První certifikační autorita, a.s.



Certifikační prováděcí směrnice

(algoritmus RSA)

Certifikační prováděcí směrnice (algoritmus RSA) je veřejným dokumentem, který je vlastnictvím společnosti První certifikační autorita, a.s., a byl vypracován jako nedílná součást komplexní bezpečnostní dokumentace. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu majitele autorských práv.

Verze 1.75

Copyright © První certifikační autorita, a.s.

OBSAH

1 Úvod 12
1.1 Přehled 12
1.2 Název a identifikace dokumentu 13
1.3 Participující subjekty 15
1.3.1 Certifikační autority 15
1.3.2 Registrační autority 15
1.3.3 Držitelé certifikátů 16
1.3.4 Spoléhající se strany 16
1.3.5 Jiné participující subjekty 16
1.4 Použití certifikátu 16
1.4.1 Přípustné použití certifikátu 16
1.4.2 Zakázané použití certifikátu 16
1.5 Správa politiky 17
1.5.1 Organizace spravující dokument 17
1.5.2 Kontaktní osoba 17
1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou 17
1.5.4 Postupy při schvalování CPS 17
1.6 Pojmy a zkratky 17
2 Odpovědnost za zveřejňování a za úložiště 25
2.1 Úložiště 25
2.2 Zveřejňování certifikačních informací 25
2.3 Čas nebo četnost zveřejňování 26
2.4 Řízení přístupu k jednotlivým typům úložišť 26
3 Identifikace a autentizace 27
3.1 Pojmenování 27
3.1.1 Typy jmen 27
3.1.2 Požadavek na významovost jmen 27
3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu 27
3.1.4 Pravidla pro interpretaci různých forem jmen 27
3.1.5 Jedinečnost jmen 27
3.1.6 Uznávání, ověřování a poslání obchodních značek 27
3.2 Počáteční ověření identity 27
3.2.1 Ověřování vlastnictví soukromého klíče 27
3.2.2 Ověřování identity organizace 28

3.2.3 Ověřování identity fyzické osoby 28
3.2.4 Neověřované informace vztahující se k držiteli certifikátu 28
3.2.5 Ověřování kompetencí 28
3.2.6 Kritéria pro interoperabilitu 28
3.2.7 Ověřování e-mailové adresy 28
3.3 Identifikace a autentizace při požadavku na výměnu klíče 29
3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče 29
3.3.2 Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu 29
3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu 29
3.4.1 Certifikáty poskytovatele 29
3.4.2 Certifikáty koncových uživatelů 30
4 Požadavky na životní cyklus certifikátu 31
4.1 Žádost o vydání certifikátu 31
4.1.1 Kdo může požádat o vydání certifikátu 31
4.1.2 Registrační proces a odpovědnosti 31
4.2 Zpracování žádosti o certifikát 31
4.2.1 Provádění identifikace a autentizace 31
4.2.2 Schválení nebo zamítnutí žádosti o certifikát 32
4.2.3 Doba zpracování žádosti o certifikát 32
4.3 Vydání certifikátů 32
4.3.1 Úkony CA v průběhu vydávání certifikátu 32
4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou 33
4.4 Převzetí vydaného certifikátu 33
4.4.1 Úkony spojené s převzetím certifikátu 33
4.4.2 Zveřejňování certifikátů certifikační autoritou 33
4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 34
4.5 Použití párových dat a certifikátu 34
4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu 34
4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou 34
4.6 Obnovení certifikátu 35
4.6.1 Podmínky pro obnovení certifikátu 35
4.6.2 Kdo může žádat o obnovení 35
4.6.3 Zpracování požadavku na obnovení certifikátu 35
4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu 35

4.6.5 Úkony spojené s převzetím obnoveného certifikátu 35
4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou 35
4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 35
4.7 Výměna veřejného klíče v certifikátu 35
4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu 35
4.7.2 Kdo může požádat o výměnu veřejného klíče v certifikátu 35
4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu...36
4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu.....36
4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem.....36
4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou 36
4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 36
4.8 Změna údajů v certifikátu 36
4.8.1 Podmínky pro změnu údajů v certifikátu 36
4.8.2 Kdo může požádat o změnu údajů v certifikátu.....36
4.8.3 Zpracování požadavku na změnu údajů v certifikátu 36
4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu 36
4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji certifikační autoritou 36
4.8.6 Zveřejňování certifikátů se změněnými údaji 37
4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 37
4.9 Zneplatnění a pozastavení platnosti certifikátu.....37
4.9.1 Podmínky pro zneplatnění.....37
4.9.2 Kdo může požádat o zneplatnění 37
4.9.3 Postup při žádosti o zneplatnění.....38
4.9.4 Prodleva při požadavku na zneplatnění certifikátu.....38
4.9.5 Doba zpracování žádosti o zneplatnění.....38
4.9.6 Povinnosti spoléhajících se stran při kontrole zneplatnění.....38
4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů 38
4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů.....38
4.9.9 Dostupnost ověřování stavu certifikátu on-line.....38
4.9.10 Požadavky při ověřování stavu certifikátu on-line 38
4.9.11 Jiné způsoby oznamování zneplatnění certifikátu.....39

4.9.12 Zvláštní postupy při kompromitaci klíče 39
4.9.13 Podmínky pro pozastavení platnosti certifikátu 39
4.9.14 Kdo může požádat o pozastavení platnosti....39
4.9.15 Postup při žádosti o pozastavení platnosti 39
4.9.16 Omezení doby pozastavení platnosti 39
4.10 Služby ověření stavu certifikátu 39
4.10.1 Funkční charakteristiky 39
4.10.2 Dostupnost služeb 39
4.10.3 Další charakteristiky služeb stavu certifikátu 40
4.11 Konec smlouvy o vydávání certifikátů....40
4.12 Úschova a obnova klíčů 40
4.12.1 Politika a postupy při úschově a obnově klíčů....40
4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace 40
5 Postupy správy, řízení a provozu 41
5.1 Fyzická bezpečnost....41
5.1.1 Umístění a konstrukce 41
5.1.2 Fyzický přístup 41
5.1.3 Elektřina a klimatizace 41
5.1.4 Vlivy vody 42
5.1.5 Protipožární opatření a ochrana 42
5.1.6 Ukládání médií 42
5.1.7 Nakládání s odpady 42
5.1.8 Zálohy mimo budovu 42
5.2 Procedurální postupy 42
5.2.1 Důvěryhodné role 42
5.2.2 Počet osob požadovaných pro zajištění jednotlivých činností 43
5.2.3 Identifikace a autentizace pro každou roli 43
5.2.4 Role vyžadující rozdělení povinností....43
5.3 Personální postupy 44
5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost 44
5.3.2 Posouzení spolehlivosti osob 44
5.3.3 Požadavky na školení....44
5.3.4 Požadavky a periodicita doškolování 45
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi 45
5.3.6 Postihy za neoprávněné činnosti 45

5.3.7 Požadavky na nezávislé dodavatele 45
5.3.8 Dokumentace poskytovaná zaměstnancům 45
5.4 Postupy zpracování auditních záznamů 45
5.4.1 Typy zaznamenávaných událostí 46
5.4.2 Periodicita zpracování záznamů 47
5.4.3 Doba uchování auditních záznamů 47
5.4.4 Ochrana auditních záznamů 48
5.4.5 Postupy pro zálohování auditních záznamů 48
5.4.6 Systém shromažďování auditních záznamů (interní nebo externí) 48
5.4.7 Postup při oznamování události subjektu, který ji způsobil 48
5.4.8 Hodnocení zranitelnosti 48
5.5 Uchovávání záznamů 48
5.5.1 Typy uchovávaných záznamů 49
5.5.2 Doba uchování záznamů 49
5.5.3 Ochrana úložiště záznamů 49
5.5.4 Postupy při zálohování záznamů 49
5.5.5 Požadavky na používání časových razítek při uchovávání záznamů 49
5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí) 49
5.5.7 Postupy pro získání a ověření uchovávaných informací 49
5.6 Výměna klíče 50
5.7 Obnova po havárii nebo kompromitaci 50
5.7.1 Postup ošetření incidentu nebo kompromitace 50
5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat 50
5.7.3 Postup při kompromitaci soukromého klíče 50
5.7.4 Schopnost obnovit činnost po havárii 51
5.8 Ukončení činnosti CA nebo RA 51
6 Řízení technické bezpečnosti 52
6.1 Generování a instalace párových dat 52
6.1.1 Generování párových dat 52
6.1.2 Předávání soukromého klíče jeho držiteli 53
6.1.3 Předávání veřejného klíče vydavateli certifikátu 53
6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám 53
6.1.5 Délky klíčů 53
6.1.6 Parametry veřejného klíče a kontrola jeho kvality 54

6.1.7 Účely použití klíče (dle rozšíření key usage X.509 v3) 54
6.2 Ochrana soukromého klíče a technologie kryptografických modulů 54
6.2.1 Řízení a standardy kryptografických modulů 54
6.2.2 Soukromý klíč pod kontrolou více osob (n z m) 54
6.2.3 Úschova soukromého klíče 55
6.2.4 Zálohování soukromého klíče 55
6.2.5 Uchovávání soukromého klíče 55
6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu 55
6.2.7 Uložení soukromého klíče v kryptografickém modulu 55
6.2.8 Postup aktivace soukromého klíče 56
6.2.9 Postup deaktivace soukromého klíče 56
6.2.10 Postup ničení soukromého klíče 56
6.2.11 Hodnocení kryptografických modulů 57
6.3 Další aspekty správy párových dat 57
6.3.1 Uchovávání veřejných klíčů 57
6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat 57
6.4 Aktivační data 58
6.4.1 Generování a instalace aktivačních dat 58
6.4.2 Ochrana aktivačních dat 58
6.4.3 Ostatní aspekty aktivačních dat 58
6.5 Řízení počítačové bezpečnosti 58
6.5.1 Specifické technické požadavky na počítačovou bezpečnost 58
6.5.2 Hodnocení počítačové bezpečnosti 59
6.6 Technické řízení životního cyklu 61
6.6.1 Řízení vývoje systému 61
6.6.2 Řízení správy bezpečnosti 62
6.6.3 Řízení životního cyklu bezpečnosti 62
6.7 Řízení bezpečnosti sítě 63
6.8 Označování časovými razítky 64
7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP 65
7.1 Profil certifikátu 67
7.1.1 Číslo verze 67
7.1.2 Rozšíření certifikátu 67
7.1.3 Objektové identifikátory algoritmů 67
7.1.4 Tvary jmen 67
7.1.5 Omezení jmen 67

7.1.6 Objektový identifikátor certifikační politiky 67
7.1.7 Použití rozšíření Policy Constraints 67
7.1.8 Syntaxe a sémantika kvalifikátorů politiky 67
7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies 68
7.2 Profil seznamu zneplatněných certifikátů 68
7.2.1 Číslo verze 68
7.2.2 Rozšíření CRL a záznamů v CRL 68
7.3 Profil OCSP 68
7.3.1 Číslo verze 71
7.3.2 Rozšíření OCSP 72
8 Hodnocení shody a jiná hodnocení 73
8.1 Periodicita nebo okolnosti hodnocení 73
8.2 Identita a kvalifikace hodnotitele 73
8.3 Vztah hodnotitele k hodnocenému subjektu 73
8.4 Hodnocené oblasti 73
8.5 Postup v případě zjištění nedostatků 73
8.6 Sdělování výsledků hodnocení 73
9 Ostatní obchodní a právní záležitosti 74
9.1 Poplatky 74
9.1.1 Poplatky za vydání nebo obnovení certifikátu 74
9.1.2 Poplatky za přístup k certifikátu 74
9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu 74
9.1.4 Poplatky za další služby 74
9.1.5 Postup při refundování 74
9.2 Finanční odpovědnost 74
9.2.1 Krytí pojištěním 74
9.2.2 Další aktiva 74
9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele 75
9.3 Důvěrnost obchodních informací 75
9.3.1 Rozsah důvěrných informací 75
9.3.2 Informace mimo rámec důvěrných informací 75
9.3.3 Odpovědnost za ochranu důvěrných informací 75
9.4 Ochrana osobních údajů 75
9.4.1 Politika ochrany osobních údajů 75
9.4.2 Informace považované za osobní údaje 75
9.4.3 Informace nepovažované za osobní údaje 76

9.4.4 Odpovědnost za ochranu osobních údajů....76
9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním....76
9.4.6 Poskytování osobních údajů pro soudní či správní účely....76
9.4.7 Jiné okolnosti zpřístupňování osobních údajů....76
9.5 Práva duševního vlastnictví....76
9.6 Zastupování a záruky....76
9.6.1 Zastupování a záruky CA....76
9.6.2 Zastupování a záruky RA....77
9.6.3 Zastupování a záruky držitele certifikátu....77
9.6.4 Zastupování a záruky spoléhajících se stran....77
9.6.5 Zastupování a záruky ostatních zúčastněných subjektů....78
9.7 Zřeknutí se záruk....78
9.8 Omezení odpovědnosti....78
9.9 Záruky a odškodnění....78
9.10 Doba platnosti, ukončení platnosti....79
9.10.1 Doba platnosti....79
9.10.2 Ukončení platnosti....79
9.10.3 Důsledky ukončení a přetrvání závazků....79
9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty....80
9.12 Novelizace....80
9.12.1 Postup při novelizaci....80
9.12.2 Postup a periodicita oznamování....80
9.12.3 Okolnosti, při kterých musí být změněn OID....80
9.13 Ustanovení o řešení sporů....80
9.14 Rozhodné právo....80
9.15 Shoda s platnými právními předpisy....81
9.16 Různá ustanovení....81
9.16.1 Rámcová dohoda....81
9.16.2 Postoupení práv....81
9.16.3 Oddělitelnost ustanovení....81
9.16.4 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv)....81
9.16.5 Vyšší moc....81
9.17 Další ustanovení....81
10 Závěrečná ustanovení....82

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	15.07.2015	Ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.1	02.11.2015	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace OID certifikačních politik (TSA, OCSP).
1.2	29.03.2016	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace OID certifikační politiky SSL.
1.3	06.04.2016	Ředitel společnosti První certifikační autorita, a.s.	Rozšíření podporovaných CP.
1.4	15.03.2017	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace OID politik. Úprava dle požadavků legislativy pro služby vytvářející důvěru, technických standardů a norem. Úprava dle požadavků programu Microsoft Trusted Root Certificate Program.
1.5	03.04.2017	Ředitel společnosti První certifikační autorita, a.s.	Aktualizace OID politik.
1.6	20.11.2017	Ředitel společnosti První certifikační autorita, a.s.	Doplnění nových politik. Změna zápisu OID politik.
1.61	30.04.2018	Ředitel společnosti První certifikační autorita, a.s.	Změna systému číslování verzí dokumentu. Doplnění postupu kontroly seznamu QSCD. Doplnění postupu kontroly CAA záznamů.
1.62	13.09.2018	Ředitel společnosti První certifikační autorita, a.s.	Doplnění nové politiky.
1.63	30.04.2019	Ředitel společnosti První certifikační autorita, a.s.	Pravidelná revize textu, oprava formálních chyb.
1.64	25.10.2019	Generální ředitel společnosti První certifikační autorita, a.s.	Doplnění nové politiky, označování funkcí v souladu s organizačním řádem.
1.65	07.03.2020	Generální ředitel společnosti První certifikační autorita, a.s.	Doplnění nové politiky, oprava formálních chyb.
1.66	29.04.2020	Generální ředitel společnosti První certifikační autorita, a.s.	Revize a upřesnění textu.
1.67	28.11.2020	Generální ředitel společnosti První certifikační autorita, a.s.	Vyznačení klasifikace dokumentu, změna úkonů CA při vydávání

			následného certifikátu, revize a upřesnění textu.
1.68	05.01.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Doplnění certifikační politiky vydávání kvalifikovaných certifikátů prostřednictvím NKČR a směrnice pro DRA NKČR.
1.69	20.04.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Doplněno distanční ověření identity žadatele pomocí služby ZealiD TRA Service. Aktualizace hodnocení kryptografických modulů. Revize textu.
1.70	22.09.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Doplnění certifikačních politik.
1.71	23.11.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Doplnění certifikačních politik.
1.72	25.04.2023	Generální ředitel společnosti První certifikační autorita, a.s.	Revize textu.
1.73	25.04.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Doplnění certifikační politiky. Revize textu.
1.74	25.04.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace seznamu odkazovaných standardů. Doplnění kontroly e-mailové adresy. Revize textu.
1.75	25.04.2026	Generální ředitel společnosti První certifikační autorita, a.s.	Revize textu.

1 ÚVOD

Tento dokument rozpracovává a upřesňuje zásady z konkrétních certifikačních politik (dále CP), které První certifikační autorita, a.s., (dále též I.CA), kvalifikovaný poskytovatel služeb vytvářejících důvěru, uplatňuje při poskytování služeb vytvářejících důvěru a při vydávání certifikátů (dále též Služby) v souladu s:

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

Pro Služby poskytované podle této certifikační prováděcí směrnice (dále též CPS), resp. příslušných certifikačních politik je využíván algoritmus RSA.

Služby, pokud je to relevantní, jsou poskytovány všem koncovým uživatelům na základě uzavřeného smluvního vztahu. I.CA nijak neomezuje potenciální koncové uživatele, poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

Pro všechny certifikáty koncových uživatelů, jejichž vydavatelem je I.CA, je dále používán termín Certifikát, resp. Certifikáty.

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

1.1 Přehled

Dokument **Certifikační prováděcí směrnice (algoritmus RSA)**, vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu vydávaných certifikátů a dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC 3647, s přihlédnutím k platným standardům Evropské unie a k právu České republiky v dané oblasti (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k ní irelevantní). Týká se certifikačních politik uvedených v kapitole 1.2.

Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument, obecně popisuje subjekty participující na poskytování Služeb a definuje přípustné využívání vydávaných certifikátů.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.

- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání certifikátu, resp. zneplatnění certifikátu, včetně definování typů a obsahů používaných jmen ve vydávaných certifikátech.
- Kapitola 4 definuje procesy životního cyklu certifikátů, tzn. žádost o vydání a vlastní vydání certifikátů, žádost o zneplatnění a vlastní zneplatnění certifikátů, služby související s ověřováním stavu certifikátů, ukončení poskytování Služeb atd.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání těchto záznamů a reakce po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.
- Kapitola 7 odkazuje na profily certifikátů a seznamů zneplatněných certifikátů v konkrétních CP a uvádí typy a délky položek pole subject a rozšíření subjectAlternativeName.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytovaných Služeb.
- Kapitola 9 zahrnuje problematiku obchodní a právní.

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu: Certifikační prováděcí směrnice (algoritmus RSA), verze 1.75

OID dokumentu: není přiřazen

Tato CPS se vztahuje k následujícím CP*:

OID	CP
1.3.6.1.4.1.23624.10.1.10.*a.b*	Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.11.*a.b*	Certifikační politika kořenové certifikační autority pro TLS certifikáty (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.30.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.31.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.32.1.*b*	Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.32.2.*b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.33.*a.b*	Certifikační politika vydávání systémových certifikátů (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.34.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě PSD2 (algoritmus RSA)

1.3.6.1.4.1.23624.10.1.35.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.37.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy na dálku (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.38.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.40.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám PSD2 (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.41.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy prostřednictvím NKČR (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.70.*a.b*	Certifikační politika vydávání komerčních certifikátů (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.71.*a.b*	Certifikační politika vydávání komerčních technologických certifikátů (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.72.*a.b*	Certifikační politika vydávání SSL certifikátů (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.74.*a.b*	Certifikační politika vydávání certifikátů pro systém elektronické identifikace (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.80.*a.b*	Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.81.*a.b*	Certifikační politika vydávání certifikátů OCSP respondérů TLS (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.90.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů SK pro elektronické podpisy (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.91.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě SK (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.92.*a.b*	Certifikační politika vydávání kvalifikovaných mandátních certifikátů SK (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.93.*a.b* (certifikáty pro podpisy) 1.3.6.1.4.1.23624.10.1.94.*a.b* (mandátní certifikáty)	Certifikační politika vydávání kvalifikovaných certifikátů SK pro vzdálené podepisování (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.190.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy dle legislativy SR (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.191.*a.b*	Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě dle legislativy SR (algoritmus RSA)

1.3.6.1.4.1.23624.10.1.192.*a.b*	Certifikační politika vydávání kvalifikovaných mandátních certifikátů dle legislativy SR (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.193.*a.b* (certifikáty pro podpisy) 1.3.6.1.4.1.23624.10.1.194.*a.b* (mandátní certifikáty)	Certifikační politika vydávání kvalifikovaných certifikátů pro vzdálené podepisování dle legislativy SR (algoritmus RSA) (algoritmus RSA)
1.3.6.1.4.1.23624.10.1.195.*a.b*	Certifikační politika vydávání certifikátů OCSP respondérů dle legislativy SR (algoritmus RSA)

* Vždy se jedná o aktuální verzi politiky ve tvaru *a.bc*, resp. *a.bcd,* která je vystavena na webu společnosti http://www.ica.cz, přičemž *a* a *b* jsou součástí OID politiky.

Služba vydávání kvalifikovaných certifikátů je v souladu s nařízením eIDAS zařazena na důvěryhodném seznamu udržovaném orgánem dohledu.

1.3 Participující subjekty

1.3.1 Certifikační autority

1.3.1.1 Kořenová certifikační autorita

Kořenová certifikační autorita společnosti První certifikační autorita, a.s., vydala ve dvoustupňové struktuře certifikačních autorit, v souladu s platnou právní úpravou a s požadavky technických standardů a norem, certifikáty podřízeným certifikačním autoritám provozovaným I.CA a svému OCSP respondéru. Tyto autority vydávají Certifikáty koncovým uživatelům a pro vlastní OCSP respondéry.

Kořenová certifikační autorita je ve stavu off-line a v žádném okamžiku tedy nemá propojení s externí sítí. Ve stavu on-line je pouze její OCSP respondér. Fyzicky je její informační systém realizován vyhrazenými počítači, HSM modul obsahující soukromý klíč je k tomuto informačnímu systému připojen prostřednictvím vyhrazeného zabezpečeného rozhraní.

1.3.1.2 Vydávající certifikační autority

Veřejné certifikační autority, provozované společností První certifikační autorita, a.s., poskytující Služby koncovým uživatelům a systému TSA.

1.3.2 Registrační autority

Registrační autority (dále „RA") využívané v procesech životního cyklu vydávaných Certifikátů. Tyto RA mohou být stacionární nebo mobilní.

1.3.3 Držitelé certifikátů

1.3.3.1 Certifikáty poskytovatele

Certifikáty jsou vydávány výhradně pro certifikační autority, jejich OCSP respondéry a pro časové servery autorit časových razítek, vše provozované I.CA. Oprávněným žadatelem a následně držitelem Certifikátů je I.CA, resp. I.CA SK jako právnická osoba.

1.3.3.2 Certifikáty koncových uživatelů

Certifikáty jsou vydávány koncovým uživatelům využívajícím Služby.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na certifikáty vydávané v rámci poskytování Služeb.

1.3.5 Jiné participující subjekty

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

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty kořenové CA smějí být používány výhradně pro ověřování jí vydaných certifikátů, seznamů jí zneplatněných certifikátů (CRL) a OCSP odpovědí vydaných jejím OCSP respondérem.

Certifikáty vydávajících certifikačních autorit smějí být používány výhradně pro ověřování certifikátů, seznamů zneplatněných certifikátů (CRL) vydaných těmito vydávajícími certifikačními autoritami a OCSP odpovědí vydaných OCSP respondéry (jsou-li implementovány) těchto vydávajících certifikačních autorit.

Certifikáty časových serverů autorit časových razítek smějí být používány výhradně pro ověřování časových razítek vydaných těmito časovými servery.

Certifikáty koncových uživatelů smějí být používány obecně v procesech PKI, tedy ověřování elektronických podpisů /elektronických značek/ elektronických pečetí, identifikace, autentizace a šifrování.

1.4.2 Zakázané použití certifikátu

Certifikáty vydávané v souladu s konkrétní CP nesmějí být používány v rozporu s použitím popsaným v konkrétní CP a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující dokument

Tuto CPS a jí odpovídající certifikační politiky spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti touto CPS a odpovídajícími certifikačními politikami, je uvedena na internetové adrese – viz kapitola 2.2.

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

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

1.5.4 Postupy při schvalování CPS

Pokud je potřebné provést změny v příslušné CPS a vytvořit její novou verzi, určuje generální ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze CPS předchází její schválení generálním ředitelem společnosti První certifikační autorita, a.s.

1.6 Pojmy a zkratky

tab. 2 – Pojmy

Pojem	Vysvětlení
bezpečné kryptografické zařízení	zařízení, na kterém je uložen soukromý klíč
CA/Browser Forum	organizace, dobrovolné sdružení certifikačních autorit
certifikát se zástupným doménovým jménem	Wildcard Certificate, certifikát obsahující nejméně jedno zástupné doménové jméno v rozšíření subjectAlternativeName
doménové jméno	označení přiřazené uzlu v doménovém jmenném systému
doménový jmenný prostor	množina všech možných doménových jmen, která jsou podřízena jednomu uzlu v doménovém jmenném systému
doménové návěští	Domain Label, seřazený seznam žádného nebo více oktetů, který tvoří část doménového jména (v DNS systému, viz též RFC 8499); při použití teorie grafů návěští identifikuje jeden uzel v části grafu všech možných doménových jmen
dvoufaktorová autentizace	autentizace využívající dvou ze tří faktorů – něco vím (heslo), něco mám (např. čipová karta, hardwarový token) nebo něco jsem (otisky prstů, snímání oční sítnice či duhovky)

elektronická pečeť	zaručená elektronická pečeť, nebo uznávaná elektronická pečeť, nebo kvalifikovaná elektronická pečeť dle právní úpravy pro služby vytvářející důvěru
elektronický podpis	zaručený elektronický podpis, nebo uznávaný elektronický podpis, nebo kvalifikovaný elektronický podpis dle právní úpravy pro služby vytvářející důvěru
GET metoda	standardně preferovaná metoda zasílání http požadavků OCSP respondéru pomocí protokolu http, metoda umožňuje ukládání do mezipaměti (druhá metoda je POST)
hashovací funkce	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou (hash)
kořenová CA	certifikační autorita vydávající certifikáty podřízeným certifikačním autoritám
kvalifikovaný certifikát pro elektronický podpis nebo pro elektronickou pečeť nebo pro autentizaci webových stránek	certifikát definovaný právní úpravou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů, resp. pečetí	prostředek pro vytváření elektronických podpisů, resp. pečetí, který splňuje požadavky stanovené v příloze II eIDAS
LDH návěští	LDH Label, typ doménového návěští v DNS – znakový řetězec složený z ASCII znaků, číslic a pomlčky s omezením, že pomlčka nesmí být na začátku a konci řetězce a celková délka nesmí přesáhnout 63 znaků (viz též RFC5890) pozn.: zkratka LDH = Letters, Digits, Hyphen = písmena, číslice, pomlčka
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
OCSP stapling	způsob minimalizace dotazů na OCSP respondér, RFC 4366 - TLS Extensions; umožní TLS serveru vracet jednou získanou OCSP odpověď na stav svého certifikátu (po dobu její platnosti) všem koncovým uživatelům přistupujícím k TLS serveru
orgán dohledu	subjekt dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru
ověřované doménové jméno	Authorization Domain Name, FQDN použité ke schválení pro uvedení v certifikátu - CA může pro účely ověřování kontroly nad doménovým jménem použít FQDN získané z DNS CNAME dotazu
párová data	soukromý a jemu odpovídající veřejný klíč
phishing	podvodná technika používaná v elektronické komunikaci na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.)
P-návěští	P-Label, XN-návěští, které obsahuje od páté pozice dále platný výstup algoritmu Punycode (RFC 3492, kapitola 6.3)

písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
podřízená CA	CA vydávající certifikáty koncovým uživatelům
POST metoda	metoda komunikace klienta s http serverem způsobem odesílání dat z klienta na server (např. odeslání dotazu na OCSP respondér prostřednictvím http protokolu)
právní úprava pro služby vytvářející důvěru	platné právní předpisy vztahující se ke službám vytvářejícím důvěru
registrant doménového jména	někdy uváděn jako vlastník doménového jména, ale správněji osoby či entity registrované registrátorem doménového jména jako mající právo dohlížet na používání doménového jména, fyzická nebo právnická osoba vypisovaná jako „Registrant" příkazem WHOIS, nebo registrátorem doménového jména
registrátor doménového jména/ registrátor	osoba nebo entita, která registruje doménová jména z pověření nebo se souhlasem: • internetové korporace pro přiřazování jmen a čísel (ICANN) - správce kořene DNS prostoru, • správce TLD (např. .com) nebo ccTLD (např. .CZ, národního správce)
registrátor PSP	autorita odpovědná za registraci a přidělování čísel PSP v konkrétním státě, obvykle národní banka, v ETSI TS 119 495 označení NCA (National Competent Authority)
služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru	služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru definovaná eIDAS
smluvní partner	subjekt zajišťující na základě písemné smlouvy pro I.CA služby vytvářející důvěru nebo jejich části – nejčastěji se jedná o smluvní RA
softcard	programová emulace čipové karty pro přístup k soukromému klíči uloženému v HSM
soukromý klíč	jedinečná data pro vytváření elektronického podpisu/pečetě
spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát
SSL certifikát	certifikát použitý pro identifikaci a šifrování v rámci komunikace prostřednictvím SSL/TLS protokolu
TWINS	obchodní produkt I.CA, obsahující dvojici certifikátů: • kvalifikovaný certifikát pro elektronický podpis, • komerční certifikát – vydaný výhradně na základě smluvního vztahu mezi I.CA a koncovým uživatelem
veřejný klíč	jedinečná data pro ověřování elektronického podpisu/pečetě
XN-návěští	XN-Label, třída návěští LDH začínající znaky "xn--" (viz RFC 5890)
základ doménového jména	Base Domain Name, část FQDN, která je prvním uzlem doménového jména nalevo od:

	• registrem kontrolovaného (jména), nebo • veřejné přípony plus registrem kontrolovaného jména, nebo veřejné přípony
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
zástupné doménové jméno	Wildcard Domain Name, znakový řetězec začínající "*." bezprostředně následovaný FQDN

tab. 3 – Zkratky

Zkratka	Vysvětlení
ASCII	American Standard Code for Information Interchange, kódová tabulka definující znaky anglické abecedy a jiné znaky používané v informatice
BIH	Bureau International de l'Heure, (anglicky The International Time Bureau), Mezinárodní časová služba
bit	z anglického *binary digit* – číslice dvojkové soustavy – základní a současně nejmenší jednotka informace v číslicové technice
BRG	dokument „Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" organizace CA/Browser Forum
CA	certifikační autorita
CAA	DNS Resource záznam – viz RFC 6844
ccTLD	country code TLD, národní doména nejvyšší úrovně, internetová doména na nejvyšší úrovni stromu internetových domén obvykle používána, nebo rezervována pro země, svrchované státy, nebo závislá území, všechny v ASCII definované národní domény nejvyššího řádu jsou tvořeny dvěma znaky
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
CP	certifikační politika
CPS	certifikační prováděcí směrnice
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
CT	Certificate Transparency, systém pro omezení chybného vydání certifikátu založený na zápisu certifikátů (resp. precertifikátů) do veřejných logů umožňujících detekci chybného vydání (zejména podvodného získání certifikátu jiným než oprávněným žadatelem)
ČR	Česká republika
ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátu

DNS	Domain Name System, hierarchický systém doménových jmen, který je realizovaný DNS servery a DNS protokolem, kterým si vyměňují informace, hlavním úkolem jsou vzájemné převody doménových jmen na IP adresy uzlů sítě a obráceně
DRA	distanční registrační autorita
DV	Domain Validation, typ SSL certifikátu
EAL	Evaluation Assurance Level, úroveň hodnocení záruky
EBA	European Banking Association, evropská bankovní asociace
EC	Elliptic Curve, eliptická křivka
ECC	Elliptic Curve Cryptography, kryptografie eliptických křivek
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EU	Evropská unie
EV	Extended Validation, typ SSL certifikátu, resp. certifikát pro autentizaci internetových stránek
EVCG	dokument "Guidelines For The Issuance And Management Of Extended Validation Certificates" organizace CA/Browser Forum
EVCP	Extended Validation Certificate Policy, typ politiky vydávání certifikátů
EZS	elektronická zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
FQDN	Fully Qualified Domain Name, plně kvalifikované doménové jméno, doménové jméno uvádějící označení všech nadřazených uzlů v internetovém doménovém jmenném systému
GDPR	General Data Protection Regulation, nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
gTLD	generic TLD, obecná doména nejvyššího řádu (např. .org pro neziskové organizace)
html	Hypertext Markup Language, značkovací jazyk pro vytváření hypertextových dokumentů

http	Hypertext Transfer Protocol, protokol pro výměnu textových dokumentů ve formátu html
https	Hypertext Transfer Protocol Secure, protokol pro zabezpečenou výměnu textových dokumentů ve formátu html
I.CA	První certifikační autorita, a.s.
I.CA SK	První certifikační autorita, s.r.o.
ICANN	Internet Corporation for Assigned Names and Numbers, organizace mj. přidělující a spravující doménová jména a IP adresy
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IP	Internet Protocol, komunikační protokol pro přenos paketů a jejich směrování využívaný v Internetu
IPS	Intrusion Prevention System, systém prevence průniku
ISMS	Information Security Management System, systém řízení bezpečnosti informací
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
IT	Information Technology, informační technologie
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
MPSV	Ministerstvo práce a sociálních věcí
NCA	National Competent Authority, autorita odpovědná za registraci a přidělování čísel PSP v konkrétním státě, obvykle národní banka
NCP	Normalized Certificate Policy, typ certifikační politiky nekvalifikovaných certifikátů, kvalitativně shodný s politikou vydávání kvalifikovaných certifikátů
NCP+	Extended Normalized Certificate Policy, certifikační politika NCP, soukromý klíč je umístěn na bezpečném kryptografickém zařízení
NKČR	Notářská komora České republiky
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
OSVČ	osoba samostatně výdělečně činná
OV	Organization Validation, typ SSL certifikátu
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování–Zavedení–Kontrola–Využití, Demingův cyklus, metoda neustálého zlepšování
PDS	PKI Disclosure Statement, zpráva pro uživatele

PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
PSD	Payment Services Directive, směrnice Evropské unie o platebních službách č. 2007/64/EC
PSD2	revidovaná směrnice Evropské unie o platebních službách č. 2015/2366 účinná od 13. ledna 2018
PSP	Payment Service Provider, poskytovatel platebních služeb
PSS	Probabilistic Signature Scheme, schéma elektronického podpisu vyvinuté M. Bellarem a P. Rogawayem a standardizované jako část PKCS#1 v2.1
PTC	Publicly-Trusted Certificate, certifikát, jehož certifikát kořenový je distribuován jako důvěryhodná kotva v běžně dostupném aplikačním programovém vybavení
PUB	Publication, označení standardu FIPS
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu nebo pečetě (dle eIDAS)
QWAC	Qualified Website Authentication Certificate, certifikát pro autentizaci internetových stránek
RA	registrační autorita
RFC	Request for Comments, označení řady standardů a dalších dokumentů popisujících internetové protokoly, systémy apod.
RSA	šifra s veřejným klíčem pro podepisování a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)
RTS	Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace
S/MIME BR	dokument „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" organizace CA/Browser Forum
SCT	Signed Certificate Timestamp, pode1psané potvrzení („razítko") z příslušného CT logu o zařazení precertifikátu
sha, SHA	typ hashovací funkce
SSL	Secure Sockets Layer, komunikační protokol, resp. vrstva vložená mezi vrstvu transportní a aplikační, která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran
TLD	Top Level Domain, doména na nejvyšší úrovni stromu internetových domén (pod jeho kořenem), v doménovém jméně je doména nejvyšší úrovně uvedena na konci
TLS	Transport Layer Security, komunikační protokol, následovník SSL
TS	Technical Specification, typ ETSI standardu

TSA	Time-Stamping Authority, autorita časových razítek
TSP	Trust Service Provider, poskytovatel služeb vytvářejících důvěru
TSS	Time-Stamp Server, server časových razítek
TSU	Time-Stamp Unit, jednotka vydávající časová razítka
UPN	User Principal Name, uživatelské jméno ve tvaru dle RFC 822
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
URI	Uniform Resource Identifier, textový řetězec s definovanou strukturou sloužící k přesné specifikaci zdroje informací
UTC	Coordinated Universal Time, standard přijatý 1.1.1972 pro světový koordinovaný čas - funkci „oficiálního časoměřiče" atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
WHOIS	databáze, která slouží k evidenci údajů o majitelích internetových domén a IP adres
ZOOÚ	aktuální právní úprava týkající se ochrany osobních údajů

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ZA ÚLOŽIŠTĚ

2.1 Úložiště

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

2.2 Zveřejňování certifikačních informací

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

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

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

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

Na výše uvedené internetové adrese lze získat informace o:

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

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

V případě zneplatnění certifikátů certifikačních autorit z důvodu podezření na kompromitaci, případně samotné kompromitace příslušného soukromého klíče oznámí I.CA tuto skutečnost

na své internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes, resp. Hospodárske noviny nebo Sme.

2.3 Čas nebo četnost zveřejňování

Viz kapitola 2.3 konkrétní CP.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům I.CA, smluvním partnerům nebo subjektům definovaným příslušnou právní úpravou. Přístup k těmto informacím je řízen pravidly popsanými v interní dokumentaci, zejména:

- „Operátor CA“,
- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Řízení bezpečnosti informací“,
- „Příručka administrátora“,
- „Bezpečnostní incidenty“,
- „HSM/Private Server“,
- „HSM/nShield XC“,
- „Správa TSS“,
- „Správa TSMC“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

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

3.1.2 Požadavek na významovost jmen

V procesu vydávání certifikátu je vždy vyžadována významovost všech ověřitelných jmen uvedených v položkách pole subject, resp. rozšíření subjectAlternativeName. Podporované položky tohoto pole a rozšíření jsou uvedeny v konkrétní CP.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Uvedeno v kapitole 3.1.3 konkrétní CP.

3.1.4 Pravidla pro interpretaci různých forem jmen

Údaje uváděné v žádosti o certifikát (formát PKCS#10) se do pole subject, resp. rozšíření subjectAlternativeName ve vydávaných certifikátech přenášejí ve tvaru, ve kterém jsou uvedeny v předkládané žádosti.

3.1.5 Jedinečnost jmen

Uvedeno v kapitole 3.1.5 konkrétní CP.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Certifikáty vydané podle konkrétní CP příslušné této CPS mohou obsahovat pouze obchodní značky, jejichž vlastnictví nebo pronájem byly doloženy. Veškeré důsledky plynoucí z neoprávněného užívání ochranné známky nesou držitelé certifikátů.

3.2 Počáteční ověření identity

Subjekty oprávněné podat žádost o vydání certifikátu jsou vyjmenovány v kapitole 4.1.1. V následujících kapitolách jsou uvedena pravidla pro počáteční ověření jejich identity.

3.2.1 Ověřování vlastnictví soukromého klíče

Vlastnictví soukromého klíče odpovídajícího veřejnému klíči v žádosti o certifikát se prokazuje předložením žádosti ve formátu PKCS#10. Ta je zmíněným soukromým klíčem elektronicky podepsána, resp. opatřena elektronickou pečetí a držitel soukromého klíče tak prokazuje, že v době tvorby elektronického podpisu, resp. elektronické pečetě soukromý klíč vlastnil.

3.2.2 Ověřování identity organizace

Postup popsán v kapitole 3.2.2 konkrétní CP a dále v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“.

3.2.3 Ověřování identity fyzické osoby

Postup je popsán v kapitole 3.2.3 konkrétní CP a dále v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Online vydávání certifikátu s ověřením přes NIA – Uživatelská dokumentace“,
- „Ověření identity žadatele přes webovou aplikaci – Identity check – Uživatelská dokumentace“,
- „Vydávání kvalifikovaných certifikátů se ztotožněním ZealiD“.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Neověřované informace jsou vždy uvedeny v kapitole 3.2.4 konkrétní CP.

3.2.5 Ověřování kompetencí

Adresu elektronické pošty je možno umístit v rozšíření certifikátu, konkrétně v poli rfc822Name položky subjectAlternativeName, pouze tehdy, byla-li tato skutečnost v procesu vydání certifikátu pro tuto žádost ověřena.

Příznak, že klíčový pár byl generován na zařízení typu QSCD lze do certifikátu vložit pouze tehdy, byla-li tato skutečnost v procesu vydání certifikátu pro tuto žádost ověřena.

Postup ověřování dalších specifických práv je popsán v kapitole 3.2.5 konkrétní CP.

3.2.6 Kritéria pro interoperabilitu

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

3.2.7 Ověřování e-mailové adresy

U certifikačních politik, kde je to relevantní, je jednou ze dvou metod prováděno ověřování e-mailové adresy, a to buď kontrolou příslušnosti adresy k registrované DNS doméně (validating authority over mailbox via domain), nebo ověřením držitele e-mailové adresy pomocí obsahu zasílaného e-mailu (validating control over mailbox via email). Užití příslušné ověřovací metody odvisí od typu smluvního vztahu s klientem.

3.2.7.1 Ověřování proti registrované DNS doméně

Metoda ověření e-mailové adresy vůči registrované DNS doméně je určena pro firemní zákazníky, kde smluvní partner má kontrolu nad příslušnou DNS doménou. V takovém případě se ověřuje příslušnost doménové části e-mailové adresy vůči interně udržovanému seznamu

registrovaných podnikových domén (podnik má s I.CA uzavřenou smlouvu a kontrola nad DNS doménou byla ověřena).

3.2.7.2 Ověřování adresy pomocí obsahu zasílaného ověřovacího e-mailu

Ověření vlastnictví e-mailové adresy z žádosti je v tomto případě prováděno zasláním ověřovacího e-mailu obsahujícího unikátní náhodnou informaci (validační link) s časově omezenou platností. Kontrolu nad e-mailovou adresou žadatel o certifikát potvrdí kliknutím na příslušné tlačítko, resp. validační link, čímž aktivuje validační proceduru na straně systému I.CA.

3.3 Identifikace a autentizace při požadavku na výměnu klíče

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Požadavky jsou vždy uvedeny v kapitole 3.3.1 konkrétní CP.

3.3.1.1 Certifikáty poskytovatele

Jedná se o vydání prvotního certifikátu, kdy platí stejné požadavky, jako v případě počátečního ověření identity.

3.3.1.2 Certifikáty koncových uživatelů

V případě SSL, EV SSL, resp. certifikátů pro autentizaci internetových stránek se vždy jedná o vydání prvotního certifikátu, kdy platí stejné požadavky, jako v případě počátečního ověření identity.

Pro ostatní typy certifikátů lze vydat tzv. následný certifikát, kdy je standardní žádost o certifikát (s novým veřejným klíčem) předávaná ke zpracování elektronicky podepsána, resp. opatřena elektronickou pečetí vytvořenou soukromým klíčem, náležícím veřejnému klíči v platném certifikátu, ke kterému je vydáván tento následný certifikát. V tomto případě není vyžadována fyzická přítomnost žadatele o certifikát na RA a žadatel o certifikát tímto elektronickým podpisem, resp. touto elektronickou pečetí potvrzuje, že údaje o subjektu nebyly změněny.

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

Výměna párových dat již zneplatněného certifikátu není podporována. Jediný způsob, jak získat nový certifikát, je získání nového certifikátu s novým veřejným klíčem.

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Konkrétní způsoby identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu jsou uvedeny v kapitole 3.4 konkrétní CP.

3.4.1 Certifikáty poskytovatele

Oprávněnou osobou žádat o zneplatnění certifikátu poskytovatele, tj. certifikátu:

- kořenové certifikační autority i jí vydaného certifikátu OCSP respondéru,
- vydávající certifikační autority i jí vydaného certifikátu OCSP respondéru,
- časového serveru autority časových razítek,

je generální ředitel I.CA.

Žadatelem o zneplatnění certifikátu kořenové certifikační autority, popř. certifikátu, souvisejícího s kvalifikovanými službami vytvářejícími důvěru, může být také představitel orgánu dohledu. Žádost musí být písemná, nebo být doručena do datové schránky I.CA.

3.4.2 Certifikáty koncových uživatelů

Možné způsoby identifikace a autentizace jsou následující:

- osobně na RA,
- prostřednictvím formuláře na webových stránkách společnosti (s využitím hesla pro zneplatnění certifikátu),
- prostřednictvím elektronicky nepodepsané elektronické zprávy (obsahující heslo pro zneplatnění certifikátu),
- prostřednictvím elektronické zprávy elektronicky podepsané, resp. opatřené elektronickou pečetí (realizovány soukromým klíčem příslušným k předmětnému certifikátu, jenž má být zneplatněn, nebo soukromým klíčem z podpisového certifikátu),
- prostřednictvím datové schránky (s využitím hesla pro zneplatnění certifikátu),
- prostřednictvím doporučené listovní zásilky na adresu sídla I.CA (s využitím hesla pro zneplatnění certifikátu).

Údaje, které musí žádost o zneplatnění certifikátu obsahovat, jsou uvedeny v kapitole 4.9.3.

I.CA si vyhrazuje právo akceptování i jiných forem postupů při identifikaci a autentizaci požadavků na zneplatnění certifikátu, které však nesmí být v rozporu s právní úpravou pro služby vytvářející důvěru.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

Žádost o vydání certifikátu může podat fyzická osoba, nebo právnická osoba nebo organizační složka státu (dále též Organizace). Subjekty oprávněné podat žádost o vydání certifikátu jsou uvedeny v kapitole 4.1.1 konkrétní CP.

4.1.2 Registrační proces a odpovědnosti

Procesy prováděné v průběhu registračního procesu jsou uvedeny v konkrétní CP.

Žadatel je povinen zejména:

- poskytovat pravdivé a úplné informace při registraci žádosti o vydání certifikátu,
- seznámit se s CP, podle které mu bude vydán certifikát.

Poskytovatel Služeb je zejména povinen Služby poskytovat v souladu s platnou právní úpravou, konkrétní CP a touto CPS, Systémovou bezpečnostní politikou – důvěryhodné systémy a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

Proces zpracování žádosti o certifikát je popsaný v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Vydávání kvalifikovaných certifikátů se ztotožněním ZealiD“,
- „Online vydávání certifikátu s ověřením přes NIA – Uživatelská dokumentace“,
- „Ověření identity žadatele přes webovou aplikaci – Identity check – Uživatelská dokumentace“,
- „Operátor CA“.

Kontrola CAA záznamů, tam, kde je to relevantní, je prováděna podle interní dokumentace:

- „Postupy ověřování" (pro SSL OV/DV certifikáty),
- „Postupy ověřování při žádosti o QC-web/EV SSL certifikát“.

4.2.1 Provádění identifikace a autentizace

Žadatel o certifikát se identifikuje a autentizuje způsobem, popsaným v kapitolách 3.2.2 a 3.2.3.

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

V případě vydávání certifikátů poskytovatele Služeb rozhodne vedení společnosti První certifikační autorita, a.s., na základě písemné žádosti o vydání certifikátu, případně o zamítnutí žádosti. Výsledek je dokumentován.

Pokud některá z ověření, prováděna pracovníkem RA skončí negativně, proces vydání certifikátu je ukončen. V opačném případě pracovník RA vydání certifikátu schválí.

Postupy pro přijetí nebo odmítnutí žádosti o certifikát jsou uvedeny v kapitole 4.2.2 konkrétní CP a v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Online vydávání certifikátu s ověřením přes NIA – Uživatelská dokumentace“,
- „Ověření identity žadatele přes webovou aplikaci – Identity check – Uživatelská dokumentace“,
- „Vydávání kvalifikovaných certifikátů se ztotožněním ZealiD“.

4.2.3 Doba zpracování žádosti o certifikát

V případě vydávání certifikátů poskytovatele doba zpracování písemné žádosti o vydání certifikátu nepřekročí pět pracovních dnů ode dne předložení žádosti vedení společnosti.

Pro certifikáty koncových uživatelů platí, že po kladném rozhodnutí o vydání certifikátu je I.CA povinna neprodleně certifikát vydat. Přibližné časové údaje pro vydání certifikátu, není-li smluvně ošetřeno jinak, jsou v následujícím seznamu:

- prvotní certifikát – doba vydání (pouze v pracovní dny a hodiny) je do 15 minut a jen ve výjimečných případech může být tato doba delší,
- následný certifikát – jednotky minut.

Výjimku tvoří SSL certifikáty, resp. certifikáty pro autentizaci internetových stránek. kdy doba zpracování žádosti o certifikát zpravidla nepřekročí pět pracovních dnů (z důvodu ověřování údajů v žádosti).

4.3 Vydání certifikátů

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání **prvotního certifikátu** provádějí operátorky/operátoři, dále jen operátoři, CA:

- vizuální kontrolu shody údajů obsažených v žádosti o certifikát (struktura PKCS#10) a údajů doplněných pracovníkem RA,
- vizuální kontroly formální správnosti údajů.

Ověřování vlastnictví soukromého klíče, kontrola podporovaných hashovacích funkcí v žádosti o certifikát (minimálně sha-256), kontrola kompetencí a kontroly formální správnosti údajů jsou prováděny jak programovým vybavením umístěným na pracovních stanicích operátorů CA, tak programovým vybavením jádra systému CA. Pokud některá z uvedených kontrol skončí negativně, proces vydání certifikátu je ukončen.

Vydávání **následného certifikátu**, pokud je to relevantní, probíhá automatizovaně, bez zásahu operátorů CA. Ověřování vlastnictví soukromého klíče, podporovaných hashovacích funkcí v žádosti o certifikát (minimálně sha-256) a kontrola kompetencí jsou prováděny programovým vybavením jádra systému CA. Pokud některá z uvedených kontrol skončí negativně, proces vydání certifikátu je ukončen.

Postupy jsou uvedeny v kapitole 4.3.1 konkrétní CP a upřesněny v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Online vydávání certifikátu s ověřením přes NIA – Uživatelská dokumentace“
- „Ověření identity žadatele přes webovou aplikaci – Identity check – Uživatelská dokumentace“,
- „Operátor CA“.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

V případě, že žadatel o certifikát je osobně přítomen vydání certifikátu, získá oznámení o jeho vydání od pracovníka RA. Pokud se jedná o certifikát koncového uživatele, je tento vždy automaticky zaslán na kontaktní e-mailovou adresu žadatele.

Uvedené postupy jsou detailně popsány v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Online vydávání certifikátu s ověřením přes NIA – Uživatelská dokumentace“
- „Ověření identity žadatele přes webovou aplikaci – Identity check – Uživatelská dokumentace“,
- „Operátor CA“.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Úkony spojené s převzetím certifikátu jsou vždy popsány v kapitole 4.4.1 konkrétní CP.

Detailně je proces je popsán v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Operátor CA“.

4.4.2 Zveřejňování certifikátů certifikační autoritou

Certifikáty poskytovatele jsou zveřejňovány na webových stránkách I.CA, certifikáty související s kvalifikovanými službami vytvářejícími důvěru jsou navíc předány orgánu dohledu.

Pro certifikáty koncových uživatelů I.CA zajistí zveřejnění jí vydaných, vyjma Certifikátů:

- obsahujících údaje, jejichž zveřejnění by bylo v rozporu s příslušnou právní úpravou (např. právní úprava týkající se ochrany osobních údajů),
- u kterých si držitel Certifikátu vymínil, že nebudou zveřejněny.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Platí ustanovení kapitoly 4.4.2 a případně požadavky právní úpravy pro služby vytvářející důvěru.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností držitele certifikátu mj. je:

- dodržovat veškerá relevantní ustanovení smlouvy o poskytování Služeb (pokud je smlouva v elektronickém tvaru, je opatřena kvalifikovaným elektronickým podpisem),
- užívat soukromý klíč a odpovídající certifikát pouze pro účely stanovené v této CP,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v certifikátu takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- neprodleně uvědomit poskytovatele Služby o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o:
  - podezření, že soukromý klíč byl zneužit, a
  - neplatnosti či nepřesnosti údajů v certifikátu,

  v takových případech požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje (např. www.ica.cz, pracoviště RA, příslušný důvěryhodný seznam) certifikáty certifikačních autorit související s certifikátem koncového uživatele vydaným podle konkrétní CP, ověřit hodnoty jejich otisků a jejich platnost,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že certifikát je platný, tj.:
  - ověřit platnost certifikátu podle RFC5280, kapitola 6 (včetně celé certifikační cesty a odvolání platnosti certifikát),
  - ověřit kvalifikovanost vydavatele kvalifikovaného certifikátu (jeho uvedení na seznamu důvěryhodných služeb s příslušnými atributy),
- dodržovat veškerá ustanovení odpovídající CP a případně právní úpravy pro služby vytvářející důvěru, vztahující se k povinnostem spoléhající se strany.

4.6 Obnovení certifikátu

Službou obnovení certifikátu je míněno vydání nového certifikátu k ještě platnému certifikátu, nebo k zneplatněnému certifikátu, nebo k expirovanému certifikátu, aniž by byl změněn veřejný klíč, nebo jiné informace v certifikátu.

Služba obnovení certifikátu není poskytována.

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Kdo může žádat o obnovení

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

Viz kapitola 4.6.

4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.6.

4.7 Výměna veřejného klíče v certifikátu

Popsáno v kapitole 4.7 konkrétní certifikační politiky.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.2 Kdo může požádat o výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Viz kapitola 4.7.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Viz kapitola 4.7.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.7.

4.8 Změna údajů v certifikátu

Popsáno v kapitole 4.8 konkrétní certifikační politiky.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

4.8.6 Zveřejňování certifikátů se změněnými údaji

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Službu pozastavení platnosti certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění

Kromě podmínek uvedených v následujících podkapitolách si I.CA vyhrazuje právo akceptování i jiných okolností podmínek na zneplatnění certifikátu.

4.9.1.1 Certifikáty poskytovatele

Certifikát musí být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče odpovídajícího veřejnému klíči tohoto certifikátu,
- žádost generálního ředitele I.CA,
- nastanou-li skutečnosti uvedené v právní úpravě pro služby vytvářející důvěru, resp. v technických standardech a normách.

4.9.1.2 Certifikáty koncových uživatelů

Certifikát musí být zneplatněn na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče odpovídajícího veřejnému klíči tohoto certifikátu,
- je porušeno ustanovení smlouvy o poskytování Služby podle konkrétní CP ze strany držitele certifikátu,
- v případech, kdy nastanou skutečnosti uvedené v právní úpravě pro služby vytvářející důvěru nebo příslušných technických standardech a normám (např. neplatnost údajů v certifikátu),
- pokud je veřejný klíč v žádosti o vydání certifikátu duplicitní s veřejným klíčem v již vydaném certifikátu.

I.CA si vyhrazuje právo akceptování i jiných podmínek na zneplatnění certifikátu koncového uživatele, které však nesmí být v rozporu s právní úpravou pro služby vytvářející důvěru.

4.9.2 Kdo může požádat o zneplatnění

Pro certifikáty poskytovatele platí, že žádost o zneplatnění mohou podat:

- generální ředitel I.CA, případně jednatel ICA SK, resp. osoby jimi pověřené,
- případně další subjekty definované právní úpravou pro služby vytvářející důvěru.

Pro certifikáty koncových uživatelů je informace uvedena v kapitole 4.9.2 konkrétní CP.

4.9.3 Postup při žádosti o zneplatnění

Způsob podání žádosti o zneplatnění certifikátu je vždy popsán v kapitole 4.9.3 konkrétní CP.

Požadavky na identifikaci a autentizaci jsou uvedeny v kapitole 3.4.

4.9.4 Prodleva při požadavku na zneplatnění certifikátu

Požadavek na zneplatnění certifikátu musí být podán bezodkladně.

4.9.5 Doba zpracování žádosti o zneplatnění

Maximální doba mezi přijetím žádosti o zneplatnění certifikátu a jeho zneplatněním je 24 hodin.

Postupy jsou uvedeny v interní dokumentaci:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Operátor CA“.

4.9.6 Povinnosti spoléhajících se stran při kontrole zneplatnění

Spoléhající se strany jsou povinny provádět veškeré úkony, uvedené v kapitole 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Periodicita vydávání seznamu zneplatněných certifikátů je uvedena v kapitole 4.9.7 konkrétní CP.

Činnosti operátorů CA v procesu vydávání CRL jsou popsány v interní dokumentaci:

- „Operátor CA“.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL je zveřejněn neprodleně po vydání, vždy jsou dodrženy podmínky popsané v kapitolách 4.9.5 a 4.9.7.

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Služba ověřováni stavu certifikátu s využitím protokolu OCSP je veřejně dostupná. Každý certifikát, vyjma certifikátů kořenové CA a OCSP respondérů, obsahuje odkaz na příslušný OCSP respondér.

Profily OCSP žádosti i odpovědi jsou v souladu s RFC 6960 a RFC 5019. certifikát OCSP respondéru obsahuje rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 6960.

4.9.10 Požadavky při ověřování stavu certifikátu on-line

Viz kapitola 4.9.9.

V případě získání rozdílné informace o stavu certifikátu prostřednictvím CRL je nutné provést opakované ověření stavu certifikátu po alespoň deseti vteřinách.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Není relevantní pro tento dokument.

4.9.12 Zvláštní postupy při kompromitaci klíče

Postup pro zneplatnění certifikátu v případě kompromitace soukromého klíče není odlišný od výše popsaného postupu pro zneplatnění certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.14 Kdo může požádat o pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.15 Postup při žádosti o pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.16 Omezení doby pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.10 Služby ověření stavu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL v certifikátech, vyjma certifikátů kořenové CA a OCSP respondérů.

Skutečnost, že certifikační autority poskytují informace o stavu certifikátu formou OCSP, je uvedena v jimi vydaných certifikátech.

Záznamy o zneplatnění na CRL nebo v OCSP odpovědi jsou udržovány minimálně do doby konce platnosti odvolaného certifikátu.

4.10.2 Dostupnost služeb

I.CA garantuje zajištění nepřetržité dostupnosti (7 dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných certifikátů a seznamů zneplatněných certifikátů (CRL) a dále dostupnost služby OCSP.

Doba odpovědi na žádost o stav certifikátu s využitím CRL nebo OCSP je za normálních provozních podmínek kratší než 10 vteřin.

Postup je popsán v interní dokumentaci, zejména:

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

4.10.3 Další charakteristiky služeb stavu certifikátu

I.CA na seznamech zneplatněných certifikátů (CRL) pro kvalifikované certifikáty uvádí, v souladu s požadavky relevantních standardů, i expirované kvalifikované certifikáty, a to po dobu tří dnů po jejich expiraci (v CRL je uváděno rozšíření ExpiredCertsOnCRL). Důvodem omezení doby, po kterou jsou expirované certifikáty na CRL uváděny, je snaha udržet rozsah CRL v rozumných mezích.

I.CA v souladu s požadavky relevantních standardů dodržuje konzistentnost informací o stavu odvolání certifikátu mezi CRL a OCSP. Pro kvalifikované certifikáty obsahují OCSP odpovědi na podporu těchto požadavků rozšíření ArchiveCutOff.

4.11 Konec smlouvy o vydávání certifikátů

Platnost smlouvy o vydání certifikátu končí s ukončením platnosti posledního podle ní vydaného certifikátu.

4.12 Úschova a obnova klíčů

Není relevantní pro tento dokument, služba úschovy a obnovy klíčů není poskytována.

4.12.1 Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Viz kapitola 4.12.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Postupy správy, řízení a provozu jsou zaměřeny především na:

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

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

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně uvedena v interní dokumentaci, zejména:

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

5.1.1 Umístění a konstrukce

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

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

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

V prostorách, kde jsou umístěny důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru, je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v

rozmezí 20 °C ± 5 °C. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

5.1.4 Vlivy vody

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

5.1.5 Protipožární opatření a ochrana

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

5.1.6 Ukládání médií

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

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

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procedurální postupy

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou ve společnosti I.CA definovány důvěryhodné role. Postup jmenování zaměstnanců do důvěryhodných rolí, specifikace těchto rolí včetně odpovídajících činností a odpovědností jsou uvedeny v interní dokumentaci, zejména:

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

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

5.2.2 Počet osob požadovaných pro zajištění jednotlivých činností

Pro procesy související s párovými daty certifikačních autorit a OCSP respondérů jsou definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

- inicializaci kryptografického modulu,
- generování párových dat veškerých certifikačních autorit a jim příslušných OCSP respondérů,
- ničení soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů, včetně jejich záloh,
- zálohování a obnovu soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů,
- aktivaci a deaktivaci soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů.

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

Podrobné informace jsou vždy uvedeny v kapitole 5.2.2 konkrétní CP a v interní dokumentaci:

- „Příručka administrátora“,
- „HSM PrivateServer – Postupy generování klíčů a certifikátů CA a OCSP“,
- „HSM nShield – Postupy generování klíčů a certifikátů CA a OCSP“,
- „HSM/Private Server“,
- „HSM/nShield XC“.

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci (jméno, certifikát) a autentizaci (heslo, soukromý klíč) k těm komponentám, které jsou pro jejich činnost nezbytné. Problematika je upravena v interní dokumentaci, zejména:

- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „Operátor CA“,
- „Příručka administrátora“.

Pro vybrané činnosti využívají pracovníci v důvěryhodných rolích dvoufaktorovou autentizaci.

5.2.4 Role vyžadující rozdělení povinností

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

- „Systémová bezpečnostní politika – důvěryhodné systémy“.

5.3 Personální postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

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

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

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

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

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

Problematika je detailně popsána v interní dokumentaci:

- „Kontrolní činnost, bezúhonnost a odbornost“.

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích I.CA jsou:

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

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

5.3.3 Požadavky na školení

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

Problematika je detailně popsána v interní dokumentaci:

- „Kontrolní činnost, bezúhonnost a odbornost“.

5.3.4 Požadavky a periodicita doškolování

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

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

Problematika je detailně popsána v interní dokumentaci:

- „Kontrolní činnost, bezúhonnost a odbornost“.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

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

5.3.6 Postihy za neoprávněné činnosti

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

- „Organizační řád“.

5.3.7 Požadavky na nezávislé dodavatele

I.CA může nebo musí některé činnosti zajišťovat smluvně, za činnost nezávislých dodavatelů plně odpovídá. Tyto obchodně právní vztahy jsou upraveny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími certifikačními politikami, relevantními částmi interní dokumentace, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou uplatňovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Postupy zpracování auditních záznamů

Zaznamenávány jsou veškeré události požadované v případě kvalifikovaných Certifikátů právní úpravou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, v ostatních případech relevantními technickými standardy a normami, mj. o životním cyklu vydávaných certifikátů, nakládání se soukromými klíči poskytovatele a o dalších událostech, jako je např. ukončení činnosti certifikační autority.

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

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

Problematika spojená s vytvářením, zpracováním a uchováváním auditních logů je detailně řešena v interní dokumentaci, zejména:

- „Příručka administrátora“,
- „Zálohování dat provozních systémů“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

5.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované právní úpravou pro služby vytvářející důvěru a příslušnými technickými standardy a normami, mj. o životním cyklu certifikátů.

Speciálním případem zaznamenávání událostí je událost generování párových dat certifikačních autorit. Celý proces generování párových dat certifikačních autorit probíhá v souladu s právní úpravou pro služby vytvářející důvěru a s relevantními technickými standardy a normami. Generování je vždy prováděno podle připraveného scénáře ve fyzicky zabezpečeném prostředí a pod kontrolou více osob v důvěryhodných rolích.

O generování párových dat certifikačních autorit je vytvořen protokol s údaji požadovanými v technických standardech, který je podepsán přítomnými osobami v důvěryhodných rolích. V případě generování klíče certifikační autority vydávající certifikáty typu SSL koncovým klientům je navíc proveden videozáznam postupu generování.

Pro generování párových dat kořenové certifikační autority dále platí, že je mu osobně přítomen auditor kvalifikovaný v souladu s platnými technickými standardy, který rovněž podepíše vytvořený protokol a potvrdí tím, že autorita při generování párových dat postupovala v souladu s připraveným scénářem a zajistila při tom integritu a důvěrnost.

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

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

S ohledem na požadavky relevantních technických standardů a norem a právní úpravy pro služby vytvářející důvěru jsou v důvěryhodných systémech I.CA do elektronického auditního logu zaznamenávány následující bezpečnostně relevantní provozní události:

- z hlediska systému významné události prostředí a klíčového hospodářství,
- spuštění a ukončení funkcí auditu,
- změny parametrů auditu,
- akce, prováděné při chybách úložiště auditních záznamů,

- všechny pokusy přístupu k systému
- všechny události vztahující se k životnímu cyklu párových dat a certifikátů CA.
- záznam o registraci žadatele,
- záznam o pokus neoprávněné registrace žadatele (s maximem dosažitelných informací o neoprávněném žadateli),
- záznam o zrušení registrace žadatele (údaje o žadateli se uchovávají),
- vše, co souvisí s životním cyklem certifikátu:
  - záznam o požadavku RA na vydání certifikátu včetně výsledku,
  - záznam o neoprávněném požadavku na vydání certifikátu včetně výsledku,
  - záznam o požadavku na vydání následného certifikátu včetně výsledku,
  - záznam o neoprávněném požadavku na vydání následného certifikátu včetně výsledku,
  - záznam o požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku,
  - záznam o neoprávněném požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku,
  - záznam o oznámení možné kompromitace dat pro vytváření elektronických podpisů, resp. pečetí podepisující / pečetící osobou,
  - záznam o zneplatnění certifikátu,
  - záznam o pokusu neoprávněného přístupu do systému,
  - záznam o zveřejnění certifikátu, včetně výsledku,
  - záznam o zanesení zneplatněného certifikátu do CRL,
  - záznam o zveřejnění CRL.

Všechny záznamy v auditním souboru obsahují následující parametry:

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

5.4.2 Periodicita zpracování záznamů

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

- „Příručka administrátora“,

v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

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

5.4.4 Ochrana auditních záznamů

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

Elektronické auditní záznamy jsou ukládány ve dvou kopiích. Auditní záznamy v papírové formě jsou umístěny mimo provozních prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci – viz kapitola 5.4.

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

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

- „Přístupy k posuzování a ošetřování rizik bezpečnosti informací – důvěryhodné systémy“,
- „Příručka administrátora“.

5.5 Uchovávání záznamů

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

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

5.5.1 Typy uchovávaných záznamů

I.CA uchovává níže uvedené záznamy (v elektronické nebo listinné podobě), které souvisejí s poskytovanými službami vytvářejícími důvěru, zejména:

- zprávy/protokoly o průběhu generování párových dat certifikačních autorit,
- pro podřízené certifikační autority vydávající certifikáty typu SSL:
  - videozáznam průběhu generování párových dat,
- záznamy související s životním cyklem Certifikátů (zejména dokumentace z ověření žádostí o vydání a zneplatnění certifikátů),
- záznamy o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- provozní a bezpečnostní dokumentaci.

5.5.2 Doba uchování záznamů

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

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště záznamů

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

Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací – viz kapitola 5.5.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací – viz kapitola 5.5.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

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

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

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

Samotná problematika přípravy a způsobu ukládání záznamů v elektronické i písemné podobě je upravena interní dokumentací – viz kapitola 5.5. Shromažďování záznamů je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

Výměna párových dat certifikačních autorit v případě standardních situací (uplynutí platnosti certifikátů certifikačních autorit) je prováděna s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) formou vydání nového certifikátu.

V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu vydávání certifikátů, tzn. změny kryptografických algoritmů, délky klíčů atd.) je tato činnost prováděna v adekvátním, co nejkratším časovém období.

Jak v případě standardních, tak nestandardních situací je výměna veřejného klíče v certifikátech certifikačních autorit veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup ošetření incidentu nebo kompromitace

V případě výskytu těchto událostí postupuje I.CA v souladu s interní dokumentací:

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

5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče

V případě vzniku důvodné obavy z kompromitace soukromého klíče certifikačních autorit postupuje I.CA, resp. I.CA SK tak, že:

- ukončí jeho používání,
- okamžitě a trvale zneplatní příslušný certifikát a zničí jemu odpovídající soukromý klíč,
- zneplatní všechny platné certifikáty vydané příslušnou certifikační autoritou,
- bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese, pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,
- v případě kvalifikovaných certifikátů oznámí orgánu dohledu informaci o zneplatnění příslušného certifikátu s uvedením důvodu.

Obdobný postup bude uplatněn i v případě, že dojde k takovému vývoji kryptoanalytických metod (např. změny kryptografických algoritmů, délky klíčů atd.), že by mohla být bezprostředně ohrožena bezpečnost služeb vytvářejících důvěru.

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interní dokumentací:

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

5.8 Ukončení činnosti CA nebo RA

Pro ukončování činnosti CA platí:

- ukončení činnosti CA musí být písemně oznámeno všem držitelům platných certifikátů, subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních Služeb a v případě kvalifikovaných certifikátů orgánu dohledu,
- ukončení činnosti CA musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- pokud je součástí ukončení činnosti CA ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně uvedení důvodu ukončení platnosti,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity Služeb,
- po dobu platnosti jediného certifikátu vydaného certifikační autoritou musí tato zajistit alespoň funkce zneplatňování certifikátu a vydávání CRL,
- následně CA prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván v souladu s pravidly této CPS, resp. konkrétní CP.

V případě odnětí statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru:

- informace musí být písemně nebo elektronicky oznámena všem držitelům platných certifikátů a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování služeb vytvářejících důvěru,
- informace musí být zveřejněna v souladu s kapitolou 2.2 a na všech pracovištích registračních autorit; součástí informace bude i sdělení, že kvalifikované systémové certifikáty nelze nadále používat v souladu s účelem jejich vydání,
- o dalším postupu rozhodne generální ředitel I.CA, resp. jednatel I.CA SK na základě rozhodnutí orgánu dohledu.

V případě ukončení činnosti konkrétního pracoviště RA je tato skutečnost oznámena na internetové adrese http://www.ica.cz.

Problematika plánovaného ukončení činnosti jako kvalifikovaného poskytovatele služeb vytvářejících důvěru je detailně uvedena v interní dokumentaci:

- „Ukončení činnosti služeb I.CA“.

Pravidla pro ukončování činnosti konkrétních certifikačních autorit a jim odpovídajících RA jsou detailně uvedena v příslušných CP.

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit, jejich OCSP respondérů a párových dat vztahujících se k certifikátům TSU systému TSA2, které probíhá v zabezpečených vyhrazených prostorách provozních pracovišť v souladu s požadavky kapitol 5.2 a 5.4.1, je prováděno v kryptografických modulech, které splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN. Uvedené kryptografické moduly jsou pod výhradní kontrolou I.CA.

Veškeré požadavky na proces generování výše uvedených párových dat jsou popsány interní a externí dokumentací, mj.:

- „Řízení fyzického přístupu do místností I.CA“,
- „HSM/Private Server“,
- „HSM/nShield XC“,
- „Správa TSS“,
- „Správa TSMC“,
- „HSM PrivateServer – Postupy generováním klíčů a certifikátů CA a OCSP“,
- „HSM nShield – Postupy generování klíčů a certifikátů CA a OCSP“.

Protokol o průběhu generování párových dat obsahuje minimálně:

- jmenný seznam přítomných zaměstnanců,
- datum a čas zahájení a ukončení generace párových dat s přesností minimálně na minuty,
- místo, kde bylo generování prováděno,
- popis zařízení, na kterém bylo generování prováděno, umožňující jednoznačnou identifikaci tohoto zařízení,
- datum vyhotovení protokolu,
- vlastnoruční podpisy všech pracovníků, kteří se generování párových dat zúčastnili.

Generování párových dat pracovníků podílejících se na vydávání certifikátů je prováděno na čipových kartách, splňujících požadavky na QSCD. Soukromé klíče těchto párových dat jsou na čipové kartě uloženy v neexportovatelném tvaru a k jejich použití je nutné zadat PIN.

Generování párových dat vztahujících se ke službám vytváření elektronického podpisu nebo elektronické pečetě koncovými uživateli na dálku je prováděno v kryptografickém modulu typu QSCD, které je pod kontrolou I.CA a splňuje požadavky hodnocení standardů ETSI a CEN. Kontrola přítomnosti na unijním seznamu a doby platnosti certifikace jsou prováděny podle interní dokumentace:

- „Příručka administrátora“.

Generování párových dat vztahujících se k certifikátům vydávaným ostatním koncovým uživatelům je prováděno na zařízeních, která jsou pod výhradní kontrolou příslušných držitelů soukromých klíčů. Úložištěm těchto párových dat může být jak hardware, tak software.

V případě kvalifikovaných certifikátů, jejichž soukromý klíč odpovídající veřejnému klíči v certifikátu je uložen na zařízení typu QSCD, jsou kontroly přítomnosti zařízení na důvěryhodném seznamu EU a doby platnosti certifikace tohoto zařízení prováděny podle interní dokumentace:

- „Personalizace QSCD“.

6.1.2 Předávání soukromého klíče jeho držiteli

Pro soukromé klíče certifikačních autorit a jejich OCSP respondérů není relevantní – soukromé klíče jsou uloženy v kryptografických modulech, které jsou pod výhradní kontrolou I.CA.

Pro soukromé klíče TSU systému TSA2 není relevantní – soukromé klíče jsou generovány a uloženy v kryptografických modulech, které jsou součástí TSU systému TSA2 a jsou pod výhradní kontrolou I.CA.

Pro soukromé klíče využívané ve službách tvorby elektronického podpisu nebo elektronické pečetě na dálku není relevantní – soukromé klíče jsou uloženy v kryptografickém modulu, který je pod kontrolou I.CA.

Služba generování párových dat ostatním držitelům certifikátů a pracovníkům podílejícím se na vydávání certifikátů není poskytována.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Pro veřejné klíče certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 a pro veřejné klíče vztahující ke službám vytváření elektronického podpisu a elektronické pečetě na dálku není relevantní, veřejný klíč byl jako součást párových dat vygenerován v kryptografickém modulu pod výhradní kontrolou I.CA.

V ostatních případech je veřejný klíč doručen vydavateli certifikátu v žádosti o vydání certifikátu (formát PKCS#10).

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Získání veřejného klíče certifikační autority obsaženého v jejím certifikátu je garantováno následujícími způsoby:

- obdržením na RA,
- z důvěryhodného seznamu ČR,
- prostřednictvím internetových informačních adres I.CA, příslušného orgánu dohledu, resp. prostřednictvím věstníku tohoto orgánu dohledu,
- každý žadatel o certifikát obdrží příslušné certifikáty certifikačních autorit při získání svého prvotního certifikátu.

6.1.5 Délky klíčů

Mohutnost klíče kořenové certifikační autority I.CA využívající algoritmus RSA je 4095 bitů, mohutnost klíčů v jí vydávaných certifikátech podřízených certifikačních autorit je minimálně 2048 bitů, mohutnost klíčů OCSP respondérů je minimálně 2048 bitů. Mohutnost klíčů ostatních vydávaných certifikátů je vždy uvedena v konkrétní CP.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 i veřejných klíčů souvisejících se službami vytváření elektronického podpisu nebo elektronické pečetě na dálku splňují požadavky uvedené v právní úpravě pro služby vytvářející důvěru, resp. v ní odkazovaných technických standardech nebo normách. Tyto klíče jsou generovány a kontrolovány příslušným technickým a programovým vybavením.

Parametry algoritmů použitých při generování veřejných klíčů ostatních držitelů certifikátů musí tyto požadavky rovněž splňovat a jsou stejným způsobem kontrolovány.

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

Možnosti použití klíče jsou uvedeny v rozšíření certifikátu.

6.2 Ochrana soukromého klíče a technologie kryptografických modulů

Konkrétní postupy ochrany soukromého klíče uloženého v kryptografickém modulu pod kontrolu I.CA jsou popsány v interní dokumentaci:

- „Řízení fyzického přístupu do místností I.CA“,
- „HSM/Private Server“,
- „HSM/nShield XC“,
- „HSM PrivateServer – Postupy generováním klíčů a certifikátů CA a OCSP“,
- „HSM nShield – Postupy generování klíčů a certifikátů CA a OCSP“,
- „Správa TSS“,
- „Správa TSMC“.

6.2.1 Řízení a standardy kryptografických modulů

Generování párových dat certifikačních autorit, jejich OCSP respondérů a TSU systému TSA2 a uložení odpovídajících soukromých klíčů je prováděno v kryptografických modulech, které splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a jsou používány v souladu s příslušnou certifikací.

Generování párových dat vztahujících se ke službám vytváření elektronického podpisu nebo elektronické pečetě koncovými uživateli na dálku je prováděno v kryptografickém modulu typu QSCD, které je pod kontrolou I.CA a splňuje požadavky standardů ETSI a CEN.

Pracovníci podílející se na vydávání certifikátů využívají čipové karty splňující požadavky na QSCD.

Používání kryptografických modulů ostatními koncovými uživateli je plně v jejich kompetenci.

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

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

6.2.3 Úschova soukromého klíče

Není relevantní pro tento dokument, služba úschovy soukromého klíče není poskytována.

6.2.4 Zálohování soukromého klíče

Soukromé klíče certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 i soukromé klíče související se službami vytváření elektronického podpisu, resp. elektronické pečetě na dálku chráněné kryptografickými moduly jsou zálohovány v zašifrované podobě, která zajišťuje stejnou úroveň ochrany jako kryptografické zařízení.

Pro soukromé klíče pracovníků podílejících se na vydávání certifikátů není relevantní, jsou vygenerovány na čipových kartách v neexportovatelném tvaru.

Zálohování soukromých klíčů vztahujících se k certifikátům ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.5 Uchovávání soukromého klíče

Soukromé klíče certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 i soukromé klíče související se službami vytváření elektronického podpisu, resp. elektronické pečetě na dálku nejsou nikde uchovávány, po uplynutí doby platnosti jsou včetně záloh zničeny.

Doba uchování soukromých klíčů pracovníků podílejících se na vydávání certifikátů je dána kapacitou paměti čipové karty.

Uchovávání soukromých klíčů vztahujících se k certifikátům ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Soukromé klíče certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 i soukromé klíče související se službami vytváření elektronického podpisu, resp. elektronické pečetě na dálku jsou generovány v kryptografických modulech (jako neexportovatelné) a nelze je z kryptografického modulu (provozovaného v certifikovaném režimu) exportovat v žádném tvaru[1]. Import soukromých klíčů do kryptografického modulu není prováděn.

Pro transfer soukromých klíčů pracovníků podílejících se na vydávání certifikátů není relevantní, jsou vygenerovány v neexportovatelném tvaru.

Transfer soukromých klíčů vztahujících se k certifikátům ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit, jejich OCSP respondérů a TSU systému TSA2 jsou v otevřeném tvaru uloženy v kryptografických modulech splňujících požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN a jsou používány v souladu s příslušnou certifikací.

Jinak jsou bezpečně v souladu s příslušnou certifikací zašifrovány.

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

Soukromé klíče vztahující se ke službám vytváření elektronického podpisu nebo elektronické pečetě koncovými uživateli na dálku jsou uloženy v kryptografickém modulu typu QSCD, který je pod kontrolou I.CA a splňuje požadavky standardů ETSI a CEN.

Soukromé klíče pracovníků podílejících se na vydávání certifikátů jsou uloženy na čipových kartách splňujících požadavky na QSCD.

Případné uložení soukromých klíčů vztahujících se k certifikátům ostatních koncových uživatelů v kryptografických modulech je plně v kompetenci těchto koncových uživatelů.

6.2.8 Postup aktivace soukromého klíče

Aktivace soukromých klíčů (umožnění jejich použití) certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 i soukromých klíčů souvisejících se službami vytváření elektronických podpisů a elektronických pečetí na dálku v kryptografických modulech je prováděna:

- v případě aktivace čipovou kartou – vložením čipové karty a zadáním hesla,
- v případě aktivace pomocí softcard – předložením softcard a hesla.

Soukromé klíče pracovníků podílejících se na vydávání certifikátů jsou aktivovány vložením čipové karty do snímače a zadáním PIN.

Aktivace soukromých klíčů vztahujících se k certifikátům ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů a závisí na způsobu uložení těchto soukromých klíčů.

6.2.9 Postup deaktivace soukromého klíče

Deaktivace soukromých klíčů certifikačních autorit a jejich OCSP respondérů v kryptografických modulech je provedena vyjmutím čipové karty nebo ukončením příslušné aplikace.

Deaktivace původního soukromého klíče TSU systému TSA2 je provedena výběrem nového profilu.

Soukromý klíč vztahující se k službám vytváření elektronických podpisů a elektronických pečetí na dálku je deaktivován:

- okamžikem vydání následného certifikátu, nebo
- okamžikem ukončení příslušné smlouvy.

Soukromé klíče pracovníků podílejících se na vydávání certifikátů jsou deaktivovány vyjmutím čipové karty ze snímače.

Deaktivace soukromých klíčů vztahujících se k certifikátům ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů a závisí na způsobu uložení těchto soukromých klíčů.

6.2.10 Postup ničení soukromého klíče

Po uplynutí doby platnosti soukromého klíče příslušné certifikační autority a na základě následného potvrzení generálním ředitelem I.CA je tento soukromý klíč včetně jeho záloh zničen určeným postupem. O provedeném zničení je pořízen písemný záznam.

V případě soukromých klíčů OCSP respondérů je jejich ničení prováděno na příkaz osoby zastupující I.CA při vydání certifikátu OCSP respondéru. O provedeném zničení je pořízen písemný záznam.

Ničení soukromých klíčů TSU systému TSA2 spočívá v bezpečném rušení bezpečně a certifikovaně šifrované adresářové struktury a je prováděno, včetně ničení záloh, na příkaz generálního ředitele I.CA nebo jím pověřeného člena představenstva I.CA. O provedeném zničení je pořízen písemný záznam.

Ničení soukromých klíčů vztahujících se k službám vytváření elektronických podpisů a elektronických pečetí na dálku, včetně jejich záloh, je prováděno v případě:

- vydání následného certifikátu, nebo
- ukončení platnosti příslušné smlouvy, nebo
- zneplatnění nebo expirace certifikátů,

prostředky kryptografického modulu.

Ničení soukromých klíčů pracovníků podílejících se na vydávání certifikátů je plně v kompetenci těchto pracovníků, není předepsáno. Nutné je pouze v případě zaplnění paměti čipové karty.

Ničení soukromých klíčů vztahujících se k certifikátům ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.11 Hodnocení kryptografických modulů

Kryptografické moduly, sloužící ke generování párových dat a ukládání soukromých klíčů certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a jsou používány v souladu s jejich certifikací.

Kryptografické moduly sloužící ke generování párových dat a ukládání soukromých klíčů vztahujících se ke službám vytváření elektronického podpisu nebo elektronické pečetě koncovými uživateli na dálku splňují právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a jsou používány v souladu s jejich certifikací.

Čipové karty použité pro generování párových dat a uložení příslušných soukromých klíčů pracovníků podílejících se na vydávání certifikátů splňují požadavky na QSCD.

Případné použití kryptografických modulů ostatními koncovými uživateli včetně jejich hodnocení je plně v kompetenci těchto koncových uživatelů.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

Veškeré veřejné klíče jsou uchovávány ve formě certifikátů po celou dobu existence I.CA.

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

Maximální doba platnosti každého vydaného certifikátu je uvedena v těle tohoto certifikátu a je stejná jako doba použitelnosti příslušných párových dat.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 i soukromých klíčů vztahujících se k službám vytváření kvalifikovaných elektronických podpisů a pečetí na dálku (čipová karta nebo softcard) jsou vytvářena před generováním nebo v průběhu generování příslušných párových dat.

Konkrétní postupy jsou popsány v interní dokumentaci:

- „HSM/Private Server“,
- „HSM/nShield XC“,
- „Správa TSS“.

Aktivačními daty soukromých klíčů pracovníků podílejících se na vydávání certifikátů je PIN, který je plně po kontrolou těchto pracovníků.

Případné použití aktivační dat koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.4.2 Ochrana aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit, jejich OCSP respondérů, TSU systému TSA2 i soukromých klíčů vztahujících se k službám vytváření kvalifikovaných elektronických podpisů a pečetí na dálku (čipová karta nebo softcard) jsou chráněna nastaveným heslem.

Konkrétní postupy jsou popsány v interní dokumentaci:

- „HSM/Private Server“,
- „HSM/nShield XC“,
- „Správa TSS“.

Ochrana aktivačních dat soukromých klíčů pracovníků podílejících se na vydávání certifikátů je plně po kontrolou těchto pracovníků.

Případná ochrana aktivačních dat koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.4.3 Ostatní aspekty aktivačních dat

Není relevantní pro tento dokument.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti komponent použitých pro poskytování služeb vytvářejících důvěru, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů a jejich periodicity, je definována v případě kvalifikovaných certifikátů služeb právní úpravou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, v ostatních případech

relevantními technickými standardy a normami, tedy standardy ETSI a CEN, uvedenými v kapitole 6.5.2. Detailně je řešení popsáno v interní dokumentaci, zejména:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Příručka administrátora“,
- „Řízení fyzického přístupu do místností I.CA“,
- „HSM/Private Server“,
- „HSM/nShield XC“,
- „Správa TSS“,
- „Správa TSMC“.

6.5.2 Hodnocení počítačové bezpečnosti

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

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 403-1 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatele důvěryhodné služby – Část 1: Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodné služby.
- ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- ČSN ETSI EN 319 411-1 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 1: Obecné požadavky.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 2: Požadavky na poskytovatele důvěryhodných služeb vydávající kvalifikované certifikáty EU.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ČSN ETSI EN 319 412-1 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 1: Přehled a společné datové struktury.
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

- ČSN ETSI EN 319 412-2 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám.
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ČSN ETSI EN 319 412-3 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 3: Profil certifikátu pro certifikáty vydávané právnickým osobám.
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ČSN ETSI EN 319 412-4 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 4: Profil certifikátu pro certifikáty webových stránek.
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- ČSN ETSI EN 319 412-5 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 5: Prohlášení „QC Statements“.
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- ČSN EN 419 221-5 Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografický modul pro důvěryhodné služby.
- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services.
- ČSN EN ISO/IEC 15408-1 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model.
- ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model.
- ČSN EN ISO/IEC 15408-2 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty.
- ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components.
- ČSN EN ISO/IEC 15408-3 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk.
- ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components.
- ČSN EN 419 241-1 – Důvěryhodné systémy podporující podpisový server – Část 1: Obecné bezpečnostní požadavky systému.
- EN 419 241-1 – Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements.
- ČSN EN 419 241-2 – Důvěryhodné systémy podporující podpisový server – Část 2: Profil ochrany pro zařízení QSCD pro serverový podpis.
- EN 419 241-2 – Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing.
- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.

- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted TSL Server Certificates.
- CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates.
- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
- ETSI TS 119 495 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- ČSN EN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.
- ISO 3166-1 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.
- ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- EN 301 549 Accessibility requirements for ICT products and services.

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací:

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

6.6.2 Řízení správy bezpečnosti

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

Bezpečnost informací se v I.CA řídí těmito normami:

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

Problematika je popsána v interní dokumentaci:

- Kontrolní činnost, bezúhonnost a odbornost.

6.6.3 Řízení životního cyklu bezpečnosti

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

- vybudování – stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou, což je popsáno v interní dokumentaci:
  - „Celková bezpečnostní politika",
  - „Politika bezpečnosti informací – důvěryhodné systémy",
  - „Přístupy k posuzování a ošetřování rizik bezpečnosti informací – důvěryhodné systémy",
  - „Rozsah ISMS – důvěryhodné systémy",
  - „Analýza rizik – Důvěryhodné systémy – Závěrečná zpráva",
  - „Prohlášení o aplikovatelnosti – důvěryhodné systémy",
  - „Plán ošetření/ zvládání rizik – důvěryhodné systémy",
  - „Zbytková rizika – manažerské shrnutí – důvěryhodné systémy",
- implementace a provoz – účelné a systematické prosazení vybraných bezpečnostních opatření, což je popsáno v interní dokumentaci:
  - „Řízení fyzického přístupu do místností I.CA“,
  - „Požární bezpečnost“,
  - „HSM/Private Server“,
  - „HSM/nShield XC“,

- „Řízení bezpečnosti informací“,
- „Zálohování dat provozních systémů“,
- „Příručka administrátora“,
- „Firewall – provozní pracoviště“,
- „Kontrolní činnost, bezúhonnost a odbornost“,
- „Změnové řízení“,
- „Bezpečnostní incidenty“,
- „Aktivační obálky RemoteSign“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Firewall – provozní pracoviště“,
- „Kamerový systém – provozní pracoviště“,
- „Krizové scénáře“,
- projekty fyzické bezpečnosti provozních pracovišť,

a v další dokumentaci vedené na provozním pracovišti (viz „Příručka administrátora“),

- monitorování a přehodnocování – zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení společnosti k posouzení, což je popsáno v dokumentech:
  - zprávy z interních kontrol,
  - zprávy z externích kontrol a auditů,
- údržba a zlepšování – provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení společnosti.

6.7 Řízení bezpečnosti sítě

Síťová infrastruktura provozního pracoviště je chráněna komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System). Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci. Veškerá komunikace mezi RA a provozními pracovišti je vedena šifrovaně.

Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

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

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

Profily certifikátů, seznamu zneplatněných certifikátů a OCSP jsou vždy uvedeny v konkrétní CP. V následujících kapitolách jsou případně popsány pouze změny, jejichž provedení si I.CA v konkrétní certifikační politice vyhradila.

Přípustné typy a délka položek ve znacích pro pole subject a subjectAlternativeName, pokud jsou tyto v certifikátu obsaženy:

- v kvalifikovaných certifikátech pro elektronický podpis, pečeť a pro autentizaci internetových stránek, systémových certifikátech, nekvalifikovaných (komerčních) SSL certifikátech (OVCP a DVCP) jsou uvedeny v tabulce ve druhém sloupci tab. 4,
- v ostatních typech certifikátů, jsou uvedeny ve třetím sloupci tabulce tab. 4.

tab. 4 - Typy a délka položek pole subject a rozšíření subjectAlternativeName

Pole | rozšíření /položka	**Kvalifikované certifikáty pro elektronický podpis, pečeť a autentizaci internetových stránek, systémové certifikáty, nekvalifikované SSL certifikáty (OVCP, DVCP)**	**Ostatní typy certifikátů**
subject		
countryName	PrintableString (2)	PrintableString (2)
givenName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
surName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
pseudonym	UTF8String (1..128)	PrintableString, UTF8String (1..128)
serialNumber	PrintableString (1..64)	PrintableString (1..64)
commonName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
initials	UTF8String (1..64)	PrintableString, UTF8String (1..64)
emailAddress	IA5String (1..64)	IA5String (1..64)
name	UTF8String (1..128)	PrintableString, UTF8String (1..128)
generationQualifier	UTF8String (1..64)	PrintableString, UTF8String (1..64)

organizationName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
organizationalUnitName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
title	UTF8String (1..64)	PrintableString, UTF8String (1..64)
stateOrProvinceName	UTF8String (1..128)	PrintableString, UTF8String (1..128)
localityName	UTF8String (1..128)	PrintableString, UTF8String (1..128)
streetAddress	UTF8String (1..128)	PrintableString, UTF8String (1..128)
postalCode	UTF8String (1..40)	PrintableString, UTF8String (1..40)
organizationIdentifier	UTF8String (1..128)	PrintableString, UTF8String (1..128)
businessCategory	UnboundDirectoryString (1..64)	
jurisdictionCountryName	PrintableString (2)	
jurisdictionStateOrProvinceName	UTF8String (1..128)	
jurisdictionLocalityName	UTF8String (1..128)	
subjectAlternativeName		
otherName.IKMPSV (1.3.6.1.4.1.11801.2.1)	UTF8String (1..10)	nepovoleno
otherName.ICA_SN (1.3.6.1.4.1.23624.4.6)	UTF8String (1..8) kontrola: pouze čísla/znaky „0" až „9"	UTF8String (1..7) kontrola: pouze čísla/znaky „0" až „9"
otherName.universalPrincipalName (1.3.6.1.4.1.311.20.2.3, Microsoft UPN)	nepovoleno	UTF8String (1..255)
rfc822Name	IA5String (1..320) kontrola: správný formát e-mail adresy	IA5String (1..320) kontrola: správný formát e-mail adresy

dNSName	IA5String (1..255) kontrola: správný formát DNS jména	nepovoleno
description	UnboundDirectoryString (1..1024)	
DN Qualifier	PrintableString (1..64)	
DMDName	UnboundDirectoryString (1..64)	

7.1 Profil certifikátu

Viz kapitola 7.

7.1.1 Číslo verze

Viz kapitola 7.

7.1.2 Rozšíření certifikátu

Viz kapitola 7.

7.1.3 Objektové identifikátory algoritmů

Viz kapitola 7.

7.1.4 Tvary jmen

Viz kapitola 7.

7.1.5 Omezení jmen

Viz kapitola 7.

7.1.6 Objektový identifikátor certifikační politiky

Viz kapitola 7.

7.1.7 Použití rozšíření Policy Constraints

Viz kapitola 7.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz kapitola 7.

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Viz kapitola 7.

7.2 Profil seznamu zneplatněných certifikátů

Viz kapitola 7.

7.2.1 Číslo verze

Viz kapitola 7.

7.2.2 Rozšíření CRL a záznamů v CRL

Pro kvalifikované certifikáty obsahuje CRL rozšíření (expiredCertsOnCRL) udávající, že v něm jsou po definovanou dobu (viz 4.10.3) obsaženy i expirované certifikáty.

7.3 Profil OCSP

Profily OCSP žádosti i odpovědi jsou v souladu s RFC 6960 a RFC 5019.

OCSP odpovědi jsou typu BasicOCSPResponse a obsahují všechna povinná pole. V případě odvolaného certifikátu je uvedeno volitelné pole revocationReason. Pro certifikáty nevydané příslušnou CA je vrácena odpověď unAuthorized. Jako přenosový protokol je používáno pouze http.

tab. 5 - Profil OCSP žádosti

Položky žádosti	Poznámky
OCSPRequest ::= SEQUENCE {	
tbsRequest TBSRequest	
TBSRequest ::= SEQUENCE {	
version [0] EXPLICIT Version DEFAULT v1,	
requestorName [1] EXPLICIT GeneralName OPTIONAL	
requestList SEQUENCE OF Request,	OCSP respondér odpoví pouze na první požadavek ze seznamu v OCSP žádosti, ostatní ignoruje (RFC 5019)
Request ::= SEQUENCE {	
reqCert CertID,	povinná položka (pokud není obsažena, odpovědí bude *malformedRequest*)
CertID ::= SEQUENCE {	
hashAlgorithm AlgorithmIdentifier,	OID hashovacího algoritmu pro následující dvě položky – identifikace vydavatele dotazovaného certifikátu, specifikuje klient; OCSP respondér neomezuje (zpracuje žádosti se všemi hash algoritmy, které umí openssl)
issuerNameHash OCTET STRING,	hash pole vydavatele (Issuer) certifikátu, který je předmětem žádosti

issuerKeyHash OCTET STRING,	hash veřejného klíče vydavatele certifikátu, který je předmětem žádosti
serialNumber CertificateSerialNumber }	sériové číslo certifikátu, který je předmětem žádosti
singleRequestExtensions [0]EXPLICIT Extensions OPTIONAL	podle RFC 5019 nesmí být použito, pokud je přítomno v žádosti, je ignorováno
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension	
Extension ::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	podle RFC 6960 se zde se může vyskytovat: - *ServiceLocator*
}	
requestExtensions [2] EXPLICIT Extensions OPTIONAL	ignorováno
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension	ignorována všechna Extensions
Extension ::= SEQUENCE {	
extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	podle RFC 6960 se může vyskytovat: - *Nonce* – je ignorováno podle RFC 5019, - *AcceptableResponses,* - *PreferredSignatureAlgorithm*s
}	
optionalSignature [0] EXPLICIT Signature OPTIONAL	ignorováno (RFC 5019)
Signature ::= SEQUENCE {	
signatureAlgorithm AlgorithmIdentifier,	
signature BIT STRING	
certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL }	
}	

tab. 6 - Profil OCSP odpovědi

Položky odpovědi	Poznámky
OCSPResponse ::= SEQUENCE {	
responseStatus OCSPResponseStatus	
OCSPResponseStatus ::= ENUMERATED	*(0)* *successful* – úspěšná odpověď na OCSPRequest, *(1)* *malformedRequest* – vraceno v případě chyby syntaxe OCSPRequest, *(2)* *internalError* – interní chyba OCSP respondéru, *(3)* *tryLater* – nepoužíváno, *(5)* *sigRequired* – nikdy nevraceno, podpis žádosti není požadován, *(6)* *unauthorized* – v případě, že OCSP respondér nepozná vydavatele = cizí certifikát (klient není oprávněn k provedení dotazu na tento server – RFC 6960, nebo server není schopen odpovědět autoritativně,

	např. nemá k dispozici autoritativní informaci o odvolání certifikátu – RFC 5019)
responseBytes [0] EXPLICIT ResponseBytes OPTIONAL }	pouze v případě OCSPResponseStatus=*successful*
ResponseBytes ::= SEQUENCE {	
responseType OBJECT IDENTIFIER	vždy „*Basic OCSP Response"*
response OCTET STRING	
BasicOCSPResponse ::= SEQUENCE {	
tbsResponseData ResponseData,	
ResponseData ::= SEQUENCE {	
version [0] EXPLICIT Version DEFAULT v1,	v1
responderID ResponderID,	
ResponderID ::= CHOICE { byName [1] Name, byKey [2] KeyHash }	vraceno byName=DN vydavatele
producedAt GeneralizedTime,	čas, kdy OCSP respondér podepsal odpověď
responses SEQUENCE OF SingleResponse,	vracena pouze jediná odpověď na první certifikát v seznamu v žádosti
SingleResponse ::= SEQUENCE {	
certID CertID,	

CertID ::= SEQUENCE {
hashAlgorithm AlgorithmIdentifier,
issuerNameHash OCTET STRING,
issuerKeyHash OCTET STRING,
serialNumber CertificateSerialNumber
}
	totožný obsah s atributem CertID uvedeným v žádosti

certStatus CertStatus,	stav odvolání platnosti certifikátu, jedna z vyjmenovaných možností níže
CertStatus ::= CHOICE {	
good [0] IMPLICIT NULL,	certifikát nebyl odvolán (v intervalu platnosti), nebo čas vytvoření OCSP odpovědi byl mimo interval platnosti certifikátu
revoked [1] IMPLICIT RevokedInfo,	certifikát byl odvolán (v intervalu platnosti)
RevokedInfo ::= SEQUENCE {	
revocationTime GeneralizedTime	čas zneplatnění certifikátu
revocationReason [0] EXPLICIT CRLReason OPTIONAL }	v odpovědi uváděn důvod
CRLReason ::= ENUMERATED	může obsahovat: *(0) unspecified,* *(1) keyCompromise,* *(2) cACompromise,* *(3) affiliationChanged,* *(4) superseded,* *(5) cessationOfOperation,* *(8) removeFromCRL,* *(9) privilegeWithdrawn,*

	(10) aACompromise I.CA nepřipouští důvod odvolání *(6) certificateHold* = dočasné pozastavení, hodnota *(7)* není použita
unknown [2] IMPLICIT UnknownInfo UnknownInfo ::= NULL	I.CA toto nepoužívá (používáno OCSPResponseStatus= unauthorized podle RFC 5019) (poskytovatel není schopen odpovědět, o stavu certifikátu „nic neví", obvykle proto, že se jedná o cizí certifikát)
}	
thisUpdate GeneralizedTime,	čas, ke kterému je znám stav certifikátu
nextUpdate [1] EXPLICIT GeneralizedTime OPTIONAL,	vždy uvedeno (povinné dle RFC 5019); čas, kdy končí platnost této odpovědi a do kdy bude dostupná nová odpověď
singleExtensions [1] EXPLICIT Extensions	
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension Extension ::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING}	odpověď může obsahovat rozšíření: - ***id-commonpki-at-certHash*** – vloženo minimálně u certifikátů SK (tzv. pozitivní prohlášení); pro hash z dotazovaného certifikátu se použije algoritmus podle podpisu certifikátu respondéru (sha256), - ***id-pkix-ocsp-archive-cutoff*** – pro kvalifikované certifikáty udává, po jakou dobu po expiraci certifikátu lze spoléhat na stav certifikátu uvedený v OCSP odpovědi
}	
responseExtensions [1] EXPLICIT Extensions OPTIONAL }	odpověď neobsahuje pole responseExtensions
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension Extension ::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	podle RFC 6960 zde může být: - id-pkix-ocsp-nonce, - id-pkix-ocsp-extended-revoke
}	
signatureAlgorithm AlgorithmIdentifier,	sha256WithRSAEncryption
signature BIT STRING,	
certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL	uváděn: - certifikát vydávající CA, - certifikát OCSP respondéru
}	
}	
}	
}	

7.3.1 Číslo verze

Viz kapitola 7.3.

7.3.2 Rozšíření OCSP

Viz tabulky v kapitola 7.3.

OCSP odpověď vracející stav Certifikátu „good" může obsahovat pozitivní prohlášení ve formě položky CertHash rozšíření singleExtensions.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

Informace o hodnocení jsou uvedeny v konkrétních certifikačních politikách.

8.1 Periodicita nebo okolnosti hodnocení

Viz kapitola 8.

8.2 Identita a kvalifikace hodnotitele

Viz kapitola 8.

8.3 Vztah hodnotitele k hodnocenému subjektu

Viz kapitola 8.

8.4 Hodnocené oblasti

Viz kapitola 8.

8.5 Postup v případě zjištění nedostatků

Viz kapitola 8.

8.6 Sdělování výsledků hodnocení

Viz kapitola 8.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za vydání certifikátů pro koncové uživatele jsou uvedeny v aktuálním ceníku služeb, který je k dispozici na internetové informační adrese I.CA nebo v případě uzavřeného smluvního vztahu mezi Organizací a I.CA v této smlouvě. Poplatky za certifikáty, jejichž držitelem je I.CA, nejsou účtovány.

Služba obnovení certifikátu není poskytována.

9.1.2 Poplatky za přístup k certifikátu

Přístup elektronickou cestou k veřejným certifikátům vydaným podle konkrétních CP – viz kapitola 2.2 – I.CA nezpoplatňuje.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) a o stavech certifikátů (OCSP) vydaných podle certifikačních politik – viz kapitola 2.2 – I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Není relevantní pro tento dokument.

9.1.5 Postup při refundování

Není relevantní pro tento dokument.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

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

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

9.2.2 Další aktiva

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

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

9.3 Důvěrnost obchodních informací

9.3.1 Rozsah důvěrných informací

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

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

9.3.2 Informace mimo rámec důvěrných informací

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

9.3.3 Odpovědnost za ochranu důvěrných informací

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

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

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

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

9.4.2 Informace považované za osobní údaje

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

Zaměstnanci I.CA, případně subjekty definované platnou právní úpravou přicházející do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech

a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního, nebo jiného obdobného poměru, nebo po provedení příslušných prací.

9.4.3 Informace nepovažované za osobní údaje

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

9.4.4 Odpovědnost za ochranu osobních údajů

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

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

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

9.4.6 Poskytování osobních údajů pro soudní či správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče certifikačních autorit pouze pro vydávání certifikátů koncovým uživatelům (vyjma kořenové certifikační autority I.CA), vydávání seznamů jimi vydaných zneplatněných certifikátů a k vydávání certifikátů jejich OCSP respondérů,
- použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,

- certifikáty vydávané koncovým uživatelům splňují v případě certifikátů kvalifikovaných náležitosti požadované právní úpravou pro služby vytvářející důvěru a příslušnými technickými standardy a normami, v případě ostatních certifikátů náležitosti požadované příslušnými technickými standardy a normami,
- zneplatní vydané certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v konkrétní CP příslušné této CPS.

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

- držitel certifikátu neporušil povinnosti plynoucí mu ze smlouvy o poskytování Služeb a konkrétní CP,
- spoléhající se strana neporušila povinnosti konkrétní CP.

Držitel certifikátu vydaného podle konkrétní CP uplatňuje záruku vždy u RA, která zpracovala jeho žádost o vydání certifikátu.

I.CA vyjadřuje a poskytuje držitelům certifikátů a veškerým spoléhajícím se stranám záruky, že při vydávání certifikátů a v průběhu doby jejich platnosti bude při jejich správě vyhovovat konkrétní CP.

Záruky zahrnují:

- kontrolu práva žádat o certifikát,
- ověření informací uváděných v žádosti o vydání certifikátu, včetně kontroly naplnění položek, obsažených v žádosti o certifikát (formát PKCS#10) a identity,
- že smlouva o vydání certifikátu odpovídá platné právní úpravě,
- že v režimu 24x7 je udržováno úložiště informací o stavu certifikátů,
- že certifikát může být zneplatněn z důvodů uvedených v právní úpravě pro služby vytvářející důvěru a konkrétní CP.

9.6.2 Zastupování a záruky RA

Určená RA:

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost, pokud se nepodařilo ověřit některou z položek žádosti s výjimkou položek neověřovaných, nebo držitel certifikátu odmítá sdělit potřebné údaje, nebo není oprávněn k podání žádosti o certifikát,
- v případě osobního podání žádosti o zneplatnění certifikátu odpovídá za včasné předání této žádostí k vyřízení na pracoviště CA,
- odpovídá za vyřizování připomínek a stížností.

9.6.3 Zastupování a záruky držitele certifikátu

Záruky držitele certifikátu jsou uvedeny ve smlouvě mezi I.CA a držitelem certifikátu.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle CP, podle které byl certifikát vydán.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

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

9.9 Záruky a odškodnění

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení platných právních předpisů týkajících se vztahů mezi poskytovatelem a spotřebitelem a dále takové záruky, které byly sjednány mezi společností První certifikační autorita, a.s., a žadatelem o Služby. Smlouva nesmí být v rozporu s platnou právní úpravou a musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak platnou právní úpravou, včetně právní úpravy pro služby vytvářející důvěru v případě certifikátů kvalifikovaných, tak příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služeb,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, se kterými má platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo odpovědnosti, s výjimkou případů, kdy poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele.

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

- za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování Služeb držitelem certifikátu, zejména za využívání v rozporu s podmínkami uvedenými v konkrétní CP, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení,
- za škodu vyplývající z použití certifikátu v období po podání žádosti o jeho zneplatnění, pokud společnost První certifikační autorita, a.s., dodrží definovanou lhůtu pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL nebo OCSP).

Reklamaci je možné podat těmito způsoby:

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

- osobně v sídle společnosti.

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

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

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

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

Nový certifikát bude příslušnému držiteli certifikátu poskytnut zdarma v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority,
- na základě rozhodnutí členů vedení I.CA s přihlédnutím ke konkrétním okolnostem,
- v případě, že CA při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát s duplicitním veřejným klíčem.

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

9.10 Doba platnosti, ukončení platnosti

Doba platnosti a podmínky ukončení platnosti certifikačních politik jsou vždy uvedeny v konkrétní CP.

9.10.1 Doba platnosti

Certifikační politiky – viz kapitole 9.10.

Tato CPS nabývá platnosti dnem uvedeným v kapitole 10 a platí do doby jejího nahrazení novou verzí, nebo minimálně po dobu platnosti posledního certifikátu vydané podle některé z certifikačních politik – viz kapitola 1.2.

9.10.2 Ukončení platnosti

Certifikační politiky – viz kapitola 9.10.

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CPS, a to v případě jejího nahrazení novou verzí, nebo ukončení činnosti poskytovatele certifikačních služeb, je generální ředitel společnosti První certifikační autorita, a.s.

9.10.3 Důsledky ukončení a přetrvání závazků

Certifikační politiky – viz kapitola 9.10.

Tato CPS platí minimálně po dobu platnosti posledního certifikátu vydaného podle některé z certifikačních politik – viz kapitola 1.2.

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

Pokud jsou zúčastněné subjekty organizačnímu částmi I.CA, řídí se komunikace mezi nimi interními pravidly I.CA.

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

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

9.12 Novelizace

Postup v případě certifikačních politik je vždy popsán v konkrétní certifikační politice.

9.12.1 Postup při novelizaci

Certifikační politiky – viz kapitola 9.12.

V případě této CPS – postup je realizován řízeným procesem popsaným v interní dokumentaci.

9.12.2 Postup a periodicita oznamování

Certifikační politiky – viz kapitola 9.12.

V případě této CPS – postup je realizován řízeným procesem popsaným v interní dokumentaci.

9.12.3 Okolnosti, při kterých musí být změněn OID

Certifikační politiky – viz kapitola 9.12.

V případě této CPS – OID není přiřazován.

9.13 Ustanovení o řešení sporů

Pokud jsou všechny strany sporu organizačnímu částmi I.CA, řídí se řešení sporů interními pravidly I.CA.

V ostatních případech platí, že pokud držitel certifikátu nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

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

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

9.14 Rozhodné právo

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

9.15 Shoda s platnými právními předpisy

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

9.16 Různá ustanovení

Další ustanovení jsou vždy popsána v konkrétní certifikační politice.

9.16.1 Rámcová dohoda

Viz kapitola 9.16.

9.16.2 Postoupení práv

Viz kapitola 9.16.

9.16.3 Oddělitelnost ustanovení

Viz kapitola 9.16.

9.16.4 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv)

Viz kapitola 9.16.

9.16.5 Vyšší moc

Viz kapitola 9.16.

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

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