

**První certifikační autorita, a.s.**



# **POLITIKA VYDÁVANIA ČASOVÝCH PEČIATOK**

Stupeň dôvernosti : verejný dokument

Tento dokument je slovenskou verziou dokumentu  
„Politika vydávání kvalifikovaných časových razítek“

Verzia 2.0

Politika vydávania časových pečiatok je verejným dokumentom, ktorý je vlastníctvom spoločnosti První certifikační autorita, a.s. a bol vypracovaný ako nedeliteľná súčasť komplexnej bezpečnostnej dokumentácie. Žiadna časť tohto dokumentu nesmie byť kopírovaná bez písomného súhlasu vlastníka autorských práv.

*Copyright © Prvá certifikačná autorita, a.s.*

<b>Politika vydávania časových pečiatok</b>	<b>Strana 2 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

Tabuľka 1 - Identifikácia

<b>Názov</b>	Politika vydávania časových pečiatok
<b>Pôvodný český názov</b>	Politika vydávání kvalifikovaných časových razítek
<b>Spoločnosť</b>	První certifikační autorita, a.s.
<b>Schválil</b>	Riaditeľ spoločnosti První certifikační autorita, a.s.

Tabuľka 2 – Vývoj dokumentu

<b>Verzia</b>	<b>Dátum vydania</b>	<b>Zhrnutie zmien</b>
1.0	01.02.2006	Prvá verzia dokumentu
2.0	01.10.2007	Použitie viacerých vyhradených serverov pre vydávanie časových pečiatok

<b>Politika vydávania časových pečiatok</b>	<b>Strana 3 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

# Obsah

<b>1 ÚVOD</b>	<b>7</b>
<b>2 PREHLAD</b>	<b>8</b>
2.1 NÁZOV A IDENTIFIKÁCIA DOKUMENTU	9
<b>3 PREHLAD POUŽITÝCH POJMOV A SKRATIEK</b>	<b>10</b>
3.1 POUŽITÉ POJMY	10
3.2 SKRATKY	12
<b>4 ZÁKLADNÉ POJMY</b>	<b>13</b>
4.1 SLUŽBY AUTORITY ČASOVÝCH PEČIATOK (TSA)	13
4.2 AUTORITA ČASOVÝCH PEČIATOK	13
4.3 ŽIADATELIA O ČASOVÚ PEČIATKU A DRŽITELIA ČASOVEJ PEČIATKY	13
4.4 SPOLIEHAJÚCA SA STRANA	13
<b>5 POLITIKA TSA</b>	<b>14</b>
5.1 POUŽITIE ČASOVÝCH PEČIATOK	14
5.2 HODNOTENIE ZHODY A INÉ HODNOTENIA	14
5.2.1 <i>Periodicita hodnotenia alebo okolnosti pre prevedenie hodnotenia</i>	14
5.2.2 <i>Identita a kvalifikácia hodnotiteľa</i>	14
5.2.3 <i>Vzťah hodnotiteľa k hodnotenej entite</i>	15
5.2.4 <i>Hodnotené oblasti</i>	15
5.2.5 <i>Postupy v prípade zistených nedostatkov</i>	15
5.2.6 <i>Oznamovanie výsledkov hodnotenia</i>	15
<b>6 ZÁVÄZKY A ZODPOVEDNOSTI</b>	<b>17</b>
6.1 ZÁVÄZKY TSA	17
6.1.1 <i>Obecné záväzky TSA</i>	17
6.1.2 <i>Záväzky TSA vo vzťahu k žiadateľom o časovú pečiátku a držiteľom časových pečiatok</i>	17
6.2 ZÁVÄZKY ŽIADATEĽOV O ČASOVÚ PEČIATKU A DRŽITEĽOV ČASOVEJ PEČIATKY	18
6.3 ZÁVÄZKY SPOLIEHAJÚCICH SA STRÁN	18
6.4 ZODPOVEDNOSŤ	18
<b>7 POŽIADAVKY NA POSTUPY TSA</b>	<b>19</b>
7.1 SPRÁVA POLITIKY	19
7.1.1 <i>Organizácia spravujúca politiku TSA alebo vykonávaciu smernicu TSA</i>	19
7.1.2 <i>Kontaktná osoba organizácie spravujúca politiku TSA alebo vykonávaciu smernicu TSA</i>	19
7.1.3 <i>Subjekt zodpovedný za rozhodovanie o súlade postupov poskytovateľa s postupmi iných poskytovateľov certifikačných služieb</i>	19
7.1.4 <i>Postupy pri schvaľovaní súladu s bodom 7.1.3</i>	19
7.2 POŽIADAVKY NA ŽIVOTNÝ CYKLUS PÁROVÝCH DÁT TSA	19
7.2.1 <i>Generovanie a inštalácia párových dát TSA</i>	20
7.2.1.1 <i>Generovanie párových dát TSA</i>	20
7.2.1.2 <i>Odovzdanie verejného kľúča TSA</i>	20
7.2.1.3 <i>Poskytovanie verejného kľúča TSA</i>	20
7.2.1.4 <i>Dĺžky párových dát</i>	20
7.2.2 <i>Ochrana súkromného kľúča (dát pre vytváranie elektronických značiek) TSA</i>	21
7.2.2.1 <i>Štandardy a podmienky používania kryptografických modulov</i>	21
7.2.2.2 <i>Zdieľanie tajomstva</i>	21
7.2.2.3 <i>Úschova súkromného kľúča (dát pre vytváranie elektronických značiek) TSA</i>	21
7.2.2.4 <i>Zálohovanie súkromného kľúča (dát pre vytváranie elektronických značiek) TSA</i>	21
7.2.2.5 <i>Uchovávanie súkromného kľúča TSA</i>	21
7.2.2.6 <i>Transfer súkromného kľúča TSA</i>	21
7.2.2.7 <i>Uloženie súkromného kľúča TSA v kryptografickom module</i>	21
7.2.2.8 <i>Postup pri aktivácii súkromného kľúča TSA</i>	22
7.2.2.9 <i>Postup pri reaktivácii súkromného kľúča TSA</i>	22
7.2.2.10 <i>Postup pri zničení súkromného kľúča (dát pre vytváranie elektronických značiek, resp. elektronických podpisov)</i>	22
7.2.3 <i>Uchovávanie verejného kľúča TSA</i>	22

<b>Politika vydávania časových pečiatok</b>	<b>Strana 4 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

7.2.4	Profil certifikátu TSA.....	22
7.2.5	Aktivačné dáta .....	23
7.2.5.1	Generovanie a inštalácia aktivačných dát .....	23
7.2.5.2	Ochrana aktivačných dát .....	23
7.2.5.3	Ostatné aspekty aktivačných dát .....	23
7.2.6	Výmena párových dát TSA.....	24
7.2.7	Ukončenie životného cyklu párových dát TSA .....	24
7.2.8	Zneplatnenie a pozastavenie platnosti certifikátu TSA.....	24
7.2.8.1	Profil zoznamu zrušených certifikátov .....	24
7.2.8.2	Podmienky pre zneplatnenie certifikátu.....	25
7.2.9	Služby súvisiace s overovaním štatútu certifikátu TSA .....	25
7.2.9.1	Funkčné charakteristiky.....	25
7.2.9.2	Dostupnosť služieb .....	25
7.2.9.3	Ďalšie charakteristiky služieb štatútu certifikátu .....	25
7.2.10	Správa kryptografického modulu používaného pri vytváraní časových pečiatok .....	25
7.2.10.1	Hodnotenie kryptografického modulu.....	26
7.3	VYDÁVANIE ČASOVÝCH PEČIATOK.....	26
7.3.1	Žiadosť o časovú pečaťku.....	26
7.3.1.1	Subjekty oprávnené podať žiadosť o časovú pečaťku.....	26
7.3.1.2	Registračný proces a zodpovednosť poskytovateľa a žiadateľa.....	26
7.3.1.3	Počítačové overenie identity.....	26
7.3.1.3.1	Overovanie identity právnickej osoby alebo organizačnej zložky štátu .....	26
7.3.1.3.2	Overovanie fyzickej osoby .....	27
7.3.2	Spracovanie žiadosti o časovú pečaťku.....	27
7.3.2.1	Identifikácia a autentizácia .....	27
7.3.2.2	Prijatie alebo zamietnutie žiadosti o časovú pečaťku .....	27
7.3.2.3	Doba spracovania žiadosti o časovú pečaťku .....	27
7.3.3	Vydanie časovej pečiatky .....	27
7.3.3.1	Úkony TSA v priebehu vydávania časovej pečiatky .....	27
7.3.3.2	Oznámenie o vydaní časovej pečiatky držiteľom vydávania časovej pečiatky .....	28
7.3.4	Prevzatie časovej pečiatky .....	28
7.3.4.1	Klient.....	28
7.3.4.2	Spoliehajúca sa strana.....	28
7.3.5	Ukončenie poskytovania služieb pre žiadateľa o časovú pečaťku.....	28
7.3.6	Token časovej pečiatky.....	28
7.3.6.1	Profil žiadosti o časovú pečaťku.....	28
7.3.6.2	Profil odpovedi na žiadosť o časovú pečaťku .....	29
7.3.7	Synchronizácia meradla času s UTC .....	30
7.3.7.1	Synchronizácia.....	30
7.3.7.2	Bezpečnosť meradla času.....	30
7.3.7.3	Detekcia odchýlenia meradla času.....	30
7.3.7.4	Prestupná sekunda .....	30
7.4	SPRÁVA A PREVÁDZKOVÁ BEZPEČNOSŤ TSA.....	31
7.4.1	Riadenie bezpečnosti.....	31
7.4.2	Hodnotenie a riadenie rizík.....	31
7.4.3	Hodnotenie zraniteľnosti.....	31
7.4.4	Postup pri oznamovaní udalosti subjektu, ktorý ju spôsobil .....	31
7.4.5	Personálna bezpečnosť .....	31
7.4.5.1	Dôveryhodné role .....	31
7.4.5.2	Počet osôb požadovaných na zabezpečenie jednotlivých činností.....	31
7.4.5.3	Identifikácia a autentizácia pre každú pozíciu .....	32
7.4.5.4	Pozície vyžadujúce rozdelenie povinností.....	32
7.4.5.5	Požiadavky na kvalifikáciu, skúsenosť a bezúhonnosť .....	32
7.4.5.6	Posúdenie spoľahlivosti osôb .....	32
7.4.5.7	Požiadavky na prípravu pre výkon pozície, vstupné školenie .....	33
7.4.5.8	Požiadavky a periodičita školení.....	33
7.4.5.9	Periodičita a postupnosť rotácie pracovníkov medzi rôznymi pozíciami .....	33
7.4.5.10	Postihy za neoprávnené činnosti zamestnancov.....	33
7.4.5.11	Požiadavky na nezávislých zhotoviteľov.....	33
7.4.5.12	Dokumentácia poskytovaná zamestnancom .....	33
7.4.6	Fyzická bezpečnosť a bezpečnosť prostredia.....	33
7.4.6.1	Umiestnenie a konštrukcia .....	33
7.4.6.2	Fyzický prístup.....	34
7.4.6.3	Elektrina a klimatizácia .....	34
7.4.6.4	Vplyv vody.....	34
7.4.6.5	Protipožiarna opatrenia a ochrana.....	34
7.4.6.6	Ukladanie médií.....	34

<b>Politika vydávania časových pečiatok</b>	<b>Strana 5 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

7.4.6.7	Manipulácia s odpadmi .....	34
7.4.6.8	Zálohy mimo budovy prevádzkového pracoviska .....	34
7.4.7	<b>Prevádzkové riadenie</b> .....	34
7.4.7.1	Špecifické technické požiadavky na počítačovú bezpečnosť .....	34
7.4.7.2	Hodnotenie počítačovej bezpečnosti .....	35
7.4.8	<b>Riadenie prístupu do systému</b> .....	35
7.4.9	<b>Vývoj a údržba dôveryhodných systémov</b> .....	35
7.4.9.1	Riadenie vývoja systému .....	35
7.4.9.2	Kontroly riadenia bezpečnosti .....	35
7.4.9.3	Riadenie bezpečnosti životného cyklu .....	35
7.4.10	<b>Obnova po havárii alebo kompromitácii</b> .....	36
7.4.10.1	Postup v prípade incidentu a kompromitácie .....	36
7.4.10.2	Poškodenie výpočtových prostriedkov, software alebo dát .....	36
7.4.10.3	Postup pri zistení odchýlenia meradla času .....	36
7.4.10.4	Postup pri kompromitácii súkromného kľúča TSA .....	36
7.4.10.5	Schopnosť obnoviť činnosť po havárii .....	36
7.4.11	<b>Ukončenie činnosti TSA</b> .....	36
7.4.12	<b>Zhoda s právnymi predpismi</b> .....	37
7.4.13	<b>Úložisko informácií a dokumentácií, ktoré sa týkajú prevádzky TSA</b> .....	37
7.4.13.1	Auditné záznamy (logy) .....	37
7.4.13.1.1	Typy zaznamenávaných udalostí .....	38
7.4.13.1.2	Periodicita spracovania záznamov .....	38
7.4.13.1.3	Doba uchovávanía auditných záznamov .....	38
7.4.13.1.4	Ochrana auditných záznamov .....	38
7.4.13.1.5	Postupy pre zálohovanie auditných záznamov .....	38
7.4.13.1.6	Systém zhromažďovania auditných záznamov (interný alebo externý) .....	38
7.4.13.2	Uchovávanie informácií a dokumentácie .....	38
7.4.13.2.1	Typy informácií a dokumentácie, ktoré sa uchovávajú .....	39
7.4.13.2.2	Doba uchovávanía uchovávaných informácií a dokumentácie .....	39
7.4.13.2.3	Ochrana úložiska uchovávaných informácií a dokumentácie .....	39
7.4.13.2.4	Postupy pri zálohovaní uchovávaných informácií a dokumentácie .....	40
7.4.13.2.5	Požiadavky na používanie časových pečiatok pri uchovávaní informácií a dokumentácie .....	40
7.4.13.2.6	Systém zhromažďovania uchovávaných informácií a dokumentácie (interný, externý) .....	40
7.4.13.2.7	Postupy pre získanie a overenie uchovávaných informácií a dokumentácie .....	40
7.4.13.3	Zodpovednosti za zverejňovanie, úložisko informácií a dokumentácie .....	40
7.4.13.3.1	Úložisko informácií a dokumentácie .....	40
7.4.13.3.2	Zverejňovanie informácií a dokumentácie .....	40
7.4.13.3.3	Periodicita zverejňovania informácií .....	41
7.4.13.3.4	Riadenie prístupu k jednotlivým typom úložísk .....	42
7.5	<b>OSTATNÉ OBCHODNÉ A PRÁVNE ZÁLEŽITOSTI</b> .....	42
7.5.1	<b>Poplatky</b> .....	42
7.5.1.1	Poplatky za vydávanie časových pečiatok .....	42
7.5.1.2	Poplatky za prístup k certifikátom poskytovateľa .....	42
7.5.1.3	Poplatky za informácie o štatúte certifikátu a o zneplatnení .....	42
7.5.1.4	Poplatky za ďalšie služby .....	42
7.5.1.5	Iné ustanovenia týkajúce sa poplatkov (vrátane refundácií) .....	42
7.5.2	<b>Finančná zodpovednosť</b> .....	42
7.5.2.1	Krytie poistenia .....	42
7.5.2.2	Ďalšie aktíva a záruky .....	42
7.5.2.3	Poistenie alebo krytie zárukou pre koncových užívateľov .....	43
7.5.3	<b>Citlivosť obchodných informácií</b> .....	43
7.5.3.1	Výpočet citlivých informácií .....	43
7.5.3.2	Informácie mimo rámec citlivých informácií .....	43
7.5.3.3	Zodpovednosť za ochranu citlivých informácií .....	43
7.5.4	<b>Ochrana osobných údajov</b> .....	44
7.5.4.1	Politika ochrany osobných údajov .....	44
7.5.4.2	Osobné údaje .....	44
7.5.4.3	Údaje, ktoré nie sú považované za osobné .....	44
7.5.4.4	Zodpovednosť za ochranu osobných údajov .....	44
7.5.4.5	Oznámenie o používaní dôverných informácií a súhlas s používaním citlivých informácií .....	44
7.5.4.6	Poskytovanie citlivých informácií pre súdne či správne účely .....	44
7.5.4.7	Iné náležitosti sprístupňovania osobných údajov .....	44
7.5.5	<b>Práva duševného vlastníctva</b> .....	44
7.5.6	<b>Zastupovanie a záruky</b> .....	45
7.5.6.1	Zastupovanie a záruky I.CA .....	45
7.5.6.2	Zastupovanie a záruky držiteľov a klientov časových pečiatok .....	45
7.5.6.3	Zastupovanie a záruky spoliehajúcich sa strán .....	45

<b>Politika vydávania časových pečiatok</b>	<b>Strana 6 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

7.5.6.4	Zastupovanie a záruky ostatných zúčastnených subjektov .....	45
7.5.7	Zrieknutie sa záruk .....	45
7.5.8	Zodpovednosť za škodu, náhrada škody.....	45
7.5.9	Doba platnosti, ukončenie platnosti .....	46
7.5.9.1	Doba platnosti .....	46
7.5.9.2	Ukončenie .....	46
7.5.9.3	Dôsledky ukončenia a pretrvanie záväzkov .....	46
7.5.10	Komunikácia medzi participujúcimi subjektami .....	47
7.5.11	Zmeny .....	47
7.5.11.1	Postup pri zmenách.....	47
7.5.11.2	Postup pri oznamovaní zmien .....	47
7.5.11.3	Okolnosti, pri ktorých musí byť zmenené OID.....	47
7.5.12	Opatrenia pri riešení sporov.....	47
7.5.13	Relevantná právna úprava .....	47
7.5.14	Zhoda s právnymi predpismi.....	47
7.5.15	Ďalšie ustanovenia .....	48
7.5.15.1	Rámcová zhoda.....	48
7.5.15.2	Postúpenie práv .....	48
7.5.15.3	Oddeliteľnosť .....	48
7.5.15.4	Platby obhajcom a zrieknutie sa práv .....	48
7.5.15.5	Vyššia moc.....	48
7.5.16	Ďalšie opatrenia .....	48
<b>8</b>	<b>ZÁVEREČNÉ USTANOVENIA .....</b>	<b>49</b>

<b>Politika vydávania časových pečiatok</b>	<b>Strana 7 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## Úvod

Tento dokument, **Politika vydávania časových pečiatok**, vypracovaný spoločnosťou Prvá certifikačná autorita, a. s. (ďalej tiež I.CA) :

- je v súlade so zákonom Českej republiky č.227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonov (zákon o elektronickom podpise ), ako vyplýva zo zmien realizovaných zákonom č.226/2002 Sb., zákonom č. 517/2002 Sb., a zákonom č.440/2004 Sb., a s ním súvisiacich predpisov a vyhlášok
- je v súlade so zákonom Slovenskej republiky č. 215/2002 Zz. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok
- sa zaoberá skutočnosťami, ktoré sa vzťahujú na :
  - I.CA, klientov, spoliehajúce sa strany, zmluvných partnerov<sup>1</sup> a iných účastníkov PKI, a ktoré súvisia s vydávanou časovou pečaťou - jeho ďalšou správou a používaním
  - aspekty, súvisiace so správou TSS
- je kompatibilné s odporúčaniami ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities a RFC 3647, s prihliadnutím k odporúčaniam orgánov EU a k právu ČR a SR v danej oblasti.

Prekontrolujte a uistite sa o tom, že tento dokument zodpovedá Vaším požiadavkám na časové pečiatky.

---

<sup>1</sup> pojmy I.CA, klient, spoliehajúce sa strany a zmluvný partner sú uvedené v kapitole 0

<b>Politika vydávania časových pečiatok</b>	<b>Strana 8 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## Prehľad

Tento dokument môže byť okrem iného využitý nezávislými inštitúciami (napr. auditorskými spoločnosťami) ako základ pre potvrdenie toho, že akreditované/kvalifikované certifikačné služby v oblasti vydávania certifikátov poskytované spoločnosťou Prvá certifikačná autorita, a.s., je možné považovať za dôveryhodné.

Spoločnosť **Prvá certifikačná autorita, a.s.**, je od:

- 18.03.2002 prvým akreditovaným/kvalifikovaným poskytovateľom certifikačných služieb v ČR pre oblasť vydávania **kvalifikovaných certifikátov** podľa zákona ČR č. 227/2000 Sb., o elektronickom podpise a o zmene niektorých ďalších zákonov (zákon o elektronickom podpise), ako vyplýva zo zmien prevedených zákonom č. 226/2002 Z.z.(ČR), zákonom č. 517/2002 Z.z.(ČR), a zákonom č. 440/2004 Z.z.(Z.z.),
- 01.02.2006 akreditovaným/kvalifikovaným poskytovateľom certifikačných služieb v ČR pre oblasť vydávania **kvalifikovaných systémových certifikátov a kvalifikovaných časových pečiatok** podľa zákona ČR č. 227/2000 Z.z.(ČR), o elektronickom podpise a o zmene niektorých ďalších zákonov (zákon o elektronickom podpise), ako vyplýva zo zmien prevedených zákonom č. 226/2002 Z.z.(ČR), zákonom č. 517/2002 Z.z.(ČR), a zákonom č. 440/2004 Z.z.(ČR),
- 21.09.2006 prvým zahraničným akreditovaným poskytovateľom certifikačných služieb v SR, ktorému bola udelená akreditácia v oblasti poskytovania **kvalifikovaných certifikátov a časových pečiatok** podľa aktuálneho znenia zákona SR č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok

Podrobný popis autority časových pečiatok je uvedený v ďalších dokumentoch, ktoré sú obecné neverejné. Neverejné dokumenty, vrátane správ, výsledkov testov a interných auditov vytvárajú dokumentačnú sadu, dosiahnuteľnú výhradne autorizovanému personálu a audítorom. V tabuľke 3 sú uvedené významné bezpečnostné dokumenty, vzťahujúce sa ku službám časových pečiatok.

Tab. 3 – Bezpečnostné dokumenty

Číslo	Názov dokumentu	Status
1.	Politika vydávania časových pečiatok	Verejný
2.	Prevádzková smernica vydávania časových pečiatok	Neverejný
3.	Správa a súhlas vedenia I.CA o hodnotení rizík autority časových pečiatok (obsahujúca analýzu rizík)	Neverejný
4.	Systémová bezpečnostná politika autority časových pečiatok	Neverejný
5.	Plán pre zvládnutie krízových situácií a plán obnovy	Neverejný
6.	Správa pre používateľov autority časových pečiatok	Verejný
7.	Sada bezpečnostných noriem a smerníc	Neverejný
8.	Celková bezpečnostná politika	Neverejný
9.	Prehlásenie o aplikovateľnosti	Neverejný

Dokument Politika vydávania 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 prevádzkovaná. Technické a operačné detaily sú uvedené v relevantných interných dokumentoch.

Vydávanie a správa certifikátov poskytovateľom sa riadi špeciálne vytvorenými internými dokumentmi „Certifikačná politika vydávania certifikátov CA/TSS“ a „Certifikačné vykonávacie smernice pre vydávanie certifikátov CA/TSS“.

V procese poskytovania akreditovaných/kvalifikovaných certifikačných služieb v oblasti vydávania certifikátov prevádzkuje spoločnosť Prvá certifikačná autorita, a.s., jedinou certifikačnú autoritu.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 9 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

V procese poskytovania akreditovaných/kvalifikovaných certifikačných služieb v oblasti vydávania časových pečiatok prevádzkuje spoločnosť Prvá certifikačná autorita, a.s, jedinou autoritu časových pečiatok, ktorej jadrom je sada kvalitatívne totožných serverov, generujúcich tieto časové pečiatky.

Informácie o ďalších poskytovaných certifikačných službách je možno získať na internetovej informačnej adrese, uvedenej v kapitole 1.17.13.3.2.

## **1.1 Názov a identifikácia dokumentu**

Názov tohto dokumentu : Politika vydávania časových pečiatok  
OID : 1.3.6.1.4.1.23624.1.4.14.2

<b>Politika vydávania časových pečiatok</b>	<b>Strana 10 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## Prehľad použitých pojmov a skratiek

Nižšie uvedený prehľad pojmov a skratky je platný pre tento dokument. V prípade pojmu môže byť na pravej strane v zátvorkách uvedený zdroj, v ktorom sa nachádza pôvodný pojem, vrátane definície. Použité skratky majú alternatívny charakter, t.j. v texte môže byť použitý ako plný text, tak aj jeho skratka, pričom oboje má totožnú obsahovú hodnotu.

### 1.2 Použité pojmy

Tabuľka 4 – Pojmy

Pojem	Vysvetlenie
Certifikát	dátová správa, ktorá je vydaná poskytovateľom certifikačných služieb, spája údaje pre overovanie elektronických podpisov s podpisujúcou osobou a umožňuje overiť jej identitu, alebo spája údaje pre overovanie elektronických značiek s označujúcou osobou a umožňuje overiť jej identitu
Čas	Svetový čas UTC
Držiteľ	fyzická osoba, právnická osoba alebo organizačná zložka štátu, ktorá požiadala o vydanie časovej pečiatky a ktorej bolo časová pečiatka vydaná
Elektronický podpis	údaje v elektronickej podobe, ktoré sú pripojené k údajom správy alebo sú s ňou logicky spojené a ktoré slúžia ako metóda k jednoznačnému overeniu identity podpísanej osoby vo vzťahu k obsahu správy
Elektronická značka	údaje v elektronickej podobe, ktoré sú pripojené k dátovej správe alebo sú s ňou logicky spojené a ktoré spĺňajú nasledujúce požiadavky: <ul style="list-style-type: none"> <li>• Sú jednoznačne spojené s označujúcou osobou a umožňujú jej identifikáciu pomocou kvalifikovaného systémového certifikátu</li> <li>• Boli vytvorené a pripojené k dátovej správe pomocou prostriedkov pre vytváranie elektronických značiek, ktoré označujúca osoba môže držať pod svojou výhradnou kontrolou</li> <li>• Sú k dátovej správe, ku ktorej sa vzťahujú pripojené takým spôsobom, že je možné zistiť akúkoľvek následnú zmenu dokumentu</li> </ul>
Hash	matematicky vypočítaná jedinečná hodnota, predstavujúca zhustenú hodnotu dlhej správy, z ktorej bola vypočítaná
I.CA	První certifikační autorita, a.s. – akreditovaný/kvalifikovaný poskytovateľ certifikačných služieb v súlade s § 2 ZoEP.
Klient	fyzická, právnická osoba alebo organizačná zložka štátu, ktorá uzavrela s I. CA zmluvu o využívaní certifikačnej služby v oblasti časových pečiatok.
Časová pečiatka	dátová správa, ktorú vydal akreditovaný/kvalifikovaný poskytovateľ certifikačných služieb a ktorá dôveryhodným spôsobom spája údaje v elektronickej podobe s časovým okamžikom, a zaručuje, že uvedené údaje v elektronickej podobe existovali pred daným časovým okamihom (§ 2, písm. R ZoEP)
Kvalifikovaný certifikát (QC)	certifikát, ktorý má náležitosti podľa platnej legislatívy (ZoEP ČR, SR) a bol vydaný akreditovaným/kvalifikovaným poskytovateľom certifikačných služieb
Kvalifikovaný systémový certifikát (QSC)	certifikát, ktorý má náležitosti podľa § 12a ZoEP ČR a bol vydaný kvalifikovaným poskytovateľom certifikačných služieb (§ 2, písm. m ZoEP ČR)
Nadriadený kvalifikovaný systémový certifikát, resp. certifikát I.CA alebo certifikát TSS	kvalifikovaný systémový certifikát alebo kvalifikovaný certifikát poskytovateľa certifikačných služieb, ktorý sa riadi špeciálnymi dokumentmi vydanými I.CA

<b>Politika vydávania časových pečiatok</b>	<b>Strana 11 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

	<ul style="list-style-type: none"> <li>• Certifikačná politika vydávania certifikátov CA,/TSS</li> <li>• Certifikačná vykonávacia smernica vydávanie certifikátov CA/ TSS</li> </ul>
Nonce	Náhodné číslo, o ktorom sa predpokladá, že ho klient vygeneruje iba jedenkrát (64 bit integer). V prípade, že toto číslo žiadosť obsahuje, potom toto číslo musí obsahovať aj odpoveď.
Odtlačok	pozri hash
Párové údaje	jedinečné údaje pre vytváranie elektronického podpisu alebo elektronickej značky spolu s odpovedajúcimi údajmi pre overovanie elektronického podpisu alebo elektronickej značky
Podpisujúca osoba	Fyzická osoba, ktorá je držiteľom prostriedku pre vytváranie elektronického podpisu a koná svojim menom, alebo menom inej fyzickej alebo právnickej osoby
ReqPolicy	Identifikátor politiky
Zmluvný partner	poskytovateľ dôveryhodných časových služieb, ktorý zaisťuje tieto služby na základe písomnej zmluvy pre I.CA
Súkromný kľúč	jedinečné údaje pre vytváranie elektronického podpisu alebo elektronickej značky
Štatút kvalifikovaného certifikátu	stav, v ktorom sa kvalifikovaný certifikát nachádza t.j. v stave platnosti, neplatnosti, zneplatnenia, zablokovania
Spoliehajúca sa strana	subjekt, spoliehajúci sa pri svojej činnosti na vydaný kvalifikovaný certifikát alebo časovú pečať
Používateľ	klient, držiteľ, spoliehajúca sa strana, žiadateľ, popr. subjekt, rozhodujúci sa o využívanie poskytovanej certifikačnej služby v oblasti časových pečiatok
Verejný kľúč	jedinečný údaj pre overovanie elektronického podpisu alebo elektronickej značky
Zablokovanie	stav, v ktorom sa kvalifikovaný certifikát alebo kvalifikovaný systémový certifikát nachádza od doby, keď ho I.CA zneplatnila, do doby, kedy I.CA zverejnila CRL, v ktorom je tento kvalifikovaný certifikát alebo kvalifikovaný systémový certifikát prvýkrát zaradený
Zaručený elektronický podpis	Elektronický podpis, ktorý spĺňa nasledujúce požiadavky: <ul style="list-style-type: none"> <li>• Je jednoznačne spojený s podpisujúcou osobou</li> <li>• Umožňujú jednoznačnú identifikáciu podpisujúcej osoby vo vzťahu k dátovej správe</li> <li>• Bol vytvorený a pripojený k dátovej správe pomocou prostriedkov, ktoré podpisujúca osoba môže držať pod svojou výhradnou kontrolou</li> <li>• Sú k dátovej správe, ku ktorej sa vzťahujú pripojené takým spôsobom, že je možné zistiť akúkoľvek následnú zmenu dokumentu</li> </ul>
Zneplatnenie	stav kvalifikovaného certifikátu, ktorý bol I.CA zneplatnený – tomuto certifikátu sa nedá už obnoviť platnosť
Žiadateľ	fyzická osoba, oprávnený konateľ právnickej osoby alebo organizačná zložka štátu, podávajúca žiadosť o využívanie služby poskytovania časových pečiatok spoločností Prvá certifikačná autorita, a.s..
Žiadosť o službu (Žiadosť)	formálny dokument žiadosti o niektorú zo služieb poskytovaných I.CA napr. žiadosť o vydanie časovej pečiatky
Žiadosť o vydanie časovej pečiatky	formálny, štandardný dokument elektronickej žiadosti o vydanie časovej pečiatky podľa prípustných noriem a smerníc definovaných v tejto politike

<b>Politika vydávania časových pečiatok</b>	<b>Strana 12 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

### 1.3 Skratky

Tabuľka 5 – Skratky

<b>Skratka</b>	<b>Vysvetlenie</b>
<b>CRL</b>	<b>Certificate Revocation List</b> (zoznam zneplatnených certifikátov)
<b>DS/NTP</b>	<b>Datume Secure/Network Time Protocol</b> – zabezpečená varianta NTP protokolu
<b>ETSI</b>	<b>European Telecommunications Standards Institute</b>
<b>IETF</b>	<b>Internet Engineering Task Force</b>
<b>EPS</b>	<b>Elektronická Požiarna Signalizácia</b>
<b>HSM</b>	<b>Hardware Security Modul</b>
<b>IETF</b>	<b>Internet Engineering Task Force</b>
<b>MV ČR</b>	<b>Ministerstvo Vnútra Českej Republiky</b>
<b>NIST</b>	<b>National Institute of Standards and Technology</b>
<b>NMI</b>	<b>National Measurement Institute</b> (Národná úrad pre miery a váhy – v USA)
<b>NTMS</b>	<b>Network Time Management System</b> (Systém správy času prostredníctvom siete)
<b>NTP</b>	<b>Network Time Protocol</b>
<b>OID</b>	(Object identifier) číselná identifikácia objektu v rámci jednotnej klasifikácie objektov podľa ISO/ITU
<b>PKI</b>	<b>Public Key Infrastructure</b>
<b>TMC</b>	<b>Trusted Master Clock</b> (hodiny v koreni služby distribúcie TT)
<b>TS</b>	<b>Time Stamp</b> (časová pečiatka)
<b>TSA</b>	<b>Time Stamping Authority</b> (autorita časových pečiatok)
<b>TSQ</b>	<b>Time Stamp Query</b> (žiadosť o časovú pečiatku)
<b>TSR</b>	<b>Time Stamp Response</b> (odpoveď na žiadosť o časovú pečiatku)
<b>TSS</b>	<b>Time Stamp Server</b> (Server generujúci časové pečiatky)
<b>TT</b>	<b>Trusted Time</b> (Dôveryhodný čas)
<b>TTDS</b>	<b>Trusted Time Distribution System</b>
<b>TTI</b>	<b>Trusted Time Infrastructure</b> (Infraštruktúra dôveryhodného času)
<b>TST</b>	<b>Time Stamp Token</b> (časť časovej pečiatky obsahujúca meno TSS, UTC čas, presnosť, sériové číslo, verzia, hash algoritmus, nonce)
<b>UPS</b>	<b>Uninterruptible Power Supply</b>
<b>UTC</b>	<b>Universal Co-ordinated Time</b> , štandard prijatý 1.1.1972 pre svetový koordinovaný čas (Coordinated Universal Time – UTC). Funkciu "oficiálneho časomerača" atómového času pre celý svet vykonáva Bureau International de l'Heure (BIPM)
<b>VoEP</b>	<ul style="list-style-type: none"> <li>vyhláška Českej republiky č. 378/2006 Z.z. o postupoch kvalifikovaných poskytovateľoch certifikačných služieb, o požiadavkách na nástroje elektronického podpisu a o požiadavkách na ochranu údajov pre vytváranie elektronických značiek (vyhláška o kvalifikovaných poskytovateľoch certifikačných služieb)</li> <li>vyhláška Slovenskej republiky č. 540/2002 Z.z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu auditorov</li> </ul>
<b>ZoEP</b>	<ul style="list-style-type: none"> <li>aktuálne znenie zákona Českej republiky č. 227/2000 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonov (zákon o elektronickom podpise), ako to vyplýva zo zmien vykonaných zákonom č. 226/2002 Sb., zákonom č. 517/2002 Sb., a zákonom č. 440/2004 Sb.</li> <li>aktuálne znenie zákona Slovenskej republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov</li> </ul>

<b>Politika vydávania časových pečiatok</b>	<b>Strana 13 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## Základné pojmy

Ak nie je uvedené inak, je ďalej v tomto dokumentu pod pojmami :

- **certifikát** mienený kvalifikovaný certifikát alebo kvalifikovaný systémový certifikát
- **časová pečiatka** mienená kvalifikovaná časová pečiatka
- **certifikát TSS** mienený certifikát TSS poskytovateľa

### 1.4 Služby autority časových pečiatok (TSA)

Procesy spojené s vydávaním časových pečiatok sú rozdelené do dvoch oblastí :

- základné procesy – 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 časového údaja TSS s poskytovateľom dôveryhodných synchronizačných časových služieb, ktorý zaisťuje tieto služby na základe písomnej zmluvy pre I. CA
  - správa ostatných systémových programových komponentov TSA

### 1.5 Autorita časových pečiatok

TSA je z pohľadu klientov a spoliehajúcich sa strán dôveryhodná komunikačná infraštruktúra vydávajúca časové pečiatky. Z titulu prevádzkovateľa nesie celkovú zodpovednosť za poskytovanie certifikačných služieb v oblasti vydávania časových pečiatok spoločnosť Prvá certifikačná autorita, a.s.

Pre základné procesy (kapitola 1.4) nie sú využívaní zmluvní partneri a generovanie časových pečiatok je vykonávané serverom/servermi (TSS), umiestneným v prevádzkovom prostredí I.CA.

### 1.6 Žiadatelia o časovú pečiatku a držitelia časovej pečiatky

Žiadateľom alebo držiteľom časovej pečiatky môže byť na základe písomnej zmluvy s I.CA individuálny koncový užívateľ (fyzická osoba), alebo právnická osoba, resp. organizačná zložka štátu zahŕňajúca niekoľko koncových užívateľov.

V prípade, že žiadateľom alebo držiteľom časovej pečiatky je individuálny koncový užívateľ, je potom tento priamo zodpovedný za to, že splní záväzky voči I.CA

V prípade, že žiadateľom alebo držiteľom časovej pečiatky je právnická osoba alebo organizačná zložka štátu, tak jej záväzky voči I.CA platí aj pre jej koncových užívateľov a táto právnická osoba alebo organizačná zložka štátu je vždy zodpovedná za to, že jej koncoví užívatelia záväzky voči I.CA splnia. Preto musí právnická osoba alebo organizačná zložka štátu vhodným spôsobom informovať vlastných koncových užívateľov.

### 1.7 Spoliehajúca sa strana

Spoliehajúcou sa stranou je individuálny koncový užívateľ (fyzická osoba), právnická osoba alebo organizačná zložka štátu, spoliehajúca sa pri svojej činnosti na vydané časové pečiatky.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 14 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## Politika TSA

### 1.8 Použitie časových pečiatok

Politika vydávania časových pečiatok nedefinuje žiadne obmedzenia použiteľnosti časovej pečiatky vydané v súlade s jej obsahom<sup>2</sup>. Časovú pečiatku možné použiť napr. v oblastiach :

- elektronických podpisov alebo elektronických značiek, keď je treba overiť, že boli vytvorené v dobe, keď certifikát verejného kľúča podpisujúci alebo označujúci entity bol platný. Táto kontrola je nevyhnutná z nasledujúcich dvoch dôvodov:
  - či nebol behom platnosti certifikátu elektronicky podpisujúcu alebo označujúcu entitu odpovedajúci súkromný kľúč kompromitovaný
  - či nebol elektronický podpis alebo značka vytvorená po ukončení doby platnosti príslušného certifikátu
- ochrane spustiteľného kódu
- transakcií prevádzaných na sieti

### 1.9 Hodnotenie zhody a iné hodnotenia

V I.CA sú vykonávané hodnotenia bezpečnosti v oblastiach, uvedených v kapitole 1.9.4. Súčasťou týchto hodnotení je okrem iného sledovanie, či sú úplne dodržované štandardy, uvedené v kapitole 1.17.7.2. Oblasť hodnotenia zhody a iných hodnotení (kapitoly 1.9.1 až 1.9.6) je upravená internou smernicou I.CA.

S ohľadom na skutočnosť, že I.CA je akreditovaným poskytovateľom certifikačných služieb (viď. kapitola 2), je ďalej podľa príslušných legislatív vykonávaný dozor nad jej činnosťou akreditačnými úradmi, konkrétne Ministerstvom vnútra Českej republiky a Národným bezpečnostným úradom Slovenskej republiky.

#### 1.9.1 Periodicita hodnotenia alebo okolnosti pre prevedenie hodnotenia

Celková kontrola bezpečnostnej zhody je prevádzaná po 4 rokoch od predchádzajúcej celkovej kontroly bezpečnostnej zhody. Behom týchto 4 rokov sú vykonávané ročné čiastočné kontroly bezpečnostnej zhody. Kontrola bezpečnostnej zhody je vykonávaná podľa požiadaviek technickej normy ČSN ISO/IEC TR 13335 - Informačné technológie – Smernica pre riadenie bezpečnosti IT 1-3.

Audit systému riadenia bezpečnosti informácií je vykonávaný po 2 rokoch od predchádzajúceho auditu systému bezpečnosti informácií a je vykonávaný podľa požiadavkou normy ČSN EN ISO 19011 - Smernica pre auditovanie systému manažmentu akosti a/alebo systému environmentálneho manažmentu.

#### 1.9.2 Identita a kvalifikácia hodnotiteľa

Identita a kvalifikácia hodnotiteľa je upravená internou smernicou I.CA.

<sup>2</sup> Časové pečiatky vydané podľa tejto politiky je možné používať v otvorených systémoch verejnej správy (napr. štátnej správy), ako aj v uzavretých systémoch súkromných spoločností

<b>Politika vydávania časových pečiatok</b>	<b>Strana 15 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

### 1.9.3 Vzťah hodnotiteľa k hodnotenej entite

V prípade auditu systému manažmentu bezpečnosti informácií je hodnotiteľom externá, nezávislá auditujúca fyzická/právnická osoba.

V prípade kontroly bezpečnostnej zhody je hodnotiteľom pracovník I.CA, poverený riaditeľom spoločnosti Prvá certifikačná autorita, a.s.

### 1.9.4 Hodnotené oblasti

Cieľom kontroly bezpečnostnej zhody je overenie že spoločnosť Prvá certifikačná autorita, a.s. :

- prevádzkuje dôveryhodné systémy v súlade so ZoEP a VoEP
- prevádza zmeny v dôveryhodných systémoch v súlade s bezpečnostnou dokumentáciou, a to jej časťami upravujúcimi riadenie zmien

Predmetom kontroly bezpečnostnej zhody :

- sú všetky dôveryhodné systémy I.CA (celková kontrola bezpečnostnej zhody), alebo
- sú všetky zmeny, ktoré I.CA previedla od prevedenia predchádzajúcej kontroly bezpečnostnej zhody, a ich vplyv na dôveryhodné systémy I.CA (čiastočná kontrola bezpečnostnej zhody), alebo
- je v prípade, že v dôveryhodných systémoch I.CA nenastali od predchádzajúcej čiastočnej kontroly bezpečnostnej zhody žiadne zmeny, overenie tejto skutočnosti.

Cieľom auditu systému manažmentu bezpečnosti informácií je objektívne a na I.CA nezávislé overenie, že je v spoločnosti zavedený a uplatňovaný systém manažmentu bezpečnosti informácií.

S ohľadom na uvedené, poskytne I.CA subjektu, ktorý audit systému manažmentu bezpečnosti informácií prevádza:

- správu o naposledy prevedenej kontrole bezpečnostnej zhody
- bezpečnostnú dokumentáciu (v aktuálnych verziách)

### 1.9.5 Postupy v prípade zistených nedostatkov

V prípade nedostatkov, zistených na základe správy o kontrole bezpečnostnej zhody, právy o audite systému riadenia bezpečnosti informácií, je bezpečnostný manažér povinný do 15 dní po získaní správy určiť, aké opatrenia k odstráneniu nedostatkov je I.CA povinná prijať.

Ak zistí príslušný akreditačný úrad (pozri kapitoly 0), že I.CA porušuje povinnosti stanovené ZoEP, VoEP (kapitoly 5.2.4 a 5.2.6) uloží jej, aby v stanovenej dobe zjedнала nápravu a prípadne určí, aké opatrenia k odstráneniu nedostatkov je I.CA povinná prijať.

### 1.9.6 Oznamovanie výsledkov hodnotenia

I.CA zaistí spracovanie správy o kontrole bezpečnostnej zhody, ktorej obsahom je :

- určenie predmetu kontroly bezpečnostnej zhody :
  - celková kontrola bezpečnostnej zhody - vymedzenie všetkých dôveryhodných systémov s uvedením kvalifikovaných/akreditovaných certifikačných služieb, ktoré sú prostredníctvom týchto systémov zabezpečované
  - čiastočná kontrola bezpečnostnej zhody - vymedzenie zmien, ktoré I.CA vykonala od prevedenia predchádzajúcej kontroly bezpečnostnej zhody a vymedzenie kvalifikovaných/akreditovaných certifikačných služieb, ktoré sú zabezpečované pomocou dôveryhodných systémov, týmito zmenami ovplyvnené
- identifikácia dokumentácie, ktorá bola predmetom kontroly bezpečnostnej zhody

<b>Politika vydávania časových pečiatok</b>	<b>Strana 16 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

- popis postupu, akým bola kontrola bezpečnostnej zhody vykonaná
- meno, popřípade mená a priezvisko osoby, ktorá kontrolu bezpečnostnej zhody vykonala
- prehlásenie subjektu, ktorý kontrolu bezpečnostnej zhody vykonal, o výsledku kontroly bezpečnostnej zhody, ktorého súčasťou je vyhlásenie o tom, že I.CA prevádzkuje dôveryhodné systémy v súlade so ZoEP, VoEP a vykonáva zmeny v dôveryhodných systémoch v súlade s bezpečnostnou dokumentáciou, a to jej časťami upravujúcimi riadenie zmien.

Správa o kontrole bezpečnostnej zhody:

- je odovzdaná bezpečnostnému manažérovi do 10 dní od ukončenia kontroly, ktorý s jej obsahom oboznámi riaditeľa I.CA a bezpečnostný výbor
- je odovzdaná príslušnému úradu do 30 dní po ukončení kontroly.

I.CA zabezpečí :

- že správa o audite systému manažmentu bezpečnosti informácií obsahuje :
  - vymedzenie predmetu auditu systému manažmentu bezpečnosti informácií, pričom vymedzenie predmetu auditu sa rozumie vymedzenie kvalifikovaných/akreditovaných certifikačných služieb, ktoré sú zabezpečované pomocou dôveryhodných systémov,
  - identifikácia dokumentácie, ktorá bola predmetom auditu systému manažmentu bezpečnosti informácií a ktorú I.CA poskytla subjektu, ktorý audit systému manažmentu bezpečnosti informácií vykonáva,
  - vyhlásenie subjektu, ktorý audit systému manažmentu bezpečnosti informácií vykonal, o výsledku auditu systému manažmentu bezpečnosti informácií, ktorého súčasťou je vyhlásenie o tom, že je v I.CA uplatňovaný systém manažmentu bezpečnosti informácií.
- zverejnenie vyhlásenia o výsledku auditu systému manažmentu bezpečnosti informácií v správe pre používateľa.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 17 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## Závazky a zodpovednosti

### 1.10 Závazky TSA

#### 1.10.1 Obecné závazky TSA

Spoločnosť První certifikační autorita, a.s., zaručuje, že :

- prístup k službám TSA s výnimkou plánovaných (vopred ohlásených), popr. neplánovaných časových prerušení (tieto okolnosti sú uvedené v internej dokumentácii) spojených s technickými zásahmi je nepretržitý
- autentifikovaný prístup k službám vydávania časových pečiatok na základe písomnej zmluvy (viď. kap. 4.3)
- striktné dodržiavanie platnej legislatívy
- súlad so zákonmi a neporušovanie autorských ani licenčných práv aktivitami spoločnosti
- ochráni všetky osobné údaje podľa platnej legislatívy
- sa hocikto môže uistiť o jej identite a jej certifikáte/certifikátov TSS
- poskytovanie kvalifikovaných certifikačných služieb vykonávajú osoby s odbornými znalosťami a kvalifikáciou nevyhnutnou pre poskytovanie kvalifikovanej certifikačnej služby a oboznámené s príslušnými bezpečnostnými postupmi
- používa bezpečné systémy a bezpečné nástroje - zaisťuje dostatočnú bezpečnosť postupov, ktoré tieto systémy a nástroje podporujú vrátane dostatočnej kryptografickej bezpečnosti týchto nástrojov
- používa bezpečné systémy pre uchovávanie časových pečiatok
- má počas celej doby svojej činnosti k dispozícii dostatočné finančné zdroje alebo iné finančné zaistenie na prevádzku v súlade s požiadavkami uvedenými ZoEP a s ohľadom na riziko vzniku zodpovednosti za škodu po celú dobu činnosti
- pred uzatvorením zmluvy (viď. kap. 4.3) s klientom o vydávaní časových pečiatok ho písomne informuje o presných podmienkach pre využívanie tejto služby, vrátane prípadných obmedzení pre jej použitie, a o podmienkach reklamácií a riešení vzniknutých sporov a o tom, či je či nie je akreditovaná
- pokiaľ jej bude odobratá akreditácia, bezodkladne informuje o tejto skutočnosti klientov a ďalšie dotknuté osoby
- uchováva informácie a dokumentáciu súvisiacu s poskytovanou službou vydávania časových pečiatok podľa požiadaviek ZoEP
- jej kmeňoví zamestnanci, prípadne iné fyzické osoby, ktoré prichádzajú do styku s osobnými údajmi sú povinný zachovávať mlčanlivosť o týchto údajoch a dátach a o bezpečnostných opatreniach, ktorých zverejnenie by ohrozilo zabezpečenie týchto údajov a dát. Povinnosť mlčanlivosti trvá aj po skončení pracovného alebo iného obdobného pomeru alebo po prevedení príslušných prác

#### 1.10.2 Závazky TSA vo vzťahu k žiadateľom o časovú pečať a držiteľom časových pečiatok

Spoločnosť První certifikační autorita, a.s., zabezpečuje a zaručuje, že :

- jej vydávaná časová pečať obsahuje všetky náležitosti stanovené ZoEP, VoEP
- použije súkromné kľúče príslušné certifikátom TSS iba k označovaniu vydávaných časových pečiatok
- dáta v elektronickej podobe, ktoré sú predmetom žiadosti o vydanie časovej pečiatky, jednoznačne odpovedajú dátam v elektronickej podobe obsiahnutým vo vydanéj časovej pečiatke
- implementovala odpovedajúce opatrenia proti falšovaniu časových pečiatok
- vydá časovú pečať bezodkladne po získaní platnej požiadavky
- žiadnym spôsobom neoveruje odtlačok (hash), ktorému má byť časová pečať priradená (s výnimkou jeho dĺžky)
- využíva dôveryhodnú časovú synchronizáciu

<b>Politika vydávania časových pečiatok</b>	<b>Strana 18 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

- jej vydaná časová pečiatka obsahuje minimálne :
  - unikátne číslo časovej pečiatky
  - označenie pravidiel, podľa ktorých bola časová pečiatka vydaná
  - jej názov a štát, v ktorom má sídlo
  - časový údaj, ktorého odchýlka nepresiahne 1 sekundu od UTC
  - dáta v elektronickej podobe - odtlačok (hash), pre ktorý bola časová pečiatka vydaná
  - elektronickú značku alebo podpis TSS

### **1.11 Závazky žiadateľov o časovú pečiatku a držiteľov časovej pečiatky**

Žiadatelia sú vždy po získaní odpovede na žiadosť o časovú pečiatku povinní zistiť chybový status. V prípade chyby nie je časová pečiatka v odpovedi obsiahnutá a žiadateľ je povinný prekontrolovať odpovedajúcu chybové hlásenie. V opačnom prípade je predplatiteľ povinný:

- overiť elektronickú značku alebo elektronický podpis TST a skontrolovať, či certifikát TSS nebol odvolaný - CRL je prístupné na elektronickej informačnej adrese (kapitola 1.17.13.3.2)
- overiť, či je vrátený odtlačok (hash) totožný s odoslaným
- 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

### **1.12 Závazky spoliehajúcich sa strán**

Obecným záväzkom spoliehajúcich sa strán je overenie elektronickej značky alebo elektronického podpisu TST. Spoliehajúca sa strana je povinná :

- overiť platnosť certifikátu TSS
- prekontrolovať, či politika, pod ktorou bola časová pečiatka vydaná, je akceptovateľná jej potrebám, popr. potrebám jej prevádzkovej aplikácie

V prípade overovania časovej pečiatky po ukončení platnosti certifikátu TSS sú spoliehajúce sa strany povinné :

- overiť, či certifikát TSS nebol v dobe vydania časovej pečiatky odvolaný - CRL je prístupné na elektronickej informačnej adrese (kapitola 1.17.13.3.2)
- overiť, či kryptografická funkcia pre tvorbu odtlačku (hash) v časovej pečiatke je stále bezpečná – uvedené na elektronickej informačnej adrese (kapitola 1.17.13.3.2)
- uistiť sa, či je dĺžka kryptografického kľúča a algoritmus stále považovaný za bezpečné - uvedené na elektronickej informačnej adrese (kapitola 1.17.13.3.2)

### **1.13 Zodpovednosť**

Všetky záruky a z nich vyplývajúce plnenia je možné uznať len vtedy, pokiaľ klient alebo spoliehajúca sa strana neporušila povinnosti, vyplývajúce im z tejto politiky. Na časové pečiatky, ktoré I.CA nevydala, sa záruky nevzťahujú.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 19 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## Požiadavky na postupy TSA

### 1.14 Správa politiky

#### 1.14.1 Organizácia spravujúca politiku TSA alebo vykonávaciu smernicu TSA

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

#### 1.14.2 Kontaktná osoba organizácie spravujúca politiku TSA alebo vykonávaciu smernicu TSA

Riaditeľ I.CA určuje kontaktnú osobu, ktorej e-mail, telefónne číslo a fax sú uvedené na internetovej informačnej adrese (kapitola 1.17.13.3.2).

#### 1.14.3 Subjekt zodpovedný za rozhodovanie o súlade postupov poskytovateľa s postupmi iných poskytovateľov certifikačných služieb

Jedinou osobou, ktorá je zodpovedná za rozhodovanie o súlade postupov I.CA s postupmi iných poskytovateľov certifikačných služieb, je riaditeľ spoločnosti První certifikační autorita, a.s.

#### 1.14.4 Postupy pri schvaľovaní súladu s bodom 7.1.3

V prípade, že je potrebné s ohľadom na kapitolu 1.14.3 previesť zmeny v tejto politike a v odpovedajúcej vykonávacej smernice, určuje riaditeľ I.CA osobu, ktorá je oprávnená zmeny vykonávať. Ďalej platí ustanovenie, uvedené v kapitole 1.14.3.

### 1.15 Požiadavky na životný cyklus párových dát TSA

Párové dáta TSA sú používané pre zaistenie integrity, dôvernosti, autentizácie a zaistenie neodmietnuteľnosti zodpovednosti. S ohľadom na rôzne úrovne hrozieb, ktoré závisia na spôsobe využívania párových dát, sa dajú kľúče rozdeliť do nasledujúcich kategórií :

- párové dáta vyhradené pre elektronické označovanie alebo elektronické podpisovanie vydávaných časových pečiatok a overovanie elektronickej značky alebo elektronického podpisu vydaných časových pečiatok
- párové dáta vyhradené pre infraštruktúru dôveryhodného času, využívané v procesoch kontroly a synchronizáciu meradla času TSS
- párové dáta využívané v procese správy systému TSA.

Nasledujúce kapitoly (7.2.1 až 7.2.10), vrátane ich podkapitol, riešia problematiku serverov generujúcich časové pečiatky (TSS). Konkrétny technický postup generovania párových dát TSS a následné vyhotovenie certifikátu TSS je popísaný v internej dokumentácii I.CA.

Konkrétny technický postup generovania párových dát TSS a následné vyhotovenie certifikátu TSS je popísaný v internej dokumentácii I.CA.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 20 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

### 1.15.1 Generovanie a inštalácia párových dát TSA

#### 1.15.1.1 Generovanie párových dát TSA

Generovanie párových dát I.CA, ktoré prebieha v zabezpečenej zóne v súlade s dokumentom „**Systémová bezpečnostní politika TSA**“ a o ktorého priebehu je vyhotovený písomný protokol, je vykonávané v kryptografickom module, ktorý splňuje [požiadavky na kryptografické funkcie](#) a je uvedený v [zozname nástrojov, u ktorých bola vyslovená zhoda](#). Použitý modul svojimi vlastnosťami odpovedá požiadavkám vyžadovaným aktuálnymi verziami ZoEP a VoEP. I.CA používa pre párové dáta, slúžiace k označovaniu alebo k podpisovaniu vydávaných časových pečiatok dĺžku rovnú 2048 bitov.

V priebehu procesu generovania párových dát I.CA, slúžiacich k označovaniu alebo podpisovaniu vydávaných časových pečiatok, musí byť fyzicky prítomný :

- riaditeľ I.CA alebo ním menovaný člen vedenia I.CA
- bezpečnostný manažér alebo bezpečnostný administrátor (konkrétne určí riaditeľ I.CA)
- administrátor systému, alebo iný poverený technicky preškolený pracovník I.CA.

Konkrétny technický postup generovania párových dát TSA, slúžiaci k označovaniu alebo podpisovaniu vydávaných časových pečiatok a následné vyhotovenie certifikátu TSS, príslušného k týmto párovým dátam, je popísaný v internej dokumentácii I.CA.

O priebehu generovania párových dát TSA, slúžiacich k označovaniu alebo podpisovaniu vydávaných časových pečiatok je vyhotovený písomný protokol obsahujúci :

- menný zoznam prítomných pracovníkov s uvedením: mena, priezviska, titulu
- dátum a čas začatia a ukončenia generovania párových dát s presnosťou minimálne na minúty
- miesto, kde ku generovaniu párových dát došlo
- popis zariadenia, na ktorom bolo generovanie vykonané, umožňujúce jednoznačnú identifikáciu tohto zariadenia
- kompletný výpis certifikátu TSS, obsahujúci dáta pre overovanie elektronických značiek alebo elektronických podpisov vydávaných časových pečiatok, obsiahnutých v práve vygenerovaných párových údajoch
- dátum vyhotovenia protokolu
- vlastnoručné podpisy všetkých pracovníkov, ktorý generovanie párových dát vykonávali

#### 1.15.1.2 Odovzdanie verejného kľúča TSA

Spôsob odovzdania verejného kľúča TSS je uvedený v internej dokumentácii I.CA.

#### 1.15.1.3 Poskytovanie verejného kľúča TSA

Dáta pre overovanie elektronických značiek alebo elektronických podpisov TSS sú obsiahnuté v jeho certifikáte TSS, ktorý je možno získať najmenej dvoma nezávislými kanálmi :

- prostredníctvom internetových informačných adries I.CA a príslušného úradu
- prostredníctvom vestníka príslušného úradu

#### 1.15.1.4 Dĺžky párových dát

I.CA používa najpreverenejší klasický asymetrický šifrový algoritmus – RSA. Mohutnosť zámenných prvkov (kľúčov - modulus) použitých pre označovanie alebo podpisovanie vydávaných časových pečiatok je 2048 bitov.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 21 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## **1.15.2 Ochrana súkromného kľúča (dát pre vytváranie elektronických značiek) TSA**

### **1.15.2.1 Štandardy a podmienky používania kryptografických modulov**

Generovanie párových dát relevantného TSS a uloženie jeho súkromného kľúča (slúžiaceho pre elektronické označovanie, resp. podpisovanie časových pečiatok) sú realizované jeho kryptografickým modulom, ktorý je uvedený v [zozname nástrojov, u ktorých bola MI ČR vyslovená zhoda](#) :

### **1.15.2.2 Zdieľanie tajomstva**

Ochrana zdieľania tajomstva je realizovaná prostriedkami kryptografického modulu. Pri vykonávaní citlivých činností, ktoré súvisia so zásadnými činnosťami (pozri. kapitoly 1.15.1.1 a 1.15.2.10), je nevyhnutná prítomnosť troch poverených pracovníkov I.CA, z čoho dvaja poznajú časť kódu k prevedeniu týchto činností.

### **1.15.2.3 Úschova súkromného kľúča (dát pre vytváranie elektronických značiek) TSA**

Služba nie je poskytovaná.

### **1.15.2.4 Zálohovanie súkromného kľúča (dát pre vytváranie elektronických značiek) TSA**

Kryptografický modul, použitý pre účely vydávania a spravovania certifikátov TSS, umožňuje zálohovanie dát pre vytváranie elektronických značiek alebo elektronických podpisov. Konkrétny technický postup je popísaný v internej dokumentácii I.CA.

### **1.15.2.5 Uchovávanie súkromného kľúča TSA**

Po uplynutí doby platnosti dát určených k označovaniu alebo podpisovaniu vydávaných časových pečiatok sú tieto dáta vrátane ich záloh zničené. Uchovávanie dát, určených k označovaniu alebo podpisovaniu časových pečiatok, predstavuje bezpečnostné riziko, a preto je u I.CA zakázané.

### **1.15.2.6 Transfer súkromného kľúča TSA**

Dáta pre vytváranie elektronických značiek alebo elektronických podpisov, prislúchajúce k dátam pre overovanie elektronických značiek alebo elektronických podpisov, sú generované priamo v kryptografickom module.

Vkladanie dát pre vytváranie elektronických značiek alebo elektronických podpisov do kryptografického modulu v prípade, že sa jedná o obnovenie týchto dát zo šifrovanej zálohy, prebieha za priamej osobnej účasti najmenej dvoch určených pracovníkov I.CA. V okamihu vkladania dát musí byť TSS odpojený od počítačovej siete.

O vložení dát pre vytváranie elektronických značiek alebo elektronických podpisov je zriadený písomný záznam, ktorý podpíšu určený pracovníci I.CA.

### **1.15.2.7 Uloženie súkromného kľúča TSA v kryptografickom module**

Dáta pre vytváranie elektronických značiek alebo elektronických podpisov, prislúchajúce k dátam pre overovanie elektronických značiek alebo elektronických podpisov, sú v kryptografickom module uložené v šifrovanom tvare.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 22 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

#### 1.15.2.8 Postup pri aktivácii súkromného kľúča TSA

Aktiváciu dát pre vytváranie elektronických značiek alebo elektronických podpisov, vygenerovaných v kryptografickom module relevantného TSS, vykonávajú určený pracovníci I.CA pomocou vlastnej aktivácie kryptografického modulu a aktivačnej čipovej karty podľa presne určeného postupu, ktorý je upravený internou smernicou.

O vykonaní aktivácie dát pre vytváranie elektronických značiek alebo elektronických podpisov je vyhotovený písomný záznam, ktorý podpíšu určení pracovníci I.CA.

#### 1.15.2.9 Postup pri reaktivácii súkromného kľúča TSA

Deaktiváciu dát pre vytváranie elektronických značiek alebo elektronických podpisov po ich vložení do kryptografického modulu relevantného TSS vykonávajú určení pracovníci I.CA prostredníctvom kryptografického modulu a aktivačnej čipovej karty podľa presne určeného postupu, ktorý je upravený internou smernicou.

O vykonanej deaktivácii dát pre vytváranie elektronických značiek alebo elektronických podpisov je vytvorený písomný záznam, ktorý podpíšu určení pracovníci I.CA.

#### 1.15.2.10 Postup pri zničení súkromného kľúča (dát pre vytváranie elektronických značiek, resp. elektronických podpisov)

Dáta pre vytváranie elektronických značiek alebo elektronických podpisov, slúžiace k označovaniu alebo podpisovaniu vydávaných časových pečiatok, sú uložené v kryptografickom module relevantného TSS. Ničenie je realizované prostriedkami kryptografického modulu. Zálohy týchto dát, uložené v zašifrovanej podobe na externých médiách, sú rovnako zničené. Ničenie spočíva vo fyzickej deštrukcii týchto nosičov.

Pri ničení dát pri vytváraní elektronických značiek alebo elektronických podpisov poskytovateľa, slúžiacich k označovaniu alebo podpisovaniu vydávaných časových pečiatok, musí byť fyzicky prítomný :

- riaditeľ I.CA alebo ním menovaný člen vedenia I.CA
- bezpečnostný manažér alebo bezpečnostný administrátor (konkrétne určí riaditeľ I.CA)
- administrátor systému a siete alebo iný poverený technický preškolený pracovník I.CA

O priebehu ničenia dát pri vytváraní elektronických značiek alebo elektronických podpisov poskytovateľa slúžiacich k označovaniu vydávaných časových pečiatok je spísaný protokol.

#### 1.15.3 Uchovávanie verejného kľúča TSA

Dáta pre overovanie elektronických značiek alebo elektronických podpisov sú nevyhnutné pre dôveryhodnosť a overovanie platnosti vydávaných časových pečiatok. Tieto dáta sú obsiahnuté v certifikátoch relevantných TSS. Oproti nim príslušných dát pre vytváranie elektronických značiek alebo elektronických podpisov, je dôležité tieto dáta uchovávať pre prípad následnej kontroly pravosti vydaných časových pečiatok a preto je zo všetkými certifikátmi TSS zachádzané spôsobom, uvedeným v kapitolách 1.17.13.1 a 1.17.13.2.

#### 1.15.4 Profil certifikátu TSA

Profil certifikátu TSS obsahuje všetky náležitosti ZoEP a jeho základné vlastnosti sú uvedené v tabuľke 6.

Tabuľka 6 – certifikát TSS

Atribút	Hodnota	Príklad
---------	---------	---------

<b>Politika vydávania časových pečiatok</b>	<b>Strana 23 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

Version	Verzia 3	2
Serial Numer	jedinečné číslo vydaného certifikátu TSS	10100629
Signature <ul style="list-style-type: none"> <li>algorithm</li> <li>parameters</li> </ul>	algoritmus pre elektronickú značku alebo elektronický podpis vydávaného certifikátu TSS voliteľné parametre	sha1withRSAEncryption
Issuer	označenie vydavateľa certifikátu Country (C) Organization (O) CommonName (CN)	CZ První certifikační autorita, a.s. I.CA - Qualified root certificate
NotBefore	dátum a UTC čas začiatku platnosti certifikátu TSS	01/02/2006 00:00:00
NotAfter	dátum a UTC čas konca platnosti certifikátu TSS	01/02/2011 00:00:00
Subjekt	Označenie držiteľa certifikátu TSS Country (C) Organization (O) Organization Unit (OU) CommonName (CN)	CZ První certifikační autorita, a.s. Time Stamp Server X <sup>3</sup> Time Stamping Authority
SubjectPublicKeyInfo <ul style="list-style-type: none"> <li>algorithm</li> <li>SubjectPublicKey</li> </ul>	identifikátor algoritmu verejného kľúča certifikátu TSS verejný kľúč držiteľa certifikátu	rsaEncryption RSA (2048)
Signature algorithm <ul style="list-style-type: none"> <li>algorithm</li> <li>parameters</li> </ul>	algoritmus pre elektronickú značku alebo elektronický podpis vydávaného certifikátu TSS voliteľné parametre	sha1withRSAEncryption
signatureValue	Elektronická značka alebo elektronický podpis vydaného certifikátu TSS	RSA (2048)

Každá vydaná časová pečiatka zahŕňa identifikátor politiky, pod ktorou bol vydaný.

### 1.15.5 Aktivačné dáta

#### 1.15.5.1 Generovanie a inštalácia aktivačných dát

Aktivačné dáta sú vytvárané v priebehu procesu inštalácie, keď sú generované párové dáta relevantného TSS.

#### 1.15.5.2 Ochrana aktivačných dát

Povinnosti poverených pracovníkov I.CA je chrániť aktivačné dáta.

#### 1.15.5.3 Ostatné aspekty aktivačných dát

Aktivačné dáta sú určené výhradne pre aktiváciu súkromného kľúča a nesmú byť použité k iným účelom ani prenášané alebo uchovávané v otvorenej podobe.

<sup>3</sup>

Kde X je číslo TSS (tzn. 1,2,3 ....)

<b>Politika vydávania časových pečiatok</b>	<b>Strana 24 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

### 1.15.6 Výmena párových dát TSA

Procesy výmeny dát pre overovanie dát elektronických značiek alebo elektronických podpisov v certifikáte relevantného TSS sú popísane v internej dokumentácii I.CA

### 1.15.7 Ukončenie životného cyklu párových dát TSA

Platnosť párových dát (s mohutnosťou kľúča 2048 bitov) určených k označovaniu alebo podpisovaniu generovaných časových pečiatok je určená na 5 rokov.

Platnosť dát určených k overovaniu označených alebo podpísaných časových pečiatok je daná platnosťou vydaných certifikátov TSS. Po tejto dobe sa dajú dáta pre overovanie elektronických značiek alebo elektronických podpisov použiť bez záruky. Pokiaľ dôjde k neočakávanému vývoju kryptoanalytických metód, ktoré by mohli ohroziť bezpečnosť použitia párových dát, bude ich životnosť skrátená. V takom prípade sa postupuje analogickým postupom uvedeným v kapitole 1.17.1010.

Pre kontrolu vydaných časových pečiatok je každý expirovaný verejný kľúč relevantného TSS ďalej archivovaný po celú dobu činnosti systému TSA.

### 1.15.8 Zneplatnenie a pozastavenie platnosti certifikátu TSA

#### 1.15.8.1 Profil zoznamu zrušených certifikátov

Tabuľka 7 – Profil CRL

<b>Položka</b>	<b>Obsah</b>	<b>Príklad</b>
Version	Verzia v2	1
Signature <ul style="list-style-type: none"> <li>algorithm</li> <li>parameters</li> </ul>	algoritmus pre elektronickú značku alebo elektronický podpis vydávaného CRL voliteľné parametre	sha1withRSAEncryption
Issuer	označenie vydavateľa CRL Country (C) Organization (O) CommonName (CN)	CZ První certifikační autorita, a.s. I.CA - Qualified root certificate
thisUpdate	dátum a UTC čas vydania CRL	Nov 30 04:51:30 2005
nextUpdate	dátum a predpokladaný UTC čas vydania nasledujúceho CRL	Nov 30 16:51:30 2005
Signature algorithm <ul style="list-style-type: none"> <li>Algorithm</li> <li>parameters</li> </ul>	algoritmus pre elektronickú značku alebo elektronický podpis vydávaného CRL voliteľné parametre	sha1withRSAEncryption
signatureValue	Elektronická značka alebo elektronický podpis vydaného CRL	RSA (2048)
CRL Numer	Číslo CRL	456

<b>Politika vydávania časových pečiatok</b>	<b>Strana 25 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

Tabuľka 8 – Rozširujúce položky CRL

<b>Položka</b>	<b>Obsah</b>	<b>Príklad</b>
revokedCertificates <ul style="list-style-type: none"> <li>• userCertificate</li> <li>• revocationDate</li> </ul>	jedinečné číslo vydaného certifikátu dátum a UTC čas zneplatnenia certifikátu	10100629 Jan 30 04:51:30 2005

#### 1.15.8.2 Podmienky pre zneplatnenie certifikátu

Certifikát relevantného TSS môže byť zneplatnený iba na základe nasledujúcich okolností :

- ak nastanú skutočnosti uvedené v ZoEP
- dôjde ku kompromitácii alebo existuje dôvodné podozrenie, že došlo ku kompromitácii dát pre vytváranie elektronických značiek alebo elektronických podpisov tohto TSS

Zneplatnenie certifikátu TSS, vykoná I.CA na základe podnetu :

- subjektov oprávnených zo zákona
- riaditeľa I.CA

#### 1.15.9 Služby súvisiace s overovaním štatútu certifikátu TSA

##### 1.15.9.1 Funkčné charakteristiky

Služby súvisiace s overovaním štatútu certifikátu relevantného TSS sú poskytované formou zverejňovania informácií:

- o verejných certifikátoch na adrese <http://www.ica.cz/>
- o zrušených certifikátoch na adresách :
  - <http://www.ica.cz/>
  - <http://qcrlp1.ica.cz/qica05.crl>
  - <http://qcrlp2.ica.cz/qica05.crl>
  - <http://qcrlp3.ica.cz/qica05.crl>

Podrobné informácie sú uvedené v kapitole 1.17.13.3.2.

##### 1.15.9.2 Dostupnosť služieb

I.CA zabezpečuje nepretržitú dostupnosť služieb, uvedených v kapitole 1.15.9.1. Postup je uvedený v interných dokumentoch I.CA. Prípadné obmedzenia sú uvedené v písomnej zmluve (viď. Kap. 4.3).

##### 1.15.9.3 Ďalšie charakteristiky služieb štatútu certifikátu

Ďalšie služby, okrem tých, ktoré sú uvedené v kapitole 1.15.9.1, nie sú poskytované.

#### 1.15.10 Správa kryptografického modulu používaného pri vytváraní časových pečiatok

Hardware relevantného TSS, ktorý je pripojený do infraštruktúry dôveryhodného synchronizačného času, obsahuje hardware HSM (FIPS 140-2 level 3) je výrobcom doručený (s využitím dôveryhodných prepravcov) do sídla spoločnosti První certifikační autorita, a.s. V procese príjmu zásielky sú kontrolované

<b>Politika vydávania časových pečiatok</b>	<b>Strana 26 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

správnosť a neporušenosť pečatí obalu zásielky od výrobcu. Po prevzatí zásielky je táto následne premiestnená na prevádzkové pracovisko, na ktorom je prevedená ďalšia kontrola pečatí obalu zásielky, vrátane pečatí samotného hardware. TSS je uložený na bezpečnom mieste s riadeným prístupom a je prevedená základná inštalácia vrátane testov, synchronizácie a kontroly. Každá vyššie uvedená činnosť je písomne zaznamenávaná. Inštalácia, inicializácia, kontrola a synchronizácia TSS prevádzajú dôveryhodné osoby a v prítomnosti svedkov. V prípade odovzdania hardware TSS do servisu, ukončenia poskytovania akreditovaných/kvalifikovaných certifikačných služieb v oblasti časových pečiatok, alebo ukončenie činnosti I.CA, sú dáta pre vytváranie elektronických značiek alebo elektronických podpisov generovaných časových pečiatok HSM zničené podľa doporučenia výrobcu. Konkrétne postupy správy TSS sú popísané v internej dokumentácii I.CA.

#### **1.15.10.1 Hodnotenie kryptografického modulu**

Kryptografický modul pre označovanie generovaných časových pečiatok je uvedený v [zozname nástrojov, u ktorých bola MI ČR vyslovená zhoda](#), lebo odpovedá požiadavkám na kryptografické moduly podľa dokumentu „Standard pre hodnotenie bezpečnosti kryptografických modulov vydaný NIST v USA – FIPS PUB 140-2 úroveň 3“.

### **1.16 Vydávanie časových pečiatok**

#### **1.16.1 Žiadosť o časovú pečať**

##### **1.16.1.1 Subjekty oprávnené podať žiadosť o časovú pečať**

Vydávanie časových pečiatok je I.CA komerčne ponúkanou službou fyzickej osobe, právnickej osobe, alebo organizačnej zložke štátu, ktorá sa zmluvne (viď. kap. 4.3) zaviazá jednať podľa tejto politiky.

Pre žiadateľa, ktorý podpisuje s I.CA zmluvu (viď. kap. 4.3) je požadovaný minimálny vek 15 rokov. Osoby od 15 do 18 rokov musia mať svojho zákonného zástupcu.

V prípade fyzickej osoby môže byť osobou, podpisujúcou zmluvu (viď. kap. 4.3) iba tá, ktorá je spôsobilá k právnym úkonom podľa príslušnej právnej normy. Pokiaľ osoba podpisujúca zmluvu (viď. kap. 4.3) nepožaduje služby priamo pre seba, ale zastupuje inú osobu, musí mať oprávnenie túto osobu zastupovať.

##### **1.16.1.2 Registračný proces a zodpovednosti poskytovateľa a žiadateľa**

Pri registrácii nového žiadateľa o službu poskytovania časových pečiatok je podľa predložených dokladov overená jeho identita a prípadne jeho oprávnenie k zastupovaniu. Pri registrácii nového žiadateľa sa vyžaduje :

- a) predloženie platného osobného dokladu žiadateľa
- b) spôsobilosť žiadateľa k právnym úkonom
- c) doklady, preukazujúce právo žiadateľa jednať za inú fyzickú alebo právnickú osobu, organizačnú zložku štátu ako zástupcu na základe plnej moci s úradne overeným podpisom zastupovaného subjektu.

##### **1.16.1.3 Počiatočné overenie identity**

###### **1.16.1.3.1 Overovanie identity právnickej osoby alebo organizačnej zložky štátu**

V prípade, keď žiadateľ vystupuje ako zástupca právnickej osoby alebo organizačnej zložky štátu, vyžaduje I.CA pri uzatváraní zmluvy (viď. kap. 4.3) o vydaní jedného alebo viacerých časových pečiatok :

<b>Politika vydávania časových pečiatok</b>	<b>Strana 27 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

- originál alebo notársky overenú kópiu výpisu z obchodného registra, živnostenského listu alebo iného dokumentu, na ktorých základe bola právnická osoba alebo organizačná zložka štátu vytvorená a ktoré musia obsahovať úplné obchodné meno, identifikačné číslo (IČO), štatutárny orgán a sídlo
- doklad oprávňujúci žiadateľa jednať v mene tejto právnickej osoby alebo organizačnej zložky štátu – vid' kapitola 1.16.1.2, odstavec c)

#### 1.16.1.3.2 Overovanie fyzickej osoby

V prípade, keď žiadateľ vystupuje ako fyzická osoba, vyžaduje I.CA pri uzatváraní zmluvy (vid' kap. 4.3) o vydaní jedného alebo viacerých časových pečiatok :

- celé občianske meno žiadateľa
- dátum narodenia žiadateľa
- číslo predloženého osobného dokladu
- adresa trvalého bydliska žiadateľa

Pokiaľ dôjde v priebehu trvania zmluvného vzťahu k I.CA k zmenám vo vyššie uvedených vyžadovaných osobných údajoch, je žiadateľ povinný tieto zmeny ohlásiť I.CA. Žiadateľ sa musí preukázať spôsobom uvedeným v kapitole 1.16.1.2.

### 1.16.2 Spracovanie žiadosti o časovú pečať

#### 1.16.2.1 Identifikácia a autentizácia

S ohľadom na komerčnú bázu a nadštandardné služby v procese vydávania časových pečiatok, vytvorí žiadateľ bezpečné a autentizované spojenie s TSA (s využitím komerčných certifikátov vydaných I.CA). V prípade neúspešného spojenia je transakcia ukončená a klient vhodným spôsobom informovaný.

#### 1.16.2.2 Prijatie alebo zamietnutie žiadosti o časovú pečať

- Klientská aplikácia vytvorí pre akékoľvek elektronické dáta (správa, dokument, transakcia atď.) ich odtlačok (hash), ktorý je následne uložený v žiadosti na vytvorenie časovej pečiatky (v normovanom formáte podľa RFC 3161). Táto dátová štruktúra je s využitím Internetu (ako prenosového média - protokol TCP/IP), odovzdaná komunikačnému serveru TSA.
- V rámci TSA je žiadosť odovzdaná archivačnému serveru TSA a následne je zaslaná jednému zo serverov TSS. Vzhľadom na skutočnosť, že je zasielaný iba odtlačok (hash), je obsah elektronických dát (správa, dokument, transakcia atď.) pre TSS naprosto neznámy (vrátane identity klienta).

#### 1.16.2.3 Doba spracovania žiadosti o časovú pečať

I.CA nestanovuje (pokiaľ nie je uvedený v zmluve (vid' kap. 4.3), pevný časový limit, v ktorom dôjde k spracovaniu žiadosti o časovú pečať, pretože ide o časový sled nasledujúcich činností, z ktorých niektoré záležia len na elektronickom prenose žiadosti k systému TSA. Časové údaje sú uvedené v nasledujúcom zozname:

- vytvorenie žiadosti o vydanie časovej pečiatky – rádovo sekundy (záleží na type aplikácie)
- vygenerovanie časovej pečiatky – rádovo ms

### 1.16.3 Vydanie časovej pečiatky

#### 1.16.3.1 Úkony TSA v priebehu vydávania časovej pečiatky

V nasledujúcom zozname sú v časovom slede uvedené činnosti TSA :

<b>Politika vydávania časových pečiatok</b>	<b>Strana 28 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

- Relevantný TSS vykoná všetky kontroly formálnej správnosti žiadosti a následne vytvorí novú dátovú štruktúru v normovanom formáte podľa RFC 3161, obsahujúce odpovedajúci chybový status
- v prípade kladného výsledku kontrol žiadosti je k odtlačku (hash), obsiahnutom v žiadosti, pridaný časový údaj, ktorý je získaný z meradla dôveryhodného času, vrátane informácie o tomto meradle a takto vytvorené dáta sú do vyššie uvedenej dátovej štruktúry uložené
- vyššie uvedená dátová štruktúra je následne elektronicky označená alebo elektronicky podpísaná dátami pre vytváranie elektronickej značky alebo elektronickeho podpisu relevantného TSS - tým sa tento server nespochybniteľným spôsobom zaručuje za správnosť informácií uvedených vo vygenerovanej časovej pečiatke
- táto dátová štruktúra – odpoveď na žiadosť o časovú pečiatku, je odoslaná archivačnému serveru TSA

#### 1.16.3.2 Oznámenie o vydaní časovej pečiatky držiteľom vydávania časovej pečiatky

Po vykonaní činnosti uvedenej v kapitole 7.3.3.1., odošle riadiaca aplikácia klientovi odpoveď.

#### 1.16.4 Prevzatie časovej pečiatky

##### 1.16.4.1 Klient

Po získaní odpovede na žiadosť o časovú pečiatku je klient povinný zistiť status. V prípade chyby nie je časová pečiatka v odpovedi obsiahnutá a klient by mal prekontrolovať status a odpovedajúcu chybovou hlásenie. V opačnom prípade je klient povinný postupovať v súlade s kapitolou 1.11.

##### 1.16.4.2 Spoliehajúca sa strana

Overovanie časovej pečiatky spoliehajúcou sa stranou prebieha v nasledujúcich krokoch :

- vytvorenie hodnoty odtlačok\_1 (hash\_1) z elektronicných dát (správa, dokument, transakcia, atď.), ktorá bude porovnávaná proti hodnote odtlačok\_2 (hash\_2), obsiahnutej v časovej pečiatke
- výber časovej pečiatky, obsahujúci hodnotu odtlačok\_2 (hash\_2)
- porovnanie hodnôt odtlačok\_1 (hash\_1) a odtlačok\_2 (hash\_2)

V prípade nezahody boli elektronicke dáta, odpovedajúcej hodnote hash\_1 zmenené. Ďalej je spoliehajúca sa strana povinná postupovať v súlade s kapitolou 1.12.

#### 1.16.5 Ukončenie poskytovania služieb pre žiadateľa o časovú pečiatku

Poskytovaná certifikačná služba vydávania časových pečiatok (obchodný vzťah) ukončuje I.CA vo chvíli, keď nie sú dodržané podmienky zmluvy (viď. kap. 4.3), uzavretej s klientom.

#### 1.16.6 Token časovej pečiatky

Časové pečiatky sú generované relevantným TSS na základe zaslanej žiadosti.

##### 1.16.6.1 Profil žiadosti o časovú pečiatku

Tab. 9 – Položky žiadosti o časovú pečiatku

Pole	Popis	Příklad
------	-------	---------

<b>Politika vydávania časových pečiatok</b>	<b>Strana 29 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

Version	Popisuje verziu požiadavky na časovú pečaťku.	1
HashAlgorithm	SHA-1	sha1withRSAEncryption
HashedMessage	Dĺžka tohto reťazca (Octect String) musí spĺňať požiadavky na dĺžku zvoleného algoritmu (SHA-1)	
ReqPolicy	Identifikátor politiky	1.3.6.1.4.1. 23624.1.4.14.2
Nonce	Náhodné číslo, o ktorom sa predpokladá, že ho klient 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 TSS FALSE, alebo nie je uvedená - odpoveď nesmie obsahovať certifikát TSS	TRUE/FALSE

### 1.16.6.2 Profil odpovedi na žiadosť o časovú pečaťku

Tab. 10 - Položky odpovede o časovú pečaťku

Položka	Popis	Príklad
<b>PKIStatus</b>	Číslo Integer, označuje : <ul style="list-style-type: none"> <li>• granted</li> <li>• grantedWithMods</li> <li>• rejection</li> <li>• waiting</li> <li>• revocationWarning</li> <li>• revocationNotification</li> </ul>	0 1 2 3 4 5
<b>PKIFailureInfo ::= BIT STRING {</b>	BIT STRING označuje : <ul style="list-style-type: none"> <li>• BadAlg - unrecognized or unsupported Algorithm Identifier</li> <li>• BadRequest - transaction not permitted or supported</li> <li>• BadDataFormat - the data submitted has the wrong format</li> <li>• TimeNotAvailable - the TSA's time source is not available</li> <li>• UnacceptedPolicy - the requested TSA policy is not supported by the TSA</li> <li>• UnacceptedExtension - the requested extension is not supported by the TSA</li> <li>• AddInfoNotAvailable - the additional information requested could not be understood or is not available</li> <li>• SystemFailure - the request cannot be handled due to system failure }</li> </ul>	0 2 5 14 15 16 17 25

Token časovej pečiatky nesmie obsahovať inú elektronickú značku alebo elektronický podpis, než elektronickú značku alebo elektronický podpis relevantného TSS.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 30 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

Tab. 11 - Položky tokenu časovej pečiatky

<b>Položka</b>	<b>Popis</b>	<b>Príklad</b>
version	verzia požiadavky na časovú pečať.	1
Policy	identifikátor politiky	1.3.6.1.4.1. 23624.1.4.14.2
messageImprint	hash, pre ktorý sa žiada o časovú pečať	musí mať rovnakú hodnotu ako v TimeStampReq
serialNumber	integer číslo – Time-Stamping users MUST be ready to accommodate integers up to 160 bits.	1234567890
Gentime	GeneralizedTime – hodnota UTC	2005/12/02 10.24:17:46
Accuracy	Presnosť – voliteľné	
Nonce	Náhodné číslo – voliteľné - o ktorom sa predpokladá, že ho klient vygeneruje iba raz (64 bit integer). V prípade, že toto číslo žiadosť obsahuje, potom toto číslo musí obsahovať aj odpoveď.	
Tsa	GeneralName – voliteľné	

Tokeny časových pečiatok, ktoré relevantný TSS generuje, obsahujú jednoznačný identifikátor politiky, popísaný v kapitole 1.1, odtlačok (hash) dátovej správy, na ktorú je proces vydania časovej pečiatky realizovaný, dátum a časovú hodnotu (odpovedajúcu reálnej hodnote UTC) a jedinečné sériové číslo.

Presnosť časového údaja, vkladaneho do vydávanej generovanej časovej pečiatky je definovaná v kapitole 1.10.2. Štruktúra časovej pečiatky (v štandarde RFC 3161) je označená (ČR) alebo podpísaná (SR) súkromným kľúčom relevantného TSS, ktorého certifikát TSS obsahuje údaje, popísané v kapitole 1.15.4 a identifikátor jednoznačne spojený so spoločnosťou První certifikační autorita, a.s.

### **1.16.7 Synchronizácia meradla času s UTC**

#### **1.16.7.1 Synchronizácia**

Synchronizácia meradla času s dôveryhodným synchronizačným zdrojom UTC je vykonávaná jedenkrát denne. Pre synchronizáciu a kontrolu časového údaja, vkladaneho do generovaných časových pečiatok, je využívané už v EU prevádzkované komerčné riešenie, založené na modeli dôveryhodnej synchronizačnej časovej infraštruktúry (TTI). Táto bezpečná a nevyvrátiteľná synchronizačná časová služba meradla času, poskytuje platné a kontrolovateľné informácie pre prípad sporov medzi poskytovateľom časových pečiatok a klientmi alebo spoliehajúcimi sa stranami. Problematika synchronizácie je riešená internou dokumentáciou.

#### **1.16.7.2 Bezpečnosť meradla času**

Problematika bezpečnosti meradla času je riešená internou dokumentáciou I.CA.

#### **1.16.7.3 Detekcia odchýlenia meradla času**

Problematika detekcie odchýlenia meradla času je riešená internou dokumentáciou I.CA.

#### **1.16.7.4 Prestupná sekunda**

Problematika výskytu prestupnej sekundy meradla času je riešená internou dokumentáciou I.CA.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 31 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## **1.17 Správa a prevádzková bezpečnosť TSA**

### **1.17.1 Riadenie bezpečnosti**

Popis štruktúry riadenia bezpečnosti v spoločnosti První certifikační autorita, a.s., je uvedený v internej dokumentácii I.CA..

### **1.17.2 Hodnotenie a riadenie rizík**

V I.CA boli vykonané nasledujúce činnosti :

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

### **1.17.3 Hodnotenie zraniteľnosti**

Vid'. kapitola 7.4.2

### **1.17.4 Postup pri oznamovaní udalosti subjektu, ktorý ju spôsobil**

V prípade neoprávnených pokusov nie je subjekt informovaný a zapísaní udalosti do auditného záznamu.

### **1.17.5 Personálna bezpečnosť**

Problematika personálnej bezpečnosti (kapitoly 1.17.5.1 až 7.4.5.12) je detailne riešená v internej dokumentácii .

#### **1.17.5.1 Dôveryhodné role**

Pre činnosti zodpovedajúce roliam podľa bezpečnostných požiadaviek štandardu pre dôveryhodné systémy (vid' VoEP), sú v spoločnosti I.CA definované dôveryhodné role, ktorých popis je uvedený v internej dokumentácii spoločnosti. Základné činnosti a zodpovednosti osôb v dôveryhodných roliach je definovaný v internej dokumentácii.

#### **1.17.5.2 Počet osôb požadovaných na zabezpečenie jednotlivých činností**

Pre nižšie uvedené činnosti je nevyhnutná prítomnosť najmenej troch poverených pracovníkov I.CA :

- generovanie párových dát I.CA,
- ničenie dát pre vytváranie elektronickej značky alebo elektronickeho podpisu I.CA vydávaných časových pečiatok

Pre nižšie uvedené činnosti je nevyhnutná prítomnosť najmenej dvoch poverených pracovníkov I.CA :

- zálohovanie/obnova dát pre vytváranie elektronickej značky alebo elektronickeho podpisu každého TSS
- aktivácia každého TSS

<b>Politika vydávania časových pečiatok</b>	<b>Strana 32 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

- fyzická kontrola chodu každého TSS

Pre uskutočňovanie ostatných úloh nie je počet prítomných osôb určený, musí však ísť výhradne o poverených pracovníkov.

### **1.17.5.3 Identifikácia a autentizácia pre každú pozíciu**

Pracovníkom sú pridelené prostriedky pre riadnu autentizáciu k tým komponentom, ktoré sú pre ich činnosť nevyhnutné - upravené internými smernicami I.CA.

### **1.17.5.4 Pozície vyžadujúce rozdelenie povinností**

V procese poskytovania akreditovaných/kvalifikovaných certifikačných služieb je minimálne zaručené, že nie je možné spojiť role definované bezpečnostným štandardom pre dôveryhodné systémy (VoEP).

### **1.17.5.5 Požiadavky na kvalifikáciu, skúsenosť a bezúhonnosť**

Pracovníci v roliah podľa bezpečnostných požiadaviek štandardu pre dôveryhodné systémy (VoEP) a ďalej v roliah riaditeľ spoločnosti, bezpečnostný manažér, manažér pre zvládanie krízových situácií a plánu obnovy, bezpečnostný auditor sú prijímaní na základe nižšie popísaných personálnych kritérií :

- je vyžadovaná absolútna občianska bezúhonnosť - preukazované tým, že tieto osoby nemajú žiadny záznam v registri trestov (výpis z registra trestov alebo čestné vyhlásenie)
- vysokoškolské vzdelanie v rámci akreditovaného bakalárskeho alebo magisterského študijného programu a najmenej 3 roky praxe v oblasti informačných a komunikačných technológií, alebo stredoškolské vzdelanie a najmenej 5 rokov praxe v oblasti informačných a komunikačných technológií, pričom z toho najmenej 1 rok v oblasti poskytovania certifikačných služieb
- znalosti v oblasti infraštruktúry verejných kľúčov a informačnej bezpečnosti
- v jednotlivých prípadoch je možné skrátiť dĺžku uvedenej praxe až o jednu tretinu stanovenej dĺžky na základe preskúšania, pri ktorom pracovník preukáže dostatočné znalosti k výkonu dôveryhodnej funkcie.

Ostatní pracovníci sú prijímaní podľa nasledujúcich kritérií:

- vysokoškolské vzdelanie v rámci akreditovaného bakalárskeho alebo magisterského študijného programu, alebo stredoškolské vzdelanie,
- základná orientácia v oblasti infraštruktúry verejných kľúčov a informačnej bezpečnosti.

### **1.17.5.6 Posúdenie spoľahlivosti osôb**

Zdrojom informácií všetkých kmeňových pracovníkov I.CA sú :

- sami títo pracovníci
- osoby, ktoré týchto pracovníkov poznajú
- verejné zdroje informácií

Pracovníci poskytujú prvotné informácie osobným pohovorom pri prijímaní do pracovného pomeru, ktoré aktualizujú pri periodických pohovoroch s nadriadeným pracovníkom v priebehu pracovného pomeru.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 33 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

#### **1.17.5.7 Požiadavky na prípravu pre výkon pozície, vstupné školenie**

Pracovníci I.CA sú odborne zaškolení pre používanie určeného programového vybavenia a špeciálnych zariadení. Zaškolenie sa uskutočňuje kombináciou metódy samo prípravy a metodickým vedením už zaškoleným pracovníkom. Bežná doba na zaškolenie je jeden mesiac.

#### **1.17.5.8 Požiadavky a periodicita školení**

Pre kmeňových pracovníkov vykonáva vedenie I.CA minimálne raz ročne interný výukový seminár, zameraný na problematiku bezpečnosti informácií.

#### **1.17.5.9 Periodicita a postupnosť rotácie pracovníkov medzi rôznymi pozíciami**

Z dôvodov možnej zastupiteľnosti v mimoriadnych prípadoch sú pracovníci I.CA motivovaní k získavaniu znalostí potrebných na zastávanie inej pozície v I.CA. Zmena pozície je možná len v mimoriadnych prípadoch (epidemické ochorenie, apod.) ako dočasné opatrenie. Pre trvalé vykonávanie inej dôveryhodnej pozície je potrebné menovanie riaditeľom I.CA.

#### **1.17.5.10 Postihy za neoprávnené činnosti zamestnancov**

Pri zistení neautorizovanej činnosti je dotýčny pracovník sankcionovaný podľa rozsahu až do výšky okamžitého prepustenia a riadi sa podľa Zákonníka práce (tento postih nebráni prípadnému trestnému stíhaniu, pokiaľ tomu zodpovedá závažnosť zistenej neautorizovanej činnosti).

#### **1.17.5.11 Požiadavky na nezávislých zhotoviteľov**

I.CA môže, alebo musí (podľa ZoEP, VoEP) niektoré činnosti zabezpečovať zmluvne. Tieto obchodno-právne vzťahy sú ošetrené bilaterálnymi obchodnými zmluvami. Ide o napr. externé registračné authority, zhotoviteľov programového aplikačného vybavenia, dodávateľov hardware, systémového programového vybavenia, externých auditorov, atď. Tieto subjekty sú povinné sa riadiť podľa zodpovedajúcich verejných certifikačných politík, politikami, relevantnými časťami internej dokumentácie I.CA, ktoré im budú poskytnuté a predpísanými normatívnymi dokumentmi. V prípade porušenia týchto povinností sú vyžadované zmluvné pokuty, prípadne je s nimi okamžite ukončená zmluva.

#### **1.17.5.12 Dokumentácia poskytovaná zamestnancom**

Kmeňoví zamestnanci I.CA majú k dispozícii okrem politiky aj príslušné normy, smernice, príručky a metodické pokyny, potrebné pre výkon ich činnosti.

### **1.17.6 Fyzická bezpečnosť a bezpečnosť prostredia**

Problematika fyzickej bezpečnosti a bezpečnosti prostredia (kapitoly 1.17.6.1 až 1.17.6.8) je detailne riešená v internej dokumentácii.

#### **1.17.6.1 Umiestnenie a konštrukcia**

Zariadenia, určené pre výkon hlavných akreditovaných/kvalifikovaných certifikačných služieb, sú umiestnené v suteréne objektu, ktorý stojí osamotene. Zabezpečená oblasť má tehlové steny s najmenšou hrúbkou 300 mm. Vstupné dvere majú prienikovú odolnosť a zámkové systémy certifikované NBÚ ČR na kategóriu „Tajné“.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 34 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

#### **1.17.6.2 Fyzický prístup**

Objekt je opložený bezpečnostným plotom a je nepretržite strážený fyzickou ostrahou a špeciálnym televíznym systémom pre snímanie, prenos a zobrazovanie pohybu osôb a dopravných prostriedkov. Prístup do vlastného objektu je kontrolovaný fyzickou ostrahou.

#### **1.17.6.3 Elektrina a klimatizácia**

V miestnosti je dostatočne dimenzovaná aktívna klimatizácia, ktorá udržiava celoročnú teplotu v rozmedzí 20 °C ± 5 °C. Prívod elektrickej energie je istený pomocou UPS, resp. diesel agregátu.

#### **1.17.6.4 Vplyv vody**

Objekt sa nachádza v lokalite, ktorá je postihnuteľná záplavovou vodou. Všetky kritické systémy sú preto umiestnené v dostatočnej výške, aby neboli zaplavené ani storočnou vodou.

#### **1.17.6.5 Protipožiarne opatrenia a ochrana**

Vstupné pancierové dvere sú opatrené protipožiarou vložkou. V miestnosti sa nachádzajú hasiace prístroje a zariadenia elektrickej požiarnej signalizácie.

#### **1.17.6.6 Ukladanie médií**

Pamäťové médiá, obsahujúce prevádzkové zálohy a záznamy v elektronickej podobe, sú ukladané v kovových skrinách, resp. v trezore riaditeľa I.CA.

Papierové médiá, ktoré je nutné podľa platnej legislatívy archivovať, sú skladované v inej geografickej lokalite, než je prevádzkové pracovisko.

#### **1.17.6.7 Manipulácia s odpadmi**

Všetok papierový kancelársky odpad je pred opustením pracovísk I.CA znehodnotený skartovaním.

#### **1.17.6.8 Zálohy mimo budovy prevádzkového pracoviska**

Kópie prevádzkových a pracovných záloh sú uložené na mieste určenom riaditeľom I.CA.

### **1.17.7 Prevádzkové riadenie**

#### **1.17.7.1 Špecifické technické požiadavky na počítačovú bezpečnosť**

Úroveň bezpečnosti použitých komponentov pre poskytovanie akreditovaných/kvalifikovaných certifikačných služieb v oblasti vydávania časových pečiatok je definovaná ZoEP a VoEP.

Detailné riešenie špecifických technických požiadaviek počítačovej bezpečnosti je popísané v internej dokumentácii.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 35 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

#### **1.17.7.2 Hodnotenie počítačovej bezpečnosti**

Hodnotenie bezpečnosti I.CA je založené na medzinárodných a národných štandardoch :

- ČSN ETSI TS 102 023 – Elektronické podpisy a infraštruktúry, Požiadavky na postupy autorít časových pečiatok.
- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements/Bezpečnostné požiadavky na dôveryhodné systémy spravujúce certifikáty pre elektronický podpis – časť 1: Požiadavky na bezpečnosť systémov.
- ETSI TS 101 456 - Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
- ČSN ISO/IEC 17799 - Informační technologie – Soubor postupů pro management bezpečnosti informací.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky
- ČSN ISO/IEC TR 13335 – Informačné technológie – Smernica pre riadenie bezpečnosti IT 1-3
- ČSN EN ISO 19011 - Smernica pre auditovanie systému manažmentu akosti a/alebo systému

#### **1.17.8 Riadenie prístupu do systému**

Riadený prístup do systému TSA kmeňovými pracovníkmi I.CA je definovaný internou dokumentáciou.

#### **1.17.9 Vývoj a údržba dôveryhodných systémov**

##### **1.17.9.1 Riadenie vývoja systému**

Pri vývoji systému je postupované v súlade s internou dokumentáciou.

##### **1.17.9.2 Kontroly riadenia bezpečnosti**

Súlad so štandardmi (viď kapitola 1.17.7.2), ZoEP a VoEP je overovaný pravidelnými auditmi systému manažmentu bezpečnosti informácií, vykonávanými pracovníkmi nezávislých audítorských firiem a kontrolami bezpečnostnej zhody, vykonávanými pracovníkmi I.CA. Táto problematika je popísaná v internej dokumentácii.

##### **1.17.9.3 Riadenie bezpečnosti životného cyklu**

Riadenie bezpečnosti životného cyklu je v I.CA vytvárané procesným prístupom typu „Plánovanie-Zavedenie-Kontrola-Využitie“ (Plan-Do.Check-Act, PDCA), ktorý sa skladá z nasledujúcich 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 spoločnosti k posúdeniu;
- využitie – na základe rozhodnutia vedenia organizácie uskutočnenie nápravných opatrení.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 36 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## **1.17.10 Obnova po havárii alebo kompromitácii**

### **1.17.10.1 Postup v prípade incidentu a kompromitácie**

Postupy sú uvedené v internom dokumente „*Plán pre zvládanie krízových situácií a plán obnovy*“.

### **1.17.10.2 Poškodenie výpočtových prostriedkov, software alebo dát**

V prípade poškodenia výpočtových prostriedkov, software alebo dát postupuje I.CA v súlade s dokumentom „*Plán pre zvládanie krízových situácií a plán obnovy*“ takým spôsobom, aby bola prevádzka obnovená v požadovaných termínoch.

### **1.17.10.3 Postup pri zistení odchýlenia meradla času**

Postup synchronizácie časového údajov meradla času je uvedený v kapitole 1.16.7.1. Pokiaľ je zistená odchýlka od UTC mimo špecifikovaný interval, definovaný pri inicializácii TSS, je jeho činnosť okamžite ukončená a do uskutočnenia novej inicializácie nie je služba vydávania časových pečiatok poskytovaná. Problematika je riešená internou dokumentáciou I.CA.

### **1.17.10.4 Postup pri kompromitácii súkromného kľúča TSA**

V prípade kompromitácie alebo vzniku dôvodnej obavy zo zneužitia dát pre vytváranie elektronických značiek alebo elektronických podpisov pre označovanie alebo podpisovanie vydávaných časových pečiatok I.CA :

- ukončí ich používanie
- okamžite a trvale zneplatní vlastný príslušný certifikát relevantného TSS
- bezodkladne :
  - o tejto skutočnosti, vrátane dôvodu informuje :
    - na svojej internetovej informačnej adrese
    - v jednom celoštátne distribuovanom denníku – vid' kapitola 1.17.13.3.2
  - pre sprístupnenie tejto informácie je využitý aj zoznam zrušených certifikátov, čím je zabezpečená dostupnosť tejto informácie minimálne dvomi na sebe nezávislými spôsobmi, umožňujúcimi diaľkový prístup a sú nepretržite dostupné
- pokiaľ je to možné, informuje držiteľov platných časových pečiatok o zneplatnení certifikátu relevantného TSS, a to prostredníctvom zaslania správy elektronickou poštou na elektronickú adresu, ktorú tieto osoby uviedli v žiadosti o vydanie časových pečiatok - súčasťou tejto informácie je dôvod ukončenia platnosti certifikátu relevantného TSS
- oznámi príslušnému úradu informáciu o zneplatnení vlastného certifikátu TSS s uvedením dôvodu zneplatnenia
- vydá nový certifikát relevantnému TSS - postup je rovnaký ako pri vydaní prvotného certifikátu tohto TSS

### **1.17.10.5 Schopnosti obnoviť činnosť po havárii**

V prípade havárie postupuje I.CA v súlade s dokumentom „*Plán pre zvládanie krízových situácií a plán obnovy*“.

## **1.17.11 Ukončenie činnosti TSA**

V prípade plánovaného ukončenia činnosti I.CA ako akreditovaného/kvalifikovaného poskytovateľa certifikačných služieb v oblasti vydávania časových pečiatok, t.j.. z iných dôvodov, než sú

<b>Politika vydávania časových pečiatok</b>	<b>Strana 37 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

mimoriadne udalosti akými sú štrajky, občianske nepokoje, vojnový stav, prírodné katastrofy celoštátneho rozsahu alebo iné výsledky pôsobenia vyššej moci, zabezpečí I.CA s ohľadom na skutočnosť, že je kvalifikovaným poskytovateľom certifikačných služieb (viď. kap. 2) vykonávanie nasledujúcich činností podľa príslušnej legislatívy:

- V prípade Českej republiky:
  - ohlási príslušnému úradu zámer ukončiť činnosť poskytovania akreditovaných/kvalifikovaných certifikačných služieb v oblasti vydávania časových pečiatok najmenej 3 mesiace pred plánovaným ukončením činnosti,
  - vynaloží všetko úsilie na to, aby evidencia, vedená podľa platnej legislatívy, bola prevzatá iným akreditovaným/kvalifikovaným poskytovateľom certifikačných služieb v oblasti vydávania časových pečiatok, v prípade, že sa jej nepodarilo túto evidenciu odovzdať inému akreditovanému/kvalifikovanému poskytovateľovi certifikačných služieb v oblasti časových pečiatok, ohlási najneskôr 30 dní pred plánovaným dátumom ukončenia činnosti túto skutočnosť príslušnému úradu a zabezpečí odovzdanie tejto evidencie na príslušnému úradu - túto informáciu zahrnie do správy, odoslanej všetkým svojim klientom, ktorí sú držiteľmi platných zmlúv o poskytovaní akreditovaných/kvalifikovaných certifikačných služieb v oblasti časových pečiatok, pokiaľ toto bude známe najmenej 2 mesiace pred plánovaným ukončením činnosti,
  - sprístupní informáciu o ukončení činnosti akreditovaného/kvalifikovaného poskytovateľa certifikačných služieb v oblasti časových pečiatok na svojej internetovej informačnej adrese najmenej 2 mesiace pred plánovaným ukončením činnosti,
  - ukončí akreditované/kvalifikované poskytovanie certifikačných služieb v oblasti vydávania časových pečiatok,
  - preukázateľne zničí svoje dáta pre vytváranie elektronických značiek alebo elektronických podpisov, slúžiace k označovaniu alebo podpisovaniu časových pečiatok.
- v prípade Slovenskej republiky :
  - ohlási príslušnému úradu zámer ukončiť činnosť poskytovania akreditovaných/kvalifikovaných certifikačných služieb v oblasti vydávania časových pečiatok najmenej 6 mesiacov pred plánovaným ukončením činnosti,
  - ohlási každému držiteľovi platnej zmluvy (viď. kap. 4.3) o poskytovaní akreditovaných certifikačných služieb v oblasti vydávania časových pečiatok zámer ukončiť činnosť poskytovania kvalifikovaných certifikačných služieb v oblasti vydávania časových pečiatok najmenej 6 mesiacov pred plánovaným ukončením činnosti,
  - môže sa dohodnúť s iným akreditovaným poskytovateľom certifikačných služieb v oblasti vydávania časových pečiatok o prevzatí záznamov o časových pečiatkach a prevádzkovej dokumentácii – pokiaľ žiadny akreditovaný poskytovateľ certifikačných služieb v oblasti vydávania časových pečiatok tieto záznamy neprevezme, prevezme tieto záznamy úrad.

Problematika plánovaného ukončenia činnosti I.CA ako akreditovaného/kvalifikovaného poskytovateľa certifikačných služieb v oblasti vydávania certifikátov je detailne uvedená v internej dokumentácii I.CA.

#### **1.17.12 Zhoda s právnymi predpismi**

TSA je prevádzkovaný v súlade s platnou legislatívou, predovšetkým ZoEP a VoEP.

#### **1.17.13 Úložisko informácií a dokumentácií, ktoré sa týkajú prevádzky TSA**

##### **1.17.13.1 Auditné záznamy (logy)**

Problematika spojená s vytváraním, spracovaním a uchovávaním auditných logov je uvedená v základných dokumentoch:

- „**Systémová bezpečnostná politika TSA**“
- „**Vykonávacía smernica vydávania časových pečiatok**“

<b>Politika vydávania časových pečiatok</b>	<b>Strana 38 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

- „**Správa a súhlas vedenia I.CA o hodnotení rizík TSA**“
- „**Prehlásenie o aplikovateľnosti (SoA)**“

a detailne popísané v upresňujúcich interných bezpečnostných normách a smerniciach, zahrňujúcich problematiku uvedenú v kapitolách 7.4.13.1.1 až 7.4.13.1.6

#### 1.17.13.1.1 Typy zaznamenávaných udalostí

V dôveryhodných systémoch I.CA sú do elektronického auditného logu zaznamenávané udalosti, požadované :

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

Všetky auditné záznamy sú v nutnej miere uskutočňované, uchovávané a spracovávané so zachovaním preukázateľnosti pôvodu, integrity, dostupnosti, dôveryhodnosti a časovej autenticity.

Auditný systém je navrhnutý a prevádzkovaný spôsobom, ktorý zaručuje udržiavanie auditných dát, rezervovanie dostatočného priestoru pre auditné dáta, automatické prepisovanie auditného súboru, prezentáciu auditných záznamov pre užívateľov vhodným spôsobom a obmedzením prístupu k auditnému súboru len pre definovaných užívateľov.

#### 1.17.13.1.2 Periodicita spracovania záznamov

Auditné záznamy sú kontrolované a vyhodnocované raz týždenne, v prípade bezpečnostného incidentu okamžite.

#### 1.17.13.1.3 Doba uchovávania auditných záznamov

Doba, po ktorú sa uchovávajú auditné záznamy, je stanovená na minimálne 10 rokov od ich vzniku.

#### 1.17.13.1.4 Ochrana auditných záznamov

Elektronické auditné záznamy sú ukladané v dvoch kópiách, každá kópia je umiestnená v inej miestnosti prevádzkových priestorov I.CA. Raz mesačne sa vykonáva uloženie auditných záznamov na médium, ktoré je umiestnené mimo prevádzkových priestorov I.CA.

#### 1.17.13.1.5 Postupy pre zálohovanie auditných záznamov

Zálohovanie auditných záznamov prebieha obdobným spôsobom ako zálohovanie ostatných elektronických informácií.

#### 1.17.13.1.6 Systém zhromažďovania auditných záznamov (interný alebo externý)

Systém zhromažďovania auditných záznamov je vo vzťahu k I.CA interný, vo vzťahu k zmluvným partnerom externý. Zhromažďovanie auditných záznamov je evidované.

### 1.17.13.2 Uchovávanie informácií a dokumentácie

Uchovávanie informácií a dokumentácie je u I.CA vykonávané podľa požiadaviek ZoEP (ČR, SR) a ďalších právnych noriem (aktuálne znenie zákona ČR č.499/2004 Sb. o archivnictví a spisové službě a o

<b>Politika vydávania časových pečiatok</b>	<b>Strana 39 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

změně některých zákonů, zákon Slovenskej národnej rady č. 149/1975 Zb. o archívniectve v znení neskorších predpisov).

Zásady uchovávania informácií a dokumentácie sú uvedené v základných interných dokumentoch:

- **„Celková bezpečnostná politika“**
- **„Systémová bezpečnostná politika TSA“**
- **„Vykonávacia smernica vydávania časových pečiatok!**
- **„Systémová bezpečnostná politika TSA!**
- **„Analýza rizík“**

Problematika uchovávania informácií a dokumentácie (kapitoly 1.17.13.2.1 až 1.17.13.2.7) je detailne riešená v internej dokumentácii.

#### 1.17.13.2.1 Typy informácií a dokumentácie, ktoré sa uchovávajú

I.CA uchováva nasledujúce typy informácií a dokumentácie, ktoré súvisia s poskytovanými akreditovanými/kvalifikovanými certifikačnými v oblasti časových pečiatok :

- elektronické alebo písomné informácie podľa platnej legislatívy
- udalosti požadované štandardami :
  - 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
- aplikačné programové vybavenie
- všetku dokumentáciu spoločnosti, ktorá je nutná pre uskutočňovanie auditov systému manažmentu bezpečnosti informácií a kontrol bezpečnostnej zhody
- všetky záznamy zrušených certifikátov
- identifikačné údaje osoby, ktorá vykonala overenie totožnosti žiadateľa,
- obchodný názov poskytovateľa, ktorý žiadosť o poskytnutie akreditovanej/kvalifikovanej certifikačnej činnosti v oblasti vydávania kvalifikovaných certifikátov služby prijal, alebo zmluvného partnera, ktorý pre poskytovateľa túto činnosť zabezpečuje,
- záznam o manipulácii (napr. prevzatie, odovzdanie, uloženie, kontrola, konverzia do elektronickej podoby apod.) s informáciami
- identifikáciu miesta, kde sú uložené informácie a dokumentácia, ktorej uchovávanie je vyžadované ZoEP
- prevádzková a bezpečnostná dokumentácia.

#### 1.17.13.2.2 Doba uchovávania uchovávaných informácií a dokumentácie

I.CA zabezpečuje uchovávanie informácií a dokumentácií, uvedených v kapitole 1.17.13.2.1 po dobu najmenej 10 rokov od ich vzniku.

Po celú dobu existencie I.CA sú uchovávané informácie vzťahujúce sa k certifikátom TSA, s výnimkou príslušných dát pre vytváranie elektronickej značky alebo elektronickeho podpisu.

#### 1.17.13.2.3 Ochrana úložiska uchovávaných informácií a dokumentácie

uchovávané informácie a dokumentácie obsahujú aj osobné dáta klientov a preto je vzhľadom k zákonom ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálnych zneniach, s prihliadnutím na zvýšenú ochranu týchto dát. Priestory, v ktorých sa uchovávané informácie a dokumentácie nachádzajú, sú zabezpečené formou opatrení, vychádzajúcich z požiadaviek objektivej a fyzickej bezpečnosti.

Uchovávané informácie a dokumentácie sú určené výhradne pre internú potrebu I.CA a sú prístupné :

- pracovníkom I.CA v dôveryhodných pozíciách

<b>Politika vydávania časových pečiatok</b>	<b>Strana 40 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

- oprávneným kontrolným subjektom, orgánom činných v trestnom konaní a súdom, pokiaľ je to právnymi normami vyžadované

O každom takto povolenom prístupe je vyhotovovaný písomný záznam.

Postupy pri ochrane úložiska uchovávaných informácií a dokumentácií sú upravené internou dokumentáciou I.CA.

#### 1.17.13.2.4 Postupy pri zálohovaní uchovávaných informácií a dokumentácie

Postupy pri zálohovaní uchovávaných informácií a dokumentácie (viď kapitola 1.17.13.2.1) sú upravené internou dokumentáciou I.CA.

#### 1.17.13.2.5 Požiadavky na používanie časových pečiatok pri uchovávaní informácií a dokumentácie

V prípade, že budú využívané časové pečiatky, musí sa ísť o časové pečiatky vydané I.CA.

#### 1.17.13.2.6 Systém zhromažďovania uchovávaných informácií a dokumentácie (interný, externý)

Problematika prípravy a spôsobu ukladania informácií a dokumentácie v elektronickej i písomnej podobe je upravená internými normami a smernicami (viď. kap. 7.4.13.2.4). Zhromažďovanie archívnych záznamov je evidované.

#### 1.17.13.2.7 Postupy pre získanie a overenie uchovávaných informácií a dokumentácie

Pracoviská, kde sú informácie a dokumentácia uchovávané, obsahuje ich zoznam vrátane dátumu uloženia.

### 1.17.13.3 Zodpovednosti za zverejňovanie, úložisko informácií a dokumentácie

Problematika spojená so zodpovednosťami za zverejňovanie, úložisko informácií a dokumentácie (kapitoly 1.17.13.3.1 až 1.17.13.3.2) je detailne riešená v internej dokumentácii.

#### 1.17.13.3.1 Úložisko informácií a dokumentácie

S ohľadom na požiadavky ZoEP zriaďuje I.CA úložisko informácií a dokumentácie.

#### 1.17.13.3.2 Zverejňovanie informácií a dokumentácie

Základné adresy, na ktorých je možné nájsť informácie o verejných informáciách I.CA, politiky, Správy pre užívateľov a ďalšie informácie podľa ZoEP, ostatné verejné dokumentácie, atd., (ďalej tiež informačné adresy), prípadne odkazy pre zistenie ďalších informácií, sú :

- První certifikační autorita, a.s. ;  
Podvinný mlýn 2178/6, 190 00 Praha 9, Česká republika;
- internetová adresa <http://www.ica.cz> (ďalej tiež **internetová informačná adresa**);
- sídla registračných autorít.

Kontaktnými adresami, ktoré slúžia v oblasti poskytovania kvalifikovaných certifikačných služieb v oblasti časových pečiatok pre kontakt klienta prípadne verejnosti s I.CA (ďalej tiež kontaktná adresa), sú :

- elektronická poštová adresa [tsa@ica.cz](mailto:tsa@ica.cz) (na túto elektronickú adresu možno zasielať aj prípadné otázky, pripomienky, alebo návrhy na zlepšenie poskytovanej služby)

<b>Politika vydávania časových pečiatok</b>	<b>Strana 41 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

Vyššie uvedené informačné a kontaktné adresy je I.CA povinná zverejniť na internetovej informačnej adrese. Určení pracovníci I.CA sú taktiež povinní tieto informácie na vyžiadanie oznámiť všetkým potencionálnym užívateľom. To isté platí aj v prípade, že dôjde ku zmene kontaktných adries.

Možnosť získania certifikátu poskytovateľa je garantovaná najmenej dvomi nezávislými kanálmi :

- prostredníctvom internetových informačných adries I.CA a príslušného úradu
- prostredníctvom Vestníku príslušného úradu

Informácie o CRL možno získať na adrese <http://www.ica.cz/>. Priamo sa zverejňujú nasledujúce informácie (ostatné informácie možno získať zo samotného CRL) :

- dátum vydania CRL,
- číslo CRL,
- odkazy na miesto, kde možno CRL získať v určených formátoch (DER, PEM, TXT)

Povoleným protokolom pre prístup k informáciám o :

- konkrétnych certifikačných politikách, správach pre užívateľov - HTTP
- vydaných verejných certifikátoch - HTTP, HTTPS, FTP
- záznamoch zrušených certifikátov - HTTP, HTTPS, FTP,

Iné protokoly nie sú povolené. I.CA môže bez udania dôvodu prístup prostredníctvom niektorých z uvedených protokolov zrušiť alebo pozastaviť, pritom je povinná dodržať príslušné ustanovenia ZoEP a VoEP Tieto zmeny je I.CA povinná zverejniť prostredníctvom svojich informačných adries. Podrobnejšie informácie o možnostiach a príslušných parametroch uvedených protokolov I.CA zverejňuje tamtiež.

V prípadoch odobratia akreditácie alebo zneužitia, prípadne vzniku dôvodnej obavy zo zneužitia jeho dát pre vytváranie elektronických značiek alebo elektronických podpisov vydávaných certifikátov alebo záznamov zrušených certifikátov, oznámi I.CA túto skutočnosť na svojej internetovej informačnej adrese a prostredníctvom celoštátne distribuovaného denníku Mladá fronta Dnes.

#### 1.17.13.3.3 Periodicita zverejňovania informácií

I.CA zverejňuje informácie s nasledujúcou periodicitou :

- tento dokument - pred prvým poskytnutím služby vydávania časových pečiatok
- správa pre užívateľa, obsahujúca o.i. výsledky auditu systému bezpečnosti informácií - po každom jeho vykonaní – pri zahájení poskytovanej certifikačnej služby v oblasti vydávania certifikátov, prípadne pri jej zmene
- získanie alebo odobratie akreditácie podľa ZoEP – okamžite
- informácie o zneplatnení certifikátu poskytovateľa s uvedením dôvodu zneplatnenia (v prípade zneužitia alebo vzniku dôvodnej obavy zo zneužitia dát pre vytváranie elektronických značiek alebo elektronických podpisov, určených pre označovanie alebo podpisovanie vydávaných certifikátov a záznamov zrušených certifikátov) – bezodkladne
- aktualizácia záznamov vydaných certifikátov – okamžite pri každom vydaní nového certifikátu
- vydávanie záznamu zrušených certifikátov - táto povinnosť je realizovaná periodickým vydávaním CRL maximálne jedenkrát za 24 hodín (spravidla po 8 hodinách). Vydávanie CRL je nepretržité – 7 dní v týždni. Internetové adresy, na ktorých možno získať CRL diaľkovým prístupom, sú uvedené na internetovej informačnej adrese I.CA a sú taktiež uvedené v každom certifikáte. I.CA zverejňuje záznamy zrušených certifikátov najmenej dvomi na sebe nezávislými spôsobmi diaľkového prístupu.
- ostatné verejné informácie – nie je vopred určené, obecné však platí, že tieto informácie musia odrážať aktuálny stav poskytovaných kvalifikovaných certifikačných služieb

<b>Politika vydávania časových pečiatok</b>	<b>Strana 42 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

#### 1.17.13.3.4 Riadenie prístupu k jednotlivým typom úložísk

Prístup ku konkrétnym typom úložísk poverenými pracovníkmi I.CA je definovaný internou dokumentáciou.

## 1.18 Ostatné obchodné a právne záležitosti

### 1.18.1 Poplatky

#### 1.18.1.1 Poplatky za vydávanie časových pečiatok

Poplatky za vydávané časové pečiatky je možné získať na adrese [tsa@ica.cz](mailto:tsa@ica.cz).

#### 1.18.1.2 Poplatky za prístup k certifikátom poskytovateľa

Prístup k certifikátom poskytovateľa elektronickou cestou, I.CA sa nespoplatňuje.

#### 1.18.1.3 Poplatky za informácie o štatúte certifikátu a o zneplatnení

Prístup k informáciám o zrušených certifikátoch alebo štatútoch certifikátov elektronickou cestou I.CA sa nespoplatňuje.

#### 1.18.1.4 Poplatky za ďalšie služby

Poplatok za odovzdanie certifikátu (prvotný, následný) prostredníctvom záznamového média (napr. disketa) je uvedený v aktuálnom cenníku služieb, ktorý je k dispozícii na internetovej informačnej adrese I.CA.

Zrušenie certifikátu a stiahnutie elektronickej verzie politiky (v elektronickej verzii vo všeobecne používanom formáte PDF) je poskytované zdarma.

Poplatky za nadštandardné služby sú stanovované zmluvne.

#### 1.18.1.5 Iné ustanovenia týkajúce sa poplatkov (vrátane refundácií)

I.CA si vyhradzuje právo zmeny výšky poplatku za vydanie časovej pečiatky. I.CA je taktiež oprávnená stanoviť pre individuálne uzavreté zmluvy (viď. kap. 4.3) odlišnú výšku týchto poplatkov.

### 1.18.2 Finančná zodpovednosť

#### 1.18.2.1 Krytie poistenia

Spoločnosť První certifikační autorita, a.s., prehlasuje, že má uzatvorené poistenie podnikateľských rizík takým spôsobom, aby boli pokryté prípadné finančné škody.

#### 1.18.2.2 Ďalšie aktíva a záruky

Spoločnosť První certifikační autorita, a.s., prehlasuje, že má k dispozícii dostatočné finančné zdroje a iné finančné zabezpečenie na prevádzku v súlade s požiadavkami uvedenými v ZoEP a s ohľadom na riziko vzniku zodpovednosti za škodu.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 43 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

Podrobné informácie o aktívach spoločnosti První certifikační autorita, a.s., je možné získať z Výročnej správy I.CA.

### **1.18.2.3 Poistenie alebo krytie zárukou pre koncových užívateľov**

Služba nie je poskytovaná.

## **1.18.3 Citlivosť obchodných informácií**

### **1.18.3.1 Výpočet citlivých informácií**

Citlivými informáciami I.CA sú :

- dáta pre vytváranie elektronických značiek alebo elektronických podpisov príslušné k dátam pre overovanie elektronických značiek alebo elektronických podpisov obsiahnutých v certifikátoch poskytovateľa
- dáta pre vytváranie elektronických značiek alebo elektronických podpisov príslušné k dátam pre overovanie elektronických značiek alebo elektronických podpisov :
  - vyhradené pre infraštruktúru synchronizácie dôveryhodného času, využívané v procesoch synchronizácie meradla času TSS
  - využívané v procesoch správy TSS
- ostatné kryptograficky podstatné informácie slúžiace k prevádzke I.CA
- vybrané obchodné informácie I.CA
- všetky informácie a dokumentácia s ohľadom na poskytovanie kvalifikovaných certifikačných služieb podľa ZoEP

Chránenými obchodnými informáciami jednotlivých RA sú :

- dáta pre vytváranie elektronických podpisov alebo elektronických značiek príslušné k dátam pre overovanie elektronických podpisov alebo elektronických značiek obsiahnutých vo vlastných alebo účelových certifikátoch RA
- ostatné kryptograficky podstatné informácie slúžiace k prevádzke RA
- všetky informácie a dokumentácia s ohľadom na poskytovanie kvalifikovaných certifikačných služieb podľa ZoEP
- všetky osobné údaje

Za chránené informácie sa taktiež považujú všetky ďalšie informácie označené niektorým zo subjektov ako citlivé.

S chránenými informáciami, bez ohľadu na typ nosiča, je zaobchádzané tak, aby bola zabezpečená ich dôverynosť a integrita.

### **1.18.3.2 Informácie mimo rámec citlivých informácií**

Za verejné sa považujú typy informácií, ktoré nepatria do žiadnej z uvedených skupín v kapitole 1.18.3.1.

### **1.18.3.3 Zodpovednosť za ochranu citlivých informácií**

Každý pracovník, ktorý príde do styku s informáciami uvedenými v kapitole 1.18.3.1, ich nesmie bez súhlasu riaditeľa I.CA poskytnúť tretej strane.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 44 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

#### **1.18.4 Ochrana osobných údajov**

Problematika ochrany osobných údajov (kapitoly 1.18.4.1 až 1.18.4.7) je riešená internou dokumentáciou I.CA..

##### **1.18.4.1 Politika ochrany osobných údajov**

Ochrana osobných údajov a ďalších neverejných informácií je v I.CA riešená v súlade s požiadavkami príslušných zákonných noriem (zákon ČR č. 227/2000 Z.z. o elektronickom podpise a o zmene niektorých ďalších zákonov, zákon ČR 101/2000 Z.z. o ochrane osobných údajov a o zmene niektorých zákonov, zákona SR 215/2002 o elektronickom podpise a o zmene a doplnení niektorých zákonov, zákona SR č. 428/2002 Z.z. o ochrane osobných údajov, vrátane zákona č. 90/2005 Z.z.).

##### **1.18.4.2 Osobné údaje**

Osobnými informáciami sú všetky osobné údaje klientov, užívateľov či pracovníkov, podliehajúce ochrane v zmysle príslušnej zákonnej normy (zákony ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálnych zneniach).

##### **1.18.4.3 Údaje, ktoré nie sú považované za osobné**

Informácie, ktoré nie sú považované za osobné sú vo všeobecnosti údaje, uvedené vo vydávanom certifikáte, pokiaľ k jeho zverejneniu dal žiadateľ o certifikát súhlas, údaje, ktoré sú verejne známe, atď.

##### **1.18.4.4 Zodpovednosť za ochranu osobných údajov**

Ochrana osobných údajov a ďalších neverejných informácií je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálnych zneniach.

##### **1.18.4.5 Oznámenie o používaní dôverných informácií a súhlas s používaním citlivých informácií**

Ochrana osobných údajov a ďalších neverejných informácií je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálnych zneniach.

##### **1.18.4.6 Poskytovanie citlivých informácií pre súdne či správne účely**

Ochrana osobných údajov a ďalších neverejných informácií je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálnych zneniach.

##### **1.18.4.7 Iné náležitosti sprístupňovania osobných údajov**

Ochrana osobných údajov a ďalších neverejných informácií je v I.CA riešená v súlade s požiadavkami zákonov ČR č. 101/2000 Sb. a SR č. 428/2002 Z.z. v aktuálnych zneniach.

#### **1.18.5 Práva duševného vlastníctva**

Táto politika, všetky súvisiace dokumenty, obsah webových stránok, dáta pre vytváranie elektronických značiek alebo elektronických podpisov, príslušné dáta k overovaniu elektronických značiek, resp. elektronických podpisov obsiahnutých v certifikátoch poskytovateľa a procedúry, zabezpečujúce

<b>Politika vydávania časových pečiatok</b>	<b>Strana 45 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

prevádzku systému, poskytujúceho akreditované/kvalifikované certifikačné služby v oblasti certifikátov, sú chránené autorskými právami spoločnosti První certifikační autorita, a.s. a predstavujú jej významné know-how.

## **1.18.6 Zastupovanie a záruky**

### **1.18.6.1 Zastupovanie a záruky I.CA**

S ohľadom na poskytované certifikačné služby v oblasti vydávania časových pečiatok I.CA zaručuje splnenie všetkých záväzkov, uvedených v kapitole 1.10. Všetky záruky a z nich vyplývajúce plnenia je možné uznať len vtedy, pokiaľ :

- klient neporušil povinnosti a záväzky vyplývajúce mu zo zmluvy medzi ním a I.CA (rozumie sa zmluva ZoEP) a tejto politiky
- spoliehajúca sa strana neporušila povinnosti tejto politiky

Klient uplatňuje záruku vždy tam, kde podpisoval zmluvu (viď. kap. 4.3). Na používanie časovej pečiatky, ktorú I.CA nevydala, sa záruky nevzťahujú.

### **1.18.6.2 Zastupovanie a záruky držiteľov a klientov časových pečiatok**

Držiteľ alebo klient časovej pečiatky ručí za informácie, ním uvedené v zmluve (viď. kap. 4.3) o poskytovaní časových pečiatok a postupuje v súlade s platnou legislatívou a touto politikou.

### **1.18.6.3 Zastupovanie a záruky spoliehajúcich sa strán**

Spoliehajúce sa strany postupujú v súlade s platnou legislatívou a touto politikou.

### **1.18.6.4 Zastupovanie a záruky ostatných zúčastnených subjektov**

Služba nie je poskytovaná.

## **1.18.7 Zrieknutie sa záruk**

Spoločnosť První certifikační autorita, a.s., sa predovšetkým striktne riadi ZoEP a nemôže sa zriecť záruk, v ňom určených.

## **1.18.8 Zodpovednosť za škodu, náhrada škody**

Platí vždy limit záruky, ktorý bol dohodnutý v písomnej podobe (viď. kap 4.3). Pokiaľ vyššie nárokovanie straty prekračujú dohodnutý limit, poskytne I.CA plnenie maximálne do výšky limitu. Pokiaľ bolo zistené porušenie povinností klienta majúce súvislosť s uvádzanou škodou, záručné plnenie sa neposkytne. S touto skutočnosťou musí byť klient oboznámený. Táto skutočnosť musí byť klientovi oznámená a zaprotokolovaná.

Ďalšie možné náhrady škody vychádzajú z ustanovení príslušných zákonov a o ich výške môže rozhodnúť súd.

Spoločnosť První certifikační autorita, a.s.:

- sa zaväzuje, že splní všetky povinnosti definované príslušnými právnymi predpismi, ako aj politikami, reflektujúcich problematiku vydávania časových pečiatok,

<b>Politika vydávania časových pečiatok</b>	<b>Strana 46 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

- poskytuje vyššie uvedené záruky po celú dobu platnosti zmluvy (viď. kap. 4.3) o poskytovaní certifikačných služieb uzavretú so zákazníkom
- iné záruky ako vyššie uvedené neposkytuje.

Spoločnosť První certifikační autorita, a.s. nezodpovedá :

- za vady poskytnutých služieb vzniknuté z dôvodu nesprávneho alebo neoprávneného využívania služieb poskytnutých v rámci plnenia zmluvy (viď. kap. 4.3) o poskytovaní certifikačných služieb držiteľom, najmä však na využívanie v rozpore s podmienkami uvedenými v politike, ako aj za vady vzniknuté z dôvodu vyššej moci, vrátane dočasného výpadku telekomunikačného spojenia a pod.

Oprávnenú reklamáciu je možné podať týmito spôsobmi:

- e-mailom na adresu: [reklamace@ica.cz](mailto:reklamace@ica.cz)
- doporučenou poštovou zásielkou na adresu

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

Reklamujúca osoba je povinná uviesť:

- číslo zmluvy (viď. kap. 4.3)
- číslo príjmového dokladu
- čo najvýstižnejší popis závad a ich prejavov.

Povinnosti I.CA:

O reklamácií rozhodne I.CA najneskôr do troch pracovných dní od doručenia reklamácie a upovedomí o tom reklamujúceho (formou elektronickej pošty alebo doporučenou poštovou zásielkou), pokiaľ sa strany nedohodnú inak.

Reklamácia, vrátane vady, bude vybavená bez zbytočných odkladov, a to najneskôr do jedného mesiaca od uplatnenia reklamácie, pokiaľ sa strany nedohodnú inak.

### **1.18.9 Doba platnosti, ukončenie platnosti**

#### **1.18.9.1 Doba platnosti**

Táto politika je platná pre každú časovú pečaťku, vydanú v súlade s týmto dokumentom.

#### **1.18.9.2 Ukončenie**

Jedinou osobou, ktorá je oprávnená schvaľovať úpravy tejto politiky a určuje jej zhodu s príslušnou vykonávacou smernicou, je riaditeľ spoločnosti První certifikační autorita, a.s.

#### **1.18.9.3 Dôsledky ukončenia a pretrvanie záväzkov**

Časové pečiatky, vydané v súlade s týmto dokumentom, zostávajú platné aj po prípadnom ukončení poskytovania akreditovaných/kvalifikovaných certifikačných služieb spoločnosti První certifikační autorita, a.s.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 47 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

#### **1.18.10 Komunikácia medzi participujúcimi subjektami**

Pre individuálne oznámenie a komunikáciu s klientmi a držiteľmi časových pečiatok môže I.CA využiť nimi dodané e-mailové adresy, poštové adresy, telefonické čísla alebo osobné rokovania.

Klienti, držiteľia časových pečiatok, žiadatelia o časové pečiatky, spoliehajúce sa strany a verejnosť môžu s I.CA komunikovať spôsobom, uvedeným na adrese <http://www.ica.cz/>.

#### **1.18.11 Zmeny**

##### **1.18.11.1 Postup pri zmenách**

Postup je realizovaný riadeným procesom, uvedeným v internom dokumente I.CA.

##### **1.18.11.2 Postup pri oznamovaní zmien**

Postup je realizovaný riadeným procesom, uvedeným v internom dokumente I.CA.

##### **1.18.11.3 Okolnosti, pri ktorých musí byť zmenené OID**

Postup je realizovaný riadeným procesom, uvedeným v internom dokumente I.CA.

#### **1.18.12 Opatrenia pri riešení sporov**

Táto politika a zodpovedajúce vykonávacie smernice a ich výklad a aplikácia sa riadi podľa platnej legislatívy.

V prípade, že klient, držiteľ časových pečiatok, spoliehajúca sa strana, žiadateľ alebo zmluvný partner nesúhlasí s predloženým výkladom, môžu použiť nasledovné stupne odvolania :

- zodpovedný pracovník I.CA (potrebné je podať písomne);
- riaditeľ I.CA (potrebné je podať písomne a zložiť finančnú istinu, ktorá je vrátená v prípade kladného vybavenia sťažnosti).

Uvedený postup dáva nesúhlasiacej strane možnosť presadzovať svoj názor rýchlejším spôsobom, než súdnou cestou.

#### **1.18.13 Relevantná právna úprava**

Obchodné činnosti spoločnosti První certifikační autorita, a.s., sa riadia právnym poriadkom ČR.

#### **1.18.14 Zhoda s právnymi predpismi**

System poskytovania certifikačných služieb v oblasti vydávania časových pečiatok je prevádzkovaný v zhode s požiadavkami ZoEP.

<b>Politika vydávania časových pečiatok</b>	<b>Strana 48 (celkom 49)</b>
<b>Copyright © První certifikační autorita, a.s.</b>	<b>Verejný dokument</b>

## **1.18.15      **Ďalšie ustanovenia****

### **1.18.15.1 Rámcová zhoda**

Tieto skutočnosti sú pre aplikáciu tohto vydania dokumentu irelevantné.

### **1.18.15.2 Postúpenie práv**

Tieto skutočnosti sú pre aplikáciu tohto vydania dokumentu irelevantné.

### **1.18.15.3 Oddeliteľnosť**

Tieto skutočnosti sú pre aplikáciu tohto vydania dokumentu irelevantné.

### **1.18.15.4 Platby obhajcom a zrieknutie sa práv**

Tieto skutočnosti sú pre aplikáciu tohto vydania dokumentu irelevantné.

### **1.18.15.5 Vyššia moc**

Zmluva (vid. kap. 4.3) o poskytovaní akreditovaných/kvalifikovaných certifikačných služieb v oblasti vydávania časových pečiatok môže obsahovať ustanovenie o pôsobení vyššej moci.

## **1.18.16      **Ďalšie opatrenia****

Tieto skutočnosti sú pre aplikáciu tohto vydania dokumentu irelevantné.

<i>Politika vydávania časových pečiatok</i>	<i>Strana 49 (celkom 49)</i>
<i>Copyright © První certifikační autorita, a.s.</i>	<i>Verejný dokument</i>

## **Závěrečné ustanovenia**

Tento dokument, vydaný spoločnosťou První certifikační autorita, a.s., nadobúda platnosť a účinnosť dňom 01.10.2007.