První certifikační autorita, a.s.



Certifikační politika

vydávání komerčních technologických certifikátů

(algoritmus RSA)

Certifikační politika vydávání komerčních technologických certifikátů (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 1.145

Copyright © První certifikační autorita, a.s.

OBSAH

1 Úvod 11
1.1 Přehled 11
1.2 Název a identifikace dokumentu 12
1.3 Participující subjekty 12
1.3.1 Certifikační autority (dále „CA") 12
1.3.2 Registrační autority (dále „RA") 12
1.3.3 Držitelé certifikátů 13
1.3.4 Spoléhající se strany 13
1.3.5 Jiné participující subjekty 13
1.4 Použití certifikátu 13
1.4.1 Přípustné použití certifikátu 13
1.4.2 Zakázané použití certifikátu 13
1.5 Správa politiky 13
1.5.1 Organizace spravující dokument 13
1.5.2 Kontaktní osoba 13
1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou 14
1.5.4 Postupy při schvalování CPS 14
1.6 Pojmy a zkratky 14
2 Odpovědnost za zveřejňování a ZA úložiště 21
2.1 Úložiště 21
2.2 Zveřejňování certifikačních informací 21
2.3 Čas nebo četnost zveřejňování 22
2.4 Řízení přístupu k jednotlivým typům úložišť 22
3 Identifikace a autentizace 23
3.1 Pojmenování 23
3.1.1 Typy jmen 23
3.1.2 Požadavek na významovost jmen 23
3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu 23
3.1.4 Pravidla pro interpretaci různých forem jmen 23
3.1.5 Jedinečnost jmen 23
3.1.6 Uznávání, ověřování a poslání obchodních značek 23
3.2 Počáteční ověření identity 23
3.2.1 Ověřování vlastnictví soukromého klíče 23
3.2.2 Ověřování identity organizace 24

3.2.3 Ověřování identity fyzické osoby 24
3.2.4 Neověřované informace vztahující se k držiteli certifikátu 24
3.2.5 Ověřování kompetencí 24
3.2.6 Kritéria pro interoperabilitu 25
3.2.7 Ověřování e-mailové adresy 25
3.3 Identifikace a autentizace při požadavku na výměnu klíče 25
3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče 25
3.3.2 Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu 26
3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu 26
4 Požadavky na životní cyklus certifikátu 27
4.1 Žádost o vydání certifikátu 27
4.1.1 Kdo může požádat o vydání certifikátu 27
4.1.2 Registrační proces a odpovědnosti 27
4.2 Zpracování žádosti o certifikát 28
4.2.1 Provádění identifikace a autentizace 28
4.2.2 Schválení nebo zamítnutí žádosti o certifikát 28
4.2.3 Doba zpracování žádosti o certifikát 28
4.3 Vydání certifikátu 28
4.3.1 Úkony CA v průběhu vydávání certifikátu 28
4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou 29
4.4 Převzetí vydaného certifikátu 29
4.4.1 Úkony spojené s převzetím certifikátu 29
4.4.2 Zveřejňování certifikátů certifikační autoritou 29
4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 29
4.5 Použití párových dat a certifikátu 29
4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu 29
4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou 30
4.6 Obnovení certifikátu 30
4.6.1 Podmínky pro obnovení certifikátu 30
4.6.2 Kdo může žádat o obnovení 30
4.6.3 Zpracování požadavku na obnovení certifikátu 30
4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu 30
4.6.5 Úkony spojené s převzetím obnoveného certifikátu 31
4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou 31

4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 31
4.7 Výměna veřejného klíče v certifikátu 31
4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu 31
4.7.2 Kdo může žádat o výměnu veřejného klíče v certifikátu....31
4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu...31
4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu....31
4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem....32
4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou 32
4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 32
4.8 Změna údajů v certifikátu 32
4.8.1 Podmínky pro změnu údajů v certifikátu 32
4.8.2 Kdo může požádat o změnu údajů v certifikátu....32
4.8.3 Zpracování požadavku na změnu údajů v certifikátu 32
4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu 32
4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji 33
4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou 33
4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 33
4.9 Zneplatnění a pozastavení platnosti certifikátu 33
4.9.1 Podmínky pro zneplatnění 33
4.9.2 Kdo může požádat o zneplatnění 35
4.9.3 Postup při žádosti o zneplatnění 35
4.9.4 Prodleva při požadavku na zneplatnění certifikátu 37
4.9.5 Doba zpracování žádosti o zneplatnění 37
4.9.6 Povinnosti spoléhajících se stran při kontrole zneplatnění 37
4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů 37
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 možné způsoby oznamování zneplatnění 38
4.9.12 Zvláštní postupy při kompromitaci klíče 38
4.9.13 Podmínky pro pozastavení platnosti certifikátu 38

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 ověřování stavu certifikátu....39
4.10.1 Funkční charakteristiky....39
4.10.2 Dostupnost služeb....39
4.10.3 Další charakteristiky služeb stavu certifikátu....39
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....41
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....42
5.2.3 Identifikace a autentizace pro každou roli....43
5.2.4 Role vyžadující rozdělení povinností....43
5.3 Personální postupy....43
5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost....43
5.3.2 Posouzení spolehlivosti osob....43
5.3.3 Požadavky na školení....44
5.3.4 Požadavky a periodicita doškolování....44
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi....44
5.3.6 Postihy za neoprávněné činnosti....44
5.3.7 Požadavky na nezávislé dodavatele....44
5.3.8 Dokumentace poskytovaná zaměstnancům....45

5.4 Postupy zpracování auditních záznamů 45
5.4.1 Typy zaznamenávaných událostí 45
5.4.2 Periodicita zpracování záznamů 45
5.4.3 Doba uchování auditních záznamů 45
5.4.4 Ochrana auditních záznamů 46
5.4.5 Postupy pro zálohování auditních záznamů 46
5.4.6 Systém shromažďování auditních záznamů (interní nebo externí) 46
5.4.7 Postup při oznamování události subjektu, který ji způsobil 46
5.4.8 Hodnocení zranitelnosti 46
5.5 Uchovávání záznamů 46
5.5.1 Typy uchovávaných záznamů 46
5.5.2 Doba uchování záznamů 47
5.5.3 Ochrana úložiště záznamů 47
5.5.4 Postupy při zálohování záznamů 47
5.5.5 Požadavky na používání časových razítek při uchovávání záznamů 47
5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí) 47
5.5.7 Postupy pro získání a ověření uchovávaných informací 47
5.6 Výměna klíče 47
5.7 Obnova po havárii nebo kompromitaci 48
5.7.1 Postup ošetření incidentu nebo kompromitace 48
5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat 48
5.7.3 Postup při kompromitaci soukromého klíče 48
5.7.4 Schopnost obnovit činnost po havárii 48
5.8 Ukončení činnosti CA nebo RA 48
6 Řízení technické bezpečnosti 50
6.1 Generování a instalace párových dat 50
6.1.1 Generování párových dat 50
6.1.2 Předávání soukromého klíče jeho držiteli 50
6.1.3 Předávání veřejného klíče vydavateli certifikátu 50
6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám 50
6.1.5 Délky klíčů 50
6.1.6 Parametry veřejného klíče a kontrola jeho kvality 51
6.1.7 Účely použití klíče (dle rozšíření key usage X.509 v3) 51
6.2 Ochrana soukromého klíče a technologie kryptografických modulů 51

6.2.1 Řízení a standardy kryptografických modulů 51
6.2.2 Soukromý klíč pod kontrolou více osob (n z m) 51
6.2.3 Úschova soukromého klíče....51
6.2.4 Zálohování soukromého klíče....51
6.2.5 Uchovávání soukromého klíče....52
6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu ..52
6.2.7 Uložení soukromého klíče v kryptografickém modulu 52
6.2.8 Postup aktivace soukromého klíče 52
6.2.9 Postup deaktivace soukromého klíče....53
6.2.10 Postup ničení soukromého klíče 53
6.2.11 Hodnocení kryptografických modulů....53
6.3 Další aspekty správy párových dat....53
6.3.1 Uchovávání veřejných klíčů....53
6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat 53
6.4 Aktivační data 54
6.4.1 Generování a instalace aktivačních dat 54
6.4.2 Ochrana aktivačních dat....54
6.4.3 Ostatní aspekty aktivačních dat....54
6.5 Řízení počítačové bezpečnosti....54
6.5.1 Specifické technické požadavky na počítačovou bezpečnost 54
6.5.2 Hodnocení počítačové bezpečnosti 54
6.6 Technické řízení životního cyklu....57
6.6.1 Řízení vývoje systému....57
6.6.2 Řízení správy bezpečnosti....57
6.6.3 Řízení životního cyklu bezpečnosti....57
6.7 Řízení bezpečnosti sítě....57
6.8 Označování časovými razítky....58
7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP....59
7.1 Profil certifikátu....59
7.1.1 Číslo verze 61
7.1.2 Rozšíření certifikátu....61
7.1.3 Objektové identifikátory algoritmů....63
7.1.4 Tvary jmen....63
7.1.5 Omezení jmen....63
7.1.6 Objektový identifikátor certifikační politiky....63
7.1.7 Použití rozšíření Policy Constraints 63

7.1.8 Syntaxe a sémantika kvalifikátorů politiky 64
7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies 64
7.2 Profil seznamu zneplatněných certifikátů 64
7.2.1 Číslo verze 64
7.2.2 Rozšíření CRL a záznamů v CRL 64
7.3 Profil OCSP 65
7.3.1 Číslo verze 65
7.3.2 Rozšíření OCSP 65
8 Hodnocení shody a jiná hodnocení 66
8.1 Periodicita nebo okolnosti hodnocení 66
8.2 Identita a kvalifikace hodnotitele 66
8.3 Vztah hodnotitele k hodnocenému subjektu 66
8.4 Hodnocené oblasti 66
8.5 Postup v případě zjištění nedostatků 66
8.6 Sdělování výsledků hodnocení 66
8.7 Interní audity 67
8.8 Kontrola nezávislých dodavatelů 67
9 Ostatní obchodní a právní záležitosti 68
9.1 Poplatky 68
9.1.1 Poplatky za vydání nebo obnovení certifikátu 68
9.1.2 Poplatky za přístup k certifikátu 68
9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu 68
9.1.4 Poplatky za další služby 68
9.1.5 Postup při refundování 68
9.2 Finanční odpovědnost 68
9.2.1 Krytí pojištěním 68
9.2.2 Další aktiva 68
9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele 69
9.3 Důvěrnost obchodních informací 69
9.3.1 Rozsah důvěrných informací 69
9.3.2 Informace mimo rámec důvěrných informací 69
9.3.3 Odpovědnost za ochranu důvěrných informací 69
9.4 Ochrana osobních údajů 69
9.4.1 Politika ochrany osobních údajů 69
9.4.2 Informace považované za osobní údaje 69
9.4.3 Informace nepovažované za osobní údaje 70

9.4.4 Odpovědnost za ochranu osobních údajů....70
9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním....70
9.4.6 Poskytování osobních údajů pro soudní či správní účely....70
9.4.7 Jiné okolnosti zpřístupňování osobních údajů....70
9.5 Práva duševního vlastnictví....70
9.6 Zastupování a záruky....70
9.6.1 Zastupování a záruky CA....70
9.6.2 Zastupování a záruky RA....71
9.6.3 Zastupování a záruky držitele certifikátu....71
9.6.4 Zastupování a záruky spoléhajících se stran....71
9.6.5 Zastupování a záruky ostatních zúčastněných subjektů....71
9.7 Zřeknutí se záruk....71
9.8 Omezení odpovědnosti....72
9.9 Záruky a odškodnění....72
9.10 Doba platnosti, ukončení platnosti....73
9.10.1 Doba platnosti....73
9.10.2 Ukončení platnosti....73
9.10.3 Důsledky ukončení a přetrvání závazků....73
9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty....73
9.12 Novelizace....73
9.12.1 Postup při novelizaci....73
9.12.2 Postup a periodicita oznamování....74
9.12.3 Okolnosti, při kterých musí být změněn OID....74
9.13 Ustanovení o řešení sporů....74
9.14 Rozhodné právo....74
9.15 Shoda s platnými právními předpisy....74
9.16 Různá ustanovení....74
9.16.1 Rámcová dohoda....74
9.16.2 Postoupení práv....74
9.16.3 Oddělitelnost ustanovení....74
9.16.4 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv)....75
9.16.5 Vyšší moc....75
9.17 Další ustanovení....75
10 Závěrečná ustanovení....76

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	29.03.2016	Ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.10	03.03.2017	Ředitel společnosti První certifikační autorita, a.s.	Úprava dle požadavků programu Microsoft Trusted Root Certificate Program.
1.11	30.04.2019	Ředitel společnosti První certifikační autorita, a.s.	Upřesnění textů v naplnění položek pole subject. Pravidelná revize textu, oprava formálních chyb.
1.12	10.12.2019	Generální ředitel společnosti První certifikační autorita, a.s.	Podpora algoritmu RSA-PSS (pkcs#1 2v1) při tvorbě zaručené elektronické pečetě vydávaného certifikátu.
1.13	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.
1.14	11.06.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace hodnocení kryptografických modulů. Položka extendedKeyUsage – upřesněn obsah. Revize textu.
1.141	26.04.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Revize textu.
1.142	02.07.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace seznamu odkazovaných standardů.
1.143	26.08.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace seznamu odkazovaných standardů, zohlednění požadavků ETSI TS 119 411-6.
1.144	16.08.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Zpřesnění profilu certifikátu. Aktualizace v souvislosti s S/MIME BR.
1.145	16.08.2026	Generální ředitel společnosti První certifikační autorita, a.s.	Upřesnění činností CA při vydávání certifikátu. Přihlášení se k požadavkům politiky CCADB. Revize textu.

1 ÚVOD

Tento dokument stanoví zásady, které První certifikační autorita, a.s., (dále též I.CA), kvalifikovaný poskytovatel služeb vytvářejících důvěru, uplatňuje při vydávání komerčních technologických certifikátů (dále též Služba, Certifikát) právnickým osobám nebo organizačním složkám státu (dále též Organizace). Pro Službu poskytovanou podle této certifikační politiky (dále též CP) je využíván algoritmus RSA.

Certifikáty vydávané podle této CP jsou určené pro ověřování elektronických podpisů vytvářených technologickými komponentami provozovanými Organizacemi a pro autentizaci klienta a šifrování.

Právní požadavky na Službu jsou definovány:

- nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění,
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- 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.

Služba je poskytována 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.

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 byla 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 politika vydávání komerčních technologických certifikátů (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). Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem, obecně popisuje subjekty participující na poskytování této Služby 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 jí vydávaných Certifikátů, tzn. žádost o vydání a vlastní vydání Certifikátu, žádost o zneplatnění a vlastní zneplatnění Certifikátu, služby související s ověřováním stavu Certifikátu, ukončení poskytování Služby 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 definuje profil vydávaných Certifikátů a seznamů zneplatněných certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytované Služby.
- Kapitola 9 zahrnuje problematiku obchodní a právní.

Bližší podrobnosti o naplnění polí a rozšíření Certifikátů vydávaných podle této CP a o jejich správě mohou být uvedeny v odpovídající certifikační prováděcí směrnici (dále CPS).

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu:	Certifikační politika vydávání komerčních technologických certifikátů (algoritmus RSA), verze 1.145
OID politiky:	1.3.6.1.4.1.23624.10.1.71.1.1

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA”)

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, certifikát podřízené certifikační autoritě (dále též Autorita), provozované I.CA. Tato Autorita vydává Certifikáty dle této CP a certifikáty pro vlastní OCSP respondér.

1.3.2 Registrační autority (dále „RA”)

Poskytování služeb společnosti První certifikační autorita, a.s., se realizuje prostřednictvím registračních autorit (stacionárních nebo mobilních), které jsou buď veřejné (poskytují služby veřejnosti), nebo klientské (poskytují služby svým zákazníkům). Tyto registrační autority:

- Přijímají žádosti o služby uvedené v této CP, zejména přijímají žádosti o vydání Certifikátu, zprostředkovávají předání Certifikátů a seznamů zneplatněných certifikátů, poskytují potřebné informace, přijímají reklamace atd.
- Jsou oprávněny z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti.
- Jsou zmocněny jménem I.CA uzavírat smlouvy o poskytování Služby.
- Zajišťují zpoplatňování služeb I.CA poskytovaných prostřednictvím RA, pokud není stanoveno smlouvou jinak.

- V případě smluvní RA plní tato jménem I.CA obdobné funkce jako vlastní RA na základě písemné smlouvy mezi I.CA a provozovatelem smluvní RA.

1.3.3 Držitelé certifikátů

Držitelem vydávaného Certifikátu je Organizace, která požádala o vydání Certifikátu pro sebe a identifikovaná v Certifikátu jako držitel soukromého klíče spojeného s veřejným klíčem, uvedeným v tomto Certifikátu.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na Certifikáty vydávané podle této CP.

1.3.5 Jiné participující subjekty

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

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP lze využívat v procesech ověřování elektronického podpisu, šifrování nebo pro autentizaci klienta.

1.4.2 Zakázané použití certifikátu

Certifikáty vydávané podle této CP nesmějí být používány v rozporu s přípustným použitím popsaným v kapitole 1.4.1 a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující dokument

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

1.5.2 Kontaktní osoba

Kontaktní osobou společnosti První certifikační autorita, a.s., v souvislosti s touto CP, resp. s odpovídající CPS, je výkonný ředitel I.CA. Platí kontaktní údaje uvedené v kapitole 2.2.

Mailová adresa certproblem@ica.cz je sledována nepřetržitě v režimu 24x7 a slouží pro hlášení problémů s Certifikátem, tedy např. podezření na kompromitaci klíče nebo na zneužití Certifikátu.

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 CPS s touto 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
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
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)
klientský portál	webová platforma umožňující určeným zástupcům Organizací, které mají s I.CA uzavřenou smlouvu, spravovat informace o vydaných certifikátech a provádět další definované akce
kořenová CA	certifikační autorita vydávající certifikáty podřízeným certifikačním autoritám
kvalifikovaný certifikát pro elektronický podpis nebo pro elektronickou pečeť	certifikát definovaný právní úpravou pro služby vytvářející důvěru

nebo pro autentizaci webových stránek	
kvalifikovaný prostředek pro vytváření elektronických podpisů, resp. pečetí	prostředek pro vytváření elektronických podpisů, resp. pečetí, který splňuje požadavky stanovené v příloze II eIDAS
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
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.)
písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
podřízená CA	CA vydávající certifikáty koncovým uživatelům
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
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

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
CCADB	Common CA Database, úložiště informací o certifikačních autoritách (CA), jejichž kořenové nebo podřízené certifikáty jsou zahrnuty v produktech a službách několika provozovatelů kořenových úložišť
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, ve formátu PEM může být i žádost o certifikát (DER je binární verze PEM)
DV	Domain Validation, typ SSL 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
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.
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
MTRP	Microsoft Trusted Root Program
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
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, podepsané 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
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.

2.2 Zveřejňování certifikačních informací

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

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

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

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.

Certifikační autorita vydávající Certifikáty vyhovuje požadavkům současné verze dokumentu „CA/Browser Forum – Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates", který je vystaven na adrese http://www.cabforum.org. V případě jakéhokoliv nesouladu mezi touto CP a zmíněným dokumentem má zmíněný dokument přednost.

Certifikační autorita vydávající Certifikáty vyhovuje požadavkům současné verze politiky CCADB uvedené na adrese https://www.ccadb.org/policy.

2.3 Čas nebo četnost zveřejňování

I.CA zveřejňuje informace s následující periodicitou:

- certifikační politika – po schválení a vydání nové verze, aktualizace v závislosti na změnách normativních požadavků na vydávané Certifikáty, revize je prováděna nejméně jednou ročně,
- certifikační prováděcí směrnice – neprodleně,
- seznam vydaných certifikátů – aktualizace při každém vydání nového certifikátu určeného ke zveřejnění,
- seznam zneplatněných certifikátů (CRL) - viz kapitola 4.9.7,
- informace o zneplatnění certifikátu certifikační autority, s uvedením důvodu zneplatnění – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb.

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, nebo subjektům definovaným příslušnou právní úpravou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

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 kapitole 7.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Certifikáty vydávané podle této CP nepodporují anonymitu ani používání pseudonymu.

3.1.4 Pravidla pro interpretaci různých forem jmen

Údaje se do pole subject, resp. rozšíření subjectAlternativeName ve vydávaných Certifikátech přenášejí ve tvaru, ve kterém jsou uvedeny v předložené žádosti.

3.1.5 Jedinečnost jmen

Autorita zaručuje jedinečnost pole subject v Certifikátu příslušného držitele soukromého klíče, resp. držitele tohoto Certifikátu.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Certifikáty vydávané podle této CP mohou obsahovat pouze obchodní značky, jejichž vlastnictví nebo pronájem byly doloženy. Veškeré důsledky plynoucí z neoprávněného užívání ochranné známky nese držitel Certifikátu.

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 opatřena elektronickou pečetí a držitel soukromého klíče tak prokazuje, že v době tvorby elektronické pečetě soukromý klíč vlastnil.

3.2.2 Ověřování identity organizace

Pro ověření Organizace musí být předložen:

- originál nebo úředně ověřená kopie výpisu z obchodního nebo jiného právním předpisem určeného rejstříku/registru, živnostenského listu, zřizovací listiny, resp. jiného dokladu stejné právní váhy, nebo
- vytištěný výtah z veřejně dostupných registrů, který předloží žadatel nebo jej vyhotoví operátor RA.

Tento dokument musí obsahovat úplné obchodní jméno, identifikační číslo (je-li přiřazeno), adresu sídla, jméno/jména osoby/osob oprávněné/oprávněných k zastupování (statutárních zástupců).

3.2.3 Ověřování identity fyzické osoby

V procesu ověřování identity osoby zastupující Organizaci je požadováno předložení osobního dokladu v listinné podobě. Pro občany ČR jím musí být platný občanský průkaz nebo cestovní pas, pro cizince je to platný cestovní pas, nebo jím v případě občanů členských států EU může být platný osobní doklad, sloužící k prokazování totožnosti na území příslušného státu.

Operátor RA porovnává fotografii osoby zastupující Organizaci na dokladu s její skutečnou podobou, v případě pochybností má právo požádat o předložení dalšího dokladu v listinné podobě, nebo případně ověřování ukončit. Další doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s původně předloženým osobním dokladem.

Pokud kontrola fotografie skončí s kladným výsledkem, jsou z prvního předloženého osobního dokladu ověřovány následující údaje:

- celé občanské jméno,
- datum a místo narození, nebo rodné číslo, je-li v dokladu uvedeno,
- číslo předloženého osobního dokladu,
- adresa trvalého bydliště (je-li v dokladu uvedena).

Pokud osoba zastupující Organizaci není osobou ze zákona oprávněnou k zastupování Organizace, je dále požadována její úředně ověřená plná moc k zastupování Organizace podepsaná statutárním zástupcem Organizace. Plnou moc lze předložit i v elektronické podobě. Musí být ve formátu PDF a elektronicky podepsaná osobou oprávněnou jednat za Organizaci, a to minimálně zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu pro elektronický podpis, v odůvodněných případech potom kvalifikovaným elektronickým podpisem.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Všechny informace uvedené v Certifikátu jsou řádně ověřovány.

3.2.5 Ověřování kompetencí

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

OID certifikační politiky prokazující, že klíčový pár byl generován a uložen na bezpečném kryptografickém zařízení, lze do Certifikátu vložit pouze tehdy, byla-li tato skutečnost v procesu vydání Certifikátu pro tuto žádost ověřena.

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.

Křížové certifikáty nejsou používány.

3.2.7 Ověřování e-mailové adresy

Ověření e-mailové adresy je prováděno dvěma způsoby, a to 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

Identifikace a autentizace při běžném požadavku na výměnu klíče (vydání následného Certifikátu) se prokazuje tak, že žádost o vydání následného Certifikátu ve struktuře PKCS#10, musí být:

- navíc opatřena elektronickým podpisem vytvořeným soukromým klíčem odpovídajícím veřejnému klíči obsaženému v platném Certifikátu, který je předmětem výměny, nebo
- obsažena v elektronické zprávě podepsané soukromým klíčem odpovídajícím veřejnému klíči v podpisovém certifikátu (certifikát vydaný volitelně žadateli o Certifikát spolu s Certifikátem a jednoznačně s ním svázaný).

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

Není relevantní pro tento dokument, služba výměny veřejného klíče po zneplatnění Certifikátu není podporována. Je nutné vydat nový Certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Subjekty oprávněné podat žádost o zneplatnění Certifikátu jsou vyjmenovány v kapitole 4.9.2. Možné způsoby identifikace a autentizace jsou popsány dále v této kapitole.

V případě **osobního předání žádosti o zneplatnění Certifikátu na RA** musí být žádost o zneplatnění Certifikátu písemná a podepsaná osobou, jejíž identita musí být řádně ověřena osobním dokladem (viz kapitola 3.2.3).

V případě **předání žádosti o zneplatnění Certifikátu elektronickou cestou** jsou přípustné tyto způsoby identifikace a autentizace:

- prostřednictvím formuláře na webových stránkách společnosti (s využitím hesla pro zneplatnění Certifikátu),
- prostřednictvím nepodepsané elektronické zprávy obsahující heslo pro zneplatnění Certifikátu odeslané na adresu revoke@ica.cz,
- prostřednictvím podepsané elektronické zprávy, kde:
  - elektronický podpis musí být realizován soukromým klíčem příslušným k podpisovému certifikátu příslušnému k Certifikátu, který má být zneplatněn, nebo
  - elektronický podpis být realizován soukromým klíčem příslušným k zneplatňovanému Certifikátu,

  zpráva musí být odeslána na adresu revoke@ica.cz,
- prostřednictvím datové schránky I.CA (s využitím hesla pro zneplatnění Certifikátu),
- prostřednictvím definované osoby pověřené za Organizaci vystupovat ve smluvním vztahu s I.CA.

V případě použití **listovní zásilky pro předání žádosti o zneplatnění Certifikátu** s využitím hesla pro zneplatnění Certifikátu musí být tato zaslána doporučeně na adresu sídla společnosti I.CA.

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 platnou právní úpravou nebo s požadavky technických standardů a norem pro tento typ Certifikátů.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

O vydání Certifikátu může požádat Organizace prostřednictvím osoby zastupující Organizaci.

4.1.2 Registrační proces a odpovědnosti

Registrační proces prováděný pouze v případě vydávání prvotního Certifikátu zahajuje osoba zastupující Organizaci dostavením se s potřebnými dokumenty a případně s žádostí o Certifikát na pracoviště RA, kde probíhá zanesení údajů obsažených v předkládaných dokladech do informačního systému Autority a zpracování žádosti o Certifikát.

Držitel soukromého klíče, resp. držitel Certifikátu jsou povinni zejména:

- seznámit se s touto CP a smluvně se zavázat jednat podle ní,
- poskytovat pravdivé a úplné informace pro vydání Certifikátu,
- překontrolovat, zda údaje uvedené v žádosti o Certifikát a ve vydaném Certifikátu jsou správné a odpovídají požadovaným údajům,
- zvolit vhodné heslo pro zneplatnění Certifikátu (minimální/maximální délka hesla 4/32 znaků, povolené znaky 0..9, A..Z, a..z).

Poskytovatel Služby je povinen zejména:

- před uzavřením smlouvy o vydání Certifikátu informovat držitele soukromého klíče, resp. držitele Certifikátu o smluvních podmínkách,
- uzavírat s držitelem Certifikátu, popř. s Organizací smlouvu o vydání Certifikátu, obsahující náležitosti požadované technickými standardy a normami,
- v procesu vydávání Certifikátu na RA ověřit všechny ověřitelné údaje uvedené v žádosti podle předložených dokladů,
- v případě, že soukromý klíč byl generován a uložen na bezpečném kryptografickém zařízení, vyžadovat prokázání této skutečnosti,
- vydat Certifikát obsahující věcně správné údaje na základě informací, které jsou poskytovateli Služby k dispozici v době vydávání tohoto Certifikátu,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- zveřejnit certifikáty Autority a kořenové CA,
- činnosti spojené se Službou poskytovat v souladu s uzavřenou smlouvou, touto CP, příslušnou CPS, Systémovou bezpečnostní politikou – důvěryhodné systémy a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Provádění identifikace a autentizace

Při vydávání **prvotního Certifikátu** jsou identifikace a autentizace prováděny podle kapitoly 3.2.3, případně kapitoly 3.2.2), v případě vydávání **následného certifikátu** pak podle kapitoly 3.3.1).

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

V procesu rozhodování o přijetí nebo zamítnutí žádosti o vydání **prvotního Certifikátu** provádějí pracovnice/pracovníci, dále jen pracovníci, RA:

- vizuální kontrolu shody údajů obsažených v žádosti o Certifikát (struktura PKCS#10) s údaji obsaženými v předkládaných dokladech,
- vizuální kontrolu formální správnosti údajů.

Ověřování vlastnictví soukromého klíče, kontrola kompetencí a kontroly formální správnosti údajů jsou prováděny i programovým vybavením systému RA.

Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen, v opačném případě je postupováno v souladu s ustanoveními kapitoly 4.3.

Postup vydání **následného Certifikátu** je popsán v kapitole 4.3.

4.2.3 Doba zpracování žádosti o certifikát

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.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání **prvotního Certifikátu:**

- mohou operátorky/operátoři, dále jen operátoři, CA, resp. programové vybavení umístěné na jejich pracovních stanicích, provádět:
  - vizuální kontrolu shody údajů obsažených v žádosti o Certifikát (struktura PKCS#10) a údajů doplněných pracovníkem RA,
  - vizuální kontrolu formální správnosti údajů,
  - ověřování vlastnictví soukromého klíče, kontrola podporovaných hashovacích funkcí v žádosti o Certifikát (minimálně sha-256), a kontroly formální správnosti údajů.

- jsou vždy programovým vybavením jádra systému CA prováděny ověřování vlastnictví soukromého klíče, kontrola podporovaných hashovacích funkcí v žádosti o Certifikát (minimálně sha-256) a kontroly formální správnosti údajů.

Pokud některá z kontrol skončí negativně, proces vydání Certifikátu je ukončen.

Vydávání **následného Certifikátu** probíhá automatizovaně. 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.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

V procesu vydávání **prvotního** Certifikátu je držitel Certifikátu, resp. osoba zastupující Organizaci žádající o Certifikát informována prostřednictvím pracovníka RA a Certifikát je zaslán na kontaktní e-mailovou adresu zadanou povinně při registraci.

V případě vydání **následného** Certifikátu je tento Certifikát zaslán na kontaktní e-mailovou adresu zadanou povinně při registraci.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání Certifikátu, je povinností držitele Certifikátu tento Certifikát přijmout. Jediným způsobem, jak odmítnout převzetí Certifikátu je zažádat v souladu s touto CP o jeho zneplatnění.

I.CA může s Organizací sjednat postup odlišný od tohoto ustanovení CP. Tímto postupem však nesmí být dotčena příslušná ustanovení právních předpisů.

4.4.2 Zveřejňování certifikátů certifikační autoritou

I.CA zajistí zveřejnění jí vydaných Certifikátů, 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.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností držitelů Certifikátů je zejména:

- dodržovat veškerá relevantní ustanovení smlouvy o poskytování této Služby,

- používat soukromý klíč a odpovídající Certifikát vydaný podle této CP pouze pro účely stanovené v této CP,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v Certifikátu vydaném podle této CP, 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) certifikáty certifikačních autorit související s Certifikátem vydaným podle této CP, ověřit hodnoty jejich otisků a jejich platnost,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že Certifikát je platný,
- dodržovat veškerá ustanovení této CP.

4.6 Obnovení certifikátu

Službou obnovení Certifikátu je podle této CP 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

Službou výměny veřejného klíče v Certifikátu je podle této CP míněno vydání nového Certifikátu (následná Certifikát) s jiným veřejným klíčem, ale s totožným obsahem položek uvedených v polí subject nebo rozšíření subjectAlternativeName Certifikátu, jehož veřejný klíč je předmětem výměny.

V případě, že proces vydání nového Certifikátu probíhá výhradně elektronickou cestou, kdy není vyžadována přítomnost fyzické osoby na pracovišti RA, jedná se o vydání následného Certifikátu. Požadavky na ověření elektronické žádosti o vydání následného Certifikátu jsou uvedeny v kapitole 4.7.1, pokud splněny nejsou, jedná se o vydání prvotního Certifikátu počínající registračním procesem.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Žádost o vydání následného Certifikátu (struktura PKCS#10) s vyměněným veřejným klíčem musí splňovat níže uvedené podmínky:

- položky pole subject a rozšíření subjectAlternativeName musí být totožné jako v Certifikátu, který je předmětem výměny,
- veřejný klíč musí být jiný než v Certifikátu, který je předmětem výměny,
- proces ověření elektronické žádosti o vydání následného Certifikátu je proveden v souladu s kapitolou 3.3.1.

4.7.2 Kdo může žádat o výměnu veřejného klíče v certifikátu

Výměnu veřejného klíče v příslušném Certifikátu je oprávněn požadovat držitel tohoto Certifikátu.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Pokud jsou splněny podmínky pro výměnu veřejného klíče, je postupováno v souladu s kapitolami 4.2 a 4.3.1, v opačném případě je řízení k vydání Certifikátu ukončeno.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Uvedeno v kapitole 4.3.2.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Uvedeno v kapitole 4.4.1.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Uvedeno v kapitole 4.4.2.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Uvedeno v kapitole 4.4.3.

4.8 Změna údajů v certifikátu

Službou změny údajů v Certifikátu je podle této CP míněno vydání nového Certifikátu s minimálně jednou změnou v obsahu položek uvedených v poli subject nebo rozšíření subjectAlternativeName vztahujících se k držiteli Certifikátu, nebo s odebraným, nebo přidaným dalším polem, jehož obsah musí být ověřen. Veřejný klíč musí být jiný než v Certifikátu, který je předmětem změny.

V případě, že proces vydání nového Certifikátu probíhá výhradně elektronickou cestou, kdy není vyžadována přítomnost fyzické osoby na pracovišti RA, jedná se o vydání následného Certifikátu. Požadavky na ověření elektronické žádosti o vydání následného Certifikátu jsou uvedeny v kapitole 4.8.1, pokud splněny nejsou, jedná se o vydání prvotního Certifikátu počínající registračním procesem.

4.8.1 Podmínky pro změnu údajů v certifikátu

Žádost o vydání následného Certifikátu (struktura PKCS#10) se změněnými údaji musí splňovat níže uvedené podmínky:

- měněné, resp. nově uvedené položky pole subject nebo rozšíření subjectAlternativeName musí být řádným způsobem ověřeny,
- veřejný klíč musí být jiný než v původním Certifikátu,
- proces ověření elektronické žádosti o vydání následného Certifikátu je proveden v souladu s kapitolou 3.3.1.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Změnu údajů v příslušném Certifikátu je oprávněn požadovat držitel tohoto Certifikátu.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Pokud jsou splněny podmínky na změnu údajů v Certifikátu, je postupováno v souladu s kapitolami 4.2 a 4.3.1, v opačném případě je řízení k vydání Certifikátu ukončeno.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Uvedeno v kapitole 4.3.2.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Uvedeno v kapitole 4.4.1.

4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Uvedeno v kapitole 4.4.2.

4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Uvedeno v kapitole 4.4.3.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádosti o zneplatnění Certifikátu přijímá I.CA nepřetržitě prostřednictvím formuláře na webových stránkách společnosti.

Nepřetržitě je možné podat žádost o zneplatnění Certifikátu také prostřednictvím e-mailu, datové schránky a listovní zásilky. Takto podaná žádost je přijata nejpozději následující pracovní den po jejím doručení.

Osobní předání a přijetí žádosti o zneplatnění Certifikátu na RA je možné pouze v pracovní době příslušné RA.

Službu pozastavení platnosti Certifikátu I.CA neposkytuje, stejně jako neposkytuje možnost požádat o zneplatnění k určitému datu v budoucnosti.

4.9.1 Podmínky pro zneplatnění

4.9.1.1 Důvody zneplatnění uživatelského certifikátu

I.CA zneplatní Certifikát během 24 hodin a uvede odpovídající kód CRLReason (viz kapitola 7.2.2), pokud nastane jeden nebo více z následujících důvodů:

1. držitel Certifikátu podal písemnou žádost o zneplatnění Certifikátu (nespecifikováno – unspecified(0); tento kód se v CRL u položky neuvádí),
2. držitel Certifikátu oznámil certifikační autoritě, že původní žádost o Certifikát byla neoprávněná a že zpětně neudělí autorizaci (CRLReason #9, privilegeWithdrawn),
3. I.CA získá důkaz, že soukromý klíč držitele Certifikátu odpovídající klíči veřejnému v Certifikátu byl kompromitován (CRLReason #1, keyCompromise),
4. I.CA je vyrozuměna o předvedené nebo prokázané metodě, kterou je možné snadno vypočítat soukromý klíč držitele ze znalosti veřejného klíče uvedeného v Certifikátu (např. slabina Debian Weak Key) (CRLReason #1, keyCompromise),
5. I.CA získá důkaz, že na metodu pro ověření vlastnictví domény nebo kontroly nad mailovou adresou pro kteroukoliv mailovou adresu v Certifikátu nelze spoléhat (CRLReason #4, superseded).

I.CA zneplatní Certifikát do pěti dnů, pokud nastane jeden nebo více z následujících důvodů:

6. Certifikát nevyhovuje požadavkům na kryptografické algoritmy a jejich požadovaným parametrům (kvalitě, viz kapitoly 6.1.5 a 6.1.6) (CRLReason #4, superseded),
7. I.CA získá důkaz, že Certifikát byl zneužit (CRLReason #9, privilegeWithdrawn),

8. I.CA je vyrozuměna, že držitel Certifikátu porušil jednu nebo více ze svých důležitých povinností plynoucích ze smlouvy o vydání Certifikátu nebo smlouvy o podmínkách používání Certifikátu (CRLReason #9, privilegeWithdrawn),
9. I.CA je vyrozuměna o okolnostech indikujících, že e-mailová adresa plně kvalifikované jméno domény uvedené v certifikátu není dále právně přípustné (tj. soud nebo arbitráž odňaly registrantovi právo používat e-mailovou adresu nebo doménové jméno, zrušily relevantní smlouvu, smlouva o licenci nebo službě mezi registrantem doménového jména a žadatelem o certifikát byla zrušena, nebo se registrantovi doménového jména nepodařilo e-mailovou adresu nebo doménové jméno udržet v aktivním stavu) CRLReason #5, cessationOfOperation),
10. I.CA je vyrozuměna, že došlo ke podstatným změnám informací obsažených v Certifikátu (CRLReason #9, privilegeWithdrawn),
11. I.CA je vyrozuměna, že Certifikát nebyl vydán v souladu s S/MIME BR, CP nebo CPS (CRLReason #4, superseded),
12. I.CA zjistí, že některá informace v Certifikátu je nepřesná nebo zavádějící (CRLReason #9, privilegeWithdrawn),
13. oprávnění I.CA vydávat Certifikáty podle S/MIME BR a této CP vypršelo, bylo zneplatněno, nebo ukončeno a I.CA nepřipravila způsob, jak udržovat CRL/OCSP úložiště (nespecifikováno – unspecified(0); tento kód se v CRL u položky neuvádí),
14. zneplatnění je vyžadováno CP nebo CPS (nespecifikováno – unspecified(0); tento kód se v CRL u položky neuvádí),
15. CRLReason #1, keyCompromise v případech, že:
    - je I.CA je vyrozuměna o předvedené nebo prokázané metodě pro kompromitaci soukromého klíče držitele Certifikátu,
    - nebo je jasný důkaz, že konkrétní metoda použitá pro generování soukromého klíče obsahovala chybu.

4.9.1.2 Důvody zneplatnění certifikátu Autority

I.CA zneplatní certifikát Autority během sedmi dnů, pokud nastane některý z uvedených případů:

1. Autorita požádá písemně o zneplatnění,
2. Autorita oznámila kořenové certifikační autoritě, že původní žádost o její certifikát byla neoprávněná a že zpětně neudělí autorizaci,
3. kořenová certifikační autorita je vyrozuměna, že soukromý klíč Autority byl kompromitován, nebo nadále nesplňuje požadavky na kryptografické algoritmy a požadované parametry (kvalitu, viz kapitola 6.1.5 a 6.1.6),
4. kořenová certifikační autorita je vyrozuměna, certifikát Autority byl zneužit,
5. kořenová CA je vyrozuměna, že certifikát Autority nebyl vydán v souladu s S/MIME BR, příslušnou CP nebo CPS, nebo nesplňuje jejich požadavky,
6. I.CA zjistí, že některá informace v certifikátu Autority je nepřesná nebo zavádějící
7. kořenová CA nebo Autorita ukončily z nějakého důvodu činnost a nepřevedly podporu zneplatňování na jinou CA,

8. právo kořenové CA nebo Autority vydávat certifikáty podle podmínek S/MIME BR nebo CP vypršelo, nebo bylo odvoláno či ukončeno a kořenová CA nezajistila pro Autoritu pokračující správu úložiště CRL/OCSP,
9. zneplatnění je vyžádáno CP a/nebo CPS kořenové CA.

4.9.2 Kdo může požádat o zneplatnění

Žádost o zneplatnění Certifikátu mohou podat:

- držitel Certifikátu
- subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování Služby podle této CP,
- prostřednictvím oprávněného pracovníka subjekty, jimž to umožňuje platná právní úprava,
- poskytovatel této Služby (oprávněným žadatelem o zneplatnění Certifikátu vydaného I.CA je v tomto případě generální ředitel I.CA, resp. zastupující osoba) a subjekt je o zneplatnění informován podepsaným e-mailem na adresu zadanou při registraci:
  - v případě, že Certifikát byl vydán na základě nepravdivých údajů,
  - pokud prokazatelně zjistí, že soukromý klíč, patřící k veřejnému klíči uvedenému v Certifikátu, byl kompromitován,
  - dozví-li se prokazatelně, že Certifikát byl použit v rozporu s omezením definovaným v kapitole 1.4.2,
  - dozví-li se prokazatelně, že držitel Certifikátu zanikl, nebo pokud údaje, na jejichž základě byl Certifikát vydán, pozbyly pravdivosti,
  - pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném certifikátu.

Držitel je povinen v případě podání žádosti o zneplatnění Certifikátu okamžitě přestat používat tento Certifikát i odpovídající soukromý klíč.

Kromě toho třetí strany (např. orgán dohledu, orgány činné v trestním řízení, spoléhající se strany, dodavatelé aplikačního SW) mohou zasílat hlášení o problému s Certifikátem informující Autoritu o důvodech pro případné zneplatnění Certifikátu.

4.9.3 Postup při žádosti o zneplatnění

V případě osobního předání žádosti o zneplatnění Certifikátu na RA musí žádost obsahovat sériové číslo Certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“), jméno, popř. jména a příjmení osoby oprávněné žádat zneplatnění Certifikátu a heslo pro zneplatnění Certifikátu. Pokud osoba oprávněná žádat zneplatnění Certifikátu heslo pro zneplatnění nezná, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla osobního dokladu předloženého při žádosti o vydání Certifikátu, nebo čísla nového primárního osobního dokladu, pokud byl původní nahrazen novým. Tímto osobním dokladem se musí pracovníkovi RA prokázat. V případě, že je žádost oprávněná, pracovník RA Certifikát zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. V případě, že žádost o zneplatnění Certifikátu nelze akceptovat (nesprávné heslo pro zneplatnění, neprokazatelná identita osoby oprávněné žádat zneplatnění Certifikátu), pokusí se pracovník RA v součinnosti s touto fyzickou osobou tyto skutečnosti napravit a pokud to z libovolného důvodu nebude možné, žádost o zneplatnění

Certifikátu bude zamítnuta. Žadatel o zneplatnění Certifikátu je vždy o výsledku informován prostřednictvím pracovníka RA.

V případě předání žádosti o zneplatnění Certifikátu elektronickou cestou jsou přípustné následující možnosti:

- Prostřednictvím formuláře na internetové informační adrese. Datum a čas zneplatnění Certifikátu jsou dány zpracováním platné žádosti o zneplatnění Certifikátu informačním systémem CA. O kladném vyřízení je žadatel informován.
- Elektronicky podepsaná elektronická zpráva – tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx,

  kde „*xxxxxxx*“ je sériové číslo Certifikátu a musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

  Zpráva musí být elektronicky podepsána soukromým klíčem odpovídajícím veřejnému klíči v podpisovém certifikátu, nebo soukromým klíčem příslušným k veřejnému klíči ve zneplatňovaném Certifikátu.
- Elektronicky nepodepsaná elektronická zpráva – tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  Heslo pro zneplatneni = yyyyyy,

  kde „*xxxxxxx*“ je sériové číslo Certifikátu a „*yyyyyy*“ je heslo pro zneplatnění. Sériové číslo musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).
- Elektronicky podepsaná či ve zvláštních případech elektronicky nepodepsaná elektronická zpráva odeslaná definovanou osobou pověřenou za Organizaci vystupovat ve smluvním vztahu s I.CA:

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  kde „*xxxxxxx*“ je sériové číslo Certifikátu. Sériové číslo musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

Pozn.: Pokud žádost splňuje požadavky tří výše uvedených možností, odpovědný pracovník Certifikát v systému CA neprodleně zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. O kladném vyřízení je žadatel informován.

V případě použití doporučené listovní zásilky pro podání žádosti o zneplatnění Certifikátu musí být žádost v následujícím tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

Zadam o zneplatneni certifikatu cislo = xxxxxxx

Heslo pro zneplatneni = yyyyyy,

kde „*xxxxxxx*“ je sériové číslo Certifikátu a „*yyyyyy*“ je heslo pro zneplatnění. Sériové číslo je buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“). V případě, že žádost uvedené požadavky splňuje, odpovědný pracovník I.CA Certifikát v informačním systému CA zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. V případě, že žádost nelze akceptovat (nesprávné heslo pro zneplatnění) bude žádost o zneplatnění Certifikátu zamítnuta. O vyřízení žádosti je žadatel informován doporučeným dopisem na poštovní adresu uvedenou jako adresa odesilatele.

Oznámení o podezření na kompromitaci soukromého klíče vztahujícího se k veřejnému klíči v Certifikátu, zneužití Certifikátu nebo jiné typy podvodu, kompromitace, zneužití, nevhodného chování spojené s vydaným Certifikátem je možné zaslat na e-mailovou adresu uvedenou v kapitole 1.5.2, případně doporučenou listovní zásilkou na adresu sídla společnosti, nebo podat prostřednictvím datové schránky – viz kapitola 2.2.

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

4.9.5.1 Požadavek na zneplatnění Certifikátu

Požadavek na zneplatnění Certifikátu je realizován bezodkladně po přijetí oprávněné žádosti o zneplatnění. CRL obsahující sériové číslo zneplatněného Certifikátu je vydán neprodleně po zneplatnění tohoto Certifikátu.

4.9.5.2 Hlášení problémů s Certifikáty

I.CA během 24 hodin po přijetí hlášeného problému s Certifikátem prozkoumá fakta a okolnosti hlášeného problému a poskytne předběžnou zprávu jak držiteli Certifikátu, tak tomu, kdo ohlásil problém.

I.CA ve spolupráci s držitelem Certifikátu a ohlašovatelem problému rozhodne, zda je nutné zneplatnění Certifikátu, o rozhodnutí informuje jak držitele Certifikátu, tak toho, kdo ohlásil problém.

Pokud je nutné zneplatnění Certifikátu, potom určí datum zneplatnění Certifikátu na základě následujících kritérií:

- povaha údajného problému,
- důsledky zneplatnění (pro držitele i spoléhající strany),
- počet obdržených hlášení o problému s Certifikátem vztahujících se k jednotlivému Certifikátu, nebo k držiteli Certifikátu,
- kdo si stěžuje (např. hlášení orgánu činného v trestním řízení, že stránka provozuje ilegální aktivity, má větší závažnost než stížnost od zákazníka uvádějícího, že nedostal objednané zboží),
- relevantní právní úprava.

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

Seznam zneplatněných certifikátů je vydáván neprodleně po kladném zpracování žádosti o zneplatnění Certifikátu. Nedojde-li ke zneplatnění Certifikátu, je nový CRL vydáván zpravidla dvakrát denně, nejvýše však 24 hodin od vydání předchozího CRL.

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, vydaný podle této CP, obsahuje odkaz na příslušný OCSP respondér.

OCSP odpovědi vyhovují normám 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

OCSP umožňuje dotazy využívající metodu GET i POST. OCSP odpovědi na stav nevydaných certifikátů nevracejí stav good.

4.9.10.1 Stav Certifikátů

Platnost OCSP odpovědi je nastavena na 24 hodin.

Při zneplatnění certifikátu se OCSP odpověď aktualizuje okamžitě (pozastavení ani obnovení platnosti Certifikátu není poskytováno).

OCSP odpovědi jsou automaticky aktualizovány (tj. platnost položky v interní cache OCSP respondéru končí) nejdéle v okamžiku, kdy je splněna dřívější z následujících podmínek:

- v polovině platnosti OCSP odpovědi (pro odpovědi s platností kratší než 16 hodin),
- 8 hodin před koncem platnosti odpovědi (pro odpovědi s platností 16 hodin nebo delší).

4.9.10.2 Stav certifikátu CA vydávající Certifikáty

I.CA aktualizuje informaci poskytovanou prostřednictvím OCSP:

- do 24 hodin po zneplatnění certifikátu CA vydávající Certifikáty,
- a nejméně každých dvanáct měsíců.

4.9.11 Jiné možné způsoby oznamování zneplatnění

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 ověřování 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 jí vydaných certifikátech.

Skutečnost, že Autorita poskytuje informace o stavu Certifikátu formou OCSP, je uvedena v jí vydaných certifikátech.

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

4.10.2 Dostupnost služeb

Autorita garantuje zajištění nepřetržité dostupnosti (7 dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných Certifikátů a seznamu 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.

I.CA udržuje prostřednictvím e-mailové adresy uvedené v kapitole 1.5.2 nepřetržitou 24x7 dostupnost tak, aby interně zareagovala na hlášení závažného problému s Certifikátem a, pokud je to nutné, předala informaci o přijatém hlášení příslušnému orgánu a případně zneplatnila Certifikát, který je předmětem hlášení.

4.10.3 Další charakteristiky služeb stavu certifikátu

Není relevantní pro tento dokument, další charakteristiky služeb stavu certifikátu nejsou poskytovány.

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:

- systémy poskytovaných určené k podpoře Služby,
- veškeré procesy podporující poskytování Služby.

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

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

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

Důvěryhodné systémy určené k podpoře Služby 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 Služby, 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 Služby 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, 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 v I.CA definovány důvěryhodné role. Postup jmenování zaměstnanců do důvěryhodných rolí, specifikace těchto rolí včetně odpovídajících činností a odpovědností jsou uvedeny v interní dokumentaci.

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.

5.2.3 Identifikace a autentizace pro každou roli

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

Pro vybrané činnosti využívají pracovníci v důvěryhodných rolích dvoufaktorovou autentizaci.

5.2.4 Role vyžadující rozdělení povinností

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

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 Služby,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

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

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

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

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.

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.

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).

5.3.7 Požadavky na nezávislé dodavatele

I.CA některé činnosti spojené s vydáváním certifikátů zajišťuje smluvně. Za činnost takových nezávislých dodavatelů plně odpovídá a dále platí:

- obchodně právní vztahy jsou upraveny bilaterálními obchodními smlouvami,
- tito nezávislí dodavatelé:
  - musí splňovat personální požadavky a požadavky na zaznamenávání událostí analogicky, jako tomu je v případě zajištění činností vlastními prostředky,
  - jsou povinni řídit se odpovídajícími certifikačními politikami, certifikační prováděcí směrnicí, relevantními interními dokumenty, které jim jsou poskytovány a předepsanými normativními dokumenty.

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

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, a to i od pověřených třetích stran zapojených v životním cyklu certifikátů. Zaznamenáváno je generování CRL a OCSP odpovědí.

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 kořenová autorita při generování párových dat postupovala v souladu s připraveným scénářem a zajistila při tom integritu a důvěrnost.

Záznam bezpečnostních událostí v systémech, na síťových prvcích a vstupů na provozní pracoviště je prováděn v souladu s požadavky standardů v kapitolách 6.5 a 6.6 tohoto dokumentu a splňuje požadavky S/MIME BR.

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.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní dokumentaci, 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 provozní prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci.

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 s důvěryhodnými systémy určenými k podpoře služeb vytvářejících důvěru je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

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

5.5.1 Typy uchovávaných záznamů

I.CA uchovává níže uvedené záznamy (v elektronické nebo listinné podobě), které souvisejí s poskytovanými službami vytvářejícími důvěru, a to i od pověřených třetích stran zapojených v životním cyklu certifikátů, 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),
- auditní záznamy podle kapitoly 5.4.1,
- 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 způsobem vycházejícím z požadavků provedené analýzy rizik a ze zákona o ochraně utajovaných informací.

Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

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

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

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

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

5.5.7 Postupy pro získání a ověření uchovávaných informací

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

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 interním plánem pro zvládání krizových situací a plánem obnovy a případně s další relevantní interní dokumentací.

5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče

V případě vzniku důvodné obavy z kompromitace soukromého klíče certifikačních autorit postupuje I.CA 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 v souladu s kapitolou 2.2, pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,
- případně 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 Služby.

5.7.4 Schopnost obnovit činnost po havárii

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

5.8 Ukončení činnosti CA nebo RA

Pro ukončování činnosti Autority platí následující pravidla:

- ukončení činnosti Autority musí být písemně oznámeno všem držitelům platných Certifikátů, subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování Služby, případně orgánu dohledu,

- ukončení činnosti Autority musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- pokud je součástí ukončení činnosti Autority 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 i jen jediného Certifikátu vydaného Autoritou musí Autorita či její nástupce v případě zániku zajistit alespoň služby zneplatňování Certifikátů a vydávání CRL,
- následně Autorita prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván podle pravidel této CP.

V případě ukončení činnosti poskytování Služby bude postupováno v souladu s uzavřenými smlouvami, případně s příslušnými technickými standardy nebo normami.

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

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit a jejich OCSP respondérů, 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.

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

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 k Certifikátům je prováděno na zařízeních, která jsou pod výhradní kontrolou příslušných držitelů soukromých klíčů. Úložištěm těchto párových dat může být jak hardware, tak software.

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.

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

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Veřejný klíč je vydavateli certifikátu doručen v žádosti o vydání certifikátu (formát PKCS#10).

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Získání veřejného klíče 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 4096 bitů, mohutnost klíčů v jí vydávaných certifikátech podřízených certifikačních autorit je minimálně

2048 bitů, mohutnost klíčů OCSP respondérů certifikačních autorit je minimálně 2048 bitů. Mohutnost klíčů v Certifikátech vydávaných podle této CP je minimálně 2048 bitů.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit a jejich OCSP respondérů 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

6.2.1 Řízení a standardy kryptografických modulů

Generování párových dat certifikačních autorit a jejich OCSP respondérů 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 jejich certifikací.

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

Používání kryptografických modulů 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 a jejich OCSP respondérů 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 koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.5 Uchovávání soukromého klíče

Soukromé klíče certifikačních autorit a jejich OCSP respondérů nejsou nikde uchovávány, po uplynutí doby platnosti jsou včetně jejich 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 koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou generovány v kryptografických modulech (jako neexportovatelné) a nelze je z kryptografického modulu (provozovaného v certifikovaném režimu) exportovat v žádném tvaru[1]. Import soukromého klíče CA 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 koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou uloženy v kryptografických modulech splňujících požadavky právní úpravy pro služby vytvářející důvěru, tedy 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 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 a jejich OCSP respondérů 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 koncových uživatelů je plně v kompetenci těchto koncových uživatelů a závisí na způsobu uložení těchto soukromých klíčů.

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

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.

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

Deaktivace soukromých klíčů vztahujících se k Certifikátům 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 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 koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.11 Hodnocení kryptografických modulů

Kryptografické moduly použité pro generování párových dat a uložení příslušných soukromých klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a jsou používány v souladu s příslušnou 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 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. Je v souladu s požadavky S/MIME BR.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit a jejich OCSP respondérů (čipová karta nebo softcard) jsou vytvářena před generováním nebo v průběhu generování příslušných párových dat.

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 a jejich OCSP respondérů (čipová karta nebo softcard) jsou chráněna nastaveným heslem.

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 je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů, a jejich periodicity definována platnými technickými standardy a normami.

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.
- ETSI TS 119 411-6 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6:

Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.

- 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.
- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- European Cybersecurity Certification Group Sub-group on Cryptography - Agreed Cryptographic Mechanisms.
- CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.
- 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.

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.

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

6.7 Řízení bezpečnosti sítě

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.

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

tab. 4 - Základní pole Certifikátu

Pole	Obsah
version	v3 (0x2)
serialNumber	jedinečné sériové číslo Certifikátu
signatureAlgorithm	podle typu žádosti (a v závislosti na algoritmu podpisu certifikátu) jedna z možností: • minimálně ***sha256withRSAEncryption*** (s parametry= NULL, pkcs#1 1v5), • ***rsassaPss*** (pkcs#1 2v1) s parametry: – hashAlgorithm: minimálně sha256, – maskGenAlgorithm: mgf1 s hash funkcí stejnou jako v hashAlgorithm, – saltLength: v závislosti na použité hash funkci, – trailerField: 0xBC (default)
issuer	vydavatel Certifikátu
validity	
notBefore	počátek platnosti Certifikátu (UTC)
notAfter	notBefore + maximálně 365 dnů, resp. 366 dnů v případě přestupného roku (UTC)
subject	viz tab. 5
subjectPublicKeyInfo*	
algorithm	rsaEncryption
subjectPublicKey	minimálně 2048 bitů
extensions	viz tab. 6
signature	zaručená elektronická pečeť vydavatele Certifikátu

* V důsledku změn relevantní právní úpravy nebo technických norem, resp. standardů může dojít ke změně algoritmu nebo minimální délky klíče držitele Certifikátu. Podrobnosti mohou být uvedeny ve Zprávě pro uživatele.

tab. 5 - Pole subject

Všechny položky[2] pole subject jsou převzaty ze žádosti o Certifikát s výjimkou položek vytvářených Autoritou.

Položka	Poznámka
countryName*	povinná, jediný výskyt, kód státu (ISO 3166), stát registrace organizace – kontext, ve kterém jsou uváděny všechny atributy subjektu
serialNumber	jednoznačná identifikace držitele Certifikátu v systému Autority (ICA - xxxxxxxx)
commonName	povinná, jediný výskyt v případě certifikátu typu S/MIME BR: obsah totožný s obsahem položky organizationName ostatní případy: • jméno, pod kterým subjekt Certifikátu (držitel soukromého klíče) běžně vystupuje, nemusí obsahovat plné registrované jméno (může obsahovat zkrácený název organizace), a může být doplněno o označení prostředku pro vytváření elektronických pečetí (název identifikující zařízení nebo komponentu ICT uživatele), • nesmí obsahovat FQDN nebo IP adresu
emailAddress	v prvotním Certifikátu nesmí být uvedena
organizationName	povinná, jediný výskyt
organizationIdentifier	povinná, jediný výskyt: • NTRss-id, (**N**ational **T**rade **R**egister, tzn. IČ), • VATss-id, (**V**alue **A**dded **T**ax, tzn. DIČ), • XX:ss-id, kde: • ss je kód státu, • id je identifikační číslo organizace v příslušném registru, XX jsou dva znaky definované autoritou příslušného státu, následované znakem ":" (dvojtečka) – pro Slovenskou republiku se jedná o řetězec „SZ“.
organizationalUnitName	volitelná, možný vícenásobný výskyt
stateOrProvinceName*	volitelná, jediný výskyt
localityName*	volitelná, jediný výskyt

[2] I.CA si vyhrazuje právo upravit množinu a obsah položek pole subject, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

streetAddress*	volitelná, jediný výskyt v případě certifikátu typu S/MIME BR: pouze pokud jsou uvedeny localityName nebo stateOrProvinceName
postalCode*	volitelná, jediný výskyt

* Položky countryName, stateOrProvinceName, localityName, streetAddress a postalCode se vztahují k adrese sídla Organizace.

7.1.1 Číslo verze

Vydávané Certifikáty jsou v souladu se standardem X.509 ve verzi 3.

7.1.2 Rozšíření certifikátu

tab. 6 – Rozšíření[3] Certifikátu

Rozšíření	Obsah	Poznámka
certificatePolicies		nekritické
.policyInformation (1)		
policyIdentifier	viz kapitola 1.2	
policyQualifiers		
cPSuri	http://www.ica.cz	
.policyInformation (2)		
policyIdentifier	jedna z možností: • OID (NCP): 0.4.0.2042.1.1 (soukromý klíč není generován a uložen na bezpečném kryptografickém zařízení), • OID (NCP+): 0.4.0.2042.1.2 (soukromý klíč je generován a uložen na bezpečném kryptografickém zařízení)	
.PolicyInformation (3)		v případě certifikátu typu S/MIME BR (Multipurpose)
policyIdentifier	Organization-validated: 2.23.140.1.5.2.2	
CRLDistributionPoints*	http://scrldp1.ica.cz/pca*RR*_rsa.crl http://scrldp2.ica.cz/pca*RR*_rsa.crl	nekritické

[3] I.CA si vyhrazuje právo upravit množinu a obsah rozšíření Certifikátu, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

authorityInformationAccess		nekritické
id-ad-ocsp*	http://ocsp.ica.cz/pca*RR*_rsa	
id-ad-caIssuers*	http://s.ica.cz/pca*RR*_rsa.cer	
basicConstraints		nekritické
cA	False	
keyUsage	na základě obsahu žádosti o Certifikát jedna z možností: • digitalSignature, • digitalSignature, nonRepudiation, • digitalSignature, keyEncipherment, • digitalSignature, keyEncipherment, nonRepudiation	kritické, povinné v případě, že žádost bude obsahovat nepodporované použití, bude odebráno v případě absence tohoto rozšíření v žádosti bude doplněna kombinace: • digitalSignature, keyEncipherment
extendedKeyUsage	na základě obsahu žádosti o Certifikát jakákoli kombinace z možností: • id-kp-clientAuth, • ms-DocumentSigning, • id-kp-emailProtection, • Microsoft SmartCard Logon s výjimkou nepovoleného uvedení samotného ms-DocumentSigning	nekritické, povinné v případě absence tohoto rozšíření v žádosti bude doplněno: • id-kp-clientAuth, id-kp-emailProtection pokud EKU neobsahuje id-kp-emailProtection, bude doplněno
subjectKeyIdentifier	hash veřejného klíče (subjectPublicKey) v Certifikátu	nekritické
authorityKeyIdentifier		nekritické
keyIdentifier	hash veřejného klíče Autority	
subjectAlternativeName		nekritické
otherName	I.CA_OID (1.3.6.1.4.1.23624.4.6): xxxxxxxx**	
otherName	User Principal Name: UPN	volitelné Microsoft OID

rfc822Name	e-mail adresa	volitelné, možný vícenásobný výskyt
nsComment	identifikační číslo bezpečného kryptografického zařízení	nekritické, volitelné – vkládá Autorita v případě ověření generování a uložení soukromého klíče na bezpečném kryptografickém zařízení
I.CA_CERT_INTERCONNECTION: 1.3.6.1.4.1.23624.4.7	v případě vydávání více typů certifikátů jednomu subjektu (vazba subjektu k vydávaným certifikátům)	nekritické

* *RR* - poslední dvě číslice roku vydání certifikátu Autority.

** Jedná se o vybraný podřetězec z položky serialNumber pole subject vytvářené Autoritou (viz tab. 5).

U rozšíření obsahujících URL může být doplněno další URL k získání objektu (tam kde to je relevantní).

7.1.3 Objektové identifikátory algoritmů

V procesu poskytování Služby jsou využívány algoritmy v souladu s příslušnými technickými standardy a normami.

7.1.4 Tvary jmen

Tvary jmen vydávaných Certifikátů vyhovují standardu RFC 5280. Dále platí ustanovení kapitoly 3.1.

7.1.5 Omezení jmen

Není relevantní pro Certifikáty vydávané koncovým uživatelům.

7.1.6 Objektový identifikátor certifikační politiky

Společnost První certifikační autorita, a.s., vkládá do vydávaných Certifikátů níže uvedené objektové identifikátory certifikačních politik:

- OID certifikační politiky I.CA, dle které je Certifikát vydán,
- OID příslušné certifikační politiky určené normou ETSI EN 319 411-1, resp. ČSN ETSI EN 319 411-1 s ohledem na uložení soukromého klíče,
- OID příslušné politiky určené S/MIME BR a MTRP v případě certifikátů typu S/MIME BR.

7.1.7 Použití rozšíření Policy Constraints

Není relevantní pro certifikáty vydávané koncovým uživatelům.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz rozšíření Certifikátu v kapitole 7.1.2 výše.

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Není relevantní pro tento dokument – rozšíření není označeno jako kritické.

7.2 Profil seznamu zneplatněných certifikátů

tab. 7 - Profil CRL[4]

Pole	Obsah
version	v2(0x1)
signatureAlgorithm	minimálně sha256withRSAEncryption
issuer	vydavatel CRL
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate*	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu – viz tab. 8
crlExtensions	rozšíření CRL – viz tab. 8
signature	zaručené elektronická pečeť vydavatele CRL

* V případě certifikátu kořenové CA thisUpdate + maximálně 365 dní, v případě certifikátu podřízené CA thisUpdate + maximálně 24 hodin.

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X.509 verze 2.

7.2.2 Rozšíření CRL a záznamů v CRL

tab. 8 - Rozšíření CRL[5]

Rozšíření	Obsah	Poznámka
crlEntryExtensions		
CRLReason*	důvod zneplatnění certifikátu	nekritické, volitelné

[4] I.CA si vyhrazuje právo upravit množinu a obsah polí CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

[5] I.CA si vyhrazuje právo upravit množinu a obsah rozšíření CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

	důvod certificateHold je nepřípustný, nepoužívá se při zneplatnění certifikátu podřízené CA je uveden jiný důvod, než unspecified (0)	
crlExtensions		
authorityKeyIdentifier		
keyIdentifier	hash veřejného klíče vydavatele CRL (Autority)	nekritické
CRLNumber	jedinečné číslo vydávaného CRL	nekritické

* Pro Certifikáty koncových uživatelů jsou používány (podle jednotlivých důvodů zneplatnění – viz kapitola 4.9.1.1) pouze následující kódy CRLReason:

- keyCompromise (RFC 5280 CRLReason #1),
- affiliationChanged (RFC 5280 CRLReason #3),
- superseded (RFC 5280 CRLReason #4),
- cessationOfOperation (RFC 5280 CRLReason #5),
- privilegeWithdrawn (RFC 5280 CRLReason #9) - tento kód nemůže přímo použít držitel Certifikátu, je určován CA (nejdéle od 15.7.2023).

V případě zvolení důvodu zneplatnění certifikátu koncového uživatele unspecified (RFC 5280 CRLReason #0) není v souladu s doporučením RFC5280 rozšíření reasonCode u položky uváděno.

Aktualizace kódu a data zneplatnění u již zneplatněné CRL položky při pozdějším získání ověřitelného důkazu o kompromitace klíče není implementována.

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.

Bližší podrobnosti jsou uvedeny v odpovídající certifikační prováděcí směrnici.

7.3.1 Číslo verze

V žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP je uvedena verze 1.

7.3.2 Rozšíření OCSP

Konkrétní rozšíření uváděná v žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP jsou uvedena v odpovídající certifikační prováděcí směrnici.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita nebo okolnosti hodnocení

Periodicita hodnocení pro program Microsoft Trusted Root Program, včetně okolností pro provádění hodnocení, je striktně dána požadavky společnosti Microsoft, auditní perioda nepřekračuje jeden rok.

Periodicita jiných hodnocení je dána technickými standardy a normami, dle kterých je hodnocení prováděno.

8.2 Identita a kvalifikace hodnotitele

Identita (akreditovaný subjekt posuzování shody) a kvalifikace hodnotitele provádějícího hodnocení, definované programem Microsoft Trusted Root Program jsou popsány v normě ETSI EN 319 403-1.

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

8.3 Vztah hodnotitele k hodnocenému subjektu

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

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

8.4 Hodnocené oblasti

Hodnocené oblasti pro program Microsoft Trusted Root Program jsou striktně dány požadavky společnosti Microsoft.

Hodnocené oblasti u jiných hodnocení jsou konkretizovány technickými standardy a normami, podle kterých je hodnocení prováděno.

8.5 Postup v případě zjištění nedostatků

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

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům technických standardů a norem, v případě hodnocení požadovaného programem Microsoft Trusted Root Program potom požadavkům společnosti Microsoft.

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

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

8.7 Interní audity

V minimálně čtvrtletních intervalech, přičemž intervaly na sebe bezprostředně navazují, je na náhodně vybraném vzorku tvořeném alespoň větším počtem z možností:

- třiceti Certifikáty vydanými v hodnoceném období, nebo
- třemi procenty z Certifikátů vydaných v hodnoceném období,

provedena kontrola splnění požadavků této CP, odpovídající CPS a S/MIME BR. O výsledku kontroly je vytvořen protokol.

Dle možností je na vybraném vzorku vydaných Certifikátů prováděna automatizovaná kontrola pro ověření technické správnosti vydaných Certifikátů. Vzorek Certifikátů pro kontrolu je vybrán nezávisle na vzorku pro předchozí kontrolu. O výsledku kontroly je vytvořen protokol.

8.8 Kontrola nezávislých dodavatelů

I.CA v pravidelných, nevýše ročních intervalech vyhodnocuje, zda je činnost nezávislých dodavatelů, kteří neprocházejí každoročním auditem, v souladu předepsanými normativními dokumenty, odpovídajícími certifikačními politikami a relevantními částmi interní dokumentace, které jim byly poskytnuty. V případě porušení povinností stanovených v uvedených dokumentech jsou uplatňovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva. O provedeném vyhodnocení je vytvořen protokol.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za vydání Certifikátu 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. Služba obnovení Certifikátu není poskytována.

9.1.2 Poplatky za přístup k certifikátu

Přístup elektronickou cestou k Certifikátům vydaným podle této CP 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 vydaných Autoritou 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 Služby 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 Služby,
- 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. Informace o zásadách ochrany osobních údajů klientů je uvedena v dokumentu „Zásady nakládání s osobními údaji klientů“ vystaveném na webu společnosti – viz kapitola 2.2.

9.4.2 Informace považované za osobní údaje

Osobními údaji jsou veškeré informace 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 CP, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz důvěryhodných systémů určených k podpoře služeb vytvářejících 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 zneplatněných certifikátů a k vydávání certifikátů OCSP respondérů,
- použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,
- certifikáty splňují náležitosti požadované příslušnými technickými standardy a normami,
- zneplatní vydané Certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP,
- při vydávání Certifikátů, v průběhu doby jejich platnosti a při jejich správě bude vyhovovat své CP a jí příslušející CPS.

Záruky dále zahrnují:

- ověření oprávnění žádat o Certifikátu,
- ověření kontroly držitele Certifikátu nad e-mailovou schránkou s adresou uvedenou v Certifikátu,
- ověření informací uváděných v žádosti o vydání Certifikátu, včetně kontroly naplnění položek obsažených v žádosti o Certifikát (formát PKCS#10), a identity,
- soulad smlouvy o vydání Certifikátu s platnými právními předpisy,
- provoz úložiště informací o stavu certifikátů v režimu 24x7,
- možnost zneplatnění Certifikátu z důvodů uvedených v právní úpravě pro služby vytvářející důvěru a v této CP.

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

- držitel Certifikátu neporušil povinnosti plynoucí mu ze smlouvy o poskytování Služby a této CP,
- spoléhající se strana neporušila povinnosti této CP.

9.6.2 Zastupování a záruky RA

Určená RA:

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost, pokud žadatel 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 Autority,
- 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 této CP.

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 touto CP. Dále neodpovídá za škody vzniklé v důsledku porušení povinností I.CA z důvodu vyšší moci.

9.9 Záruky a odškodnění

Pro poskytování Služby platí relevantní ustanovení platné právní úpravy týkající se vztahů mezi poskytovatelem a spotřebitelem a dále takové záruky, které byly sjednány mezi společností První certifikační autorita, a.s., a žadatelem o Službu. Smlouva musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované uzavřenou smlouvou i příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služby,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, se kterými má platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo odpovědnosti, s výjimkou případů, kdy poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele.

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

- za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování Služby držitelem Certifikátu, zejména za využívání v rozporu s podmínkami uvedenými v této 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 a jejích projevů,
- 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 doporučené zásilky), pokud se strany nedohodnou jinak.

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do 30dnů 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 Autorita 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

9.10.1 Doba platnosti

Tato CP nabývá platnosti dnem uvedeným v kapitole 10 a platí minimálně po dobu platnosti posledního podle ní vydaného Certifikátu.

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

Po ukončení platnosti této CP přetrvávají z ní vyplývající závazky I.CA, a to po dobu platnosti posledního podle ní vydaného Certifikátu.

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

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

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

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interním dokumentu.

9.12.2 Postup a periodicita oznamování

Vydání nové verze CP je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněn OID

OID politiky musí být změněn v případě, že se zásadně sníží záruky za důvěryhodnost Certifikátu s významným účinkem na akceptovatelnost tohoto Certifikátu v souladu s technickými standardy a normami.

V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

9.13 Ustanovení o řešení sporů

V případě, že 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 Služby je provozován ve shodě s právními předpisy EU a České republiky a dále s relevantními mezinárodními standardy.

9.16 Různá ustanovení

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost ustanovení

V případě konfliktu mezi požadavky S/MIME BR, resp. odkazovaných technických standardů a platnou právní úpravou budou požadavky uvedené v této CP minimalizovány tak, aby byly

platné a v souladu s touto platnou právní úpravou. Okamžitě, a ještě před prvním vydáním Certifikátu podle upravených pravidel, bude vydána nová verze CP a na konci této kapitoly bude doplněn odkaz na právní předpis, který si úpravu vyžádal a popis této úpravy. Rovněž před prvním vydáním Certifikátu podle upravených pravidel bude zaslána zpráva o úpravě organizaci CA/Browser Forum.

Úprava požadavků provedená podle těchto pravidel přestane platit, pokud přestane platit odpovídající ustanovení právního předpisu, nebo pokud dojde ke změně požadavků S/MIME BR, resp. odkazovaných technických standardů.

Všechny výše uvedené úpravy a oznámení budou provedeny do devadesáti dnů.

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

Není relevantní pro tento dokument.

9.16.5 Vyšší moc

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

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

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