První certifikační autorita, a.s.

Prováděcí směrnice

vydávání kvalifikovaných elektronických časových razítek systémem TSA2

(algoritmus RSA)

Verze 2.05

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
2.00	13.04.2017	Ředitel společnosti První certifikační autorita, a.s.	První vydání.
2.01	30.04.2019	Ředitel společnosti První certifikační autorita, a.s.	Revize dokumentu, opraveny formální chyby.
2.02	29.04.2020	Generální ředitel společnosti První certifikační autorita, a.s.	Revize dokumentu.
2.03	11.06.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Struktura dle RFC 3647, vyznačena klasifikace dokumentu, revize a upřesnění textu. Aktualizace hodnocení kryptografických modulů.
2.04	30.05.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Doplnění pracoviště eSeL.
2.05	05.10.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace seznamu odkazovaných standardů.

1 ÚVOD

Tento dokument, Prováděcí směrnice vydávání kvalifikovaných elektronických časových razítek systémem TSA2 (algoritmus RSA), dále též Směrnice, rozpracovává a upřesňuje zásady uvedené v dokumentu Politika vydávání kvalifikovaných elektronických časových razítek systémem TSA2 (algoritmus RSA), dále též Politika. Směrnice byla společností První certifikační autorita, a. s., dále též I.CA, vypracována na základě požadavků platné právní úpravy, zabývá se skutečnostmi vztahujícími se k procesům vydávání a využívání kvalifikovaných elektronických časových razítek (dále též Služba, časová razítka) a zahrnuje všechny požadavky politiky BTSP (Best practices Time-Stamp Policy) uvedené ve standardu ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. Právní požadavky jsou definovány:

- nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění,
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- zákonem Slovenské republiky č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),
- právní úpravou týkající se ochrany osobních údajů v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

I.CA nijak neomezuje potenciální koncové uživatele, poskytování Služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

Pozn.: Pokud jsou v dalším textu uváděny odkazy na technické standardy, normy nebo právní předpisy, jedná se vždy buď o uvedený technický standard, normu nebo právní předpis, resp. o technický standard, normu či právní předpis, který je nahrazuje. Pokud by byl tento dokument v rozporu s technickými standardy, normami nebo právními předpisy, které nahradí dosud platné, bude vydána jeho nová verze.

1.1 Přehled

Tato Směrnice je vypracována na obecné úrovni, detaily jsou popsány v interní dokumentaci. Je rozdělena do deseti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument, obecně popisuje subjekty participující na poskytování této Služby a definuje přípustné využívání vydávaných časových razítek.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání certifikátu TSU, odkazuje na dokument Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě TSA2 (algoritmus RSA).

- Kapitola 4 definuje procesy životního cyklu vydávaných časových razítek, tzn. uzavření smlouvy, zpracování žádosti o časové razítko, vydání časového razítka a ukončení poskytování Služby, žádost o zneplatnění a vlastní zneplatnění certifikátu TSU atd.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání záznamů a reakce po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů a technologie kryptografických modulů.
- Kapitola 7 odkazuje na Politiku, kde jsou uvedeny základní položky certifikátu TSU a struktury žádosti o časové razítko, odpovědi na žádost o časové razítko a časového razítka.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytované Služby.
- Kapitola 9 zahrnuje problematiku obchodní a právní.
- Kapitola 10 obsahuje závěrečná ustanovení.

V procesu poskytování služby vytvářející důvěru v oblasti vydávání časových razítek (dále též Služba) provozuje společnost První certifikační autorita, a.s., systém TSA2 skládající se z jednotlivých jednotek TSU. Podrobný popis procesů této autority časových razítek je uveden v dalších dokumentech, které jsou obecně neveřejné. Tyto dokumenty, včetně dalších zpráv, výsledků testů a interních kontrol tvoří dokumentační sadu, dosažitelnou výhradně autorizovanému personálu a auditorům. V následující tabulce jsou uvedeny významné interní dokumenty, vztahující se ke Službě.

Číslo	Název dokumentu	Klasifikace
1.	Politika vydávání kvalifikovaných elektronických časových razítek systémem TSA2 (algoritmus RSA)	Veřejný dokument
2.	Prováděcí směrnice vydávání kvalifikovaných elektronických časových razítek systémem TSA2 (algoritmus RSA) - tento dokument	Veřejný dokument
3.	Systémová bezpečnostní politika – důvěryhodné systémy	I.CA – Jen pro vnitřní potřebu
4.	Plán pro zvládání krizových situací a plán obnovy	I.CA – Důvěrné
5.	Zpráva pro uživatele TSA	Veřejný dokument
6.	sada interních směrnic	I.CA – Jen pro vnitřní potřebu, resp. I.CA – Důvěrné
7.	Celková bezpečnostní politika	I.CA – Jen pro vnitřní potřebu

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu:	Prováděcí směrnice vydávání kvalifikovaných elektronických časových razítek systémem TSA2 (algoritmus RSA), verze 2.05
OID:	není přiřazen

1.3 Participující subjekty

1.3.1 Autorita časových razítek

Systém TSA2 je z pohledu klientů důvěryhodná výpočetní a komunikační infrastruktura, vydávající časová razítka. Z titulu provozovatele nese celkovou odpovědnost za poskytování služeb vytvářejících důvěru v oblasti vydávání časových razítek společnost První certifikační autorita, a.s.

Systém autority časových razítek se skládá z jednotlivých serverů vydávajících časová razítka (TSU). Každý takový server má unikátní soukromý klíč a certifikát odpovídajícího klíče veřejného.

1.3.2 Žadatelé o časová razítka

Žadatelem o časové razítko mohou být na základě písemné smlouvy s I.CA individuální koncový uživatel (fyzická osoba), právnická osoba nebo organizační složka státu.

1.3.3 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na časová razítka vydávaná podle Politiky.

1.3.4 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, případně orgány dohledu a další, kterým to podle platné právní úpravy přísluší.

1.4 Použití časového razítka

1.4.1 Přípustné použití časového razítka

Tato Směrnice, resp. jí odpovídající Politika nedefinuje žádná omezení použitelnosti časového razítka, vydaného v souladu s jejím obsahem[1].

1.4.2 Zakázané použití časového razítka

Viz 1.4.1.

[1] Časová razítka vydaná podle Politiky lze využívat jak v otevřených systémech veřejných služeb (např. státní správy), tak v uzavřených systémech soukromých společností.

1.5 Správa politiky

1.5.1 Organizace spravující dokument

Tuto Směrnici, resp. jí odpovídající Politiku spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s Politikou, resp. s touto Směrnicí je uvedena na internetové adrese – viz kapitola 2.2.

1.5.3 Osoba rozhodující o souladu Směrnice s Politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených v této Směrnici s Politikou, je generální ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování Směrnice

Pokud je potřebné provést změny v této Směrnici a vytvořit její novou verzi, určuje generální ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést.

Nabytí platnosti nové verze Směrnice předchází její schválení generálním ředitelem společnosti První certifikační autorita, a.s.

1.6 Přehled použitých pojmů a zkratek

tab. 2 - Pojmy

Pojem	Vysvětlení
bit	z anglického *binary digit* – číslice dvojkové soustavy – základní a současně nejmenší jednotka informace v číslicové technice
dvoufaktorová autentizace	autentizace využívající dvou ze tří faktorů – něco vím (heslo), něco mám (např. čipová karta, hardwarový token) nebo něco jsem (otisky prstů, snímání oční sítnice či duhovky)
elektronická pečeť	zaručená elektronická pečeť, nebo uznávaná elektronická pečeť, nebo kvalifikovaná elektronická pečeť dle právní úpravy pro služby vytvářející důvěru
hashovací funkce	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou (hash)
klient	žadatel o časové razítko nebo spoléhající se strana
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
orgán dohledu	subjekt dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru
párová data	soukromý a jemu odpovídající veřejný klíč

písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
právní úprava pro služby vytvářející důvěru	platné právní předpisy České republiky a Slovenské republiky vztahující se ke službám vytvářejícím důvěru a nařízení eIDAS
smluvní partner	poskytovatel služeb zajišťující na základě písemné smlouvy pro I.CA služby vytvářející důvěru nebo jejich části – nejčastěji se jedná o smluvní RA
soukromý klíč	jedinečná data pro vytváření elektronické pečetě
spoléhající se strana	subjekt spoléhající se při své činnosti na časové razítko vydané I.CA
veřejný klíč	jedinečná data pro ověřování elektronické pečetě
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
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

tab. 3 - Zkratky

Zkratka	Vysvětlení
CA	certifikační autorita
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
ČR	Česká republika
ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátu
eIDAS	nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
eSeL	Elektronická sbírka a elektronická legislativa, nástroj pro tvorbu, zpracování a využití legislativy
ESI	Electronic Signatures and Infrastructures

ETSI	the European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EZS	elektronická zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
GDPR	Global Data Protection Regulation, nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
GPS	Global Positioning System, globální družicový polohový systém
html	Hypertext Markup Language, značkovací jazyk pro vytváření hypertextových dokumentů
http	Hypertext Transfer Protocol, protokol pro výměnu textových dokumentů ve formátu html
https	Hypertext Transfer Protocol Secure, protokol pro zabezpečenou výměnu textových dokumentů ve formátu html
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IP	Internet Protocol, komunikační protokol síťové vrstvy
IPS	Intrusion Prevention System, systém prevence průniku
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, číselná identifikace objektu
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování–Zavedení–Kontrola–Využití, Demingův cyklus, metoda neustálého zlepšování
PDF	Portable Document Format, standard formátu souboru
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
RA	registrační autorita
RFC	Request for Comments, označení řady standardů a dalších dokumentů popisujících internetové protokoly, systémy apod.
RSA	šifra s veřejným klíčem pro podepisování a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)
sha, SHA	typ hashovací funkce

TS	Technical Specification, typ ETSI standardu
TSA	Time-Stamping Authority, autorita časových razítek
TSU	Time-Stamp Unit, jednotka vydávající časová razítka
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
USNO	United States Naval Observatory, agentura poskytující polohové, navigační a časové údaje
UTC	Coordinated Universal Time, standard přijatý 1.1.1972 pro světový koordinovaný čas - funkci „oficiálního časoměřiče" atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
UTC(k)	fyzická realizace UTC
ZOOÚ	aktuální právní úprava týkající se ochrany osobních údajů

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ZA ÚLOŽIŠTĚ

2.1 Úložiště

Společnost První certifikační autorita, a.s., zřizuje a provozuje úložiště veřejných i neveřejných informací.

2.2 Zveřejňování informací

Základní adresy (dále též informační adresy), na nichž lze získat informace o společnosti První certifikační autorita, a.s., případně odkazy pro zjištění dalších informací, jsou:

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

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

Elektronická adresa, která slouží pro kontakt veřejnosti s I.CA, je tsa@ica.cz, ID datové schránky I.CA je a69fvfb.

Na výše uvedené internetové adrese lze získat informace o:

- certifikátech certifikačních autorit a časových autorit,
- veřejných certifikátech – přímo se zveřejňují následující informace (ostatní informace lze získat z certifikátu):
  - číslo certifikátu,
  - obsah položky Obecné jméno (commonName),
  - údaj o počátku platnosti (s uvedením hodiny, minuty a sekundy),
  - odkazy na místo, kde lze certifikát získat v určených formátech (DER, PEM, TXT),
- seznamech zneplatněných certifikátů (CRL) - přímo se zveřejňují následující informace (ostatní informace lze získat ze samotného CRL):
  - datum vydání CRL,
  - číslo CRL,
  - odkazy na místo, kde lze CRL získat v určených formátech (DER, PEM, TXT),
- certifikačních a jiných politikách, prováděcích směrnicích a ostatních veřejných informacích.

Povolenými protokoly pro přístup k veřejným informacím jsou http a https. I.CA může bez udání důvodu přístup k některým informacím zrušit nebo pozastavit.

V případě zneplatnění certifikátů sloužících v procesech vydávání časových razítek z důvodu podezření na kompromitaci, případně samotné kompromitace příslušného soukromého klíče oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím

celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes a Hospodárske noviny nebo Sme.

2.3 Čas nebo četnost zveřejňování

I.CA zveřejňuje informace týkající se oblasti časových razítek s následující periodicitou:

- Politika – před prvním vydáním časového razítka podle této Politiky,
- Směrnice – neprodleně (je-li určena ke zveřejnění),
- seznam vydaných certifikátů – aktualizace při každém vydání nového certifikátu,
- seznam zneplatněných certifikátů (CRL) - po každém zneplatnění certifikátu TSA a dále v pravidelných intervalech, nejvýše 24 hodin od vydání předchozího CRL,
- zneplatnění certifikátu CA vydávající certifikáty pro jednotlivé TSU, nebo certifikátu TSU systému TSA2 s uvedením důvodu zneplatnění – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb vytvářejících důvěru.

2.4 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 právní úpravou pro služby vytvářející důvěru. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci:

- „Celková bezpečnostní politika“,
- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Řízení bezpečnosti informací“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“,
- „Ochrana osobních údajů v I.CA“,
- „Řízení fyzického přístupu do místností I.CA“,
- „Příručka administrátora“.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Veškerá jména v certifikátech TSU jsou konstruována v souladu s platnými technickými standardy a normami.

3.1.2 Požadavek na významovost jmen

V procesu vydávání certifikátu TSU je vždy vyžadována významovost všech ověřitelných jmen uvedených v položkách pole subject. Podporované položky tohoto pole jsou uvedeny v kapitole 7.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Certifikáty TSU nepodporují anonymitu, ani používání pseudonymu.

3.1.4 Pravidla pro interpretaci různých forem jmen

Údaje uváděné v procesu žádosti o certifikát se do certifikátů TSU přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokumentech.

3.1.5 Jedinečnost jmen

Je zaručena jedinečnost pole subject v certifikátu TSU.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Certifikáty TSU mohou obsahovat pouze obchodní značky vlastněné společností První certifikační autorita, a.s.

3.2 Počáteční ověření identity

Popsáno v kapitole 3.2 dokumentu Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA).

3.2.1 Ověřování vlastnictví soukromého klíče

Viz kapitola 3.2.

3.2.2 Ověřování identity organizace

Viz kapitola 3.2.

3.2.3 Ověřování identity fyzické osoby

Viz kapitola 3.2.

3.2.4 Neověřované informace o držiteli certifikátu

Všechny informace musí být řádným způsobem ověřeny.

3.2.5 Ověřování kompetencí

Není relevantní pro tento dokument.

3.2.6 Kritéria pro interoperabilitu

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

3.3 Identifikace a autentizace při požadavku na výměnu klíče

Popsáno v kapitole 3.3 dokumentu Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA).

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Viz kapitola 3.3

3.3.2 Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu

Viz kapitola 3.3

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Popsáno v kapitole 3.4 dokumentu Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA).

4 ŽIVOTNÍ CYKLUS ČASOVÝCH RAZÍTEK

Služby autority časových razítek TSA2 provozované společností První certifikační autorita, a.s., zahrnující oblasti vytváření a vydávání časových razítek a implementaci autentizace žadatelů o časová razítka, jsou poskytovány v souladu s relevantní právní úpravou a s technickými standardy.

4.1 Uzavření smlouvy

Vydávání časových razítek je v 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 Politiky.

4.2 Zpracování žádosti o časové razítko

4.2.1 Identifikace a autentizace

Identifikace a autentizace žadatele o časové razítko jsou prováděny jedním z těchto způsobů:

- na bázi nekvalifikovaného certifikátu vydaného I.CA,
- jménem a heslem,
- statickou IP adresou.

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

4.2.2 Přijetí nebo zamítnutí žádosti o časové razítko

Žadatel o vydání časového razítka vytvoří autentizované spojení s komunikačním serverem systému TSA2. 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 TSA2. V případě, že žádost nesplňuje požadavky Politiky, je systémem TSA2 zamítnuta.

4.2.3 Doba zpracování žádosti o 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 činností, z nichž některé záleží pouze na elektronickém přenosu žádosti od žadatele o časové razítko k systému TSA2. 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 TSA2 – řádově milisekundy.

4.3 Vydání časového razítka

4.3.1 Úkony autority časových razítek v průběhu vydávání časového razítka

Systém TSA2 provádí veškeré kontroly formální správnosti žádosti o časové razítko a na základě jejich výsledku vytvoří konkrétní TSU odpověď, obsahující stav odpovědi a v případě kladného výsledku kontrol i časové razítko (viz RFC 3161). Časový údaj (UTC) je získán z měřidla důvěryhodného času. Časové razítko je opatřeno elektronickou pečetí konkrétního TSU.

Každá odpověď na žádost o časové razítko je umístěna v příslušném úložišti systému TSA2.

4.3.2 Oznámení o vydání časového razítka držiteli časového razítka

Poté, co byly provedeny činnosti, uvedené v kapitole 4.3.1, je odpověď na žádost o časové razítko (viz tab. 6) odeslána systémem TSA2 zpět žadateli.

4.4 Převzetí časového razítka

4.4.1 Povinnosti žadatele o časové razítko

Po obdržení odpovědi na žádost o časové razítko je žadatel povinen zjistit její stav. Obsahuje-li odpověď časové razítko, je žadatel povinen postupovat v souladu s kapitolou 9.6.3 Politiky.

4.4.2 Povinnosti spoléhající se strany

Spoléhající se strana je povinna postupovat v souladu s kapitolou 9.6.4 Politiky.

4.5 Ukončení poskytování služeb pro žadatele o časové razítko

Službu vydávání časových razítek pro konkrétního uživatele (obchodní vztah) ukončuje buď tento uživatel, tj. žadatel o časové razítko, nebo I.CA, nejsou-li ze strany žadatele dodrženy podmínky písemné smlouvy.

4.6 Párová data TSU a jejich platnost

4.6.1 Výměna párových dat

Platnost certifikátu TSU systému TSA2 je uvedena v tomto certifikátu. Platnost párových dat (veřejný a soukromý klíč) pro tvorbu, resp. ověřování elektronické pečetě časových razítek je omezena platností tohoto certifikátu (obvykle na dobu šesti let).

V prvním roce po vygenerování párových dat a vydání certifikátu veřejného klíče je klíč soukromý používán pro tvorbu elektronické pečetě časového razítka. Před koncem tohoto období jsou vygenerována nová párová data a vydán certifikát nového veřejného klíče. K tvorbě elektronické pečetě časových razítek je dále využíván nejnovější soukromý klíč. Veřejné klíče, staré i nejnovější, jsou využívány k ověřování elektronických pečetí vytvořených odpovídajícím soukromým klíčem.

V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu tvorby elektronických pečetí a je nutná změna kryptografických algoritmů, délky klíčů atd., je generování nových párových dat a vydání příslušného certifikátu provedeno neprodleně. Postup je popsán interní dokumentací:

- „Správa TSS“.

4.6.2 Zneplatnění certifikátu TSU

Certifikát TSU může být zneplatněn pouze na základě následujících okolností:

- nastanou-li skutečnosti uvedené v právní úpravě pro služby vytvářející důvěru,
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority vydávající certifikáty pro TSU systému TSA2 a svůj OCSP respondér,
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci soukromého klíče konkrétního TSU.

Profil seznamu zneplatněných certifikátů odpovídá relevantním technickým standardům a normám.

4.7 Synchronizace měřidla času s UTC

4.7.1 Synchronizace

TSU servery, a to jak ty umístěné v prostorách I.CA, tak v lokalitě eSeL, synchronizují průběžně svůj čas s primárním zdrojem času (komerční řešení), který získává časovou informaci ze systému GPS poskytovanou UTC(k) laboratoří USNO.

Postup je popsán interní dokumentací:

- „Správa TSS“;
- „Správa TSMC“.

4.7.2 Bezpečnost měřidla času

Měřidlo času TSU serverů umístěných v prostorách I.CA je v těchto prostorách rovněž umístěno a jeho zabezpečení je popsáno v interní dokumentaci:

- „Řízení fyzického přístupu do místností I.CA“,
- „Požární bezpečnost“.

Měřidlo času TSU serverů pro pracoviště eSeL je umístěno v datovém centru státní správy s dostatečnou úrovní bezpečnosti (viz kapitola 5.1.1).

Podrobný popis je uveden v interní dokumentaci:

- „Řízení fyzického přístupu do místností I.CA“,
- „Požární bezpečnost“,
- „Příručka administrátora“,
- „Obnova komponenty provozního pracoviště“,

- „Přemístění provozního pracoviště“,
- „Správa TSS“,
- „Správa TSMC“.

4.7.3 Detekce odchýlení měřidla času

Systémový čas TSU serverů, a to jak těch umístěných v prostorách I.CA, tak v lokalitě eSeL, kontroluje (audituje) v pravidelných intervalech spouštěná kontrolní aplikace proti druhému nezávislému zdroji času umístěnému v jiné lokalitě. Čas tohoto zdroje je opět pomocí interního GPS modulu synchronizován s UTC.

Výsledkem úspěšné kontroly je časově omezený auditní „token", který povolí TSU vydávání časových razítek do doby, která je v tokenu uvedena. Před uplynutím této doby musí proběhnout nová (úspěšná) kontrola, jinak TSU zastaví vydávání časových razítek.

V případě zjištění odchylky větší, než je maximální přípustná odchylka pro vydávání časových razítek nastavená v konfiguraci, vytvoří kontrolní aplikace neplatný token (na základě toho TSU okamžitě zastaví vydávání časových razítek) a současně vygeneruje alarm pro provozní obsluhu (o zastavení vydávání časových razítek).

Postup je popsán v interní dokumentaci:

- „Správa TSS“.

4.7.4 Přestupná sekunda

Přestupná sekunda je řešena na TSU manuálně, postup je popsán interní dokumentací:

- „Správa TSS“.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Postupy správy, řízení a provozu jsou zaměřeny především na:

- důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru,
- veškeré procesy podporující poskytování služeb vytvářejících důvěru.

Postupy správy, řízení a provozu jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, Systémová bezpečnostní politika – důvěryhodné systémy, Certifikační prováděcí směrnice, Plán pro zvládání krizových situací a plán obnovy, tak v upřesňující interní dokumentaci. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně popsána interní dokumentací:

- „Řízení fyzického přístupu do místností I.CA“,
- „Požární bezpečnost“,
- „Kontrolní činnost, bezúhonnost a odbornost”,
- „Bezpečnostní incidenty“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Kamerový systém – provozní pracoviště“,
- projekty fyzické bezpečnosti jednotlivých provozních pracovišť.

5.1.1 Umístění a konstrukce

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

Důvěryhodné systémy určené k podpoře Služby v prostorách I.CA jsou umístěny ve vyhrazených prostorách provozních pracovišť. Tyto prostory jsou zabezpečené obdobně, jako zabezpečené oblasti kategorie „Důvěrné“ podle zákona o ochraně utajovaných informací.

Důvěryhodné systémy určené k podpoře Služby pro pracoviště eSeL jsou umístěny v datových centrech státní správy stavebně konstruovaných jako objekt v objektu, odolných proti výbuchu, vybavených celoplášťovou ochranou, střežených v režimu 24x365 a se zavedenými režimovými opatřeními pro přístup osob i materiálu.

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

V prostorách, kde jsou umístěny důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20 °C ± 5 °C. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

5.1.4 Vlivy vody

Důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště jsou podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěny důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

5.1.6 Ukládání médií

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

Papírová média, která je nutno uchovávat, jsou skladována v jiné geografické lokalitě, než je umístěno pracoviště, na kterém záznamy vznikly.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procedurální postupy

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou v I.CA definovány důvěryhodné role. Postup jmenování zaměstnanců do důvěryhodných rolí, specifikace těchto rolí včetně odpovídajících činností a odpovědností jsou popsány interní dokumentací:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Řízení bezpečnosti informací“,

- „Příručka administrátora“.

Všichni zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, který by mohl ohrozit nestrannost operací I.CA.

5.2.2 Počet osob požadovaných pro zajištění jednotlivých činností

Pro níže uvedené činnosti je nezbytná přítomnost více než jediné osoby:

- generování párových dat TSU systému TSA2,
- ničení soukromého klíče TSU systému TSA2,
- zálohování/obnova soukromého klíče TSU systému TSA2.

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

Pro činnosti spojené s certifikační autoritou vydávající certifikáty pro TSU systému TSA2 je problematika popsána v její certifikační politice.

5.2.3 Identifikace a autentizace pro každou roli

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

Pro vybrané činnosti využívají pracovníci v důvěryhodných rolích dvoufaktorovou autentizaci.

5.2.4 Role vyžadující rozdělení povinností

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou popsány interní dokumentací.

5.3 Personální postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

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

- občanská bezúhonnost – prokazováno výpisem z rejstříku trestů, nebo čestným prohlášením,
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně tři roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně pět let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně jeden rok v oblasti poskytování služeb vytvářejících důvěru,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Ostatní zaměstnanci I.CA podílející se na zajištění služeb vytvářejících důvěru jsou přijímáni na základě následujících kritérií:

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

Pro vykonávání řídící funkce musí mít vedoucí zaměstnanci zkušenosti získané praxí nebo odbornými školeními s ohledem na důvěryhodnost Služby, znalost bezpečnostních postupů s odpovědností za bezpečnost a zkušenosti s bezpečností informací a hodnocením rizik.

Problematika je popsána interní dokumentací:

- „Kontrolní činnost, bezúhonnost a odbornost".

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích I.CA jsou:

- sami tito zaměstnanci,
- osoby, které tyto zaměstnance znají,
- veřejné zdroje informací.

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

5.3.3 Požadavky na školení

Zaměstnanci I.CA jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samostudia a metodickým vedením již zaškoleným pracovníkem. Školení zahrnuje oblasti informační bezpečnosti, ochrany osobních údajů a další relevantní témata. Problematika je popsána interní dokumentací:

- „Kontrolní činnost, bezúhonnost a odbornost".

5.3.4 Požadavky a periodicita doškolování

Dvakrát za 12 měsíců jsou zaměstnancům I.CA poskytovány aktuální informace o vývoji v předmětných oblastech.

Pro pracovníky RA je minimálně jednou za tři roky pořádáno školení zaměřené na procesy spojené s činností RA.

Problematika je popsána interní dokumentací:

- „Kontrolní činnost, bezúhonnost a odbornost".

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

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

5.3.6 Postihy za neoprávněné činnosti

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem popsaným interní dokumentací a řídícím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

5.3.7 Požadavky na nezávislé dodavatele

I.CA může nebo musí některé činnosti zajišťovat smluvně, za činnost nezávislých dodavatelů plně odpovídá. Tyto obchodně právní vztahy jsou upraveny 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 politikami, relevantními částmi interní dokumentace, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou uplatňovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

S ohledem na požadavky:

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps,
- ČSN ETSI EN 319 421 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající časová razítka, resp.
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps,

jsou v důvěryhodných systémech I.CA do elektronického auditního logu zaznamenávány následující bezpečnostně relevantní provozní události:

- z hlediska systému významné události prostředí a klíčového hospodářství,
- spuštění a ukončení funkcí auditu,
- změny parametrů auditu,
- akce prováděné při chybách úložiště auditních záznamů,
- všechny pokusy o přístupu k systému,
- veškeré události, vztahující se k požadavkům na certifikát TSU,
- veškeré chyby (včetně časových odchylek mimo povolenou toleranci), spojené s důvěryhodným zdrojem času,

- veškeré události, vztahující se k životnímu cyklu párových dat TSU,
- veškeré události, vztahující se k životnímu cyklu certifikátů TSU,
- veškeré události, vztahující se k synchronizaci časového údaje měřidla času serveru vydávajícího časová razítka s UTC,
- veškeré události, vztahující se ke ztrátě synchronizace.

Všechny záznamy v auditním souboru obsahují následující údaje:

- datum (rok, měsíc, den) a čas (hodina, minuta, sekunda) události,
- typ události,
- identitu entity, která je za akci odpovědná,
- úspěšnost /neúspěšnost auditované události.

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

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

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných interní dokumentací:

- „Příručka administrátora“,

v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

Nestanoví-li relevantní právní úprava jinak, jsou auditní záznamy uchovávány po dobu nejméně 10 let od jejich vzniku.

5.4.4 Ochrana auditních záznamů

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

Elektronické auditní záznamy jsou ukládány ve dvou kopiích. Auditní záznamy TSU serverů umístěných v prostorách I.CA v papírové formě jsou umístěny mimo provozní prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je popsána interní dokumentací:

- „Příručka administrátora“,
- „Zálohování dat provozních systémů“,
- „Dokumenty agendy certifikačních služeb“.

5.4.5 Postupy pro zálohování auditních záznamů

Zálohování elektronických auditních záznamů probíhá obdobným způsobem, jako zálohování ostatních elektronických informací. Zálohování auditních záznamů v papírové formě prováděno není. Postup je popsán interní dokumentací:

- „Příručka administrátora“,
- „Zálohování dat provozních systémů“.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů CA interní.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s., prováděno v periodických intervalech jako součást analýzy rizik. Sledování zranitelnosti zařízení a programového vybavení souvisejících se službami vytvářejícími důvěru je popsáno interní dokumentací. Hodnocením a řízením rizik se zabývá interní dokumentace:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Přístupy k posuzování a ošetřování rizik bezpečnosti informací – důvěryhodné systémy“,
- „Kontrolní činnost, bezúhonnost a odbornost“,
- „Bezpečnostní incidenty“.

5.5 Uchovávání záznamů

Uchovávání záznamů, tj. informací a dokumentace, je ve společnosti První certifikační autorita, a.s., upraveno interní dokumentací:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Řízení fyzického přístupu do místností I.CA“,
- „Zálohování dat provozních systémů“,
- „Příručka administrátora“,
- „Správa TSS“,
- „Správa TSMC“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

5.5.1 Typy uchovávaných záznamů

I.CA uchovává následující typy záznamů (v elektronické nebo listinné podobě), které souvisejí s poskytovanými službami vytvářejícími důvěru v oblasti časových razítek, zejména:

- smlouvy o poskytování Služby,
- dokumenty a záznamy související s životním cyklem vydaných certifikátů TSU systému TSA2, včetně těchto certifikátů a certifikátů s nimi souvisejících,
- vydaná časová razítka včetně žádostí o jejich vydání,
- záznamy o činnosti jednotlivých TSU systému TSA2,
- záznamy o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- provozní a bezpečnostní dokumentaci.

5.5.2 Doba uchování záznamů

Záznamy vztahující se k certifikátům všech certifikačních autorit I.CA a jim odpovídajících OCSP respondérů, s výjimkou příslušných soukromých klíčů, jsou uchovávány po celou dobu existence I.CA. Totéž platí pro certifikáty TSU systému TSA2. Ostatní záznamy jsou uchovávány v souladu s ustanoveními kapitoly 5.4.3.

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště záznamů

Prostory, ve kterých se uchovávané záznamy nacházejí, jsou zabezpečeny způsobem vycházejícím z požadavků provedené analýzy rizik a ze zákona o ochraně utajovaných informací.

Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

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

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

Záznamy jsou ukládány na místo určené výkonným ředitelem I.CA.

Samotná problematika přípravy a způsobu ukládání záznamů v elektronické i písemné podobě je upravena interní dokumentací. Shromažďování uchovávaných záznamů je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací

Uchovávané informace a záznamy jsou umístěny v lokalitách k tomu určených a jsou přístupné:

- zaměstnancům I.CA, pokud je to k jejich činnosti vyžadováno,
- oprávněným dohledovým a kontrolním subjektům a orgánům činným v trestním řízení, pokud je to právními předpisy vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

Viz kapitola 4.6.1.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup ošetření incidentu nebo kompromitace

V případě výskytu těchto událostí postupuje I.CA v souladu s interním plánem pro zvládání krizových situací a plánem obnovy a případně s další relevantní interní dokumentací.

5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče TSU

V případě kompromitace nebo vzniku důvodné obavy ze zneužití soukromého klíče TSU systému TSA2 I.CA:

- okamžitě ukončí jeho používání a prokazatelně zneplatní certifikát tohoto 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 klienty služby vydávání časových razítek o zneplatnění certifikátu relevantního TSU, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, kterou tyto osoby uvedly ve smlouvě – součástí této informace je důvod ukončení platnosti certifikátu relevantního TSU,
- oznámí příslušnému orgánu dohledu informaci o zneplatnění certifikátu TSU s uvedením důvodu zneplatnění,
- vydá nový certifikát relevantnímu TSU – postup je stejný jako při vydání prvotního certifikátu tohoto TSU.

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interním plánem pro zvládání krizových situací a plánem obnovy a s další relevantní interní dokumentací:

- „Plán pro zvládání krizových situací a plán obnovy“,
- „Bezpečnostní incidenty“,

- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“.

5.8 Ukončení činnosti autority časových razítek

Pro ukončování činnosti systému TSA2 platí následující pravidla:

- ukončení činnosti musí být písemně oznámeno orgánu dohledu a všem subjektům, které mají uzavřenou písemnou smlouvu vztahující se k poskytování Služby,
- ukončení činnosti musí být zveřejněno na internetové adrese I.CA,
- soukromé klíče TSU systému TSA2 musí být prokazatelně zničeny a o tomto zničení proveden záznam, který bude uchováván podle pravidel Politiky,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu.

Problematika ukončení činnosti I.CA jako kvalifikovaného poskytovatele služeb vytvářejících důvěru je detailně popsána v interní dokumentaci.

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat TSU systému TSA2 probíhá v zabezpečené oblasti a je prováděno v kryptografickém modulu, který splňuje požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN. O generování je pořízen písemný záznam.

Veškeré požadavky na proces generování párových dat jsou popsány interní dokumentací, mj.:

- „Řízení fyzického přístupu do místností I.CA“,
- „Správa TSS“.

6.1.2 Předávání soukromého klíče jeho držiteli

Není relevantní pro tento dokument, soukromé klíče TSU jsou uloženy v kryptografickém modulu.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Veřejný klíč TSU systému TSA2 je certifikační autoritě předáván jako součást žádosti o certifikát (formát pkcs#10).

6.1.4 Poskytování veřejného klíče TSU spoléhajícím se stranám

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

- prostřednictvím internetových informačních adres I.CA,
- prostřednictvím internetové adresy orgánu dohledu.

6.1.5 Délky klíčů

Systém TSA2 používá asymetrický šifrový algoritmus RSA. Mohutnost klíčů použitých pro opatřování vydávaných časových razítek zaručenou elektronickou pečetí je minimálně 2048 bitů.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejného klíče TSU systému TSA2 splňují požadavky uvedené v právní úpravě pro služby vytvářející důvěru, resp. v ní odkazovaných technických standardech nebo normách a jsou kontrolovány příslušným technickým a programovým vybavením.

6.1.7 Účely použití klíče (dle rozšíření key usage X.509 v3)

Možnosti použití klíče jsou uvedeny v rozšíření certifikátu TSU systému TSA2.

6.2 Ochrana soukromého klíče a technologie kryptografických modulů

6.2.1 Řízení a standardy kryptografických modulů

Soukromé klíče, sloužící pro vytváření elektronických pečetí vydávaných časových razítek, jsou uloženy v kryptografickém modulu, který splňuje požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a je používán v souladu s jeho certifikací.

6.2.2 Soukromý klíč pod kontrolou více osob (n z m)

Pokud je pro činnosti spojené s kryptografickým modulem nezbytná přítomnost více osob, pak každá z nich zná část pouze kódu k provedení těchto činností.

6.2.3 Úschova soukromého klíče

Není relevantní pro tento dokument.

6.2.4 Zálohování soukromého klíče

Soukromý klíč TSU systému TSA2 chráněný kryptografickým modulem je zálohován v zašifrované podobě, která zajišťuje stejnou úroveň ochrany jako kryptografické zařízení. Postup je popsán interní dokumentací:

- „Správa TSS“.

6.2.5 Uchovávání soukromého klíče

Soukromý klíč TSU systému TSA2 není nikde uchováván, po uplynutí doby platnosti je včetně záloh zničen. Postup je popsán interní dokumentací:

- „Správa TSS“.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Soukromý klíč TSU systému TSA2 je generován v kryptografickém modulu (jako neexportovatelný) a nelze jej z kryptografického modulu (provozovaného v certifikovaném režimu) exportovat v žádném tvaru[2]. Import soukromého klíče CA do kryptografického modulu není prováděn.

[2] Výjimkou je zašifrovaná záloha, kterou lze použít pouze v kryptografickém modulu (resp. v HA/LB modulech), kde byl klíč vygenerován.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče TSU systému TSA2 se v otevřeném tvaru nacházejí pouze v kryptografickém modulu splňujícím požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a je používán v souladu s jeho certifikací.

6.2.8 Postup aktivace soukromého klíče

Aktivace soukromého klíče TSU systému TSA2 vygenerovaného v kryptografickém modulu je prováděna pracovníkem v důvěryhodné roli Security Officer(1) výběrem příslušného profilu. O provedené aktivaci je pořízen písemný záznam. Postup je popsán interní dokumentací:

- „Správa TSS“.

6.2.9 Postup deaktivace soukromého klíče

Deaktivace původního soukromého klíče TSU systému TSA2 je provedena výběrem nového profilu. Postup je popsán interní dokumentací:

- „Správa TSS“.

6.2.10 Postup ničení soukromého klíče

Soukromé klíče TSU systému TSA2 jsou uloženy v kryptografickém modulu. Jejich ničení spočívá v bezpečném rušení bezpečně a certifikovaně šifrované adresářové struktury.

6.2.11 Hodnocení kryptografických modulů

Kryptografický modul TSU systému TSA2 splňuje požadavky standardů ETSI a CEN.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

Veřejné klíče, sloužící k ověřování elektronických pečetí vydávaných časových razítek, jsou obsaženy v certifikátech relevantních TSU. Tyto certifikáty jsou uchovávány za celou dobu existence I.CA.

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

Doba platnosti certifikátu TSU systému TSA2 je uvedena v těle tohoto certifikátu a je stejná jako doba použitelnosti párových dat. Po této době lze data pro ověřování elektronických pečetí použít bez záruky.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data TSU systému TSA2 jsou vytvářena v průběhu inicializace příslušného kryptografického modulu.

6.4.2 Ochrana aktivačních dat

Aktivační data TSU systému TSA2 jsou uložena na čipové kartě.

6.4.3 Ostatní aspekty aktivačních dat

Není relevantní pro tento dokument.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování služeb vytvářejících důvěru je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů a jejich periodicity, definována právní úpravou pro služby vytvářející důvěru, resp. v ní odkazovanými technickými standardy a normami. Detailní řešení specifických technických požadavků počítačové bezpečnosti a jejich řešení je popsáno v interní dokumentaci:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Řízení fyzického přístupu do místností I.CA“,
- „Zálohování dat provozních systémů“,
- „Příručka administrátora“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Správa TSS“,
- „Správa TSMC“,
- „Plán pro zvládání krizových situací a plán obnovy“.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti I.CA je založeno na požadavcích uvedených v technických standardech a normách, zejména:

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 421 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající časová razítka.

- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ČSN ETSI EN 319 422 Elektronické podpisy a infrastruktury (ESI) - Protokol pro vyznačení času a profily časového razítka.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 403-1 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatele důvěryhodné služby – Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodné služby.
- ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- ČSN ETSI EN 319 411-1 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 1: Obecné požadavky.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 2: Požadavky na poskytovatele důvěryhodných služeb vydávající kvalifikované certifikáty EU.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ČSN EN 419 221-5 Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografický modul pro důvěryhodné služby.
- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services.
- ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.
- ČSN EN ISO/IEC 15408-2 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty.
- ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.
- ČSN EN ISO/IEC 15408-3 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk.
- ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.
- FIPS PUB 140-2 Requirements for Cryptographic Modules.

- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ČSN EN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti.
- ISO/IEC 17021 Conformity assessment - Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment - Requirements for bodies certifying products, processes and services.
- EN 301 549 Accessibility requirements for ICT products and services.
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací:

- „Změnové řízení“,
- „Metodika vývoje“.

6.6.2 Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu s technickými standardy a normami, je prováděna v rámci periodických kontrol služeb vytvářejících důvěru a dále formou auditů systému řízení bezpečnosti informací (ISMS).

Bezpečnost informací se v I.CA řídí těmito normami:

- ČSN EN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.
- ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky.
- ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti.

Problematika je popsána interní dokumentací:

- „Kontrolní činnost, bezúhonnost a odbornost”.

6.6.3 Řízení životního cyklu bezpečnosti

Řízení životního cyklu bezpečnosti je v I.CA prováděno procesním přístupem typu „techniky – Požadavky“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování – stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou,
- implementace a provoz – účelné a systematické prosazení vybraných bezpečnostních opatření,

- monitorování a přehodnocování – zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení společnosti k posouzení,
- údržba a zlepšování – provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení společnosti.

6.7 Řízení bezpečnosti sítě

Důvěryhodné systémy určené k podpoře Služby, umístěné na provozních pracovištích I.CA nebo v lokalitě, kde jsou umístěny systémy pro pracoviště eSeL, nejsou přímo dostupné z veřejné sítě Internet. Tyto systémy jsou chráněny komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System).

Pokud jsou důvěryhodné systémy určené k podpoře Služby umístěny mimo prostory I.CA, je garantován výhradní přístup pracovníků I.CA.

Podrobný popis správy bezpečnosti sítě je uveden v interní dokumentaci:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Příručka administrátora“,
- „Firewall – provozní pracoviště“,
- „Plán pro zvládání krizových situací a plán obnovy“
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“.

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7 PROFIL CERTIFIKÁTU TSU, STRUKTURA ŽÁDOSTI O ČASOVÉ RAZÍTKO, ODPOVĚDI NA ŽÁDOST A ČASOVÉHO RAZÍTKA

Základní položky certifikátu TSU a struktury jsou uvedeny v Politice. Podrobný popis profilu certifikátu TSU je uveden v dokumentu Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA), dostupném na internetové adrese I.CA.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

V I.CA jsou prováděna hodnocení bezpečnosti, jejichž součástí je mimo jiné sledování, zda jsou plně dodržovány standardy, uvedené v kapitole 6.5.2. Oblasti hodnocení jsou upraveny interní dokumentací:

- „Kontrolní činnost, bezúhonnost a odbornost“.

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

8.1 Periodicita nebo okolnosti hodnocení

Periodicita hodnocení, včetně okolností pro provádění hodnocení, je dána právní úpravou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, dle kterých je hodnocení prováděno.

Periodicita jiných hodnocení je dána příslušnými technickými standardy a normami.

8.2 Identita a kvalifikace hodnotitele

Identita (akreditovaný subjekt posuzování shody) a kvalifikace hodnotitele provádějícího hodnocení podle právní úpravy pro služby vytvářející důvěru, je dána touto právní úpravou a jí odkazovanými technickými standardy a normami.

Kvalifikace hodnotitele provádějícího jiná hodnocení je dána příslušnými technickými standardy a normami.

8.3 Vztah hodnotitele k hodnocenému subjektu

V případě interního hodnotitele platí, že tento není ve vztahu podřízenosti vůči organizační jednotce, která zajišťuje provoz služeb vytvářejících důvěru.

V případě externího hodnotitele platí, že se jedná o subjekt, který není s I.CA majetkově ani personálně svázán.

8.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného právní úpravou pro služby vytvářející důvěru jsou hodnocené oblasti konkretizovány touto právní úpravou, v ostatních případech jsou hodnocené oblasti dány technickými standardy a normami, podle kterých je hodnocení prováděno.

8.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manažer I.CA, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat Službu přeruší I.CA tuto službu do doby, než budou tyto nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům právní úpravy pro služby vytvářející důvěru a příslušných technických standardů a norem.

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

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

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo časových razítek

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

9.1.2 Poplatky za přístup k certifikátům poskytovatele

Přístup k certifikátům CA a TSU systému TSA2 elektronickou cestou I.CA nezpoplatňuje.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) a o stavech jí vydaných certifikátů (OCSP) I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Poplatky za nadstandardní služby jsou stanovovány smluvně.

9.1.5 Postup při refundování

I.CA je oprávněna stanovit pro individuálně uzavřené smlouvy odlišnou výši poplatku za vydání časového razítka.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

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

Společnost První certifikační autorita, a.s., sjednala pro všechny zaměstnance pojištění odpovědnosti za škody způsobené zaměstnavateli v rozsahu, určeném představenstvem společnosti.

9.2.2 Další aktiva

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiná finanční zajištění na poskytování služeb vytvářejících důvěru s ohledem na riziko vzniku odpovědnosti za škodu.

Podrobné informace o aktivech společnosti První certifikační autorita, a.s., je možno získat z Výroční zprávy společnosti První certifikační autorita, a.s., zveřejněné v obchodním rejstříku.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

9.3 Důvěrnost obchodních informací

9.3.1 Rozsah důvěrných informací

Důvěrnými informacemi I.CA jsou veškeré informace, které nejsou označeny jako veřejné a nejsou zveřejňovány způsobem uvedeným v kapitole 2.2, zejména:

- veškeré soukromé klíče, sloužící v procesu poskytování služeb vytvářejících důvěru,
- obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

9.3.2 Informace mimo rámec důvěrných informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kapitole 2.2.

9.3.3 Odpovědnost za ochranu důvěrných informací

Žádný zaměstnanec I.CA, který přijde do styku s důvěrnými informacemi, je nesmí bez souhlasu generálního ředitele I.CA poskytnout třetí straně.

9.4 Ochrana osobních údajů

Problematika je podrobně popsána interní dokumentací:

- „Ochrana osobních údajů v I.CA“,
- „Řízení bezpečnosti informací“.

9.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných právních předpisů, tedy zejména ZOOÚ a GDPR.

9.4.2 Informace považované za osobní údaje

Osobními údaji jsou veškeré údaje podléhající ochraně ve smyslu příslušných právních předpisů.

Zaměstnanci I.CA, případně subjekty definované platnou právní úpravou přicházející do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního, nebo jiného obdobného poměru, nebo po provedení příslušných prací.

9.4.3 Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které nespadají do působnosti příslušných právních předpisů.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný generální ředitel I.CA.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Problematika oznamování o používání osobních údajů a souhlasu s jejich zpracováním je v I.CA řešena v souladu s požadavky příslušných právních předpisů.

9.4.6 Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů pro soudní, resp. správní účely je v I.CA řešeno v souladu s požadavky příslušných právních předpisů.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně podle požadavků příslušných právních předpisů.

9.5 Práva duševního vlastnictví

Tato Směrnice, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systémů poskytujících služby vytvářející důvěru jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky autority časových razítek

9.6.1.1 Obecné závazky autority časových razítek

Společnost První certifikační autorita, a.s., zaručuje zejména:

- přístup ke Službě:
  - nepřetržitý, s výjimkou plánovaných (předem ohlášených) časových přerušení spojených s technickými zásahy,
  - za podmínek uvedených v písemné smlouvě,
- autentizovaný přístup ke Službě na základě písemné smlouvy,
- striktní dodržování platné právní úpravy vztahující se k celému procesu vydávání časových razítek, včetně neporušování autorských ani licenčních práv,
- poskytování Služby osobami s odbornými znalostmi a kvalifikací nezbytnou pro poskytování této 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 v právní úpravě pro služby vytvářející důvěru 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 kvalifikovaným poskytovatelem Služby,
- mlčenlivost 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).

9.6.1.2 Závazky autority časových razítek ve vztahu k žadatelům o časová razítka a k jejich držitelům

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

- jí vydávaná časová razítka obsahují všechny náležitosti stanovené právní úpravou pro služby vytvářející důvěru,
- použije soukromé klíče certifikátů CA vydávajících certifikáty pro jednotlivá TSU pouze v procesech vydávání certifikátů pro TSU, pro vydávání jejich OCSP respondérů a pro vydávání seznamů zneplatněných certifikátů,
- použije soukromé klíče OCSP respondérů příslušných CA pouze v procesech poskytování odpovědí na stav certifikátu vydaného touto CA,
- použije soukromé klíče příslušné certifikátům TSU pouze k opatřování vydávaných časových razítek elektronickou pečetí,
- implementovala odpovídající opatření proti padělání časových razítek,
- vydá časové razítko neprodleně po obdržení platného požadavku,
- žádným způsobem neověřuje hash, kterému má být časové razítko přiřazeno (s výjimkou jeho délky),
- využívá důvěryhodnou časovou synchronizaci,
- jí vydaná odpověď na žádost o časové razítko obsahuje minimálně:
  - sériové číslo, které je pro konkrétní TSU systému TSA2 jedinečné,
  - identifikátor politiky, podle níž bylo časové razítko vydáno,
  - časový údaj odpovídající hodnotě koordinovaného světového času (UTC) v době vytváření časového razítka s přesností odpovídající požadavkům relevantních technických standardů (odchylka menší než 1 s, obvykle do 500 ms),
  - data v elektronické podobě obsažená v žádosti o časové razítko (hash dokumentu opatřovaného časovým razítkem),
  - elektronickou pečeť TSU.

9.6.2 Zastupování a záruky RA

Není relevantní pro tento dokument.

9.6.3 Zastupování a záruky žadatele o časové razítko a jeho držitele

Žadatel o časové razítko, resp. jeho držitel ručí za informace, které uvedl ve smlouvě o poskytování časových razítek a postupuje v souladu s právní úpravou pro služby vytvářející důvěru, Politikou a zmíněnou smlouvou.

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

- ověřit platnost elektronické pečetě časového razítka a následně všech certifikátů, vztahujících se k TSU, která tuto elektronickou pečeť vytvořila,
- ověřit, zda vrácený hash je totožný s tím odeslaným v žádosti,
- v případě, že žádost obsahovala položky „nonce“ nebo „reqPolicy“ ověřit, že jejich hodnota v odpovědi je totožná.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s Politikou. Jejich závazkem je zejména:

- ověření platnosti elektronické pečetě časového razítka včetně kontroly odvolání certifikátů v certifikační cestě,
- vzít v úvahu případné omezení použitelnosti časových razítek uvedená v této Politice,
- vzít v úvahu další opatření předepsaná smlouvou.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., poskytuje pouze záruky uvedené v kapitole 9.6.

9.8 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované právní úpravou pro služby vytvářející důvěru a Politikou. Dále neodpovídá za škody vzniklé v důsledku porušení povinností I.CA z důvodu vyšší moci.

9.9 Záruky a odškodnění

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení platné právní úpravy týkající se vztahů mezi poskytovatelem a spotřebitelem a dále takové záruky, které byly sjednány mezi společností První certifikační autorita, a.s., a žadatelem o Službu. Smlouva

nesmí být v rozporu s právní úpravou pro služby vytvářející důvěru a musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak platnou právní úpravou, včetně právní úpravy pro služby vytvářející důvěru, tak příslušnými politikami,
- splní výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služby,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, se kterými má platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo odpovědnosti, s výjimkou případů, kdy poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele,
- 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 o poskytování Služby držitelem časového razítka, zejména za využívání v rozporu s podmínkami uvedenými v Politice,
- za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení.

Reklamaci je možné podat těmito způsoby:

- e-mailem na adresu reklamace@ica.cz,
- prostřednictvím datové schránky I.CA,
- doporučenou poštovní zásilkou na adresu sídla společnosti,
- osobně v sídle společnosti.

Reklamující osoba (držitel časového razítka nebo spoléhající se strana) je povinna uvést:

- co nejvýstižnější popis závady,
- sériové číslo reklamovaného produktu,
- požadovaný způsob vyřízení reklamace.

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

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

Další možné náhrady škody vycházejí z ustanovení příslušné právní úpravy a o jejich výši může rozhodnout soud.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tento dokument nabývá platnosti dnem uvedeným v kapitole 10 a platí do odvolání.

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

Ukončení Služby neznamená neplatnost časového razítka vydaného v době platnosti Politiky.

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

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

Komunikovat s I.CA lze taktéž způsoby uvedenými na internetové informační adrese.

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným interní dokumentací.

9.12.2 Postup a periodicita oznamování

Vydání nové verze Směrnice je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněn OID

OID není přidělen, v případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

9.13 Ustanovení o řešení sporů

V případě, že držitel časového razítka nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

- odpovědný pracovník I.CA (nutné elektronické nebo listinné podání),
- generální ředitel I.CA (nutné elektronické nebo listinné podání).

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

9.14 Rozhodné právo

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

9.15 Shoda s platnými právními předpisy

Systém poskytování služeb vytvářejících důvěru je provozován ve shodě s právními předpisy EU a České republiky a dále s relevantními mezinárodními standardy.

9.16 Různá ustanovení

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto Směrnicí, stanoví, že provádění některého povinného požadavku je protiprávní, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a v souladu s platnou právní úpravou.

9.16.4 Zřeknutí se práv

Není relevantní pro tento dokument.

9.16.5 Vyšší moc

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývajících ze smluvních vztahů s klientem vzniklých na základě zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu, popř. výpadku komunikačního spojení.

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato Směrnice vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem uvedeným v tab. 1.