání kvalifikovaného časového razítka, obsahující hodnotu otisk_2 (hash_2)
- porovnání hodnot otisk_1 (hash_1) a otisk_2 (hash_2)

V případě neshody byla elektronická data, odpovídající hodnotě hash_1 změněna**.** Dále je spoléhající se strana povinna postupovat v souladu s kapitolou 6.3

7.3.5 Ukončení poskytování služeb pro žadatele o kvalifikované časové razítko

Poskytovaná certifikační služba vydávání kvalifikovaných časových razítek (obchodní vztah) ukončuje I.CA ve chvíli, kdy nejsou dodrženy podmínky smlouvy (viz kapitola 4.3), uzavřené s klientem.

7.3.6 Token kvalifikovaného časového razítka

Kvalifikovaná časová razítka jsou generována relevantním TSS na základě zaslané žádosti.

7.3.6.1 Profil žádosti o kvalifikované časové razítko

Tab. 9 – Položky žádosti o kvalifikované časové razítko

Pole	Popis	Příklad
Version	Popisuje verzi požadavku na kvalifikované časové razítko.	1
HashAlgorithm	SHA-1	sha1withRSAEncryption
HashedMessage	Délka tohoto řetězce (Octect String) musí splňovat požadavky na délku zvoleného algoritmu (SHA-1)	
ReqPolicy	Identifikátor politiky	1.3.6.1.4.1. 23624.1.4.14.2
Nonce	Náhodné číslo, o kterém se předpokládá, že jej klient vygeneruje pouze jednou (64 bit integer). V případě, že toto číslo žádost obsahuje, pak toto číslo musí obsahovat i odpověď.	
CertReq	TRUE – odpověď musí obsahovat certifikát TSS FALSE, nebo není uvedeno - odpověď nesmí obsahovat certifikát TSS	TRUE/FALSE

7.3.6.2 Profil odpovědi na žádost o kvalifikované časové razítko

Tab. 10 - Položky odpovědi o kvalifikované časové razítko

Položka	Popis	Příklad
PKIStatus	Číslo Integer, značící : • granted • grantedWithMods • rejection • waiting • revocationWarning • revocationNotification	 0 1 2 3 4 5
PKIFailureInfo ::= BIT STRING {	BIT STRING značící : • BadAlg - unrecognized or unsupported Algorithm Identifier • BadRequest - transaction not permitted or supported • BadDataFormat - the data	 0 2 5

	submitted has the wrong format • TimeNotAvailable - the TSA's time source is not available • UnacceptedPolicy - the requested TSA policy is not supported by the TSA • UnacceptedExtension - the requested extension is not supported by the TSA • AddInfoNotAvailable - the additional information requested could not be understood or is not available • SystemFailure - the request cannot be handled due to system failure }	14 15 16 17 25

Token kvalifikovaného časového razítka nesmí obsahovat jinou elektronickou značku, resp. elektronický podpis, než elektronickou značku, resp. elektronický podpis relevantního TSS.

Tab. 11 - Položky tokenu časového razítka

Položka	Popis	Příklad
version	verze požadavku na kvalifikované časové razítko.	1
Policy	Identifikátor politiky	1.3.6.1.4.1. 23624.1.4.14.2
messageImprint	hash, pro který se žádá o kvalifikované časové razítko	musí mít stejnou hodnotu jako v TimeStampReq
serialNumber	Integer číslo - Time-Stamping users MUST be ready to accommodate integers up to 160 bits.	1234567890
Gentime	GeneralizedTime – hodnota UTC	2005/12/02 10.24:17:46
Accuracy	Přesnost – volitelně	
Nonce	Náhodné číslo – volitelně - o kterém se předpokládá, že jej klient vygeneruje pouze jednou (64 bit integer). V případě, že toto číslo žádost obsahuje, pak toto číslo musí obsahovat i odpověď.	
Tsa	GeneralName – volitelně	

Tokeny kvalifikovaných časových razítek, které relevantní TSS generuje, obsahují jednoznačný identifikátor politiky, popsaný v kapitole 2.1, otisk (hash) datové zprávy, na kterou je proces vydání kvalifikovaného časového razítka realizován, datum a časovou hodnotu (odpovídající reálné hodnotě UTC) a jedinečné sériové číslo.

Přesnost časového údaje, vkládaného do vydávaného generovaného časového razítka je definovaná v kapitole 6.1.2. Struktura kvalifikovaného časového razítka (ve standardu RFC 3161) je označena, resp. podepsána soukromým klíčem relevantního TSS, jehož certifikát obsahuje údaje, popsané v kapitole 7.2.4 a identifikátor jednoznačně spojený se společností První certifikační autorita, a.s.

7.3.7 Synchronizace měřidla času s UTC

7.3.7.1 Synchronizace

Synchronizace měřidla času s důvěryhodným synchronizačním zdrojem UTC je prováděna jednou denně. Pro synchronizaci a kontrolu časového údaje, vkládaného do generovaných kvalifikovaných časových razítek, je využíváno již v EU provozované komerční řešení, založené na modelu důvěryhodné synchronizační časové infrastruktury (TTI). Tato bezpečná a nevyvratitelná synchronizační časová služba měřidla času, poskytuje platné a kontrolovatelné informace pro případ sporů mezi poskytovatelem kvalifikovaných časových razítek a klienty nebo spoléhajícími se stranami. Problematika synchronizace je řešena interní dokumentací.

7.3.7.2 Bezpečnost měřidla času

Problematika bezpečnosti měřidla času je řešena interní dokumentací I.CA.

7.3.7.3 Detekce odchýlení měřidla času

Problematika detekce odchýlení měřidla času je řešena interní dokumentací I.CA.

7.3.7.4 Přestupná sekunda

Problematika výskytu přestupné vteřiny měřidla času je řešena interní dokumentací interní dokumentací I.CA.

7.4 Správa a provozní bezpečnost TSA

7.4.1 Řízení bezpečnosti

Popis struktury řízení bezpečnosti ve společnosti První certifikační autorita, a.s. je uveden v interní dokumentaci I.CA..

7.4.2 Hodnocení a řízení rizik

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

7.4.3 Hodnocení zranitelnosti

Viz kapitola 7.4.2

7.4.4 Postup při oznamování události subjektu, který ji způsobil

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

7.4.5 Personální bezpečnost

Problematika personální bezpečnosti (kapitoly 7.4.5.1 až 7.4.5.12) je detailně řešena v interní dokumentaci .

7.4.5.1 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, jejichž popis je uveden v interní dokumentaci společnosti. Základní činnosti a odpovědnosti osob v důvěryhodných rolí je definován v interní dokumentaci.

7.4.5.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro níže uvedené činnosti je nezbytná přítomnost nejméně tří pracovníků I.CA :

- generování párových dat každého TSS
- ničení dat pro vytváření elektronické značky, resp. elektronického podpisu vydávaných kvalifikovaných časových razítek

Pro níže uvedené činnosti je nezbytná přítomnost nejméně dvou pracovníků I.CA :

- zálohování/obnova dat pro vytváření elektronické značky, resp. elektronického podpisu každého TSS
- aktivace každého TSS
- fyzická kontrola chodu každého TSS

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

7.4.5.3 Identifikace a autentizace pro každou roli

Pracovníkům jsou přiděleny prostředky pro řádnou autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné - upraveno interními směrnicemi I.CA.

7.4.5.4 Role vyžadující rozdělení povinností

V procesu poskytování certifikačních služeb v oblasti kvalifikovaných časových razítek je 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).

7.4.5.5 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 kritérií :

- 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

7.4.5.6 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.

7.4.5.7 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.

7.4.5.8 Požadavky a periodicita školení

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

7.4.5.9 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.

7.4.5.10 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).

7.4.5.11 Požadavky na nezávislé zhotovitele

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.

7.4.5.12 Dokumentace poskytovaná zaměstnancům

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

7.4.6 Fyzická bezpečnost a bezpečnost prostředí

Problematika fyzické bezpečnosti a bezpečnosti prostředí (kapitoly 7.4.6.1až 7.4.6.8) je detailně řešena v interní dokumentaci .

7.4.6.1 Umístění a konstrukce

Zařízení, určená k výkonu hlavních kvalifikovaných certifikačních služeb, jsou umístěna v suterénu objektu, který stojí osamoceně. Zabezpečená oblast má cihlové stěny o nejmenší tloušťce 300 mm. Vstupní dveře mají průnikovou odolnost a zámkové systémy certifikované NBÚ ČR na kategorii „Tajné“.

7.4.6.2 Fyzický přístup

Objekt je obehnán bezpečnostním plotem a je nepřetržitě střežen fyzickou ostrahou a speciálním televizním systémem pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků. Přístup do vlastního objektu je kontrolován fyzickou ostrahou.

7.4.6.3 Elektřina a klimatizace

V místnosti je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20 °C ± 5 °C. Přívod elektrické energie je jištěn pomocí UPS, resp. diesel agregátu.

7.4.6.4 Vliv vody

Objekt se nachází v lokalitě, která je postižitelná zátopovou vodou. Všechny kritické systémy jsou proto umístěny v dostatečné výši, aby nebyly zaplaveny ani stoletou vodou.

7.4.6.5 Protipožární opatření a ochrana

Vstupní pancéřové dveře jsou opatřeny protipožární vložkou. V místnosti se nachází hasící přístroj a zařízení elektrické požární signalizace.

7.4.6.6 Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v kovových skříních, popř. trezoru ředitele I.CA.

Papírová média, která je nutno dle platné legislativy archivovat, jsou skladována v jiné geografické lokalitě než je umístěno provozní pracoviště.

7.4.6.7 Nakládání s odpady

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

7.4.6.8 Zálohy mimo budovu provozního pracoviště

Kopie provozních a pracovních záloh jsou uloženy na místě určeném ředitelem I.CA.

7.4.7 Provozní řízení

7.4.7.1 Specifické technické požadavky na počítačovou bezpečnost

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

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

7.4.7.2 Hodnocení počítačové bezpečnosti

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

- ČSN ETSI TS 102 023 – Elektronické podpisy a infrastruktury; Požadavky na postupy autorit časových razítek.
- 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.
- ETSI TS 101 456 - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
- ČSN ISO/IEC 17799 - Informační technologie – Soubor postupů pro management bezpečnosti informací.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky
- ČSN ISO/IEC TR 13335 - Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3
- ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému

7.4.8 Řízení přístupu do systému

Řízení přístup do TSA kmenovými pracovníky I.CA je definován interní dokumentací.

7.4.9 Vývoj a údržba důvěryhodných systémů

7.4.9.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

7.4.9.2 Kontroly řízení bezpečnosti

Soulad se standardy (viz kapitola 7.4.7.2), ZoEP a VoEP je ověřován pravidelnými audity systému řízení bezpečnosti informací, prováděnými pracovníky nezávislých auditorských firem a kontrolami bezpečnostní shody, prováděnými pracovníky I.CA. Tato problematika je popsána v interní dokumentaci.

7.4.9.3 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.

7.4.10 Obnova po havárii nebo kompromitaci

7.4.10.1 Postup v případě incidentu a kompromitace

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

.

7.4.10.2 Poškození výpočetních prostředků, software nebo dat

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

7.4.10.3 Postup při zjištění odchýlení měřidla času

Postup synchronizace časového údaje měřidla času je uveden v kapitole 7.3.7.1. Pokud je zjištěná odchylka od UTC mimo specifikovaný interval, definovaný při inicializaci TSS, je činnost TSS okamžitě ukončena a do provedení nové inicializace není služba vydávání kvalifikovaných časových razítek poskytována. Problematika je řešena interní dokumentací I.CA.

7.4.10.4 Postup při kompromitaci soukromého klíče TSA

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 certifikát relevantního TSS
- bezodkladně :
    - o této skutečnosti, včetně důvodu informuje :
        - na své internetové informační adrese
        - v jednom celostátně distribuovaném deníku – viz kapitola 7.4.13.3.2
    - 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 relevantního 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 relevantního TSS
- oznámí příslušnému úřadu informaci o zneplatnění vlastního certifikátu TSS s uvedením důvodu zneplatnění

- vydá nový certifikát relevantnímu TSS - postup je stejný jako při vydání prvotního certifikátu tohoto TSS

7.4.10.5 Schopnosti obnovit činnost po havárii

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

7.4.11 Ukončení činnosti TSA

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 s ohledem na skutečnost, že je aktreditovaným poskytovatelem certifikačních služeb (viz kapitola 2) provedení následujících činností dle příslušných legislativ :

- v případě 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 časových razítek, v případě, že se jí nepodařilo tuto evidenci předat jinému kvalifikovanému poskytovateli certifikačních služeb v oblasti vydávání časových razítek, 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 časových razítek, pokud toto bude známo nejméně 2 měsíce před plánovaným ukončením činnosti
    - zpřístupnění informaci o ukončení činnosti I.CA v oblasti vydávání kvalifikovaných časových razítek na své internetové informační adrese nejméně 2 měsíce před plánovaným ukončením činnosti
    - ukončí kvalifikované poskytování certifikačních služeb v oblasti vydávání časových razítek
    - prokazatelné zničí svá data pro vytváření elektronických značek, sloužící k označování vydávaných kvalifikovaných časových razítek

- v případě Slovenské republiky :
    - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek nejméně 6 měsíců před plánovaným ukončením činnosti
    - ohlásí každému držiteli platné smlouvy (viz kapitola 4.3) o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek nejméně 6 měsíců před plánovaným ukončením činnosti
    - může se dohodnout s jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání časových razítek o převzetí záznamů o časových razítkách a provozní dokumentaci – pokud žádný kvalifikovaný poskytovatel certifikačních služeb v oblasti vydávání časových razítek tyto záznamy nepřevezme, převezme tyto záznamy úřad

Problematika plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání časových razítek je detailně uvedena v interní dokumentaci I.CA.

7.4.12 Shoda s právními předpisy

TSA je provozován v souladu s platnou legislativou, zejména ZoEP a VoEP.

7.4.13 Úložiště informací a dokumentace, které se týkají provozu TSA

7.4.13.1 Auditní záznamy (logy)

Zásady vytváření, zpracování a uchovávání auditních logů jsou uvedeny v základních dokumentech :

- ***„Systémová bezpečnostní politika TSA“***
- ***„Prováděcí směrnice vydávání kvalifikovaných časových razítek“***
- ***„Zpráva a souhlas vedení I.CA o hodnocení rizik TSA“***
- ***„Prohlášení o aplikovatelnosti (SoA)“***

a detailně popsány v upřesňujících interních bezpečnostních normách a směrnicích, zahrnujících problematiku, uvedenou v podkapitolách 7.4.13.1.1 až 7.4.13.1.6.

7.4.13.1.1 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 102 023 - Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities
- platnou legislativou

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.

7.4.13.1.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány jednou týdně, v případě bezpečnostního incidentu okamžitě.

7.4.13.1.3 Doba uchovávání auditních záznamů

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

7.4.13.1.4 Ochrana auditních záznamů

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 auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

7.4.13.1.5 Postupy pro zálohování auditních záznamů

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

7.4.13.1.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

7.4.13.2 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, zákon Slovenskej národnej rady č. 149/1975 Zb. o archívnictve v znení neskorších predpisov).

Zásady uchovávání informací a dokumentace jsou uvedeny v základních dokumentech :

- ***„Celková bezpečnostní politika“***
- ***„Systémová bezpečnostní politika TSA“***
- ***„Prováděcí směrnice vydávání kvalifikovaných časových razítek“***
- ***„Zpráva a souhlas vedení I.CA o hodnocení rizik TSA“***
- ***„Prohlášení o aplikovatelnosti (SoA)“***

a detailně popsány v upřesňující interní bezpečnostní dokumentaci, zahrnující problematiku, uvedenou v podkapitolách 7.4.13.2.1 až 7.4.13.2.7.

7.4.13.2.1 Typy informací a dokumentace, které se uchovávají

I.CA uchovává následující typy informací a dokumentace, které související s poskytovanými kvalifikovanými certifikačními v oblasti kvalifikovaných časových razítek :

- elektronické nebo písemné informace dle platné legislativy
- události požadované standardy :
  - CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
  - ETSI TS 102 023 - Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities
- aplikační programové vybavení
- veškerou dokumentaci společnosti, která je nutná pro provádění auditů systému řízení bezpečnosti informací a kontrol bezpečnostní shody :
- veškeré seznamy zneplatněných certifikátů
- identifikační údaje osoby, která provedla ověření totožnosti žadatele
- obchodní název poskytovatele, který žádost o poskytování kvalifikované certifikační služby v oblasti vydávání kvalifikovaných časových razítek přijal, nebo smluvního partnera, který pro poskytovatele tuto činnost zajišťuje,
- záznam o manipulaci (tj. např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atp.) s informacemi
- identifikace místa, kde jsou uloženy informace a dokumentace, jejichž uchování je vyžadováno ZoEP
- provozní a bezpečnostní dokumentaci

7.4.13.2.2 Doba uchovávání uchovávaných informací a dokumentace

I.CA zajišťuje uchovávání informací a dokumentace, uvedených v kapitole 7.4.13.2.1 po dobu nejméně 10 let od jejich vzniku.

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

7.4.13.2.3 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. a SR č. 428/2002 Z.z. 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.

7.4.13.2.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace (viz kapitola 7.4.13.2.1) jsou upraveny interní dokumentací I.CA.

7.4.13.2.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

7.4.13.2.6 Systém shromažďování uchovávaných informací a dokumentace (interní, externí)

Problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směrnicemi (viz kapitola 7.4.13.2.4). Shromažďování archivních záznamů je evidováno.

7.4.13.2.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

7.4.13.3 Odpovědnosti za zveřejňování, úložiště informací a dokumentace

Problematika spojená s odpovědnostmi za zveřejňování, úložiště informací a dokumentace (kapitoly 7.4.13.3.1 až 7.4.13.3.2) je detailně řešena v interní dokumentaci.

7.4.13.3.1 Úložiště informací a dokumentace

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

7.4.13.3.2 Zveřejňování informací a dokumentace

Základní adresy, na nichž lze nalézt informace o veřejných informacích I.CA, politiky, Zprávy pro uživatele a další informace dle ZoEP, ostatní veřejné dokumentace, atd., (dále též informační adresy), případně odkazy pro zjištění dalších informací, jsou :

a) První certifikační autorita, a.s.;

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

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

c) sídla registračních autorit.

Kontaktní adresa, které slouží v oblasti poskytování kvalifikovaných certifikačních služeb v oblasti kvalifikovaných časových razítek pro kontakt klienta popř. veřejnosti s I.CA (dále též kontaktní adresa), jsou :

a) elektronická poštovní adresa tsa@ica.cz (na tuto elektronickou adresu lze zasílat i případné dotazy, připomínky, nebo návrhy na zlepšení poskytované služby)

Výše uvedené informační a kontaktní adresy je I.CA povinna zveřejnit na internetové informační adrese. Určení pracovníci I.CA jsou rovněž povinni tyto informace na vyžádání sdělit všem potencionálním uživatelům. Totéž platí i v případě, že dojde ke změně kontaktních adres.

Možnost získání certifikátu poskytovatele je garantována nejméně dvěma nezávislými kanály :

- prostřednictvím internetových informačních adres I.CA a příslušného úřadu
- prostřednictvím Věstníku příslušného úřadu

Informace o CRL lze získat na adrese http://www.ica.cz/. 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)

Povoleným protokolem pro přístup k informacím o :

- konkrétních certifikačních politikách, zprávách pro uživatele - HTTP
- vydaných veřejných certifikátech - HTTP, HTTPS, FTP
- seznamech zneplatněných certifikátů - HTTP, HTTPS, FTP,

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

7.4.13.3.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou :

- tento dokument - před prvním poskytnutím služby vydávání kvalifikovaných časových razítek
- zpráva pro uživatele – při zahájení poskytované certifikační služby v oblasti vydávání certifikátů, popř. při její změně
- získání nebo odejmutí akreditace dle ZoEP – okamžitě

- informace o zneplatnění certifikátů poskytovatele 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) a kvalifikovaných časových razítek – bezodkladně
- aktualizace seznamu vydaných certifikátů – okamžitě při každém vydání nového certifikátu
- vydávání seznamu zneplatněných certifikátů - tato povinnost je realizována periodickým vydáváním CRL minimálně jedenkrát za 24 hodin (zpravidla po 8 hodinách). Vydávání CRL je nepřetržité – 7 dní v týdnu. Internetové adresy, na kterých lze získat CRL dálkovým přístupem, jsou uvedeny na internetové informační adrese I.CA a jsou rovněž uvedeny v každém certifikátu. I.CA zveřejňuje seznamy zneplatněných certifikátů nejméně dvěma na sobě nezávislými způsoby dálkového přístupu.
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí odrážet aktuální stav poskytovaných kvalifikovaných certifikačních služeb

7.4.13.3.4 Řízení přístupu k jednotlivým typům úložišť

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

7.5 Ostatní obchodní a právní záležitosti

7.5.1 Poplatky

7.5.1.1 Poplatky za vydávání kvalifikovaných časových razítek

Informace o poplatcích za vydávaná kvalifikovaná časová je možno získat na adrese tsa@ica.cz.

7.5.1.2 Poplatky za přístup k certifikátům poskytovatele

Přístup k certifikátům poskytovatele elektronickou cestou I.CA nezpoplatňuje.

7.5.1.3 Poplatky za informace o statutu certifikátu a o zneplatnění

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

7.5.1.4 Poplatky za další služby

Poplatek za předání certifikátu (prvotní, následný) prostřednictvím záznamového média (např. disketa) je uveden v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA.

Zneplatnění certifikátu a stažení elektronických verzí politik (ve formátu PDF) je poskytováno zdarma.

Poplatky za nadstandardní služby jsou stanovovány smluvně.

7.5.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

I.CA si vyhrazuje právo změny výše poplatku za vydání kvalifikovaného časového razítka. I.CA je rovněž oprávněna stanovit pro individuálně uzavřené smlouvy (viz kapitola 4.3) odlišnou výši těchto poplatků.

7.5.2 Finanční odpovědnost

7.5.2.1 Krytí pojištění

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

7.5.2.2 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.

7.5.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Služba není poskytována.

7.5.3 Citlivost obchodních informací

7.5.3.1 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 poskytovatele
- data pro vytváření elektronických značek, resp. elektronických podpisů příslušná k datům pro ověřování elektronických značek, resp. elektronických podpisů :
    - vyhrazená pro infrastrukturu synchronizačního důvěryhodného času, využívaná v procesech synchronizace a kontroly měřidla času TSS
    - využívaná v procesu správy systému TSA.
- 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 ve vlastních nebo účelových certifikátech RA
- ostatní kryptograficky podstatné informace sloužící k provozu RA
- veškeré informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb dle ZoEP
- veškeré osobní údaje

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.

7.5.3.2 Informace mimo rámec citlivých informací

Za veřejné se považují typy informací, které nepatří do žádné z uvedených skupin v kapitole 7.5.3.1.

7.5.3.3 Odpovědnost za ochranu citlivých informací

Každý pracovník, který přijde do styku s informacemi uvedenými v kapitole 7.5.3.1, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

7.5.4 Ochrana osobních údajů

Problematika ochrany osobních údajů (kapitoly 7.5.4.1 až 7.5.4.7) je řešena interní dokumentací I.CA..

7.5.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem (zákon ČR č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, zákon ČR č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, zákona SR č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, zákona SR č. 428/2002 Z. z. o ochrane osobných údajov vrátane Zákona č. 90/2005 Z. z.).

7.5.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje klientů, uživatelů či pracovníků, podléhající ochraně ve smyslu příslušné zákonné normy (zákony ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálních zněních).

7.5.4.3 Údaje, které nejsou považovány za osobní

Informace, které nejsou považovány za důvěrné jsou obecně údaje, uvedené ve vydávaném certifikátu, pokud k jeho zveřejnění dal žadatel o certifikát souhlas, údaje, které jsou veřejně známými, atd.

7.5.4.4 Odpovědnost za ochranu osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákonů ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálních zněních.

7.5.4.5 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 zákonů ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálních zněních.

7.5.4.6 Poskytování citlivých informací pro soudní či správní účely

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákonů ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálních zněních.

7.5.4.7 Jiné náležitosti zpřístupňování osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky zákonů ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálních zněních.

7.5.5 Práva duševního vlastnictví

Tato politika, veškeré související dokumenty, obsah webových stránek, data pro vytváření elektronických značek, resp. elektronických podpisů příslušná k datům pro ověřování elektronických značek, resp. elektronických podpisů obsažených v certifikátech poskytovatele a procedury, zajišťující provoz systému, poskytujícího kvalifikované certifikační služby v oblasti certifikátů a kvalifikovaných časových razítek, jsou chráněny autorskými právy společnosti První certifikační autorita, a.s. a představují její významné know-how.

7.5.6 Zastupování a záruky

7.5.6.1 Zastupování a záruky I.CA

S ohledem na poskytované certifikační služby v oblasti vydávání kvalifikovaných časových razítek I.CA zaručuje splnění všech závazků, uvedených v kapitole 6.1. Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud :

- klient neporušil povinnosti plynoucí mu ze smlouvy (viz kapitola 4.3) o poskytování kvalifikované certifikační služby a této politiky
- spoléhající se strana neporušila povinnosti této politiky

Klient uplatňuje záruku vždy tam, kde podepisoval smlouvu (viz kapitola 4.3). Na používání kvalifikovaného časového razítka, který I.CA nevydala, se záruky nevztahují.

7.5.6.2 Zastupování a záruky držitelů a klientů kvalifikovaných časových razítek

Držitel nebo klient kvalifikovaného časového razítka ručí za informace, jím uvedené ve smlouvě (viz kapitola 4.3) o poskytování kvalifikovaných časových razítek a postupují v souladu s platnou legislativou a touto politikou.

7.5.6.3 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s platnou legislativou a touto politikou.

7.5.6.4 Zastupování a záruky ostatních participujících subjektů

Služba není poskytována

7.5.7 Zřeknutí se záruk

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

7.5.8 Odpovědnost za škodu, náhrada škody

Platí vždy limit záruky, který byl sjednán v písemné podobě (viz kapitola 4.3). Pokud byla výše nárokované ztráty vyšší než sjednaný limit, poskytne I.CA plnění maximálně do výše limitu. Pokud bylo zjištěno porušení povinností klienta mající souvislost s uváděnou škodou, záruční plnění se neposkytne. S touto skutečností bude klient seznámen. Tato skutečnost musí být klientovi oznámena a zaprotokolována.

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

Společnost První certifikační autorita, a.s. :

- se zavazuje, že splní veškeré povinnosti definovanými jak příslušnými právními předpisy, tak politikami, reflektující problematiku vydávání kvalifikovaných časových razítek
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy (viz kapitola 4.3) o poskytování certifikačních služeb uzavřené se zákazníkem
- jiné záruky, než výše uvedené, neposkytuje

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

- Za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb, poskytnutých v rámci plnění smlouvy (viz kapitola 4.3) o poskytování certifikačních služeb držitelem, zejména za provozování v rozporu s podmínkami uvedenými v politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.

Oprávněnou reklamaci je možné podat těmito způsoby :

- e-mailem na adresu : reklamace@ica.cz
- doporučenou poštovní zásilkou na adresu :

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

Reklamující osoba je povinna uvést :

- číslo smlouvy (viz kapitola 4.3)
- 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.

7.5.9 Doba platnosti, ukončení platnosti

7.5.9.1 Doba platnosti

Tato politika je platná pro každé kvalifikované časové razítko, vydané v souladu s tímto dokumentem.

7.5.9.2 Ukončení

Jedinou osobou, která je oprávněna schvalovat úpravy této politiky a určuje její shodu s odpovídající prováděcí směrnicí, je ředitel společnosti První certifikační autorita, a.s.

7.5.9.3 Důsledky ukončení a přetrvání závazků

Kvalifikovaná časová razítka vydaná v souladu s tímto dokumentem zůstávají platná i po případném ukončení poskytování kvalifikovaných certifikačních služeb společnosti První certifikační autorita, a.s.

7.5.10 Komunikace mezi participujícími subjekty

Pro individuální oznámení a komunikaci s klienty a držiteli kvalifikovaných časových razítek může I.CA využít jimi dodané e-mailové adresy, poštovní adresy, telefonická čísla nebo osobní jednání.

Klienti, držitelé kvalifikovaných časových razítek, žadatelé o kvalifikovaná časová razítka, spoléhající se strany a veřejnost mohou s I.CA komunikovat způsobem, uvedeným na adrese http://www.ica.cz/.

7.5.11 Změny

7.5.11.1 Postup při změnách

Postup je realizován řízeným procesem, uvedeném v interním dokumentu I.CA.

7.5.11.2 Postup při oznamování změn

Postup je realizován řízeným procesem, uvedeném v interním dokumentu I.CA.

7.5.11.3 Okolnosti, při kterých musí být změněno OID

Postup je realizován řízeným procesem, uvedeném v interním dokumentu I.CA.

7.5.12 Opatření při řešení sporů

Tato politika a odpovídající prováděcí směrnice a jejich výklad a aplikace se řídí platnou legislativou.

V případě, že klient, držitel kvalifikovaných časových razítek, spoléhající se strana, žadatel nebo smluvní partner nesouhlasí s předloženým výkladem, mohou použít následující stupně odvolání :

- 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.

7.5.13 Relevantní právní úprava

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

7.5.14 Shoda s právními předpisy

Systém poskytování certifikačních služeb v oblasti vydávání kvalifikovaných časových razítek je provozován ve shodě s požadavky ZoEP.

7.5.15 Další ustanovení

7.5.15.1 Rámcová shoda

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

7.5.15.2 Postoupení práv

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

7.5.15.3 Oddělitelnost

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

7.5.15.4 Platby obhájcům a zřeknutí se práv

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

7.5.15.5 Vyšší moc

Smlouva (viz kapitola 4.3) o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání kvalifikovaných časových razítek může obsahovat ustanovení o působení vyšší moci.

7.5.16 Další opatření

Tyto skutečnosti jsou pro aplikaci vydání tohoto dokumentu irelevantní.

8 Závěrečná ustanovení

Tento dokument, vydaný společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 01.11.2007.