První certifikační autorita, a.s.

Prováděcí směrnice

vydávání kvalifikovaných časových razítek

(algoritmus RSA)

Verze 1.0

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	07.01.2016	Ředitel společnosti První certifikační autorita, a.s.	První vydání.

1 ÚVOD

Tento dokument, Prováděcí směrnice vydávání kvalifikovaných časových razítek (algoritmus RSA), dále též Směrnice, byl společností První certifikační autorita, a. s., dále též I.CA, vypracován na základě požadavků platné legislativy a zabývá se skutečnostmi vztahujícími se k procesům vydávání a využívání kvalifikovaných časových razítek a je v souladu:

- se zákonem České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů 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), ve znění pozdějších předpisů,
- s aktuálním zněním zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise a s ním spojených prováděcích vyhlášek,
- s doporučeními:
  - ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities,
  - ETSI TS 101 861 Time Stamping Profile,

a je přihlíženo k doporučením orgánů EU a k právu České republiky a Slovenské republiky v dané oblasti.

Pozn.: Pokud jsou v textu uváděny odkazy na standardy nebo zákony, jedná se vždy buď o uvedený standard nebo zákon, resp. o standard či zákon, který ho nahrazuje.

Směrnice rozpracovává a konkretizuje dokument Politika vydávání kvalifikovaných časových razítek (algoritmus RSA) - dále též Politika.

1.1 Přehled

Tato Směrnice je rozdělena do šesti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem.
- Kapitola 2 uvádí seznamy použitých pojmů a zkratek.
- Kapitola 3 základní pojetí služby autority časových razítek, obecně popisuje subjekty, které se na službě podílejí.
- Kapitola 4 popisuje použitelnost vydávaných kvalifikovaných časových razítek a postupy hodnocení shody.
- Kapitola 5 zahrnuje problematiku obchodní a právní, popisuje závazky a odpovědnosti zúčastněných stran.
- Kapitola 6 popisuje postupy autority časových razítek, včetně popisu profilů certifikátů TSU a vydávaných kvalifikovaných časových razítek.

Podrobný popis procesů 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 tab. 2 jsou uvedeny významné interní dokumenty, vztahující se k certifikačním službám v oblasti kvalifikovaných časových razítek.

tab. 2 - Relevantní interní dokumenty

Číslo	Název dokumentu	Status
1.	Politika vydávání kvalifikovaných časových razítek (algoritmus RSA)	veřejný
2.	Prováděcí směrnice vydávání kvalifikovaných časových razítek (algoritmus RSA) - tento dokument	veřejný
3.	Analýza rizik, Závěrečná zpráva - kvalifikované certifikační služby	neveřejný
4.	Prohlášení o aplikovatelnosti - kvalifikované certifikační služby	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 interních směrnic	neveřejný
9.	Celková bezpečnostní politika	neveřejný

V procesu poskytování kvalifikovaných certifikačních služeb v oblasti vydávání kvalifikovaných časových razítek provozuje společnost První certifikační autorita, a.s., jediný systém TSA skládající se z jednotlivých serverů TSU.

1.2 Název a identifikace dokumentu

Název tohoto dokumentu: Prováděcí směrnice vydávání kvalifikovaných časových razítek (algoritmus RSA)

OID: není přiřazeno

2 PŘEHLED POUŽITÝCH POJMŮ A ZKRATEK

Dále uvedený přehled pojmů a zkratek 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.

2.1 Použité pojmy

tab. 3 - 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)
elektronický podpis	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě
elektronická značka	údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky: ▪ jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, ▪ byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, ▪ jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat
hash	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou
klient	žadatel o kvalifikované 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 - má náležitosti podle platné legislativy
kvalifikovaný certifikát, kvalifikovaný systémový certifikát, nadřízený	certifikát, který má náležitosti podle platné legislativy

kvalifikovaný systémový certifikát, certifikát poskytovatele, certifikát pro správu	
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
párová data	jedinečná data pro vytváření elektronické značky/podpisu spolu s odpovídajícími daty pro ověřování elektronické značky/podpisu
písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
smluvní partner	poskytovatel vybraných certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části - nejčastěji se jedná o smluvní RA
soukromý klíč	jedinečná data pro vytváření elektronické značky/podpisu
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 elektronické značky/podpisu
zákon o ochraně utajovaných informací	zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
žadatel o kvalifikované časové razítko	individuální koncový uživatel (fyzická osoba), právnická osoba nebo organizační složka státu (zahrnující několik koncových uživatelů), resp. systém, provozovaný výše zmíněnými subjekty

2.2 Zkratky

tab. 4 - Zkratky

Pojem	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
CWA	CEN Workshop Agreement, referenční dokument CEN
ČR	Česká republika
ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátu
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace

ESI	Electronic Signatures and Infrastructures
ETSI	the European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EZS	elektronický zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
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
I.CA	První certifikační autorita, a.s., akreditovaný poskytovatel certifikačních služeb
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IP	Internet Protocol, komunikační protokol síťové vrstvy
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
MV ČR	Ministerstvo vnitra České republiky
NIST	National Institute of Standards and Technology, laboratoř měřících standardů při ministerstvu obchodu USA
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)
Sb.	Sbírka zákonů
SHA	typ hashovací funkce

TS	Technical Specification, typ ETSI standardu
TSA	Time Stamping Authority, autorita časových razítek, obsahující více serverů, vydávajících časová razítka, kdy každý z nich disponuje jedinečným soukromým klíčem a odpovídajícím certifikátem
TSS	Time Stamp Service, služba časových razítek
TSU	Time Stamp Unit, server vydávající časová razítka
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
UTC	Universal Co-ordinated 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)
ZoEP	▪ zákon České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů ▪ zákon Slovenské republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov, ve znění pozdějších předpisů
ZOOÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů), ve znění pozdějších předpisů
Z.z.	Zbierka zákonov

3 ZÁKLADNÍ POJETÍ

3.1 Služby autority časových razítek (TSA)

Služby autority časových razítek, provozovaných společností První certifikační autorita, a.s., zahrnující oblasti vytváření a vydávání kvalifikovaných časových razítek a implementaci autentizace žadatelů o kvalifikovaná časová razítka, jsou poskytovány v souladu s relevantní legislativou a technickými standardy.

3.2 Autorita časových razítek

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

3.3 Žadatelé o kvalifikované časové razítko

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

3.4 Spoléhající se strana

Spoléhající se stranou jsou v případě této Směrnice subjekty spoléhající se při své činnosti na kvalifikovaná časová razítka vydávaná podle této směrnice a odpovídající politiky.

4 POLITIKA TSA

4.1 Použití kvalifikovaných časových razítek

Tato Směrnice nedefinuje žádná omezení použitelnosti kvalifikovaného časového razítka, vydaného v souladu s jejím obsahem[1], resp. s obsahem jí odpovídající Politiky. Časová razítka je možné použít např. v oblastech:

- elektronických značek/podpisů, 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.

4.2 Hodnocení shody a jiná hodnocení

V I.CA jsou prováděna hodnocení bezpečnosti v oblastech, uvedených v kapitole 4.2.4. Součástí těchto hodnocení je mimo jiné sledování, zda jsou plně dodržovány standardy, uvedené v kapitole 6.4.7.2. Oblasti hodnocení jsou upraveny interním dokumentem:

- „Kontrolní činnost, bezúhonnost a odbornost“.

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

4.2.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Periodicita hodnocení systému řízení bezpečnosti informací a kontroly bezpečnostní shody, je dána požadavky ZoEP a standardy ETSI.

4.2.2 Identita a kvalifikace hodnotitele

Kvalifikace auditora provádějícího hodnocení podle ZoEP, je dána tímto zákonem, resp. jím odkazovanými technickými standardy.

4.2.3 Vztah hodnotitele k hodnocenému subjektu

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

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

4.2.4 Hodnocené oblasti

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

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

4.2.5 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 konkrétní certifikační službu, přeruší I.CA tuto službu, než budou tyto nedostatky odstraněny.

4.2.6 Sdělování výsledků hodnocení

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

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

Sdělování výsledků hodnocení taktéž podléhá požadavkům příslušných standardů, dle kterých je hodnocení prováděno.

5 ZÁVAZKY A ODPOVĚDNOSTI

5.1 Závazky TSA

5.1.1 Obecné závazky TSA

Společnost První certifikační autorita, a.s., zaručuje 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 kvalifikovaných časových razítek na základě písemné smlouvy,
- striktní dodržování platné legislativy vztahující se k celému procesu vydávání kvalifikovaných 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 v platné legislativě a s ohledem na riziko vzniku odpovědnosti za škodu po celou dobu své činnosti,
- písemné informování žadatele o vydávání kvalifikovaných 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).

5.1.2 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 kvalifikovaná časová razítka obsahují všechny náležitosti stanovené platnou legislativou,

- použije soukromé klíče certifikátů CA vydávajících certifikáty pro jednotlivá TSU pouze v procesech vydávání certifikátů pro TSU a koncové uživatele 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 elektronickému označování/podepisování vydávaných kvalifikovaných časových razítek,
- implementovala odpovídající opatření proti padělání kvalifikovaných časových razítek,
- vydá kvalifikované časové razítko neprodleně po obdržení platného požadavku,
- žádným způsobem neověřuje hash, kterému má být kvalifikované časové razítko přiřazeno (s výjimkou jeho délky),
- využívá důvěryhodnou časovou synchronizaci,
- jí vydané odpověď na žádost o kvalifikované časové razítko obsahuje minimálně:
  - sériové číslo, které je pro konkrétní TSU systému TSA jedinečné,
  - identifikátor politiky, pod níž bylo kvalifikované časové razítko vydáno,
  - časový údaj odpovídající hodnotě koordinovaného světového času (UTC) v době vytváření kvalifikovaného časového razítka s přesností jedna sekunda,
  - data v elektronické podobě obsažená ve vydaném kvalifikovaném časovém razítku, odpovídající datům v elektronické podobě, obsažených v žádosti o vydání kvalifikovaného časového razítka,
  - elektronickou značku/podpis TSU.

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

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.

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

- ověřit platnost elektronické značky/podpisu kvalifikovaného časového razítka a následně všech certifikátů, vztahujících se k TSU, který tuto elektronickou značku/podpis vytvořil,
- ověřit, zda vrácený 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.

5.3 Závazky spoléhajících se stran

Spoléhající se strany postupují v souladu s touto Směrnicí a odpovídající Politikou..

Závazkem spoléhajících se stran je ověření zejména platnosti elektronické značky/podpisu.

5.4 Odpovědnost

Platí vždy takové záruky, které byly sjednány mezi společností První certifikační autorita, a.s., a žadatelem o poskytování služby dle této Politiky. Smlouva nesmí být v rozporu s platnou legislativou a musí být vždy v písemné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak příslušnými právními předpisy, tak příslušnými certifikačními politikami a touto Směrnicí, resp. odpovídající Politikou,
- splní výše uvedené závazky po celou dobu platnosti smlouvy o poskytování služby,
- 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 vzniklé z důvodu nesprávného nebo neoprávněného využívání poskytovaných služeb v rozporu s touto Směrnicí, resp. odpovídající Politikou, a příslušnými certifikačními politikami,
- za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.).

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 je povinna uvést co nejvýstižnější popis závad a jejich projevů.

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.

6 POŽADAVKY NA POSTUPY TSA

6.1 Správa politiky

6.1.1 Organizace spravující politiku TSA nebo prováděcí směrnici TSA

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

6.1.2 Kontaktní osoba organizace spravující politiku TSA nebo prováděcí směrnici TSA

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s touto Směrnicí, resp. s odpovídající Politikou, je uvedena na internetové adrese viz kap. 6.4.13.3.2.

6.1.3 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.

6.1.4 Postupy při schvalování souladu s bodem 7.1.3

V případě, že je potřebné provést změny v této Směrnici s ohledem na soulad dle kap. 6.1.3 a vytvořit její novou verzi, určuje ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Detailní řešení je popsáno v interním dokumentu:

- „Změnové řízení“.

Nabytí platnosti nové verze Směrnice předchází její schválení ředitelem společnosti První certifikační autorita, a.s. Dále platí požadavky kap. 6.5.8.1.

6.2 Požadavky na životní cyklus párových dat TSA

Uvedeno v dokumentu Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA).

6.2.1 Generování a instalace párových dat

6.2.1.1 Generování párových dat

Generování párových dat TSU systému TSA probíhá v zabezpečené oblasti a je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 úroveň 3. Konkrétní technický postup generování párových dat, sloužících k elektronickému označování/podepisování vydávaných kvalifikovaných časových razítek je popsán v interních dokumentech:

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

O generování je pořízen písemný záznam obsahující mj.:

- jmenný seznam přítomných pracovníků s uvedením jména, příjmení a titulu, včetně jejich podpisu,
- datum a čas zahájení a ukončení generování párových dat s přesností minimálně na minuty,
- místo, kde ke generování párových dat došlo,
- popis zařízení, na kterém bylo generování prováděno, umožňující jednoznačnou identifikaci tohoto zařízení.

6.2.1.2 Poskytování veřejných klíčů

Veřejné klíče, sloužící pro ověřování elektronických značek/podpisů vydávaných kvalifikovaných 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 MV ČR.

6.2.1.3 Délky párových dat

Systém TSA používá asymetrický šifrový algoritmus RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) použitých pro označování/podepisování vydávaných kvalifikovaných časových razítek je minimálně 2048 bitů.

6.2.2 Ochrana soukromého klíče (dat pro vytváření elektronických značek/podpisů)

6.2.2.1 Standardy a podmínky používání kryptografických modulů

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

6.2.2.2 Zálohování soukromých klíčů

Kryptografický modul použitý pro správu dat, sloužících pro vytváření elektronických značek/podpisů vydávaných kvalifikovaných časových razítek, umožňuje jejich zálohování. Záloha je prováděna s využitím jeho nativních prostředků v zašifrované podobě. Konkrétní postup je popsán v interním dokumentu:

- „Správa TSS“.

6.2.2.3 Uchovávání soukromých klíčů

Po uplynutí doby platnosti soukromých klíčů, určených k elektronickému označování/podepisování vydávaných kvalifikovaných časových razítek, jsou tyto klíče včetně jejich záloh zničeny. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, proto je v I.CA zakázáno. Konkrétní postup je popsán v interním dokumentu:

- „Správa TSS“.

6.2.2.4 Transfer soukromých klíčů

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

Vkládání soukromých klíčů, sloužících k vytváření elektronických značek/podpisů vydávaných kvalifikovaných časových razítek, do kryptografického modulu konkrétního TSU v případě, že se jedná o nahrání těchto klíčů ze šifrované zálohy je písemně zaprotokolováno a podepsáno určenými pracovníky I.CA. V okamžiku vkládání dat musí být TSU odpojen od počítačové sítě.

6.2.2.5 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.

6.2.2.6 Aktivační data

Aktivační data jsou vytvářena v průběhu procesu instalace TSU.

6.2.2.7 Postup při aktivaci soukromých klíčů

Aktivaci soukromých klíčů, sloužících k vytváření elektronických značek/podpisů vydávaných kvalifikovaných časových razítek, vygenerovaných v kryptografického modulu relevantního TSU, provádí určení pracovníci I.CA. Konkrétní postup je popsán v interním dokumentu:

- „Správa TSS“.

O provedení aktivace soukromých klíčů je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

6.2.2.8 Postup při deaktivaci soukromých klíčů

Deaktivaci soukromých klíčů, sloužících pro vytváření elektronických značek/podpisů vydávaných kvalifikovaných časových razítek, provádí určení pracovníci I.CA. Konkrétní postup je popsán v interním dokumentu:

- „Správa TSS“.

O provedení deaktivace těchto soukromých klíčů je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

6.2.2.9 Postup při ničení soukromých klíčů

Soukromé klíče, sloužící k označování/podepisování vydávaných kvalifikovaných časových razítek, jsou uloženy 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.

6.2.2.10 Uchovávání veřejných klíčů

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

6.2.3 Profil certifikátu

Základní popis profilu certifikátu TSU systému TSA je uveden v Politice. Podrobný popis profilu certifikátu TSU systému TSA je uveden v dokumentu Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA), dostupném na internetové adrese I.CA. Certifikáty jednotlivých TSU lze získat na stránkách I.CA nebo MV ČR.

6.2.4 Výměna párových dat

Platnost certifikátu TSU systému TSA je uvedena v tomto certifikátu. Platnost párových dat (veřejný a soukromý klíč) pro tvorbu elektronické značky/podpisu, resp. ověřování elektronické značky/podpisu kvalifikovaných 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 značky/podpisu kvalifikovaného časového razítka. Před koncem tohoto období jsou vygenerována nová párová data a vydán certifikát příslušného veřejného klíče. K tvorbě elektronické značky/podpisu kvalifikovaných časových razítek je dále využíván nejnovější soukromý klíč. Veřejné klíče, staré i nejnovější, jsou využívány k ověřování elektronických značek/podpisů vytvořených odpovídajícím soukromým klíčem.

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

Procesy výměny dat pro ověřování dat elektronických značek/podpisů podpisů v certifikátu relevantního TSU jsou podrobně popsány v interním dokumentu:

- „Správa TSS“.

6.2.5 Ukončení životního cyklu párových dat

Doba platnosti certifikátu TSU systému TSA je uvedena v těle tohoto certifikátu. Po této době lze data pro ověřování elektronických značek/podpisů použít bez záruky.

Pokud dojde k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu vydávání kvalifikovaných časových razítek, bude doba platnosti párových dat zkrácena.

6.2.5.1 Zneplatnění a pozastavení platnosti certifikátu

6.2.5.1.1 Seznam zneplatněných certifikátů

Profil seznamu zneplatněných certifikátů odpovídá mezinárodně uznávaným normám a standardům.

6.2.5.1.2 Podmínky pro zneplatnění certifikátu

Certifikát TSU může být zneplatněn pouze na základě následujících okolností:

- nastanou-li skutečnosti uvedené v platné legislativě,
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek/podpisů, používaných k vytváření elektronické značky/podpisu vydávaných certifikátů a seznamů zneplatněných certifikátů,
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek/podpisů konkrétního TSU.

6.2.6 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 kvalifikovaných časových razítek nebo ukončení činnosti I.CA, jsou data pro vytváření elektronických značek/podpisů generovaných kvalifikovaných časových razítek zničena dle doporučení výrobce. Konkrétní postupy správy TSU jsou popsány v interním dokumentu:

- „Správa TSS“.

6.2.6.1 Hodnocení kryptografického modulu

Kryptografický modul, sloužící pro elektronické označování/podepisování vydávaných kvalifikovaných časových razítek, splňuje požadavky na kryptografické moduly FIPS 140-2 úroveň 3.

6.3 Vydávání kvalifikovaných časových razítek

6.3.1 Uzavření smlouvy

Vydávání kvalifikovaných 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 této Směrnice, resp. odpovídající Politiky.

6.3.2 Zpracování žádosti o kvalifikované časové razítko

6.3.2.1 Identifikace a autentizace

S ohledem na komerční bázi a nadstandardní služby v procesu vydávání kvalifikovaných časových razítek je proces identifikace a autentizace žadatele o kvalifikované časové razítko realizován jedním z níže uvedených způsobů:

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

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

6.3.2.2 Přijetí nebo zamítnutí žádosti o kvalifikované časové razítko

Žadatel o vydání kvalifikovaného 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 kvalifikované časové razítko (v normovaném formátu dle RFC 3161). Takto vytvořená datová struktura je předána systému TSA. V případě, že žádost nesplňuje požadavky této Směrnice, resp. příslušné Politiky, je systémem TSA zamítnuta.

6.3.2.3 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 kvalifikované časové razítko, neboť se jedná časový sled následujících činností, z nichž některé záleží pouze na elektronickém přenosu žádosti od žadatele o kvalifikované časové razítko k systému TSA. Přibližné časové údaje jsou uvedeny v následujícím seznamu:

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

6.3.3 Vydání kvalifikovaného časového razítka

6.3.3.1 Úkony TSA v průběhu vydávání kvalifikovaného časového razítka

Systém TSA provádí veškeré kontroly formální správnosti žádosti o kvalifikované časové razítko a na základě jejich výsledku vytvoří konkrétní TSU odpověď, obsahující stav odpovědi a v případě kladného výsledku kontrol i kvalifikované časové razítko (viz RFC 3161). Časový údaj (UTC) je získán z měřidla důvěryhodného času. Kvalifikované časové razítko je elektronicky označeno/podepsáno daty pro vytváření elektronické značky/podpisu konkrétního TSU s využitím algoritmu Sha256WithRSAEncryption (tím se tento server nezpochybnitelným způsobem zaručuje za správnost informací uvedených ve vydaném kvalifikovaném časovém razítku).

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

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

Poté, co byly provedeny činnosti, uvedené v kapitole 6.3.3.1, je výše uvedená datová struktura (s případnou doplňující zprávou) odeslána systémem TSA zpět žadateli.

6.3.4 Převzetí kvalifikovaného časového razítka

6.3.4.1 Žadatel o kvalifikované časové razítko

Po obdržení výše uvedené datové struktury je žadatel povinen zjistit stav odpovědi. Obsahuje-li odpověď kvalifikované časové razítko, je žadatel povinen postupovat v souladu s kapitolou 5.2.

6.3.4.2 Spoléhající se strana

Spoléhající se strana je povinna postupovat v souladu s kapitolou 5.3.

6.3.5 Ukončení poskytování služeb pro žadatele o kvalifikované časové razítko

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

6.3.6 Struktury žádosti, odpovědi a kvalifikovaného časového razítka

6.3.6.1 Struktura žádosti o kvalifikované časové razítko

Struktura žádosti o kvalifikované časové razítko je popsána v dokumentu Politika.

Pokud dojde k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost tvorby hash v žádosti o kvalifikované časové razítko - viz položka HashAlgorithm v žádosti, vyhrazuje si I.CA právo tento algoritmus nepodporovat a danou žádost odmítnout. Informace o nepodporovaných algoritmech bude I.CA zveřejňovat prostřednictvím své internetové adresy.

6.3.6.2 Struktura odpovědi na žádost o kvalifikované časové razítko

Struktury odpovědi na žádost o kvalifikované časové razítko a kvalifikovaného časového razítka jsou popsány v dokumentu Politika.

6.3.7 Synchronizace měřidla času s UTC

6.3.7.1 Synchronizace

Synchronizace měřidla času s důvěryhodným zdrojem UTC je prováděna jednou denně. Pro synchronizaci a kontrolu časového údaje, vkládaného do vydávaných kvalifikovaných časových razítek, je využíváno 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 popsána interní dokumentací.

6.3.7.2 Bezpečnost měřidla času

Měřidlo času je umístěno v prostorách I.CA a jeho zabezpečení je popsáno v interních dokumentech:

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

6.3.7.3 Detekce odchýlení měřidla času

Detekce odchýlení měřidla času od synchronizačního zdroje UTC je obsahem výše uvedeného komerčního řešení, založeného na modelu důvěryhodné synchronizační časové infrastruktury.

6.3.7.4 Přestupná sekunda

Výskyt přestupné vteřiny je obsahem výše uvedeného komerčního řešení, založeného na modelu důvěryhodné synchronizační časové infrastruktury.

6.4 Správa a provozní bezpečnost TSA

6.4.1 Řízení bezpečnosti

Řízení bezpečnosti ve společnosti První certifikační autorita, a.s., je popsáno v interních dokumentech:

- „Řízení bezpečnosti informací“,
- „Bezpečnostní incidenty“.

6.4.2 Hodnocení a řízení rizik

V I.CA byly provedeny následující činnosti:

- identifikace 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.

Problematikou hodnocení a řízení rizik se zabývají interní dokumenty:

- „Systémová bezpečnostní politika TSA“,

- „Kontrolní činnost, bezúhonnost a odbornost“,
- „Bezpečnostní incidenty“.

6.4.3 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 s certifikačními službami je popsáno v interní dokumentaci uvedené v 6.4.2.

6.4.4 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

6.4.5 Personální bezpečnost

6.4.5.1 Důvěryhodné role

Pro vybrané činnosti jsou v I.CA definovány důvěryhodné role, které jsou spolu s odpovídajícími činnostmi a odpovědnostmi popsány v interních dokumentech:

- „Systémová bezpečnostní politika TSA“,
- „Řízení bezpečnosti informací“.

6.4.5.2 Počet osob požadovaných na zajištění jednotlivých činností

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

- generování párových dat TSU systému TSA,
- ničení dat pro vytváření elektronické značky/podpisu vydávaných kvalifikovaných časových razítek,
- zálohování/obnova dat pro vytváření elektronické značky/podpisu každého TSU systému TSA.

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

6.4.5.3 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.

6.4.5.4 Role vyžadující rozdělení povinností

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

6.4.5.5 Požadavky na kvalifikaci, zkušenost a bezúhonnost

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

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

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

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

Problematika je detailně popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost".

6.4.5.6 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.

6.4.5.7 Požadavky na přípravu pro výkon role, vstupní školení

Zaměstnanci 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.

Problematika je detailně popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost".

6.4.5.8 Požadavky a periodicita školení

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

Problematika je detailně popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost".

6.4.5.9 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.

6.4.5.10 Postihy za neoprávněné činnosti zaměstnanců

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

6.4.5.11 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, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

6.4.5.12 Dokumentace poskytovaná zaměstnancům

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

6.4.6 Fyzická bezpečnost a bezpečnost prostředí

Problematika fyzické bezpečnosti je detailně popsána v interních dokumentech:

- „Řízení fyzického přístupu do místností I.CA",
- „Požární bezpečnost",
- „Obnova komponenty provozního pracoviště",
- „Přemístění provozního pracoviště".

6.4.6.1 Umístění a konstrukce

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

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

6.4.6.2 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 snímání, přenos a zobrazování pohybu osob a dopravních prostředků.

6.4.6.3 Elektřina a klimatizace

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

6.4.6.4 Vliv vody

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

6.4.6.5 Protipožární opatření a ochrana

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

6.4.6.6 Ukládání médií

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

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

6.4.6.7 Nakládání s odpady

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

6.4.6.8 Zálohy mimo budovu provozního pracoviště

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

6.4.7 Provozní řízení

6.4.7.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování certifikačních služeb je definována technickými standardy. Role přímo se podílející na generování párových dat a vydávání certifikátu TSU systému TSA používají dvoufaktorovou autentizaci.

Detailní řešení specifických technických požadavků počítačové bezpečnosti a jejich řešení je popsáno v interních dokumentech:

- „Systémová bezpečnostní politika TSA“,
- „Řízení fyzického přístupu do místností I.CA“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Příručka administrátora“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Správa TSS“,
- „Plán pro zvládání krizových situací a plán obnovy“.

6.4.7.2 Hodnocení počítačové bezpečnosti

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

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements /Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis - část 1: Požadavky na bezpečnost systémů.
- ČSN ETSI TS 102 023 – Elektronické podpisy a infrastruktury; Požadavky na postupy autorit časových razítek.
- ČSN ETSI TS 101 456 Elektronické podpisy a infrastruktury - Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty.
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 2: Požadavky politiky na certifikační autority vydávající kvalifikované certifikáty.
- ČSN ETSI EN 319 411-3 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 3: Požadavky politiky na certifikační autority vydávající certifikáty veřejného klíče.
- ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
- ISO/IEC 17021 Conformity assessment - Requirements for bodies providing audit and certification of management systems.

6.4.8 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 interních dokumentech:

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

6.4.9 Vývoj a údržba důvěryhodných systémů

6.4.9.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interními dokumenty:

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

6.4.9.2 Kontroly řízení bezpečnosti

Soulad se standardy (viz kap. 6.4.7.2) je ověřován pravidelnými audity systému řízení bezpečnosti informací, prováděnými auditory kvalifikovanými v souladu s relevantními technickými standardy. Problematika je popsána v interním dokumentu:

- „Kontrolní činnost, bezúhonnost a odbornost”.

6.4.9.3 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.

6.4.10 Obnova po havárii nebo kompromitaci

6.4.10.1 Postup v případě incidentu a kompromitace

Postupy jsou popsány v interních dokumentech:

- „Plán pro zvládání krizových situací a plán obnovy“,
- „Bezpečnostní incidenty“,
- „Obnova komponenty provozního pracoviště“,

- „Přemístění provozního pracoviště“.

6.4.10.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz předchozí kapitola.

6.4.10.3 Postup při zjištění odchýlení měřidla času

Postup synchronizace časového údaje měřidla času je uveden v kapitole 6.3.7. 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 tímto TSU poskytována. Problematika je popsána v interním dokumentu:

- „Správa TSS“.

6.4.10.4 Postup při kompromitaci soukromého klíče TSA

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

- okamžitě 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 klienty služby vydávání kvalifikovaných 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 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.

6.4.10.5 Schopnosti obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interními dokumenty:

- „Plán pro zvládání krizových situací a plán obnovy“,
- „Bezpečnostní incidenty“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“.

6.4.11 Ukončení činnosti TSA

Pro ukončování činnosti TSA platí následující pravidla:

- ukončení činnosti musí být písemně oznámeno všem subjektům, které mají uzavřenou písemnou smlouvu a dozorovému orgánu,
- ukončení činnosti musí být zveřejněno na internetové adrese,
- dokumentované zničení soukromých klíčů TSU.

6.4.12 Shoda s právními předpisy

Systém TSA je provozován ve shodě s legislativními požadavky a dále s relevantními mezinárodními standardy.

6.4.13 Úložiště informací a dokumentace, které se týkají provozu TSA

6.4.13.1 Auditní záznamy (logy)

Zásady vytváření, zpracování a uchovávání auditních logů jsou popsány v interních dokumentech:

- „Systémová bezpečnostní politika TSA“,
- „Řízení fyzického přístupu do místností I.CA“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Příručka administrátora“,
- „Správa TSS“.

6.4.13.1.1 Typy zaznamenávaných událostí

S ohledem na požadavky:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements,
- ETSI TS 102 023 - Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities,
- ZoEP,

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 kvalifikovaná 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.

6.4.13.1.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interním dokumentu:

- „Příručka administrátora“,

v případě bezpečnostního incidentu okamžitě.

6.4.13.1.3 Doba uchovávání auditních záznamů

Nestanoví-li relevantní legislativní norma jinak, jsou auditní záznamy uchovávány po dobu nejméně deseti let od jejich vzniku.

6.4.13.1.4 Ochrana auditních záznamů

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

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

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

Ochrana výše uvedených typů auditních záznamů je popsána v interních dokumentech, zejména:

- „Příručka administrátora“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Dokumenty agendy certifikačních služeb“.

6.4.13.1.5 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. Procesy jsou popsány v interních dokumentech, zejména :

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

6.4.13.1.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

6.4.13.2 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace v souladu s požadavky relevantní legislativy a technických standardů je u I.CA prováděno podle interních dokumentů:

- „Řízení fyzického přístupu do místností I.CA“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Příručka administrátora“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

6.4.13.2.1 Typy informací a dokumentace, které se uchovávají

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

- smlouvy o poskytování certifikační služby,
- dokumenty a záznamy související s životním cyklem vydaných certifikátů TSU systému TSA, včetně těchto certifikátů a certifikátů s nimi souvisejících,
- případný videozáznam průběhu generování párových dat CA vydávající certifikáty TSU systému TSA,
- další záznamy potřebné pro služby CA vydávající certifikáty TSU systému TSA (např. seznamy zneplatněných certifikátů),
- vydaná kvalifikovaná časová razítka včetně žádostí o jejich vydání,
- záznamy o činnosti jednotlivých TSU systému TSA,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentace.

6.4.13.2.2 Doba uchovávání uchovávaných informací a dokumentace

Informace, vztahující se k certifikátům CA vydávajících certifikáty TSU systému TSA, s výjimkou příslušných soukromých klíčů, jsou uchovávány po celou dobu existence I.CA. Totéž platí pro certifikáty TSU systému TSA. Ostatní informace a dokumentace jsou uchovávány v souladu s kap. 6.4.13.1.3.

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací - viz kap. 6.4.13.2.

6.4.13.2.3 Ochrana úložiště uchovávaných informací a dokumentace

Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků objektové a fyzické bezpečnosti a zákona o ochraně utajovaných informací.

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací - viz kap. 6.4.13.2.

6.4.13.2.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací - viz kap. 6.4.13.2.

6.4.13.2.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

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

Informace a dokumentace jsou ukládány na místo určené ředitelem I.CA.

Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interní dokumentací - viz kap. 6.4.13.2. Shromažďování uchovávaných informací je evidováno.

6.4.13.2.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

Postupy jsou popsány v interní dokumentaci - viz kap. 6.4.13.2.

6.4.13.3 Odpovědnosti za zveřejňování, úložiště informací a dokumentace

Problematika spojená s odpovědností za zveřejňování, úložiště informací a dokumentace je detailně popsána v interních dokumentech:

- „Řízení fyzického přístupu do místností I.CA“,
- „Řízení bezpečnosti informací“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Příručka administrátora“,
- „Správa TSS“,
- „Systémová bezpečnostní politika TSA“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

6.4.13.3.1 Úložiště informací a dokumentace

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

6.4.13.3.2 Zveřejňování informací a dokumentace

Základní adresy (dále též informační adresy), na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s., 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.

Elektronickou adresou sloužící pro kontakt klientů popř. veřejnosti s I.CA je tsa@ica.cz. Na tuto elektronickou adresu lze zasílat i případné dotazy, připomínky nebo návrhy na zlepšení poskytované služby.

Na výše uvedené internetové adrese lze získat informace o:

- 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).

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 případech vzniku důvodné obavy ze zneužití soukromých klíčů, sloužících v procesech vydávání certifikátů koncovým uživatelům, vydávání seznamů zneplatněných certifikátů, nebo poskytování informací o stavu certifikátů, oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes.

6.4.13.3.3 Periodicita zveřejňování informací

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

- Politika - před prvním vydáním kvalifikovaného 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 TSU systému 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 TSA s uvedením důvodu zneplatnění – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných certifikačních služeb.

6.4.13.3.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům I.CA, nebo subjektům definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci - viz kap. 6.4.13.3.

6.5 Ostatní obchodní a právní záležitosti

6.5.1 Poplatky

6.5.1.1 Poplatky za vydávání kvalifikovaných časových razítek

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

6.5.1.2 Poplatky za přístup k certifikátům poskytovatele

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

6.5.1.3 Poplatky za informace o stavu certifikátu a o zneplatnění

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

6.5.1.4 Poplatky za další služby

Stažení elektronické verze této Směrnice (ve formátu PDF) je poskytováno zdarma.

Poplatky za nadstandardní služby jsou stanovovány smluvně.

6.5.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

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

6.5.2 Finanční odpovědnost

6.5.2.1 Krytí pojištění

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

6.5.2.2 Další aktiva a záruky

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiné finanční zajištění na poskytování certifikačních služeb 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.

6.5.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

6.5.3 Citlivost obchodních informací

6.5.3.1 Výčet citlivých informací

Citlivými a důvěrnými informacemi I.CA jsou veškeré informace, které nejsou zveřejňovány způsobem uvedeným v kap. 6.4.13.3.2, zejména:

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

6.5.3.2 Informace mimo rámec citlivých informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kap. 6.4.13.3.2.

6.5.3.3 Odpovědnost za ochranu citlivých informací

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

6.5.4 Ochrana osobních údajů

6.5.4.1 Politika ochrany osobních údajů

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

6.5.4.2 Osobní údaje

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

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.

6.5.4.3 Údaje, které nejsou považovány za důvěrné

Za citlivé nejsou považovány údaje, které nespadají do působnosti ZOOÚ.

6.5.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

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

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

6.5.4.6 Poskytování citlivých informací pro soudní či správní účely

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

6.5.4.7 Jiné náležitosti zpřístupňování osobních údajů

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

6.5.5 Práva duševního vlastnictví

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

6.5.6 Doba platnosti, ukončení platnosti

6.5.6.1 Doba platnosti

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

6.5.6.2 Ukončení platnosti

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

6.5.6.3 Důsledky ukončení a přetrvání závazků

Ukončení služeb vydávání kvalifikovaných časových razítek dle Politiky odpovídající této Směrnici neznamená neplatnost kvalifikovaného časového razítka vydaného v době platnosti Politiky.

6.5.7 Komunikace mezi zúčastněnými subjekty

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

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

6.5.8 Změny

6.5.8.1 Postup při změnách

Postup je realizován řízeným procesem popsaným v interní dokumentaci.

6.5.8.2 Postup při oznamování změn

Vydání nové verze Směrnice je vždy oznámeno formou zveřejňování informací.

6.5.8.3 Okolnosti, při kterých musí být změněno OID

OID není přiřazován.

6.5.9 Řešení sporů

Při případném sporu lze postupně kontaktovat:

- odpovědného pracovníka RA,
- odpovědného pracovníka I.CA (nutné doporučené písemné podání),
- ředitele I.CA (nutné doporučené písemné podání).

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

6.5.10 Rozhodné právo

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

6.5.11 Shoda s právními předpisy

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

6.5.12 Další ustanovení

6.5.12.1 Rámcová dohoda

Není relevantní pro tento dokument.

6.5.12.2 Postoupení práv

Není relevantní pro tento dokument.

6.5.12.3 Oddělitelnost ustanovení

Není relevantní pro tento dokument.

6.5.12.4 Zřeknutí se práv

Není relevantní pro tento dokument.

6.5.12.5 Vyšší moc

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

6.5.12.6 Další opatření

Není relevantní pro tento dokument.

7 ZÁVĚREČNÁ USTANOVENÍ

Tento dokument vydaný společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 07.01.2016.