

D. Trust Certifikačná Autorita, a.s.



POLITIKA ČASOVÝCH PEČIATOK

**(POLITIKA ČASOVEJ AUTORITY I.CA
PRE VYDÁVANIE ČASOVÝCH PEČIATOK)**

Obsah

ÚVOD	3
1 PÔSOBNOSŤ	3
2 ODKAZY	4
3 DEFINÍCIE A SKRATKY	5
3.1 DEFINÍCIE	5
3.2 SKRATKY	6
4 ZÁKLADNÉ USTANOVENIA	7
4.1 SLUŽBA AUTORITY ČASOVÝCH PEČIATOK (TSS)	7
4.2 AUTORITA ČASOVÝCH PEČIATOK (TSA I.CA)	7
4.3 KLIENT	7
4.4 VŠEOBECNÉ USTANOVENIA A POLITIKA TSA I.CA	8
4.4.1 Účel	8
4.4.2 Úroveň špecifikácie	8
4.4.3 Prístup	8
5 POLITIKA TSA I.CA	9
5.1 CELKOVÝ PREHLAD	9
5.2 IDENTIFIKÁCIA POLITIKY	10
5.3 POUŽITELNOSŤ ČASOVÝCH PEČIATOK	10
5.4 ZHODA	10
6 ZÁVÄZKY A POVINNOSTI STRÁN	10
6.1 ZÁVÄZKY TSA I.CA	11
6.2 ZÁVÄZKY KLIENTOV	11
6.3 ZÁVÄZKY SPOLIEHAJÚCICH SA STRÁN	12
6.4 ZODPOVEDNOSŤ I.CA	12
6.5 FINANČNÁ ZODPOVEDNOSŤ	12
7 POŽIADAVKY TSA I.CA	12
7.1 PREVÁDZKOVANIE SMERNICE A VÝKLAD POLITIKY	13
7.1.1 Prevádzková smernica TSA I.CA	13
7.1.2 Výklad politiky autority časových pečiatok I.CA	13
7.2 ŽIVOTNÝ CYKLUS KLÚČOVÉHO HOSPODÁRSTVA	14
7.2.1 Generovanie kľúčov TSA I.CA	14
7.2.2 Ochrana súkromného kľúča TSU	15
7.2.3 Distribúcia verejného kľúča TSU	15
7.2.4 Obnovenie kľúčov TSU	15
7.2.5 Zničenie kľúča TSU	15
7.2.6 Správa serveru časových pečiatok	15
7.3 VYDÁVANIE ČASOVÝCH PEČIATOK	16
7.3.1 Token časovej pečiatky	16
7.3.2 Synchronizácia hodín s UTC	18
7.4 MANAGEMENT TSA I.CA	19
7.4.1 Bezpečnostný management	19
7.4.2 Hodnotenie rizík	20
7.4.3 Personálna bezpečnosť	20
7.4.4 Bezpečnosť fyzická, objektová a prostredia	20
7.4.5 Operačný management	21
7.4.6 Management prístupu k systému	21
7.4.7 Dôveryhodné prostredie	21
7.4.8 Kompromitácia služieb TSA I.CA	22
7.4.9 Ukončenie činnosti	22
7.4.10 Zhoda so zákonmi ČR, normami a štandardami	22
7.4.11 Záznam udalostí	22
7.5 ORGANIZAČNÁ SCHÉMA	23
7.6 PLATNOSŤ A ÚČINNOSŤ	23

ÚVOD

Spoločnosť D. Trust Certifikačná Autorita, a.s., (ďalej tiež „DTCA“) poskytuje akreditované certifikačné služby v zmysle zákona NR SR č. 215/2002 Z.z. o elektronickom podpise v spolupráci s českou spoločnosťou První certifikační autorita, a.s., Praha (ďalej tiež „I.CA“), ktorá je akreditovaným poskytovateľom certifikačných služieb v Českej republike. Vydávanie časových pečiatok vykonáva pre DTCA na základe uzatvorenej zmluvy spoločnosť První certifikační autorita, a.s.

Tento dokument špecifikuje základné pravidlá používané autoritou časových pečiatok I.CA, prevádzkovanou spoločnosťou První certifikační autorita, a.s., v procese poskytovania časových služieb (vydávanie časových pečiatok, distribúcia času z dôveryhodného zdroja), definuje účastníkov procesu vydávania časových pečiatok, ich zodpovednosti, práva a rozsah použitia. Podrobný popis týchto pravidiel je uvedený v interných dokumentoch, uvedených v kapitole 4.4.2. Štruktúra a obsah tohto dokumentu je kompatibilný s doporučeniami ETSI¹.

Vydané časové pečiatky je možné použiť k ochrane elektronického podpisu² s dlhodobou platnosťou, ochrane spustiteľného kódu a transakcií vykonávaných na sieti.

Základnou internetovou adresou, na ktorej možno nájsť informácie o spoločnosti První certifikační autorita, a.s., je adresa <http://www.ica.cz>, na ktorej môžete nájsť informácie o všetkých poskytovaných službách – vydávanie certifikátov, časových pečiatok. Na tejto adrese možno nájsť prípadné odkazy a základné informácie o vyššie uvedených témach.

Elektronická korešpondenčná adresa, ktorá slúži pre kontakt klienta s prevádzkovateľom systému, je info@ica.cz. Na túto elektronickú adresu možno zasielať prípadné otázky, pripomienky alebo návrhy na zlepšenie poskytovania služieb.

Základná korešpondenčná adresa spoločnosti První certifikační autorita, a.s., je:

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

1 Pôsobnosť

Názov : Politika časovej autority I.CA
Spoločnosť : První certifikační autorita, a.s.
Schválil : riaditeľ spoločnosti První certifikační autorita, a.s.

Tabuľka 1

Verzia	Dátum	Popis zmien
1.0	01.07.2003	Pilotná prevádzka

¹ ETSI TS 102 023 v.1.2.1. (2003-01), Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities

² IETF RFC 3126, Electronic Signature Formats for long term electronics signature, September 2001

1.01	01.03.2004	Komerčná prevádzka
1.011	01.04.2005	Formálna revízia

Požiadavky na činnosť systému autority časových pečiatok I.CA, prevádzkovaným spoločnosťou První certifikační autorita, a.s., uvedené v tomto dokumente³ sú založené na:

- použitie spoľahlivého časového zdroja
- X.509 certifikátoch
- technológii PKI – s ohľadom na dôvernosť, integritu, neodmietnuteľnosť zodpovednosti a autenticitu

a aplikované pre akékoľvek aplikácie, ktoré vyžadujú dôkaz, že dátový objekt, ku ktorému je pripojená časová pečiatka, vygenerovaná systémom autority časových pečiatok I.CA (ďalej len „TSA I.CA“), existoval bezprostredne pred časovým údajom uloženým v tejto časovej pečiatke.

Služba časovej pečiatky I.CA je prídavnou službou základných služieb certifikačnej autority, prevádzkovej spoločnosťou První certifikační autorita, a.s. Pre získanie detailnejších informácií, t.j. aké sú požiadavky, uvedené v tomto dokumente, realizované systémom TSA I.CA použité pri poskytovaní tejto služby, môžu klienti kontaktovať prevádzkovateľa TSA I.CA.

2 Odkazy

TSA I.CA dodržiava predovšetkým nasledujúce legislatívne predpisy, normy, štandardy a doporučenia:

- RFC 2527 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework (ďalej len RFC 2527)
- ETSI TS 101 456 V1.1.1 – Policy requirements for certification authorities issuing qualified certificates (ďalej tiež ETSI TS 101 456)
- DRAFT REVISED ITU-T RECOMMENDATION X.509 /ISO/IEC 9594-8: „Information technology –open systems interconnection – the directory: public-key and attribute certificate frameworks“ (ďalej tiež ISO/IEC 9594-8)
- ETSI TS 102 023 V1.2.1. (2003-01) – Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities (ďalej tiež ETSI TS 102 023)
- ETSI TS 101 861 V1.2.1 (2002-03) – Time Stamping Profile (ďalej tiež ETSI TS 101 861)
- RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- RFC 2630 – Cryptographic Message Syntax
- IČSN ISO/IEC TR 13335 1-3 : Informačná technológia – Smernica pre riadenie bezpečnosti IT – Časť 1-3, ČNI 1999-2000
- ČSN ISO/IEC 15408 1-2: Informačná technológia – Bezpečnostné techniky – kritéria pre hodnotenie bezpečnosti informačných technológií

³ Tento dokument môže byť mimo iného využívaný nezávislými inštitúciami (napr. audítorské spoločnosti) ako základ pre potvrdenie toho, že systém TSA I.CA, prevádzkovaný spoločnosťou První certifikační autorita, a.s., môže byť dôveryhodný pre zaistenie časových služieb.

- ISO 15408 Common Criteria for Information Technology Security Evaluation, v2.1 ISO 15408, ISO/IEC 1999
- BS ISO/IEC 17799:20001999, preklad a interpretácia pre české prostredie
- BS 7799-2:20021999, preklad a interpretácia pre české prostredie

3 Definície a skratky

Pre účely tohto dokumentu platia definície a skratky, ktoré sú uvedené v nasledujúcich podkapitolách.

3.1 Definície

V tabuľke 2 sú uvedené definície vzťahujúce sa k tomuto dokumentu.

Tabuľka 2

Definície	Popis
Časová pečiatka	dátová štruktúra úspešného procesu vydania časovej pečiatky, časová pečiatka vyjadruje skutočnosť, že dátový objekt (viď. žiadosť o časovú pečiatku), ku ktorému je pripojená táto časová pečiatka, existoval bezprostredne pred časovým údajom uloženým v tejto časovej pečiatke
Certifikát TSA I.CA	certifikát serveru časových pečiatok pre podpisovanie vydaných časových pečiatok
HASH funkcia	jednosmerná transformácia, ktorá z variabilných vstupných veličín vráti jednoznačnú hodnotu (textový reťazec) pevnej dĺžky, ktorá sa nazýva HASH hodnota
HASH hodnota	predstavuje zhustenú hodnotu dlhej správy z ktorej bola vypočítaná, vo význame digitálneho odtlačku prstu veľkého dokumentu. Opačný proces je nemožný.
Klient	fyzická alebo právnická osoba (predplatiť, alebo spoliehajúca sa strana), ktorá na základe písomnej zmluvy vstupuje alebo vstúpila do zmluvného vzťahu so spoločnosťou První certifikační autorita, a.s.
Odpoveď. na žiadosť o časovú pečiatku (TSR)	Dátová štruktúra obsahujúca výsledkový status a token časovej pečiatky
Predplatiť	entita, požadujúca služby TSA I.CA a ktorá explicitne alebo implicitne súhlasila s podmienkami TSA I.CA
Služba autority časových pečiatok (TSS)	Dátová komunikačná infraštruktúra TSA I.CA, vydávajúca a spravujúca časové pečiatky

Spoliehajúca sa strana	Entita, spoliehajúca sa na už vydanú časovú pečať
Time Stamping Authority – TSA	organizovaná sada (systém) ICT produktov a komponent (HW,SW) pre podporu služieb vydávania časových pečiatok
TSA I.CA	organizovaná sada (systém) ICT produktov a komponent pre podporu služieb vydávania časových pečiatok prevádzkovaná spoločnosťou První certifikační autorita, a.s.
Time –stamping jednotka (TSU)	sada hardwaru a softwaru, ktorá je spravovaná ako jedna jednotka a ktorá má v dobe podpisu časovej pečiatky aktívny jediný kľúč
Token časovej pečiatky(TST)	Dátová štruktúra v normovanom tvare (RFC 3161)
Trusted time	Infraštruktúra pre distribúciu dôveryhodného času
Universal Coordinated Time	Štandard prijatý 1.1.1972 pre svetový koordinovaný čas (COORDINATED Universal Time – UTC). Funkcia oficiálneho časomerača atómového času pre celý svet vykonáva Bureau International de l'Heure (BIPM)
Výsledkový status	informácie o úspešnosti alebo chybovom kóde pri spracovaní žiadosti o časovú pečať
Žiadosť o časovú pečať (TSQ)	dátová štruktúra v normovanom tvare (RFC 3161)

3.2 Skratky

V tabuľke 3 sú uvedené skratky, ktoré sú v tomto dokumente používané

Tabuľka 3

Definícia	Popis
BIPM	Bureau International des Poids et Mesures
CP	Certificate Policy, Certifikačný poriadok
CCTV	Closed Circuit Television (uzatvorený kamerový systém)
CPS	Certificate Policy Statement, Certifikačná prováděcí smernica
CRL	Certificate Revocation List
EPS	Elektronická požiarňa signalizácia
ETSI	European Telecommunications Standards Institute
EZS	Elektronický Zabezpečovací Systém
IETF	Internet Engineering Task Force
NIST	National Institute of Standards and

	Technology
NTP	Network Time Protocol
PKI	Public Key Infrastructure
RA	Registračná Autorita
TSQ	Time Stamp Query
TSR	Time Stamp Response
TSS	Time Stamping Service
TST	Time Stamp Token
TSU	Time Stamp Unit
UTC	Universal Co-ordinated Time

4 Základné ustanovenia

4.1 Služba autority časových pečiatok (TSS)

Poskytovanie služieb autority časových pečiatok možno rozdeliť do dvoch základných okruhov:

- poskytovanie časových pečiatok – generovanie a vydávanie časových pečiatok
- podporné procesy – monitorovanie a riadenie operácií, spojených s procesom vydávania časových pečiatok. V rámci tohto okruhu sú napríklad zaistené:
 - synchronizácia a bezpečný prístup k presnému a auditnému časovému zdroju UTC (kapitola 7.3.2)
 - správa systémových programových komponentov

4.2 Autorita časových pečiatok (TSA I.CA)

Autorita časových pečiatok TSA I.CA je z pohľadu klientov, ktorí ich služby využívajú, dôveryhodná komunikačná infraštruktúra vydávajúca časové pečiatky. Z titulu prevádzkovateľa TSA I.CA nesie spoločnosť První certifikační autorita, a.s. celkovú zodpovednosť za poskytovanie služieb časových pečiatok tak, ako je definované v kapitole 4.1.

V prípade TSA I.CA, prevádzkovanou spoločnosťou První certifikační autorita, a.s., nie sú pre proces poskytovania časových pečiatok (kap. 4.1), využívané zmluvné strany a celková činnosť je vykonávaná výhradne jedinou TSU, umiestnenou v prostredí TSA I.CA. Pre podporné procesy, konkrétne distribúcia, synchronizácia a kalibrácia dôveryhodného času (kap. 4.1) je využitá zmluvná strana (kap. 7.3.2).

4.3 Klient

Klientom TSA I.CA môže byť individuálny koncový užívateľ alebo organizácia zahŕňajúca niekoľko koncových užívateľov.

V prípade, že klientom je organizácia, potom jej záväzky voči TSA I.CA musia platiť aj pre ich koncových užívateľov a organizácia je vždy zodpovedná za to, že jej koncoví užívatelia

tieto záväzky splnia správne (kapitoly 6.2,6.3). Preto musia organizácie vlastných koncových užívateľov vhodným spôsobom informovať.

V prípade, že klientom je koncový užívateľ, potom je tento priamo zodpovedný za to, že záväzky voči systému TSA I.CA splní správne (kapitoly 6.2,6.3).

4.4 Všeobecné ustanovenia a politika TSA I.CA

Dokument Politika časových pečiatok je ďalej konkretizovaný dokumentom Prevádzková smernica TSA I.CA, ktorý detailne upravuje činnosť TSA I.CA a prípadných ďalších služieb. TSA I.CA vydáva časové pečiatky každému predplatiteľovi. Predpisy popisujúce účtovacie poplatky sú uvedené v cenníku, ktorý je umiestnený na adrese <http://www.ica.cz>. Na tejto adrese sú taktiež uvedené dokumenty, poprípade odkazy na dokumenty a normy, týkajúce sa ako aj TSA I.CA, systému prevádzkovaného spoločnosťou První certifikační autorita, a.s., tak aj problematike TSA všeobecne.

4.4.1 Účel

Dokument Politika časových pečiatok je verejným dokumentom, ktorý je majetkom spoločnosti První certifikační autorita, a.s. Aktuálna verzia tohto dokumentu je zverejnená na adrese <http://www.ica.cz>. Stiahnutie elektronickej podoby dokumentu nie je spolplatňované. V papierovej podobe je dokument k dispozícii na registračných autoritách za poplatok uvedený v aktuálnom cenníku.

4.4.2 Úroveň špecifikácie

Podrobný popis systému autority časových pečiatok I.CA , prevádzkovaného spoločnosťou První certifikační autorita, a.s., je uvedený v ďalších dokumentoch, ktoré sú všeobecne neverejné. Neverejné dokumenty, vrátane správ, výsledkov testov a interných auditov vytvárajú dokumentačnú sadu, dostupnú výhradne autorizovanému personálu a audítorom. V tabuľke 4 sú uvedené významné dokumenty, vzťahujúce sa k TSA I.CA (kapitola 4.1).

Tabuľka 4

Číslo	Názov dokumentu	Status
1.	Politika časových pečiatok (TSA I.CA Policy)	Verejný
2.	Prevádzková smernica TSA I.CA (TSA I.CA Practice Statement)	Neverejný
3.	Analýza rizík TSA I.CA	Neverejný
4.	Bezpečnostná architektúra TSA I.CA	Neverejný
5.	Špecifikácia bezpečnosti TSA I.CA (SBP TSA I.CA)	Neverejný
6.	Plán obnovy TSA I.CA	Neverejný
7.	Technický projekt TSA I.CA	Neverejný

4.4.3 Prístup

Dokument Politika časových pečiatok je vypracovaný na všeobecnej úrovni a nepopisuje technické detaily dátového komunikačného systému, štruktúry organizácie, operačných

procedúr alebo technickej ochrany. Taktiež nijak nešpecifikuje prostredie, v ktorom je TSA I.CA prevádzkovaná. Technické a prevádzkové detaily sú uvedené v relevantných interných dokumentoch (kapitola 4.4.2).

5 Politika TSA I.CA

5.1 Celkový prehľad

Dokument Politika časových pečiatok je súbor pravidiel užívaných v procese poskytovania časových služieb a regulujúcich stupeň bezpečnosti konkrétneho systému autority časových pečiatok I.CA. Všeobecné pravidlá sú uvedené v kapitole 4.4. Profil certifikátu verejného kľúča (slúžiaceho pre kontrolu podpísaného TST) TSA I.CA vydaného certifikačnou autoritou, prevádzkovanou spoločnosťou První certifikační autorita, a.s. (vydávajúcou komerčné certifikáty), sa riadi doporučeniami IETF a jeho základné vlastnosti sú uvedené v tabuľke 5.

Tabuľka 5

Pole	Hodnota, popr. limit hodnoty
Version	V3
Serial Number	Jedinečná hodnota každého komerčného certifikátu vydaného spoločnosťou První certifikační autorita, a.s.
Signature Algorithm	Sha 1RSA (OID:1.2.840.113549.1.1.5)
Issuer (Distinguished Name)	<ul style="list-style-type: none"> • Common Name (CN)=I.CA_Time_Stamping_Authority • Organization (O)=První certifikační autorita, a.s. • Country (C)=CZ
Not before (validity period beginning date)	Universal Time Coordinated.
Not after (validity period ending date)	Universal Time Coordinated.
Subject (Distinguished Name)	Rozlišujúce mená splňujúce požiadavky X.501
Subject Public Key Info	Zakódovaný v súlade s RFC2459, obsahuje informáciu o RSA verejných kľúčov. Veľkosť kľúča je 2048 bitov.
Signature	Podpis certifikátu vytvorený a zakódovaný v súlade s požiadavkami popísanými v RFC 2459.

Systém TSA I.CA, poskytujúca služby prostredníctvom spoločnosti První certifikační autorita, a.s., vydáva časové pečiatky podľa doporučenia ETSI. Každá časová pečiatka zahŕňa identifikátor politiky autority časových pečiatok I.CA (kapitola 5.2).

5.2 Identifikácia politiky

Identifikátor politiky, riadiaci vydávanie a správu časových pečiatok uvedený v tabuľke 6 je obsiahnutý v každej vydanéj časovej pečiatke. Táto politika je k dispozícii klientom TSA I.CA podľa pravidiel popísaných v kapitole 4.4.2.

Tabuľka 6

Identifikátor politiky	Názov politiky
id-ianaPrivate (136141) id-pvt(6625) necol (0) neco2 (1)	TSA I.CA identifikuje politiku poskytovanú v rámci časových služieb spoločnosti První certifikační autorita, a.s.

5.3 Použitelnosť časových pečiatok

Tento dokument nedefinuje žiadne obmedzenia použiteľnosti časovej pečiatky vydanéj podľa tejto politiky⁴. Všeobecne platí, že časová pečiatka slúži ako dôkaz, že dátový objekt, ku ktorému je pripojená časová pečiatka, existoval bezprostredne pred časovým údajom uloženým v tejto časovej pečiatke. Časové pečiatky, vydané systémom TSA I.CA, ktorá je prevádzkovaná spoločnosťou První certifikační autorita, a.s., je možné použiť v oblastiach:

- elektronických podpisov, kde je treba overiť, že boli vytvorené v dobe, kedy certifikát verejného kľúča podpisujúcej entity bol platný. Táto kontrola je nevyhnutná z nasledujúcich dvoch dôvodov:
 - v priebehu doby platnosti certifikátu podpisujúcej entity bol zodpovedajúci súkromný kľúč kompromitovaný a z toho dôvodu bol certifikát zrušený,
 - podpis bol vytvorený po ukončení doby platnosti príslušného certifikátu.
- ochrana spustiteľného kódu
- transakcií prevádzkovaných na sieti

5.4 Zhoda

Vydané TST zahŕňa identifikátory popísané v kapitole 5.2 Politiky časové autority I.CA. Sú podporované iba tie žiadosti, ktoré zahŕňajú znaky uvedené v tomto dokumente. Dokument Politika časových pečiatok ďalej zaručuje súlad poskytovaných služieb s predpismi špecifikovanými v kapitole 6.1. a spoľahlivosť riadiaceho mechanizmu popísaného v kapitole 7.

6 Závazky a povinnosti strán

V tejto kapitole sú opísané všetky povinnosti, zodpovednosti a záruky TSA I.CA a klientov. Vzájomné zmluvy medzi spoločnosťou První certifikační autorita, a.s., t.j. poskytovateľom služieb vydávania časových pečiatok (prípadne smluvným partnerem spoločnosti První

⁴ vydané časové pečiatky možno využívať ako v otvorených systémoch verejných služieb (napr. štátnej správy), tak v uzatvorených systémoch súkromných spoločností.

certifikační autorita, a.s.) a klientmi, ktorí tieto služby využívajú, opisujú obojstranné záväzky a zodpovednosti, vrátane finančnej zodpovednosti spoločnosti První certifikační autorita, a.s. Dokument Politika časovej autority I.CA je neoddeliteľnou časťou zmluvy podpísanej medzi spoločnosťou První certifikační autorita, a.s. (prípadne smluvným partnerem spoločnosti První certifikační autorita, a.s.) a klientom. Spoločnosť První certifikační autorita, a.s. zaručuje, že akékoľvek požiadavky na TSA I.CA, vrátane smerníc a pracovných postupov vzťahujúcich sa k vydávaniu časových pečiatok, správe systému a bezpečnostnému auditu, sú v súlade s internými dokumentmi, uvedenými v kapitole 7.

6.1 Závazky TSA I.CA

Spoločnosť První certifikační autorita, a.s. zaručuje nepretržitý prístup k službám TSA I.CA s výnimkou plánovaných, poprípade neplánovaných časových prerušení spojených s technickými zásahmi. Tieto okolnosti sú uvedené vo vnútorných smerniciach. Čas UTC, využívaný v priebehu vydávania časových pečiatok, zaručuje presnosť ± 500 ms.

Spoločnosť První certifikační autorita, a.s. ďalej zaisťuje, že:

- poskytované služby TSA I.CA zodpovedajú všeobecne uznávaným štandardom, popísaným v kapitole 5.1. ,
- vydaná časová pečiatka neobsahuje falošné dáta alebo chyby,
- aktivity spoločnosti, s ohľadom na poskytované služby TSA I.CA, sú v súlade so zákonmi, neporušujú autorské ani licenčné práva.

System TSA I.CA:

- používa dôveryhodný zdroj času,
- do každej časovej pečiatky vkladá dôveryhodnú hodnotu času,
- do každej novo generovanej časovej pečiatky vkladá jednoznačne celé číslo,
- po obdržaní platnej požiadavky od žiadateľa, v súlade s Politikou časovej autority I.CA, generuje časovú pečiatku,
- v každej časovej pečiatke je obsiahnutý identifikátor, ktorý jednoznačne identifikuje bezpečnostnú politiku, pod ktorou bola časová pečiatka vygenerovaná,
- žiadnym spôsobom neoveruje odtlačok, ktorý má byť časovo opečiatkovaný (s výnimkou jeho dĺžky),
- do časovej značky nezahrňuje žiadne identifikácie žiadajúcej entity,
- každá časová pečiatka je podpísaná kľúčom, vygenerovaným výhradne len pre tento účel a táto vlastnosť kľúča je vyznačená v príslušnom certifikáte,
- pokiaľ je požadované žiadateľom, ktorý využíva rozšírenie (extensions field), zahrnie do časovej značky aj ďalšie informácie a to len v tom prípade, že tieto rozšírenia sú podporované TSA I.CA. Pokiaľ toto nie je možné, TSA I.CA odpovie chybovým hláseniam.

6.2 Závazky klientov

Po obdržaní odpovede (TSR) na žiadosť (TSQ) o časovú pečiatku je klient povinný zistiť chybový status. V prípade chyby nie je časová pečiatka v odpovedi obsiahnutá a predplatiťel

je povinný prekontrolovať chybový status a zodpovedajúce chybové hlásenie. V opačnom prípade je predplatiteľ povinný:

- overiť elektronický podpis TST a skontrolovať, či certifikát TSA I.CA nebol zrušený – CRL je prístupné na adrese <http://www.ica.cz/>
- overiť, či vrátená hash hodnota je totožná s odoslanou
- v prípade, že žiadosť obsahovala položku „nonce“ overiť, že jej hodnota v odpovedi je totožná
- v prípade, že žiadosť obsahovala položku „reqPolicy“ overiť, že jej hodnota v odpovedi je totožná.

6.3 Závazky spoliehajúcich sa strán

Všeobecným záväzkom spoliehajúcich sa strán je overenie elektronického podpisu TST. Spoliehajúca sa strana je povinná:

- overiť platnosť certifikátu TSA I.CA a jeho periódu platnosti,
- prekontrolovať či politika, pod ktorou bola vydaná časová pečiatka, je akceptovateľná jej potrebám, poprípade potrebám ňou prevádzkovanvej aplikácie.

V prípade overovania časovej pečiatky po ukončení platnosti TSA I.CA, sú spoliehajúce sa strany povinné:

- overiť, či certifikát TSA I.CA nebol odvolaný v dobe vydania časových pečiatok – CRL je prístupné na adrese <http://www.ica.cz/>
- overiť, či kryptografická hash funkcia použitá v časovej pečiatke je stále bezpečná
- uistiť sa, či dĺžka kryptografického kľúča a algoritmus sú stále považované za bezpečné

6.4 Zodpovednosť I.CA

Akékoľvek záruky a z nich plynúce plnenia je možné uznať len vtedy, pokiaľ klient neporušil povinnosti plynúce mu zo zmluvy medzi ním a spoločnosťou První certifikační autorita, a.s. a z tejto politiky. Na časové pečiatky, ktoré neboli vydané TSA I.CA, sa záruky nevzťahujú.

6.5 Finančná zodpovednosť

Finančná zodpovednosť spoločnosti První certifikační autorita, a.s., je zakotvená vo vzájomnej zmluve medzi spoločnosťou První certifikační autorita, a.s. a klientom.

7 Požiadavky TSA I.CA

Systém autority časových pečiatok I.CA zaznamenáva všetky bezpečnostne relevantné udalosti spojené s procesom vydávania časových pečiatok. Tento prístup umožňuje

vyhľadávanie dôkazu v prípade sporov spojených s použitím časovej pečiatky klientom. Tieto záznamy sú auditované a bezpečne uložené, čo umožňuje, že budú v špecifikovanej dobe a v dostatočnom rozsahu informácií k dispozícii zainteresovaným stranám. Archív týchto informácií je bezpečne umiestnený v geograficky odlišnej lokalite. Prevádzkové zálohy relevantných komponentov TSA I.CA sú bezpečne umiestnené v dvoch geograficky odlišných lokalitách.

Typ a popis udalostí, ktoré sú systémom zaznamenávané a ukladané, je definovaný v relevantných interných dokumentoch.

7.1 Prevádzkovanie smernice a výklad politiky

7.1.1 Prevádzková smernica TSA I.CA

Základom funkčnosti TSA I.CA sú procedúry, riadiace mechanizmy a technická infraštruktúra, ktoré sú popísané v kapitole 6. Ďalšie riadiace a kontrolné mechanizmy sú popísané v nadväzných interných dokumentoch ako je Prevádzková smernica TSA I.CA a ďalších (kapitola 4.4.2)

Základom hodnotenia zraniteľnosti TSA I.CA je vypracovaná analýza rizík, ktorej výsledky sú zohľadnené v interných dokumentoch Prevádzková smernica TSA I.CA a ďalších (kapitola 4.4.2)

Dokument Politika časovej autority I.CA je nadradenou a neoddeliteľnou súčasťou dokumentu Prevádzkovej smernice TSA I.CA, ktoré spolu s ďalšími internými dokumentmi (kapitola 4.4.2) upravujú pravidlá služieb, vzťahujúcich sa k procesu vydávania časových pečiatok.

Vytváranie procedúr, ich regulácia a modifikácia, vytváranie dlhodobých obchodných plánov podlieha dozoru tímu, ktorého členmi sú predstavitelia managementu, PKI konzultantov, systémových inžinierov, bezpečnostných špecialistov, vývojových špecialistov a právnikov. Kontakt na tento tím je uvedený v úvodnej časti tohto dokumentu.

7.1.2 Výklad politiky autority časových pečiatok I.CA

Každá časová pečiatka vydaná systémom TSA I.CA, obsahuje identifikátor politiky, definovaný v kapitole 5.2. Kryptografické hash funkcie použité v procese vydávania časových pečiatok sú v súlade s normatívnymi požiadavkami NIST (kapitola 7.2.1). Presnosť času, ktorý je uvedený v TST, je definovaný v kapitole 6.1.

Obmedzenia TSA I.CA sú definované v kapitole 5.3. Závazky predplatiteľov sú popísané v kapitole 6.2, zatiaľ čo záväzky spoliehajúcich sa strán v kapitole 6.3. Klient je povinný overiť TST postupom, uvedeným v kapitolách 6.2 a 6.3 TSA I.CA je prevádzkovaný v súlade so zákonmi Českej republiky a doporučeniami EÚ. Finančné zodpovednosti sú definované v kapitole 6.5.

Predpisy, vzťahujúce sa k problematike zálohovania a archivácie sú uvedené v relevantných interných dokumentoch. Spoločnosť První certifikační autorita, a.s. má definované havarijné plány pre prípadné pohromy aj procedúry regulujúce zotavenie systému TSA I.CA.

Dokument Politika časových pečiatok a jeho výklad sa riadi platným poriadkom Českej republiky.

V prípade, že klient nesúhlasí s predloženým výkladom, môže využiť odvolanie na vyššiu inštanciu.

Jednotlivé stupne všeobecne tvoria:

- zodpovedný pracovník spoločnosti První certifikační autorita, a.s. (nutné písomné podanie)
- vedenie spoločnosti První certifikační autorita, a.s. (nutné písomné podanie a zloženie finančnej istiny, ktorá je vrátená v prípade kladného vybavenia sťažnosti). Veľkosť finančnej istiny je uvedená v aktuálnom cenníku.

Uvedený postup dáva nesúhlasiacej strane možnosť presadzovať svoj názor rýchlejším spôsobom, než je súdna cesta.

Aktuálna verzia tohto dokumentu je zverejnená na adrese <http://www.ica.cz>.

7.2 Životný cyklus kľúčového hospodárstva

Systém TSA I.CA využíva kryptografické kľúče pre zaistenie integrity, dôvernosti, autentizácie a zaistenia neodmietnuteľnosti zodpovednosti. S ohľadom na rôzne úrovne hrozieb, ktoré závisia na spôsobe využívania kľúčov, možno kľúče rozdeliť do nasledujúcich kategórií:

- kľúče pre podpisovanie TST - kľúčový pár vyhradený len pre podpisovanie vydaných TST,
- kľúč infraštruktúry dôveryhodného času – kľúčový pár využívaný v procese distribúcie času od dôveryhodného zdroja k TSU (server časových pečiatok), kalibrácie a auditu servera časových pečiatok,
- servisný kľúč, kľúčový pár využívaný v procese správy systému.

7.2.1 Generovanie kľúčov TSA I.CA

Kľúče TSA I.CA sú generované v bezpečnom hardwarovom prostriedku splňujúcom požiadavky NIST FIPS 140-1 level 3. Požiadavky na postupy pre generovanie kľúčov TSA I.CA sú uvedené v internom dokumente (vrátane personálnej bezpečnosti) a podrobne popísané v nadväzných interných smerniciach. Prostredie generovania kľúčov TSA I.CA spĺňa doporučenia pre dôveryhodné operačné systémy a požiadavky na úroveň bezpečnosti EAL4. Algoritmus kľúča TSA I.CA je popísaný v kapitole 5.1.

7.2.2 Ochrana súkromného kľúča TSU

Postupy pre obnovu kľúčov v prípade havárie systému, pohromy, atď., vrátane okolností, doprevádzajúcich generovanie kľúčov, sú spolu s vhodnými procedúrami popísané v interných dokumentoch, ktoré sú podrobené pravidelnému auditu. Bezpečnostná úroveň prostredia a bezpečnosť hardwarového prostriedku sú popísané v kapitolách 7.2.1 a 7.2.6.

7.2.3 Distribúcia verejného kľúča TSU

Certifikáty TSA I.CA spolu so zodpovedajúcimi verejnými kľúčmi sú publikované na adrese <http://www.ica.cz/>. Verejné kľúče TSA I.CA sú podpísané certifikačnou autoritou I.CA (vydávajúca komerčné certifikáty) prevádzkovanou spoločnosťou První certifikační autorita, a.s. Podrobné informácie sú uvedené v interných dokumentoch.

7.2.4 Obnovenie kľúčov TSU

Proces obnovenia kľúčov TSU môže byť:

- **programový** – procedúra obnovenia kľúča TSA I.CA sa vykonáva tri roky pred vypršaním platnosti aktuálneho certifikátu TSA I.CA. Súkromný kľúč je uložený v HSM module. Expirovaný kľúčový pár je v HSM archivovaný po dobu šesť rokov a potom je súkromný kľúč zničený. Pre kontrolu časových pečiatok je každý expirovaný verejný kľúč TSA I.CA ďalej archivovaný po celú dobu činnosti TSA I.CA. Podrobné informácie sú uvedené v relevantných interných dokumentoch.
- **neprogramový** – v prípade keď je kľúč nahradený novým z dôvodu kompromitácie. Podrobné informácie sú uvedené v relevantných interných dokumentoch.

7.2.5 Zničenie kľúča TSU

Postupy pre prípady, keď je kľúč kompromitovaný alebo doba jeho platnosti vypršala, sú spolu s ďalšími procedúrami uvedené v interných dokumentoch. Ďalšie informácie sú dostupné v kapitole 7.2.4.

V prípade, že vypršala doba platnosti certifikátu TSU, systém TSA I.CA odmietne každú požiadavku na vydanie časovej pečiatky.

7.2.6 Správa serveru časových pečiatok

Hardware vyhradeného servera, ktorý je pripojený do infraštruktúry dôveryhodného času, obsahuje hardware security modul (FIPS 140-1 level 3) je výrobcom doručený (s využitím dôveryhodných prepravcov) do sídla spoločnosti První certifikační autorita, a.s. V procese prijímania zásielky sú kontrolované správnosť a neporušenosť pečatí obalu zásielky od výrobcu. Po prevzatí zásielky je táto následne premiestnená na pracovisko, ktoré prevádzkuje systém vydávania časových pečiatok. Na tomto pracovisku je vykonaná ďalšia kontrola pečatí, obalu zásielky, vrátane pečatí samotného hardwaru. Server časových pečiatok je

uložený na bezpečnom mieste so riadeným prístupom a je vykonaná základná inštalácia vrátane testov a kalibrácie. Každá vyššie uvedená činnosť je písomne zaznamenávaná. Inštalácia, inicializácia a kalibrácia časového serveru sú vykonávané dôveryhodným personálom a v prítomnosti svedkov. V prípade ukončenia činnosti systému TSA I.CA alebo predania hardwaru časového serveru do servisu sú kľúče z hardwaru security modulu vymazané a zničené podľa doporučenia výrobcu. Akékoľvek operácie s časovým serverom sú podrobne popísané v interných dokumentoch (kapitola 4.4.2) a nadväzujúcich smerniciach.

7.3 Vydávanie časových pečiatok

7.3.1 Token časovej pečiatky

Časové pečiatky sú vydávané servrom systému TSA I.CA na základe zaslanej žiadosti (TSQ) prostredníctvom odpovede (TSR).

Profil žiadosti o časovú pečiatku (TSQ) má nasledujúci (RFC 3161) formát :

```

TimeStampReq::=SEQUENCE {
  version          INTEGER{ v1(1)},
  messageImprint   MessageImprint,
  reqPolicz        TSA PoliczId      OPTIONAL,
  nonce            INTEGER            OPTIONAL,
  certReq          BOOLEAN           DEFAULT FALSE,
  extensions       [0]               IMPLICIT Extensions Optional }

```

kde

```

MessageImprint::=SEQUENCE {
  Hash Algorithm AlgorithmIdentifier,
  HashedMessage OCTET STRING }

```

Pole	Popis
Version	Popisuje verziu požiadavky na časovú pečiatku
Hash Algortithm	SHA-1
HashedMessage	Dĺžka tohto reťazca (Octect String) musí spĺňať požiadavky na dĺžku zvoleného algoritmu (SHA-1)
ReqPolicy	Identifikátor Politiky časovej autority I.CA
Nonce	Náhodné číslo, o ktorom sa predpokladá, že ho predplatiťel' vygeneruje iba raz (64 bit integer). V prípade, že toto číslo žiadosť obsahuje, potom toto číslo musí obsahovať aj odpoveď.
CertReq	TRUE - odpoveď musí obsahovať certifikát TSA I.CA. FALSE- alebo nie je uvedené, odpoveď

	nesmie obsahovať certifikát TSA I.CA
Extensions	Definované v RFC 2459. Pokiaľ sú využité (kritické/nekritické) a TSA server ich nerozpozná, potom server časovú pečiatku nesmie vydať a musí vrátiť chybu (unacceptedExtensions)

Profil odpoveď (TSR) na žiadosť (TSQ) o časovú pečiatku má nasledujúci (RFC 3161) formát:

```
TimeStampReq::=SEQUENCE {
status                PKIStatusInfo,
timeStampToken       TimeStampToken Optional }
```

kde

PKI StatusInfo ::=Sequence { status PKIStatus , statusString..... PKIFreeText OPTIONAL, failInfo..... PKIFailureInfo OPTIONAL
PKIStatus ::=INTEGER { granted (0) grantedWithMods (1) rejection (2) waiting (3) revocationWarning (4) revocationNotification (5) }
PKIFailureInfo ::=BIT STRING { BadAlg (0) --unrecognized or unsupported Algorithm Identifier badRequest (2) --transaction not permitted or supported badDataFormat (5) --the date submitted has the wrong format timeNotAvailable (14) -- the TSA's time source is not available unacceptePolicy (15) -- the requested TSA policy is not supported by the TSA unacceptedExtension (16) -- the requested extension is not supported by the TSA addInfoNotAvailable (17) -- the additional information requested could not be understood or is not available systemFailure (25) --the request cannot be handled due to system failure }

TimeStampToken je definovaný ako ContentInfo ([CMS]) a musí zahŕňať „signed data content type“.

TimeStampToken ::= ContentInfo

- n contentType is id-signedData ([CMS])
- n content is SignedData ([CMS])

Dátová štruktúra SignedData obsahuje pole typu EncapsulatedContentInfo, ktoré majú nasledujúci význam:

- eContentType jednoznačná špecifikácia
- eContent samotný obsah v tvare OCTET STRING. Jedná sa o hodnotu TSTInfo v kódovaní DER

Token časovej pečiatky nesmie obsahovať iný podpis, než podpis TSA I.CA.

```

TSTInfo ::= SEQUENCE {
version                INTEGER {v1(1) },
Policy                TSAPolicyId,
messageImprint        MessageImprint,
-- musí mať rovnakú hodnotu ako v TimeStampReq
serialNumber          INTEGER,
--Time-Stamping users MUST be ready to accommodate integers up to 160 bits.
genTime               GeneralizedTime,
accuracy              Accuracy          OPTIONAL,
ordering              BOOLEAN          DEFAULT FALSE,
nonce                 INTEGER          OPTIONAL,
--pokiaľ obdobné pole je aj v TimeStampReq musí byť uvedené a hodnoty musia byť totožné
tsa                   [0] GeneralName  OPTIONAL,
extensions             [1]IMPLICIT Extensions  OPTIONAL }

```

Tokeny časových pečiatok, ktoré vydá vyhradený server systému TSA I.CA, musia obsahovať jednoznačný identifikátor politiky, popísaný v kapitole 5.2, hash hodnotu dátového objektu, na ktorý je proces časovej pečiatky realizovaný, dátum a časovú hodnotu (zodpovedajúcu reálnej hodnote UTC) a jedinečné sériové číslo.

Presnosť času použitého v TST je definovaný v kapitole 6.1. Token časovej pečiatky (v štandarde RFC 3161) je podpísaný súkromným kľúčom TSA I.CA, ktorého certifikát obsahuje údaje, popísané v kapitole 5.1. a identifikátor jednoznačne spojený so spoločnosťou První certifikační autorita, a.s.

7.3.2 Synchronizácia hodín s UTC

Pre distribúciu, synchronizáciu a kalibráciu svetového času (UTC) z dôveryhodného zdroja je využívaný model „Trusted Time“. Jedná sa o autorizovanú kalibračnú a auditovateľnú službu, poskytujúcu svetový čas z dôveryhodného zdroja pre server časových pečiatok, s ktorým je integrovaná. Táto bezpečná a nevyvrátiteľná časová kalibračná služba overuje integritu časových pečiatok a poskytuje platné a auditovateľné informácie pre prípad sporov medzi poskytovateľom časových služieb a klientmi.

Bezpečná distribúcia svetového času z dôveryhodného zdroja, odpovedajúca modelu „Trusted Time“ je založená na hierarchii štyroch vrstiev:

- NMI – zdroj UTC,
- distribúcia času – kalibračné a auditné služby,
- distribúcia časových pečiatok – vydávanie časových pečiatok,
- klient časových pečiatok – požiadavky na časové pečiatky.

V rámci procesu distribúcie je využitá technológia PKI, ktorá zaisťuje autenticitu, integritu, dosledovateľnosť (zaistenie neprerušeneho reťazca merania od času použitého v priebehu vytvorenia časovej pečiatky po dôveryhodný časový zdroj). Technológia PKI je využitá pre elektronické podpisovanie ako týchto meraní, tak samotnej časovej pečiatky.

Hodiny TSA I.CA vkladajú čas do časových pečiatok s presnosťou popísanou v kapitole 6.1. Synchronizácia a kalibrácia s UTC je aktivovaná automaticky v definovanom intervale. V prípade chybného fungovania alebo dekalibrácie použitých hodín a teda nemožnosti splnenia požiadaviek na presnosť času, ktorá je definovaná v kapitole 6.1, bude žiadosť o vydanie časovej pečiatky zamietnutá.

Procedúry a postupy zaisťujúce bezpečnosť ovládacích prvkov chrániacich neautorizovanú operáciu, ktorej cieľom je dekalibrácia hodín, akákoľvek manipulácia alebo fyzické zničenie hodín sú popísané v interných dokumentoch. Systém TSA I.CA ďalej obsahuje prvky, umožňujúce zistenie akéhokoľvek rozdielu medzi hodinovým časom systému a časom v uvedenom v TST, ktoré spĺňajú doporučenia BIPM a NTP.

7.4 Management TSA I.CA

7.4.1 Bezpečnostný management

Bezpečnostný management TSA I.CA je vytváraný podľa anglickej normy BS 7799-2:2002. Jedná sa o procesný prístup „Plánovanie – Zavedenie – Kontrola – Využitie“ (Plán-Do-Check-Act, PDCA), ktorý sa skladá z nadväzujúcich procesov:

- vybudovanie – definovanie bezpečnostnej politiky, plánov, cieľov, procesov a postupov s ohľadom na riadenie rizík a bezpečnosť informácií tak, aby boli v súlade s celkovou bezpečnostnou politikou,
- implementácia a prevádzka bezpečnostnej politiky, plánov, cieľov, procesov a postupov,
- monitorovanie a prehodnocovanie – posúdenie procesu s ohľadom na bezpečnostnú politiku a odovzdanie poznatkov vedeniu organizácie k posúdeniu,
- využitie - na základe rozhodnutia vedenia organizácie prevedenie nápravných opatrení.

Neoddeliteľnou súčasťou bezpečnostného managementu je správa dokumentácie (schvaľovanie dokumentov pred ich vydaním, revízia, aktualizácia a opätovné schválenie dokumentov, zaistenie prístupnosti a použitie jedine posledných verzií príslušných dokumentov, zaistenie identifikácie dokumentov externého pôvodu, zaistenie riadenej,

distribúcie dokumentov, atď.) a záznamov (návštevná kniha, záznamy o audite a záznam o autorizácii prístupu, atď.).

Oblasti vzťahujúce sa k bezpečnostnému managementu sú podrobne uvedené v interných dokumentoch (kapitola 4.4.2).

7.4.2 Hodnotenie rizík

Základom pre zaistenie stability činnosti TSA I.CA je vypracovanie analýzy rizík systému TSA I.CA. Opatrenia z nej vychádzajúce sú konkretizované v interných dokumentoch (kapitola 4.4.2).

Pre vykonanie analýzy bol použitý anglický prostriedok CRAMM (verzia 4.0). Pri analýze rizík informačného systému TSA I.CA boli vykonané tieto činnosti:

- stanovenie aktív (programové vybavenie, technické vybavenie, dáta) informačného systému a ich väzieb,
- hodnotenie aktív informačného systému,
- stanovenie relevantných hrozieb a zraniteľností,
- hodnotenie hrozieb a zraniteľností,
- určenie miery rizika pre každú kombináciu aktíva (skupiny aktív), hrozby a zraniteľností.

7.4.3 Personálna bezpečnosť

Témy, vzťahujúce sa k personálnej bezpečnosti a spĺňajúce normu ISO 17799, sú detailne popísané v interných dokumentoch (kapitola 4.4.2) a zahŕňajúce oblasti:

- kvalifikačných požiadaviek, skúseností, preverovanie nových pracovníkov,
- overovanie znalostí,
- požiadavky na školenia a ich pravidelnosť,
- požiadavky na zmeny rolí,
- sankcie pri neautorizovaných činnostiach,
- požiadavky na zmluvný personál,
- požiadavky na proces poskytovania dokumentácie personálu.

7.4.4 Bezpečnosť fyzická, objektová a prostredia

Oblasti, vzťahujúce sa k fyzickej, objektovej a bezpečnosti prostredia, sú uvedené a detailne popísané v interných dokumentoch (kapitola 4.4.2) a zahŕňajú napríklad:

- umiestnenie a konštrukcia,
- fyzický prístup,
- prívod elektrickej energie,
- ohrozenie vodou a ohňom,
- uloženie archívnych a záložných médií,

- atď.

Požiadavky systému TSA I.CA na bezpečnosť fyzickú a objektovú, vrátane bezpečnosti prostredia spĺňajú normu ISO 17799.

7.4.5 Operačný management

Spoločnosť První certifikační autorita, a.s. má s ohľadom na bezpečnosť vypracované procedurálne postupy, zodpovedajúce požiadavkám ETSI (IETF RFC 3126). Ďalej sú vypracované postupy, ktoré obmedzujú prístup k technickej a bezpečnostnej dokumentácii projektu TSA I.CA vrátane upresnení stupňa diskretnosti jednotlivých častí projektu a menovitého určenia, kto sa môže s dokumentáciou zoznamovať.

Všetky dokumenty (interné a externé), vrátane procedurálnych postupov sú periodicky kontrolované audítorom.

7.4.6 Management prístupu k systému

Management prístupových práv k systému zahŕňa dva základné okruhy – fyzický a procedurálny.

7.4.6.1 Fyzický

Objekt, v ktorom je systém TSA I.CA prevádzkovaný, je obkolesený bezpečnostným plotom a je nepretržite strážený fyzickou kontrolou a špeciálnym televíznym systémom pre snímanie, prenos a zobrazovanie pohybu osôb a dopravných prostriedkov. Prístup do vlastného objektu je kontrolovaný fyzickou kontrolou. Chodba pred dverami do zabezpečenej oblasti, v ktorej sa nachádzajú zariadenie slúžiace pre vytváranie časových pečiatok, je strážená EZS, CCTV a EPS. Riadenie fyzického prístupu do zabezpečenej oblasti je upravené internými dokumentmi (kapitola 4.4.2) a smernicami.

7.4.6.2 Procedurálny

Sú definované dôveryhodné úlohy a funkcie z nich vyplývajúce, počty osôb pre vykonávanie bezpečnostne kritických úloh, vrátane spôsobu ich identifikácie a autentizácie. Procedúry vzťahujúce sa k tejto téme sú uvedené a detailne popísané v interných dokumentoch (kapitola 4.4.2) a smerniciach.

7.4.7 Dôveryhodné prostredie

Generovanie kľúčových párov TSA I.CA prebieha vždy v dôveryhodnom prostredí popísanom v kapitole 7.2.1. Každá zmena v systéme je monitorovaná a zaznamenávaná do súboru auditných logov.

7.4.8 Kompromitácia služieb TSA I.CA

V prípade vyzradenia súkromných kľúčov TSA I.CA je nutné postupovať spôsobom, uvedeným v internom dokumente (kapitola 4.4.2).

7.4.9 Ukončenie činnosti

V prípade ukončenia činnosti TSA I.CA z iných dôvodov, než sú mimoriadne udalosti, akými sú štrajky, občianske nepokoje, vojnový stav, prírodné katastrofy celoštátneho rozsahu alebo iné výsledky pôsobenia vyššej moci, zaistí spoločnosť První certifikační autorita, a.s. vykonanie nasledujúcich činností:

- ohlási zámer ukončiť činnosť ako poskytovateľ služieb vydávajúcí časové pečiatky minimálne tri mesiace pred plánovaným ukončením činnosti,
- ukončí vydávanie časových pečiatok,
- sprístupní informácie o ukončení činnosti poskytovateľa služieb vydávajúceho časové pečiatky na svojej internetovej informačnej adrese minimálne dva mesiace pred plánovaným ukončením činnosti,
- preukázateľne zničí svoje dáta pre vytváranie elektronických podpisov slúžiacich k podpisovaniu TST
- zneplatní všetky doposiaľ platné certifikáty a uchová všetky informácie a dokumentáciu o vydaných časových pečiatkach po dobu 10 rokov

Procedúry vzťahujúce sa k tejto téme, sú podrobne popísané v interných dokumentoch (kapitola 4.4.2).

7.4.10 Zhoda so zákonmi ČR, normami a štandardami

TSA I.CA je prevádzkovaná v súlade s:

- zákonmi Českej republiky,
- doporučeniami a štandardami EÚ,
- požiadavky ETSI dokumentov,
- normami a štandardami, ktoré sa vzťahujú k problematike bezpečnosti organizácie a ICT (kapitola 2),
- normami a štandardami, ktoré sa vzťahujú k problematike PKI (kapitola 2).

7.4.11 Záznam udalostí

System TSA I.CA umožňuje zaznamenávanie všetkých bezpečnostne relevantných udalostí spojených s poskytovaním časových služieb (kapitola 7).

7.5 Organizačná schéma

System TSA I.CA je prevádzkovaný spoločnosťou První certifikační autorita, a.s., pôsobiacou na území Českej republiky na adrese Podvinný mlýn 2178/6, 190 00 Praha 9.

Organizačná štruktúra spoločnosti První certifikační autorita, a.s. je popísaná v interných dokumentoch spoločnosti.

7.6 Platnosť a účinnosť

Tento dokument nadobúda platnosť a účinnosť dňom 01.04.2005.