První certifikační autorita, a.s.
(akreditovaný poskytovatel certifikačních služeb)

POLITIKA VYDÁVÁNÍ KVALIFIKOVANÝCH ČASOVÝCH RAZÍTEK

Stupeň důvěrnosti: veřejný dokument

Verze 3.0

Tabulka 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Pozn.
3.0	23. 12. 2009	Ředitel společnosti První certifikační autorita, a.s.	Vydávání certifikátů s parametry, splňujícími požadavky platné legislativy na problematiku hashovacích funkcí (využívání algoritmů rodiny SHA-2) a minimální přípustné délky kryptografického klíče pro algoritmus RSA (2048 bitů). Akceptace požadavků, vyplývajících se sdělení Ministerstva vnitra České republiky k algoritmům používaným v oblasti časových razítek.

Obsah

1 Úvod

Tento dokument byl vypracován na základě požadavků platné legislativy (odkazující se na doporučení technické specifikace ETSI[1] TS 102 176-1), vztahující k problematice využívání kryptografických algoritmů v procesu vytváření elektronického podpisu a algoritmů, využívaných k vytvoření otisku dat při vytváření žádosti o časové razítko.

Dokument **Politika vydávání kvalifikovaných časových razítek,** vypracovaný společností První certifikační autorita, a. s. se zabývá skutečnostmi vztahující k procesům vydávání a využívání kvalifikovaných časových razítek, 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
- s vyhláškou 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)
- s aktuálním zněním zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a s ním spojených vykonávacích vyhlášok
- s doporučeními ETSI TS 102 023 (Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities) , RFC 3647 (Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework) a ETSI TS 101861 (Time Stamping Profile) 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 společností První certifikační autorita, a. s., splňují Vaše požadavky.

[1] European Telecommunications Standards Institute

2 Přehled

Tento dokument může být mimo jiné využit nezávislými institucemi 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 procesů autority časových razítek je uveden v dalších dokumentech, které jsou obecně neveřejné. Neveřejné dokumenty, včetně zpráv, výsledků testů a interních kontrol tvoří dokumentační sadu, dosažitelnou výhradně autorizovanému personálu a auditorům. V tabulce 2 jsou uvedeny významné bezpečnostní dokumenty, vztahující se k certifikačním službám v oblasti kvalifikovaných časových razítek.

Tabulka 2 – Bezpečnostní dokumentace

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.	Prohlášení o aplikovatelnosti	Neveřejný
5.	Systémová bezpečnostní politika TSA	Neveřejný
6.	Plán pro zvládání krizových situací a plán obnovy	Neveřejný
7.	Zpráva pro uživatele TSA	Veřejný
8.	Sada bezpečnostních norem a směrnic	Neveřejný
9.	Celková bezpečnostní politika	Neveřejný
10.	Prohlášení o aplikovatelnosti	Neveřejný
11.	Certifikační politika nadřízených kvalifikovaných systémových certifikátů I.CA	Neveřejný

Dokument Politika vydávání kvalifikovaných časových razítek je vypracován na obecné úrovni. Technické detaily datového komunikačního systému, struktury společnosti, operačních procedur nebo technické ochrany jsou uvedeny v relevantních interních dokumentech.

Vydávání a správa kořenových certifikátů a certifikátů serverů TSU se řídí interními dokumenty, jejichž správa je ve společnosti První certifikační autorita, a.s. řízena speciálními dokumenty.

V procesu poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek provozuje společnost První certifikační autorita, a.s jedinou autoritu časových razítek, jejímž jádrem je sada kvalitativně totožných TSU.

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. 23624.1.1.50.3.0

3 Přehled použitých pojmů a zkratek

Dále uvedený přehled pojmů a zkratky je platný pro tento dokument. 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 3 – Pojmy

Pojem	Vysvětlení
elektronický podpis, zaručený elektronický podpis, resp. elektronická značka	údaje, resp. informace, které splňují požadavky platné legislativy[2]
kvalifikovaný certifikát, kvalifikovaný systémový certifikát	certifikát, který má náležitosti podle platné legislativy
Hash (otisk, fingerprint, …)	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou
Klient	žadatel o časové razítko a/nebo spoléhající se strana
Kvalifikované časové razítko, resp. 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, kvalifikovaný systémový certifikát, nadřízený kvalifikovaný systémový certifikát	certifikát, který má náležitosti podle platné legislativy
Párová data	jedinečná data pro vytváření elektronického podpisu nebo elektronické značky spolu s odpovídajícími daty pro ověřování elektronického podpisu nebo elektronické značky
Soukromý klíč	jedinečná data pro vytváření elektronického podpisu nebo elektronické značky
Spoléhající se strana	subjekt spoléhající se při své činnosti na kvalifikovaný certifikát, kvalifikovaný systémový certifikát nebo kvalifikované časové razítko vydané I.CA
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu nebo elektronické značky
Žadatel o časové razítko	individuální koncový uživatel (fyzická osoba), právnická osoba nebo organizační složka státu (zahrnující několik koncových uživatelů), resp. systém, provozovaný výše zmíněnými subjekty

[2] Viz ZoEP

3.2 Zkratky

Tabulka 4 – Zkratky

Zkratka	Vysvětlení
CRL	**C**ertificate **R**evocation **L**ist (seznam zneplatněných certifikátů)
EPS	**E**lektrická **p**ožární **s**ignalizace
HSM	**H**ardware **S**ecurity **M**odul (bezpečné úložiště privátního klíče)
I.CA	První certifikační autorita, a.s. – akreditovaný poskytovatel certifikačních služeb
MV ČR	**M**inistersvo **v**nitra **Č**eské **r**epubliky
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
NBÚ SR	Národní bezpečnostní úřad Slovenské republiky
OID	(Object Identifier) číselná identifikace objektu v rámci jednotné klasifikace objektů podle ISO/ITU
PKI	**P**ublic **K**ey **I**nfrastructure
TSA	**T**ime **S**tamping **A**uthority (Autorita časových razítek)
TSS	**T**ime **S**tamp **S**ervice (Služba časových razítek)
TSU	**T**ime **S**tamp **U**nit (server, generující časová razítka)
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) • sada vyhlášek Slovenské republiky, vztahujících se k problematice aktuálního znění zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a o zmene a doplnení niektorých zákonov
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

4.1 Služby autority časových razítek (TSA)

Služby autority časových razítek, provozovaných společností První certifikační autorita, a.s., zahrnují oblasti vytváření kvalifikovaných časových razítek a implementaci autentizace žadatelů o časová razítka, jsou poskytovány v souladu se ZoEP, VoEP.

4.2 Autorita časových razítek

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

4.3 Žadatelé o kvalifikované časové razítko (dále časové razítko)

Žadatelem o časové razítko může být na základě písemné smlouvy s I.CA individuální koncový uživatel (fyzická osoba), právnická osoba nebo organizační složka státu (zahrnující několik koncových uživatelů), resp. systém, provozovaný výše zmíněnými subjekty.

V případě, že žadatelem o časové razítko je individuální koncový uživatel, je pak tento přímo zodpovědný za to, že splní závazky vůči I.CA.

V případě, že žadatelem o časové razítko 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 splní závazky vůči I.CA. Proto musí právnická osoba nebo organizační složka státu vhodným způsobem informovat vlastní koncové uživatele.

4.4 Spoléhající se strana

Spoléhající se stranou jsou subjekty, uvedené v kapitole 4.3.

5 Politika TSA

5.1 Použití kvalifikovaných časových razítek

Tento dokument nedefinuje žádná omezení použitelnosti časového razítka, vydaného v souladu s jeho obsahem[3]. Časová razítka je možné použít např. v oblastech :

- elektronických podpisů/značek, kdy je třeba ověřit, že byly vytvořeny v době, kdy certifikát veřejného klíče podepisující, resp. označující entity byl platný
- 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. Oblasti hodnocení je upravena interní směrnicí I.CA.

5.2.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

S ohledem na skutečnost, že společnost První certifikační autorita, a.s. je akreditovaným poskytovatel certifikačních služeb, jsou periodicita hodnocení, včetně okolností pro provádění hodnocení striktně dány požadavky ZoEP a VoEP, jedná se zejména o audit systému řízení bezpečnosti informací, který je prováděn každé dva roky, kontroly bezpečnostní shody v intervalu 4 let (celková), resp. každého roku (částečná) a auditu bezpečnosti poskytování certifikačních činností (každý rok).

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

5.2.2 Identita a kvalifikace hodnotitele

Identita a kvalifikace hodnotitele provádějícího hodnocení požadované ZoEP a VoEP je dána touto legislativou, v ostatních případech je vyžadována certifikace pro uvedenou činnost.

5.2.3 Vztah hodnotitele k hodnocené entitě

V případě provádění hodnocení požadovaného ZoEP a VoEP je vztah hodnotitele k poskytovateli certifikačních služeb dán touto legislativou, v ostatních případech se jedná o externího hodnotitele.

5.2.4 Hodnocené oblasti

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

5.2.5 Postupy v případě zjištěných nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manager, který je povinen zajistit odstranění případných nedostatků.

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

5.2.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána řediteli, resp. bezpečnostnímu managerovi společnosti.

V nejbližším možném termínu svolá bezpečnostní manager schůzi bezpečnostního výboru, na které budou mimo vedení společnosti přítomni vedoucí jednotlivých oddělení, které s výsledky hodnocení seznámí.

Sdělování výsledků hodnocení taktéž podléhá požadavkům ZoEP a VoEP.

6 Závazky a odpovědnosti

6.1 Závazky TSA

6.1.1 Obecné závazky TSA

S ohledem na poskytovanou službu zaručuje společnost První certifikační autorita a.s. zejména :

- přístup ke službám TSA :
  - nepřetržitý, s výjimkou plánovaných (předem ohlášených), popř. neplánovaných časových přerušení (tyto okolnosti jsou uvedeny v interní dokumentaci) spojených s technickými zásahy **nebo**
  - za podmínek, uvedených v písemné smlouvě
- autentizovaný přístup ke službám vydávání časových razítek na základě písemné smlouvy
- striktní dodržování platné legislativy (ZoEP) vztahující se k celému procesu vydávání časových razítek, včetně neporušování autorských ani licenčních práv aktivitami společnosti
- poskytování kvalifikovaných certifikačních služeb osobami s odbornými znalostmi a kvalifikací nezbytnou pro poskytování této certifikační služby a obeznámenými s příslušnými bezpečnostními postupy
- používání bezpečných systémů a bezpečných nástrojů, zajištění dostatečné bezpečnosti postupů, které tyto systémy a nástroje podporují včetně dostatečné kryptografické bezpečnosti těchto nástrojů
- 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
- písemné informování žadatele o vydávání časových razítek o přesných podmínkách pro využívání této služby před uzavřením smlouvy, včetně případných omezení pro její použití, a o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je či není akreditována
- povinnost zachovávání mlčenlivosti kmenových zaměstnanců, případně jiných fyzických osob, které přicházejí do styku s osobními údaji 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. zaručuje zejména, že :

- jí vydávaná časová razítka obsahují všechny náležitosti stanovené ZoEP, VoEP
- použije soukromé klíče příslušné certifikátům TSU pouze k elektronickému podepisování/označování vydávaných časových razítek
- data v elektronické podobě, která jsou předmětem žádosti o vydání časového razítka, jednoznačně odpovídají datům v elektronické podobě obsaženým ve vydaném časovém razítku
- implementovala odpovídající opatření proti padělání časových razítek
- vydá časové razítko neprodleně po obdržení platného požadavku
- žádným způsobem neověřuje otisk (hash), kterému má být časové razítko přiřazeno (s výjimkou jeho délky)
- využívá důvěryhodnou časovou synchronizaci
- jí vydané odpověď na žádost o časové razítko obsahuje minimálně :
  - sériové číslo, které je pro konkrétní TSU systému TSA jedinečné
  - identifikátor politiky, pod níž bylo časové razítko vydáno
  - časový údaj odpovídající hodnotě koordinovaného světového času (UTC) v době vytváření kvalifikovaného časového razítka s přesností 1 sekunda
  - data v elektronické podobě obsažená ve vydaném časovém razítku, odpovídající datům v elektronické podobě, obsažených v žádosti o vydání časového razítka
  - elektronickou značku/podpis TSU

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

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

- ověřit platnost elektronické značky/podpisu časového razítka a následně všech certifikátů, vztahujících se k TSU, který tuto elektronickou značku vytvořil
- ověřit, zda vrácený otisk (hash) je totožný s odeslaným v žádosti
- v případě, že žádost obsahovala položku „nonce“ a/nebo „reqPolicy“ ověřit, že její hodnota v odpovědi je totožná

6.3 Závazky spoléhajících se stran

Závazkem spoléhajících se stran je ověření zejména :

- vydaného časového razítka - konkrétně se jedná o hash ověřovaných dat, platnost elektronické značky (v době vytváření elektronické značky) a zda politika, pod kterou bylo časové razítko vydáno, je akceptovatelná jejich potřebám, popř. potřebám provozovaných aplikací.
- bezpečnosti procesu vytváření časového razítka s důrazem na kryptografická funkce pro tvorbu otisku (hash), délku kryptografického klíče a algoritmus pro tvorbu elektronické značky

6.4 Odpovědnost

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud žadatel/držitel časového razítka nebo spoléhající se strana neporušili povinnosti, plynoucí jim z této politiky. Na 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

Tuto politiku, resp. jí odpovídající prováděcí směrnici spravuje společnost První certifikační autorita, a.s.

7.1.2 Kontaktní osoba organizace spravující politiku TSA nebo prováděcí směrnici TSA

Ředitel společnosti První certifikační autorita, a.s. určuje osobu, jejíž kontaktní údaje jsou uvedeny na internetové 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 společnosti První certifikační autorita, a.s. 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 provést změny a tedy i vytvořit novou verzi této politiky, určuje ředitel společnosti První certifikační autorita, a.s. osobu, která je oprávněna tyto změny provádět. Nabytí platnosti nové verze politiky (uvedeno v kapitole 8) předchází jejich schválení ředitelem společnosti První certifikační autorita, a.s.

7.2 Požadavky na životní cyklus párových dat TSA

Následující kapitoly popisují komplexní problematiku životního cyklu párových dat (veřejný a soukromý klíč) TSU. Konkrétní technologické postupy jsou popsány 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 ZoEP a VoEP.

7.2.1.2 Poskytování veřejných klíčů

Veřejné klíče, sloužící pro ověřování elektronických značek/podpisů vydávaných časových razítek, jsou obsažena v certifikátu relevantního TSU. Tento certifikát je možno získat nejméně dvěma nezávislými kanály :

- prostřednictvím internetových informačních adres I.CA
- prostřednictvím internetové adresy MV ČR

7.2.1.3 Délky párových dat

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

7.2.2 Ochrana soukromého klíče (dat pro vytváření elektronických značek)

Následující kapitoly popisují problematiku TSU. Konkrétní technický postup generace párových dat TSU, následné vyhotovení certifikátu TSU, ochrany soukromých klíčů a postupy při správě TSU jsou popsány v interní dokumentaci I.CA.

7.2.2.1 Standardy a podmínky používání kryptografických modulů

Soukromé klíče, sloužící pro vytváření elektronických značek vydávaných časových razítek, jsou uloženy v kryptografickém modulu, který splňuje požadavky standardu FIPS PUB 140-2 úroveň 3 a platné legislativy.

7.2.2.2 Sdílení tajemství

Ochrana sdílením tajemství je realizována prostředky kryptografického modulu. Při provádění citlivých činností, které souvisejí se zásadními činnostmi I.CA, je nezbytná přítomnost tří pověřených pracovníků I.CA v důvěryhodných rolích, z nichž dva znají část kódu k provedení těchto činností.

7.2.2.3 Zálohování soukromých klíčů (dat pro vytváření elektronických značek)

Kryptografický modul, použitý pro správu a využívání soukromých klíčů, sloužících pro vytváření elektronických značek/podpisů vydávaných časových razítek, umožňuje i jejich zálohování v zašifrovaném tvaru.

7.2.2.4 Uchovávání soukromých klíčů

Po uplynutí doby platnosti soukromých klíčů, určených k elektronickému označování/podepisování vydávaných časových razítek, jsou tyto klíče včetně jejich záloh zničeny. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, a proto je u I.CA zakázáno.

7.2.2.5 Transfer soukromých klíčů

Soukromé klíče, sloužící k vytváření elektronických značek/podpisů vydávaných časových razítek, jsou generována přímo v kryptografickém modulu relevantního TSU.

Vkládání soukromých klíčů, sloužících k vytváření elektronických značek/podpisů vydávaných časových razítek, do kryptografického modulu konkrétního TSU v případě, že se jedná o obnovení těchto klíčů ze šifrované zálohy, probíhá za přímé osobní účasti nejméně dvou určených pracovníků I.CA a je písemně zaprotokolováno a podepsáno určenými pracovníci I.CA. V okamžiku vkládání dat musí být TSU odpojen od počítačové sítě.

7.2.2.6 Uložení soukromých klíčů v kryptografickém modulu

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

7.2.2.7 Aktivační data

Aktivační data jsou vytvářena v průběhu procesu instalace, kdy jsou generována párová data pro elektronické označování/podepisování vydávaných časových razítek, jsou určena výhradně pro procesy poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek a nesmí být přenášena nebo uchovávána v otevřené podobě.

7.2.2.8 Postup při aktivaci soukromých klíčů

Aktivaci soukromých klíčů, sloužících k vytváření elektronických značek vydávaných časových razítek, vygenerovaných v kryptografického modulu relevantního TSU, provádí určení pracovníci I.CA prostřednictvím vlastní aktivace daného kryptografického modulu a aktivační čipové karty podle přesně určeného postupu. O provedení aktivace soukromých klíčů je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

7.2.2.9 Postup při deaktivaci soukromých klíčů

Deaktivaci soukromých klíčů, sloužících pro vytváření elektronických značek vydávaných časových razítek, provádí určení pracovníci I.CA prostřednictvím kryptografického modulu a aktivační čipové karty podle přesně určeného postupu. O provedení deaktivace těchto soukromých klíčů je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

7.2.2.10 Postup při zničení soukromých klíčů (dat pro vytváření elektronických značek)

Soukromé klíče, sloužící k označování vydávaných časových razítek jsou uložena v kryptografickém modulu. Ničení těchto klíčů je realizováno prostředky kryptografického modulu. Zálohy těchto klíčů, uložené v zašifrované podobě na externích médiích, jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů.

7.2.2.11 Uchovávání veřejných klíčů

Veřejné klíče, sloužícím k ověřování elektronických značek vydávaných časových razítek, jsou nezbytná pro důvěryhodnost a ověřování platnosti vydaných časových razítek. Tyto klíče jsou obsaženy v certifikátech relevantních TSU. Oproti jim příslušných soukromých klíčů, je důležité veřejné klíče uchovávat pro případ následné kontroly pravosti vydaných časových razítek.

7.2.3 Profil certifikátu

Základní profil certifikátu TSU systému TSA včetně popisu obsahu jednotlivých položek je uveden v Tabulce 5. Podrobný popis profilu certifikátu TSU (certifikáty jednotlivých TSU lze získat na stránkách I.CA nebo Ministerstva vnitra České republiky) je uveden v interní dokumentaci (viz Tabulka 2).

Tabulka 5 – Základní položky certifikátu TSU

Položka	Obsah
Version	verze v3
Serial Numer	jedinečné číslo vydaného certifikátu
SignatureAlgorithm	identifikátor použitého I.CA pro elektronickou značku/podpis vydávaného certifikátu konktrétnímu TSU (sha256WithRSAEncryption)
Issuer	označení vydavatele certifikátu (viz Tabulka 6)
Validity • NotBefore • NotAfter	 počátek platnosti vydávaného certifikátu (UTC) konce platnosti vydávaného certifikátu (UTC)
Subject	označení držitele certifikátu (viz Tabulka 7)
SubjectPublicKeyInfo	

• Algorithm • SubjectPublicKey	identifikátor algoritmu využívaný veřejným klíčem uvedeným ve vydávaném certifikátu veřejný klíč vydávaného certifikátu (2048bitů)
Extensions	Rozšíření certifikátu

Tabulka 6 – Issuer

Položka	Obsah
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName(OU)	I.CA – Accredited Provider of Certification Services
CommonName (CN)	I.CA – Qualified Certification Authority, MM/RRRR
Country (C)	CZ

Pozn.
MM/RRRR – měsíc a rok vydání certifikátu

Tabulka 7 – Subject

Položka	Obsah
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName (OU)	I.CA - Accredited Provider of Certification Services
CommonName (CN)	I.CA - Time Stamping Authority, TSS/TSU X, MM/RRRR
Country (C)	CZ

Pozn
X – číslo TSU
MM/RRRR – měsíc a rok vydání certifikátu

7.2.4 Výměna párových dat

Výměna dat pro ověřování elektronických podpisů/značek ve vydávaných časových razítkách je v případě standardních situací (vypršení platnosti certifikátu relevantního TSU) s dostatečným časovým předstihem před vypršením doby platnosti platnosti tohoto certifikátu prováděna formou vydání nového certifikátu relevantního TSU. V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu tvorby elektronických podpisů/značek, tzn. změny kryptografických algoritmů, délky klíčů, atd.) je tato činnost prováděna v adekvátním časovém období.

Jak v případě standardních situací, tak nestandardních situací je výměna dat pro ověřování elektronických značek v certifikátu relevantního TSU veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

7.2.5 Ukončení životního cyklu párových dat

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

Platnost dat, určených k ověřování označených časových razítek je dána platností vydaných certifikátů relevantního TSU. Po této době lze data pro ověřování elektronických značek použít bez záruky.

Pokud dojde k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu vydávání časových razítek, bude doba platnosti párových dat zkrácena. V takovém případě se postupuje analogicky postupům uvedených v kapitole 7.4.10.4.

7.2.5.1 Zneplatnění a pozastavení platnosti certifikátu

7.2.5.1.1 Seznam zneplatněných certifikátů

Profil seznamu zneplatněných certifikátů odpovídá mezinárodně uznávaným normám a standardům.

7.2.5.1.2 Podmínky pro zneplatnění certifikátu

Certifikát TSU může být zneplatněn pouze na základě následujících okolností :

- nastanou-li skutečnosti uvedené v ZoEP a VoEP
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek, používaných k označování kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek konkrétního TSU

7.2.6 Správa kryptografického modulu používaného při vytváření kvalifikovaných časových razítek

Hardware relevantního TSU, který je připojen do infrastruktury důvěryhodného synchronizačního času 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. TSU 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 TSU jsou prováděny osobami v důvěryhodných rolích a v přítomnosti svědků. V případu předání hardware TSU do servisu, ukončení poskytování kvalifikovaných certifikačních služeb v oblasti časových razítek nebo ukončení činnosti I.CA, jsou data pro vytváření elektronických značek/podpisů generovaných časových razítek zničena dle doporučení výrobce. Konkrétní postupy správy TSU jsou popsány v interní dokumentaci I.CA.

7.2.6.1 Hodnocení kryptografického modulu

Kryptografický modul, sloužící pro elektronické označování/podepisování vydávaných časových razítek, splňuje požadavky 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 Uzavření smlouvy

Vydávání časových razítek je I.CA komerčně nabízenou službou fyzické osobě, právnické osobě nebo organizační složce státu, která se na základě písemné smlouvy, uzavírané způsobem běžným v obchodním styku, zaváže jednat podle této politiky.

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 časových razítek je proces identifikace a autentizace žadatele o časové razítko realizován na bázi tzv. „komerčního“ certifikátu, vydaného I.CA.

I.CA si vyhrazuje právo na využití jiného způsobu identifikace a autentizace žadatele o časové razítko.

7.3.2.2 Přijetí nebo zamítnutí žádosti o kvalifikované časové razítko

Žadatel o vydání časového razítka vytvoří autentizované spojení s komunikačním serverem systému TSA. V případě neúspěšného spojení je transakce ukončena a žadatel je vhodným způsobem informován.

Po úspěšném ukončení procesu identifikace a autentizace žadatel vytvoří žádost o časové razítko (v normovaném formátu dle RFC 3161). Takto vytvořená datová struktura je předána systému TSA.

7.3.2.3 Doba zpracování žádosti o kvalifikované časové razítko

I.CA nestanovuje, není-li v písemné smlouvě uvedeno, pevný časový limit, ve kterém dojde ke zpracování žádosti o časové razítko, neboť se jedná časový sled následujících činností, z nichž některé záleží pouze na elektronickém přenosu žádosti od žadatele o časové razítko k systému TSA. Přibližné časové údaje jsou uvedeny v následujícím seznamu :

- vygenerování žádosti o vydání časového razítka na straně žadatele – řádově sekundy
- vygenerování časového razítka na straně systému TSA – řádově ms

7.3.3 Vydání kvalifikovaného časového razítka

7.3.3.1 Úkony TSA v průběhu vydávání kvalifikovaného časového razítka

Systém TSA provádí veškeré kontroly formální správnosti žádosti o časové razítko a na základě jejich výsledku vytvoří konkrétní TSU odpověď, obsahující v případě kladného výsledku kontrol časové razítko (viz RFC 3161). Časový údaj (UTC), jehož přesnost při vytváření časového razítka je 1 sekunda, je získán z měřidla důvěryhodného času. Odpověď je elektronicky označena/podepsána daty pro vytváření elektronické značky/podpisu konkrétního TSU (tím se tento server nezpochybnitelným způsobem zaručuje za správnost informací uvedených ve vygenerovaném časovém razítku).

Každá odpověď na žádost o časové razítko, obsahující mimo výše uvedených údajů i další potřebné informace (mimo jiné o měřidlu důvěryhodného času), je umístěna v příslušném úložišti systému TSA.

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

Poté, co byly provedeny činnosti, uvedené v kapitole 7.3.3.1, je výše uvedená datová struktura (s případnou doplňující zprávou) odeslána systémem TSA zpět žadateli.

7.3.4 Převzetí kvalifikovaného časového razítka

7.3.4.1 Žadatel o časové razítko

Po obdržení výše uvedené datové struktury je žadatel povinen zjistit status odpovědi. Obsahuje-li odpověď časové razítko, je žadatel povinen postupovat v souladu s kapitolou 6.2.

7.3.4.2 Spoléhající se strana

Ověřování 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 časovém razítku
- vybrání 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 časových razítek (obchodní vztah) ukončuje buď žadatel o časové razítko, nebo I.CA (nejsou-li ze strany žadatele dodrženy podmínky smlouvy).

7.3.6 Struktury žádosti, odpovědi a časového razítka

Časová razítka jsou generována relevantním TSU na základě zaslané žádosti.

7.3.6.1 Žádost

Tabulka 8 – Formát žádosti

Položka	Popis/hodnota	Pozn.
Version	Verze/1	povinná položka
messageImprint • HashAlgorithm • HashedMessage	 OID hash algoritmu/SHA1, SHA-256, SHA-512 hash dat, pro které je požadované časové razítko (délka tohoto řetězce musí splňovat požadavky na délku zvoleného algoritmu)	povinná položka
reqPolicy	Identifikátor politiky/ viz kapitola 2.1	nepovinná položka
Nonce	Náhodné číslo/(64 bitů) o kterém je předpokládáno, že je žadatel vygeneruje pouze jednou	nepovinná položka
certReq	požadavek na certifikát TSU/ • TRUE – odpověď musí obsahovat certifikát TSU • FALSE, nebo není uvedeno - odpověď nesmí obsahovat certifikát TSU	povinná položka, v případě vydávání časových razítek v souladu se slovenskou legislativou musí být TRUE

Pokud dojde k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost tvorby otisku v žádosti o časové razítko (viz HashAlgorithm v Tabulce 8), vyhrazuje si I.CA právo tento algoritmus nepodporovat a danou žádost odmítnout. Informace o nepodporovaných algoritmech bude I.CA zveřejňovat prostřednictvím své internetové adresy (viz kapitola 7.4.13.3.2).

7.3.6.2 Odpověď

Odpověď na žádost o časové razítko obsahuje status a v případě úspěšného vydání i časové razítko (viz RFC 3161).

Tabulka 9 – Status odpovědi

Položka	Popis	Hodnota
PKIStatus	Číslo (integer), značící stav odpovědi na žádost o časové razítko. V případě, že časové razítko je	• 0 – vydané • 1 – vydané upravené • 2 – zamítnutí žádosti • 3 – čekání • 4 – hrozí bezprostřední

	v odpovědi obsaženo, hodnota MUSÍ být 0 nebo 1, v případě jiné hodnoty statusu NESMÍ být v odpovědi časové razítko obsaženo	zneplatnění certifikátu TSU • 5 – certifikát TSU zneplatněn
PKIFailureInfo ::= BIT STRING {	BIT STRING – v případě, že časové razítko není v odpovědí obsaženo pak tato položka definuje důvod odmítnutí žádosti	• BadAlg (0) – neznámý nebo nepodporovaný algoritmus • BadRequest (2) – nepovolená nebo nepodporovaná transakce • BadDataFormat (5) – špatná formát zaslaných dat • TimeNotAvailable (14) – nedostupný zdroj času • UnacceptedPolicy (15) – TSA požadovanou politiku nepodporuje • UnacceptedExtension (16) – TSA nepodporuje požadované rozšíření • AddInfoNotAvailable (17) – požadované doplňující informace nebyly pochopeny nebo dostupné • SystemFailure (25) – požadavek nemohl být s ohledem na chybu systému zpracován

Tab. 10 – Časové razítko

Položka	**Popis/hodnota**
Version	verze/1
Policy	identifikátor politiky/viz kapitola 2.1
messageImprint • **HashAlgorithm** • **HashedMessage**	odpovídající položka žádosti o kvalifikované časové razítko (viz Tabulka 8)/musí mít stejnou hodnotu jako odpovídající položka v žádosti
serialNumber	integer číslo do 160 bitů/ jedinečné číslo, které přiřazuje konkrétní TSU
genTime	generalizedTime/časový údaj odpovídající hodnotě UTC v době vytváření časového razítka
Accuracy	přesnost/přesnost časového údaje, obsaženého ve vydaném časovém razítku
Ordering	definování vztahu dvou kvalifikovaných časových razítek/TRUE
Nonce	viz Tabulka 8/v případě, je obsažena v žádosti, musí být obsažena i v odpovědi a musí mít stejnou hodnotu jako odpovídající položka v žádosti

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 časových razítek, je využíváno již v EU (Evpropská Unie) provozované komerční řešení, založené na modelu důvěryhodné synchronizační časové infrastruktury. Tato bezpečná a nevyvratitelná synchronizační časová služba měřidla času, poskytuje platné a kontrolovatelné informace pro případ sporů mezi poskytovatelem časových razítek a klienty. Problematika synchronizace je řešena interní dokumentací.

7.3.7.2 Bezpečnost měřidla času

Měřidlo času je umístěno v zabezpečených prostorách I.CA a jeho komplexní bezpečnost je řešena interní dokumentací.

7.3.7.3 Detekce odchýlení měřidla času

Problematika detekce odchýlení měřidla času od synchronizačním zdrojem UTC je řešena v rámci výše uvedeného komerčního řešení.

7.3.7.4 Přestupná sekunda

Problematika výskytu přestupné vteřiny měřidla času je řešena v rámci výše uvedeného komerčního řešení.

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

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

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

7.4.5.1 Důvěryhodné role

Pro vybrané činnosti jsou ve společnosti I.CA definovány důvěryhodné role, která jsou spolu s odpovídajícími činnostmi a odpovědnostmi definovány 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 TSU
- ničení dat pro vytváření elektronické značky vydávaných časových razítek

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

- zálohování/obnova dat pro vytváření elektronické značky každého TSU vydávajícího časová razítka
- aktivace každého TSUu vydávajícího časová razítka
- fyzická kontrola chodu každého TSU vydávajícího časová razítka

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

7.4.5.4 Role vyžadující rozdělení povinností

Role, vyžadující rozdělení povinností v procesu poskytování kvalifikovaných certifikačních služeb, jsou definované v interní bezpečnostní dokumentaci.

7.4.5.5 Požadavky na kvalifikaci, zkušenost a bezúhonnost

Pracovníci v důvěryhodných rolích jsou vybíráni a přijímáni na základě dále popsaných personálních kriterií :

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

Ostatní pracovníci jsou přijímáni na základě následujících kriterií :

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

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.

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 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 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 politiky, prováděcí směrnice, bezpečnostní a provozní dokumentace veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

7.4.6 Fyzická bezpečnost a bezpečnost prostředí

7.4.6.1 Umístění a konstrukce

Objekt provozního pracoviště je umístěn v geograficky odlišné lokalitě než ředitelství společnosti, obchodní a vývojová pracoviště, pracovišť registračních autorit a obchodních míst.

Zařízení, určená k výkonu hlavních kvalifikovaných certifikačních služeb v oblasti vydávání kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, jsou umístěna ve vyhrazených prostorách provozního pracoviště. Tyto prostory jsou zabezpečené obdobně jako zabezpečené oblasti kategorie „Důvěrné“.

7.4.6.2 Fyzický přístup

Fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozního pracoviště je uveden v interní dokumentaci společnosti. Ochrana objektu je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a speciálním systémem pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků.

7.4.6.3 Elektřina a klimatizace

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

7.4.6.4 Vliv vody

Všechny kritické systémy provozního pracoviště jsou umístěny takovým způsobem, aby nebyly zaplaveny ani stoletou vodou.

7.4.6.5 Protipožární opatření a ochrana

V objektu provozního pracoviště je instalován elektronické požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení, určená k výkonu hlavních kvalifikovaných certifikačních služeb v oblasti vydávání kvalifikovaných certifikátů nebo kvalifikovaných systémových certifikátů, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

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 ZoEP a VoEP 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

Interní subsystémy systému TSA jsou dostupné pouze pověřeným pracovníkům I.CA, smluvním partnerům nebo subjektům, definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly, uvedenými v interní dokumentaci.

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

Proces kontrol řízení bezpečnosti je ověřován pravidelnými audity systému managementu bezpečnosti informací a bezpečnosti poskytovaných certifikačních služeb.

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 interním 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 serveru TSU, je jeho činnost 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 pro označování vydávaných kvalifikovaných časových razítek I.CA :

- ukončí jejich používání a prokazatelně zneplatní certifikát relevantního TSU - o této skutečnosti, včetně důvodu informuje na své internetové informační adrese, pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů
- pokud je to možné, informuje držitele platných kvalifikovaných časových razítek o zneplatnění certifikátu relevantního TSU, 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 TSU
- oznámí příslušnému úřadu informaci o zneplatnění vlastního certifikátu TSU s uvedením důvodu zneplatnění
- vydá nový certifikát relevantnímu TSU - postup je stejný jako při vydání prvotního certifikátu tohoto TSU

7.4.10.5 Schopnosti obnovit činnost po havárii

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

7.4.11 Ukončení činnosti TSA

V případě plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání časových razítek, 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 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 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 popsány v základních dokumentech (viz Tabulka 2) a detailněrozpracovány v upřesňujících interních bezpečnostních normách a směrnicích.

7.4.13.1.1 Typy zaznamenávaných událostí

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

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

Auditní systém je navržen a provozován způsobem, který zaručuje udržování 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 v intervalech, definovaných v interní bezpečnostní dokumentaci, v případě bezpečnostního incidentu okamžitě.

7.4.13.1.3 Doba uchovávání auditních záznamů

Pokud nebude stanoveno jinak, je doba, po kterou se uchovávají auditní záznamy, stanovena na minimálně 10 let od jejich vzniku.

7.4.13.1.4 Ochrana auditních záznamů

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem, zajišťujícím jejich ochranu před jejich změnami, krádeží a zničení (ať již úmyslnému, tak neúmyslnému).

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

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

Ochrana výše uvedených typů auditních záznamůje definovanána v interní bezpečnostní dokumentaci.

7.4.13.1.5 Postupy pro zálohování auditních záznamů

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

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. Zásady uchovávání informací a dokumentace jsou uvedeny j v základních dokumentech (viz Tabulka 2) a detailněr ozpracovány v upřesňujících interních bezpečnostních normách a směrnicích.

-

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 :

- smlouvy o poskytování certifikační služby
- auditní záznamy definované v kapitole 7.4.13.1.1 tohoto dokumentu
- aplikační programové vybavení a veškerou dokumentaci společnosti, která je nutná pro provádění kontrol
- vydaná časová razítka včetně žádostí o jejich vydání
- elektronické nebo písemné informace požadované ZoEP, VoEP
- veškeré certifikáty TSU a seznamy zneplatněných certifikátů
- veškeré informace, vztahující se k certifikátům TSU s výjimkou příslušných dat pro vytváření elektronické značky/podpisu

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 (nebude-li stanoveno jinak).

7.4.13.2.3 Ochrana úložiště uchovávaných informací a dokumentace

Uchovávané informace a dokumentace mohou obsahovat obsahují i osobní data, a proto je s ohledem na platnou legislativu 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 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

7.4.13.3.1 Úložiště informací a dokumentace

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

7.4.13.3.2 Zveřejňování informací a dokumentace

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

a) adresa sídla společnosti :

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

b) internetová adresa http://www.ica.cz

c) sídla registračních autorit

Kontaktní adresou, slouží pro kontakt klientů popř. veřejnosti s I.CA, je elektronická poštovní adresa tsa@ica.cz (na tuto elektronickou adresu lze zasílat i případné dotazy, připomínky, nebo návrhy na zlepšení poskytované služby).

I.CA zveřejňuje kontaktní adresu na své internetové adrese. Určení pracovníci I.CA jsou rovněž povinni tyto informace na vyžádání sdělit všem potencionálním klientům. Totéž platí i v případě, že dojde ke změně kontaktních adres.

Možnost získání certifikátu certifikační autority a TSU je garantována prostřednictvím internetové adresy I.CA a MV ČR, resp. NBÚ SR.

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 veřejným informacím jsou obecně 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 dat pro vytváření elektronických značek/podpisů vydávaných certifikátů nebo seznamů zneplatněných certifikátů, oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím nejméně jednoho celostátně distribuovaného deníku.

7.4.13.3.3 Periodicita zveřejňování informací

S ohledem na oblast časových razítek I.CA zveřejňuje informace s následující periodicitou :

- politiky - před prvním vydáním certifikátu podle této politiky
- zprávy pro uživatele – při zahájení, resp. při změně poskytované certifikační služby
- získání nebo odejmutí akreditace – bezodkladně
- informace o zneplatnění kořenového certifikátu I.CA a TSU s uvedením důvodu zneplatnění (v případě zneužití nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek/podpisů, určených pro označování vydávaných časových razítek, certifikátů a seznamů zneplatněných certifikátů) – bezodkladně
- seznam zneplatněných certifikátů (CRL) - minimálně jedenkrát za 24 hodin (zpravidla à 8 hodin)
- 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

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení. Neveřejné informace jsou dostupné pouze pověřeným pracovníkům I.CA, smluvním partnerům nebo subjektům, definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly, uvedenými v interní dokumentaci.

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

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 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 a důvěrnými informacemi I.CA jsou zejména :

- data pro vytváření elektronických značek/podpisů, příslušná k datům pro ověřování elektronických značek/podpisů, obsažených v kořenových certifikátech I.CA a v certifikátech TSU

- data pro vytváření elektronických značek/podpisů příslušná k datům pro ověřování elektronických značek/podpisů obsažených v účelových certifikátech I.CA
- ostatní kryptograficky podstatné informace sloužící k provozu I.CA
- vybrané obchodní informace I.CA
- veškeré interní informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb dle ZoEP
- veškeré osobní údaje

7.5.3.2 Informace mimo rámec citlivých informací

Za veřejné se považují zejména 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.

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

7.5.4 Ochrana osobních údajů

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.

7.5.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje, podléhající ochraně ve smyslu příslušných zákonných norem.

7.5.4.3 Údaje, které nejsou považovány za důvěrné

Informace, které nejsou považovány za důvěrné jsou obecně údaje, zveřejňované způsobem, uvedeným v kapitole 7.4.13.3.2.

7.5.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů a dalších neveřejných informací je odpovědna I.CA.

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

Problematiky oznámování o používání důvěrných informací a souhlasu s používáním citlivých informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

7.5.4.6 Poskytování citlivých informací pro soudní či správní účely

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

7.5.4.7 Jiné náležitosti zpřístupňování osobních údajů

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

Osoby, uvedené v kapitole 7.5.3.3, může zbavit mlčenlivosti ten, v jehož zájmu tuto povinnost mají, nebo soud.

7.5.5 Práva duševního vlastnictví

Tento dokument, veškeré související dokumenty, obsah webových stránek, certifikáty CA, klíče I.CA a procedury, zajišťující provoz systému, poskytujícího veškeré kvalifikované certifikační služby, 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

I.CA zejména zaručuje, že :

- použije soukromé klíče, příslušné kořenovým certifikátům I.CA pouze k označování vydávaných certifikátů a seznamu zneplatněných certifikátů
- použije soukromé klíče, příslušné certifikátům TSU pouze k označování vydávaných časových razítek
- vydávané certifikáty a časová razítka splňují náležitosti, požadované ZoEP a VoEP, na jejíž základě byla získána akreditace

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

- žadatel o časové razítko neporušil povinnosti plynoucí mu ze smlouvy o poskytování kvalifikované certifikační služby a tohoto dokumentu
- spoléhající se strana neporušila povinnosti tohoto dokumentu

7.5.6.2 Zastupování a záruky držitelů a žadatelů o kvalifikované časové razítko

Držitel nebo žadatel o kvalifikované časové razítko ručí za informace, jím uvedené ve smlouvě 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, zejména ustanoveními kapitoly 6.3..

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

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

Společnost První certifikační autorita, a.s. :

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

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

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

- Za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb, poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb držitelem, resp. žadatelem o časové raítko, 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
- 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

Tento dokument nabývá platnosti dnem, uvedeným v kapitole 8 do odvolání.

7.5.9.2 Ukončení platosti

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

Uvedeno v kapitole 7.5.9.1.

7.5.10 Komunikace mezi participujícími subjekty

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

Držitelé, resp. 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

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

7.5.12 Opatření při řešení sporů

Tento dokument a jí odpovídající CPS, jejich výklad a aplikace se řídí ZoEP a VoEP.

V případě, že držitel, resp. žadatel o kvalifikovaná časová razítka a/nebo spoléhající se strana, 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 cesta.

7.5.13 Rozhodné právo

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

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 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 23.12.2009.