První certifikační autorita, a.s.



Certifikační politika

vydávání certifikátů OCSP respondérů TLS

(algoritmus RSA)

Certifikační politika vydávání certifikátů OCSP respondérů TLS (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 1.001

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 12
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 13
1.5.4 Postupy při schvalování CPS 13
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 24
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 25
3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu 25
4 Požadavky na životní cyklus certifikátu 26
4.1 Žádost o vydání certifikátu 26
4.1.1 Kdo může požádat o vydání certifikátu 26
4.1.2 Registrační proces a odpovědnosti 26
4.2 Zpracování žádosti o certifikát 26
4.2.1 Provádění identifikace a autentizace 26
4.2.2 Schválení nebo zamítnutí žádosti o certifikát 26
4.2.3 Doba zpracování žádosti o certifikát 27
4.3 Vydání certifikátu 27
4.3.1 Úkony CA v průběhu vydávání certifikátu 27
4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou 27
4.4 Převzetí vydaného certifikátu 28
4.4.1 Úkony spojené s převzetím certifikátu 28
4.4.2 Zveřejňování certifikátů certifikační autoritou 28
4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 28
4.5 Použití párových dat a certifikátu 28
4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu 28
4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou 28
4.6 Obnovení certifikátu 28
4.6.1 Podmínky pro obnovení certifikátu 29
4.6.2 Kdo může žádat o obnovení 29
4.6.3 Zpracování požadavku na obnovení certifikátu 29
4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu 29
4.6.5 Úkony spojené s převzetím obnoveného certifikátu 29
4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou 29

4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 29
4.7 Výměna veřejného klíče v certifikátu 29
4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu 29
4.7.2 Kdo může žádat o výměnu veřejného klíče v certifikátu....29
4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu...30
4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu....30
4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem....30
4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou 30
4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 30
4.8 Změna údajů v certifikátu 30
4.8.1 Podmínky pro změnu údajů v certifikátu 30
4.8.2 Kdo může požádat o změnu údajů v certifikátu....30
4.8.3 Zpracování požadavku na změnu údajů v certifikátu 30
4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu 30
4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji 30
4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou 31
4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům 31
4.9 Zneplatnění a pozastavení platnosti certifikátu 31
4.9.1 Podmínky pro zneplatnění 31
4.9.2 Kdo může požádat o zneplatnění 31
4.9.3 Postup při žádosti o zneplatnění 31
4.9.4 Prodleva při požadavku na zneplatnění certifikátu 32
4.9.5 Doba zpracování žádosti o zneplatnění 32
4.9.6 Povinnosti spoléhajících se stran při kontrole zneplatnění 32
4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů 32
4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů 32
4.9.9 Dostupnost ověřování stavu certifikátu on-line....32
4.9.10 Požadavky při ověřování stavu certifikátu on-line 32
4.9.11 Jiné možné způsoby oznamování zneplatnění 32
4.9.12 Zvláštní postupy při kompromitaci klíče 32
4.9.13 Podmínky pro pozastavení platnosti certifikátu 32

4.9.14 Kdo může požádat o pozastavení platnosti....33
4.9.15 Postup při žádosti o pozastavení platnosti....33
4.9.16 Omezení doby pozastavení platnosti....33
4.10 Služby ověřování stavu certifikátu....33
4.10.1 Funkční charakteristiky....33
4.10.2 Dostupnost služeb....33
4.10.3 Další charakteristiky služeb stavu certifikátu....33
4.11 Konec smlouvy o vydání certifikátu....33
4.12 Úschova a obnova klíčů....33
4.12.1 Politika a postupy při úschově a obnově klíčů....34
4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace....34
5 Postupy správy, řízení a provozu....35
5.1 Fyzická bezpečnost....35
5.1.1 Umístění a konstrukce....35
5.1.2 Fyzický přístup....35
5.1.3 Elektřina a klimatizace....35
5.1.4 Vlivy vody....35
5.1.5 Protipožární opatření a ochrana....36
5.1.6 Ukládání médií....36
5.1.7 Nakládání s odpady....36
5.1.8 Zálohy mimo budovu....36
5.2 Procedurální postupy....36
5.2.1 Důvěryhodné role....36
5.2.2 Počet osob požadovaných pro zajištění jednotlivých činností....36
5.2.3 Identifikace a autentizace pro každou roli....37
5.2.4 Role vyžadující rozdělení povinností....37
5.3 Personální postupy....37
5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost....37
5.3.2 Posouzení spolehlivosti osob....37
5.3.3 Požadavky na školení....38
5.3.4 Požadavky a periodicita doškolování....38
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi....38
5.3.6 Postihy za neoprávněné činnosti....38
5.3.7 Požadavky na nezávislé dodavatele....38
5.3.8 Dokumentace poskytovaná zaměstnancům....38

5.4 Postupy zpracování auditních záznamů 39
5.4.1 Typy zaznamenávaných událostí 39
5.4.2 Periodicita zpracování záznamů 39
5.4.3 Doba uchování auditních záznamů 39
5.4.4 Ochrana auditních záznamů 39
5.4.5 Postupy pro zálohování auditních záznamů 40
5.4.6 Systém shromažďování auditních záznamů (interní nebo externí) 40
5.4.7 Postup při oznamování události subjektu, který ji způsobil 40
5.4.8 Hodnocení zranitelnosti 40
5.5 Uchovávání záznamů 40
5.5.1 Typy uchovávaných záznamů 40
5.5.2 Doba uchování záznamů 40
5.5.3 Ochrana úložiště záznamů 41
5.5.4 Postupy při zálohování záznamů 41
5.5.5 Požadavky na používání časových razítek při uchovávání záznamů 41
5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí) 41
5.5.7 Postupy pro získání a ověření uchovávaných informací 41
5.6 Výměna klíče 41
5.7 Obnova po havárii nebo kompromitaci 42
5.7.1 Postup ošetření incidentu nebo kompromitace 42
5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat 42
5.7.3 Postup při kompromitaci soukromého klíče 42
5.7.4 Schopnost obnovit činnost po havárii 42
5.8 Ukončení činnosti CA nebo RA 42
6 Řízení technické bezpečnosti 43
6.1 Generování a instalace párových dat 43
6.1.1 Generování párových dat 43
6.1.2 Předávání soukromého klíče jeho držiteli 43
6.1.3 Předávání veřejného klíče vydavateli certifikátu 43
6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám 43
6.1.5 Délky klíčů 43
6.1.6 Parametry veřejného klíče a kontrola jeho kvality 44
6.1.7 Účely použití klíče (dle rozšíření key usage X.509 v3) 44
6.2 Ochrana soukromého klíče a technologie kryptografických modulů 44

6.2.1 Řízení a standardy kryptografických modulů 44
6.2.2 Soukromý klíč pod kontrolou více osob (n z m) 44
6.2.3 Úschova soukromého klíče....44
6.2.4 Zálohování soukromého klíče....44
6.2.5 Uchovávání soukromého klíče....44
6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu ..45
6.2.7 Uložení soukromého klíče v kryptografickém modulu 45
6.2.8 Postup aktivace soukromého klíče 45
6.2.9 Postup deaktivace soukromého klíče....45
6.2.10 Postup ničení soukromého klíče....45
6.2.11 Hodnocení kryptografických modulů....46
6.3 Další aspekty správy párových dat....46
6.3.1 Uchovávání veřejných klíčů....46
6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat....46
6.4 Aktivační data 46
6.4.1 Generování a instalace aktivačních dat 46
6.4.2 Ochrana aktivačních dat....46
6.4.3 Ostatní aspekty aktivačních dat....46
6.5 Řízení počítačové bezpečnosti....47
6.5.1 Specifické technické požadavky na počítačovou bezpečnost 47
6.5.2 Hodnocení počítačové bezpečnosti 47
6.6 Technické řízení životního cyklu....49
6.6.1 Řízení vývoje systému....49
6.6.2 Řízení správy bezpečnosti....49
6.6.3 Řízení životního cyklu bezpečnosti....49
6.7 Řízení bezpečnosti sítě....50
6.8 Označování časovými razítky....50
7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP....51
7.1 Profil certifikátu....51
7.1.1 Číslo verze 51
7.1.2 Rozšíření certifikátu....52
7.1.3 Objektové identifikátory algoritmů....52
7.1.4 Tvary jmen....52
7.1.5 Omezení jmen....52
7.1.6 Objektový identifikátor certifikační politiky....52
7.1.7 Použití rozšíření Policy Constraints 52

7.1.8 Syntaxe a sémantika kvalifikátorů politiky 53
7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies 53
7.2 Profil seznamu zneplatněných certifikátů 53
7.2.1 Číslo verze 53
7.2.2 Rozšíření CRL a záznamů v CRL 53
7.3 Profil OCSP 54
7.3.1 Číslo verze 54
7.3.2 Rozšíření OCSP 54
8 Hodnocení shody a jiná hodnocení 55
8.1 Periodicita nebo okolnosti hodnocení 55
8.2 Identita a kvalifikace hodnotitele 55
8.3 Vztah hodnotitele k hodnocenému subjektu 55
8.4 Hodnocené oblasti 55
8.5 Postup v případě zjištění nedostatků 55
8.6 Sdělování výsledků hodnocení 55
9 Ostatní obchodní a právní záležitosti 56
9.1 Poplatky 56
9.1.1 Poplatky za vydání nebo obnovení certifikátu 56
9.1.2 Poplatky za přístup k certifikátu 56
9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu 56
9.1.4 Poplatky za další služby 56
9.1.5 Postup při refundování 56
9.2 Finanční odpovědnost 56
9.2.1 Krytí pojištěním 56
9.2.2 Další aktiva 56
9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele 57
9.3 Důvěrnost obchodních informací 57
9.3.1 Rozsah důvěrných informací 57
9.3.2 Informace mimo rámec důvěrných informací 57
9.3.3 Odpovědnost za ochranu důvěrných informací 57
9.4 Ochrana osobních údajů 57
9.4.1 Politika ochrany osobních údajů 57
9.4.2 Informace považované za osobní údaje 57
9.4.3 Informace nepovažované za osobní údaje 58
9.4.4 Odpovědnost za ochranu osobních údajů 58
9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním 58

9.4.6 Poskytování osobních údajů pro soudní či správní účely 58
9.4.7 Jiné okolnosti zpřístupňování osobních údajů 58
9.5 Práva duševního vlastnictví 58
9.6 Zastupování a záruky 58
9.6.1 Zastupování a záruky CA 58
9.6.2 Zastupování a záruky RA 59
9.6.3 Zastupování a záruky držitele certifikátu 59
9.6.4 Zastupování a záruky spoléhajících se stran 59
9.6.5 Zastupování a záruky ostatních zúčastněných subjektů 59
9.7 Zřeknutí se záruk 59
9.8 Omezení odpovědnosti 59
9.9 Záruky a odškodnění 59
9.10 Doba platnosti, ukončení platnosti 59
9.10.1 Doba platnosti 59
9.10.2 Ukončení platnosti 60
9.10.3 Důsledky ukončení a přetrvání závazků 60
9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty 60
9.12 Novelizace 60
9.12.1 Postup při novelizaci 60
9.12.2 Postup a periodicita oznamování 60
9.12.3 Okolnosti, při kterých musí být změněn OID 60
9.13 Ustanovení o řešení sporů 60
9.14 Rozhodné právo 60
9.15 Shoda s platnými právními předpisy 61
9.16 Různá ustanovení 61
9.16.1 Rámcová dohoda 61
9.16.2 Postoupení práv 61
9.16.3 Oddělitelnost ustanovení 61
9.16.4 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv) 61
9.16.5 Vyšší moc 61
9.17 Další ustanovení 61
10 Závěrečná ustanovení 62

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.000	26.02.2024	Generální ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.001	12.09.2026	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace seznamu odkazovaných standardů. Upřesnění činností CA při vydávání certifikátu. Přihlášení se k požadavkům politiky CCADB. Zohlednění nového organizačního schématu. 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 certifikátů OCSP respondérů kořenové certifikační autority TLS a certifikačních autorit vydávajících certifikáty typu SSL/TLS (dále též Služba, Certifikát). Pro Službu poskytovanou podle této certifikační politiky (dále též CP) je využíván algoritmus RSA.

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.

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. technický standard, normu či právní předpis, který je nahrazuje. Pokud by byl tento dokument v rozporu se technickými standardy, normami nebo právními předpis, které nahradí dosud platné, bude vydána jeho nová verze.

1.1 Přehled

Dokument **Certifikační politika vydávání certifikátů OCSP respondérů TLS (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 technickým standardům a normám 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.

OCSP respondéry, provozované společností První certifikační autorita, a.s., jsou autorizovanými respondéry v souladu se standardem RFC 6960, tzn. certifikát veřejného klíče OCSP respondéru je vydán tou certifikační autoritou, která vydala certifikát koncovému uživateli, na jehož stav tento OCSP respondér odpovídá.

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 certifikátů OCSP respondérů TLS (algoritmus RSA), verze 1.001
OID politiky:	1.3.6.1.4.1.23624.10.1.81.1.0

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA”)

Kořenová certifikační autorita vydává v hierarchické dvoustupňové struktuře certifikačních autorit, v souladu s platnou právní úpravou a s požadavky technických standardů a norem, certifikáty pro jí podřízené certifikační autority.

Kořenová certifikační autorita TLS a podřízené certifikační autority vydávající certifikáty typu SSL/TLS (dále též Autorita, resp. Autority) vydávají certifikáty svým OCSP respondérům dle této CP.

1.3.2 Registrační autority (dále „RA”)

Na procesech životního cyklu certifikátů vydávaných dle této CP se podílí registrační autorita ve vlastnictví I.CA.

1.3.3 Držitelé certifikátů

Držitelem vydávaného Certifikátu je společnost První certifikační autorita, a.s., která požádala o vydání Certifikátu pro sebe a je 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, případně orgány dohledu a další, kterým to podle platné právní úpravy přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP smějí být používány výhradně pro ověřování odpovědí s využitím protokolu OCSP na stav certifikátu vydaného příslušnou certifikační autoritou.

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 generální ředitel I.CA. Platí kontaktní údaje uvedené v kapitole 2.2.

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených v 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)
kořenová CA	certifikační autorita vydávající certifikáty podřízeným certifikačním autoritám
kvalifikovaný certifikát pro elektronický podpis nebo pro elektronickou pečeť nebo pro autentizaci webových stránek	certifikát definovaný právní úpravou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů, resp. pečetí	prostředek pro vytváření elektronických podpisů, resp. pečetí, který splňuje požadavky stanovené v příloze II eIDAS
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
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
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
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 informace o společnosti První certifikační autorita, a.s., jsou:

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

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

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

Na výše uvedené internetové adrese lze získat informace o:

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

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

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

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

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,
- 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. Podporované položky tohoto pole 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 uváděné v žádosti o Certifikát (formát PKCS#10) se do pole subject ve vydávaných Certifikátech přenášejí ve tvaru, ve kterém jsou uvedeny v předkládané žádosti.

3.1.5 Jedinečnost jmen

Autorita zaručuje jedinečnost pole subject pro Certifikáty vydávané různými certifikačními autoritami.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Certifikáty vydané podle této CP mohou obsahovat pouze obchodní značky vlastněné společností První certifikační autorita, a.s.

3.2 Počáteční ověření identity

V následujících kapitolách jsou uvedena pravidla pro ověřování identity I.CA při žádosti o vydání Certifikátu a pro ověřování identity zástupce I.CA při vydání certifikátu.

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

Certifikáty vydávané dle této CP jsou vydávány pouze pro právnickou osobu I.CA. Její identita se prokazuje výpisem z Obchodního rejstříku.

3.2.3 Ověřování identity fyzické osoby

Kapitola popisuje způsob ověřování identity fyzické osoby, tj. osoby zastupující I.CA při podání žádosti o vydání Certifikátu.

V procesu ověřování identity osoby zastupující I.CA při vydání Certifikátu jsou vyžadovány dva doklady, primární a sekundární, obsahující údaje uvedené níže v této kapitole.

Primárním osobním dokladem pro občany ČR musí být platný občanský průkaz nebo cestovní pas. Primárním osobním dokladem pro cizince je platný cestovní pas, nebo jím v případě občanů členských států EU může být platný osobní doklad, sloužící k prokazování totožnosti na území příslušného státu.

Z tohoto dokladu jsou ověřovány následující údaje:

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

Sekundární osobní doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s primárním osobním dokladem a musí obsahovat alespoň jeden z následujících údajů:

- datum narození (nebo rodné číslo, je-li uvedeno),
- adresu trvalého bydliště,
- fotografii obličeje.

Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Všechny informace musí být řádným způsobem ověřeny.

3.2.5 Ověřování kompetencí

Není relevantní pro tento dokument.

3.2.6 Kritéria pro interoperabilitu

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

3.3 Identifikace a autentizace při požadavku na výměnu klíče

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Je nutné vydat nový Certifikát s novým veřejným klíčem. Platí stejné požadavky, jako v případě počátečního ověření identity.

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

Službu výměny klíče po zneplatnění Certifikátu I.CA nepodporuje. 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.

Žádost o zneplatnění Certifikátu musí být vždy písemná a podepsaná osobou zastupující I.CA při vydávání Certifikátu. Její identita musí být řádně ověřena primárním osobním dokladem.

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

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 osoba zastupující I.CA při vydání Certifikátu.

4.1.2 Registrační proces a odpovědnosti

Písemná žádost o vydání Certifikátu je předkládána vedení společnosti První certifikační autorita, a.s., prostřednictvím osoby zastupující I.CA při vydání Certifikátu a musí obsahovat název a OID této certifikační politiky, včetně uvedení jména Autority (tzv. commonName), která Certifikát vydá. Žádost musí být Osobou podepsána.

Osoba zastupující I.CA při vydání Certifikátu je povinna zejména:

- seznámit se s touto CP a 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:

- v procesu vydávání Certifikátu na RA ověřit všechny ověřitelné údaje uvedené v žádosti podle předložených dokladů,
- 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 vydané Certifikáty,
- činnosti spojené se Službou poskytovat v souladu s právní úpravou pro služby vytvářející důvěru, příslušnými technickými standardy a normami, 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 Certifikátu jsou identifikace a autentizace prováděny podle kapitol 3.2.2 a 3.2.3.

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

Na základě písemné žádosti rozhodne vedení společnosti První certifikační autorita, a.s., o vydání Certifikátu, případně o zamítnutí žádosti. Výsledek je dokumentován.

4.2.3 Doba zpracování žádosti o certifikát

Doba zpracování písemné žádosti o vydání Certifikátu nepřekročí pět pracovních dnů ode dne předložení žádosti vedení společnosti.

Po kladném rozhodnutí o vydání Certifikátu je I.CA povinna Certifikát vydat. Doba vydání Certifikátu nepřekročí jednotky minut.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání OCSP certifikátu kořenovou certifikační autoritou TLS provádějí pracovnice/pracovník (dále jen pracovníci) RA:

- kontroly, uvedené v kapitole 4.2.1,
- vizuální kontrolu shody údajů obsažených v žádosti o Certifikát (struktura PKCS#10),
- vizuální kontroly formální správnosti údajů.

Ověřování vlastnictví soukromého klíče, podporovaných hashovacích funkcí v žádosti o Certifikát (minimálně sha-256) a kontroly formální správnosti údajů jsou prováděny jak programovým vybavením umístěným na pracovní stanici pracovníka RA, tak programovým vybavením jádra systému CA. Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen.

V procesu vydávání OCSP certifikátu podřízenou certifikační autoritou:

- 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 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 uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

V procesu vydávání certifikátu OCSP respondéru podřízené certifikační autority vydávající certifikáty typu SSL/TLS je držitel tohoto certifikátu, resp. zástupce I.CA žádající o vydání tohoto certifikátu informován prostřednictvím pracovníka RA a zmíněný certifikát je zaslán na kontaktní e-mailovou adresu zadanou povinně při registraci. Uvedený postup informování neplatí pro případ vydávání certifikátu OCSP respondéru kořenové certifikační autority TLS, která je izolovaným systémem.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

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

4.4.2 Zveřejňování certifikátů certifikační autoritou

Certifikáty vydané podle této CP jsou zveřejněny způsobem podle bodu 2.2.

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 držitele Certifikátu mj. je:

- dodržovat veškerá relevantní ustanovení smlouvy o poskytování Služeb,
- užívat soukromý klíč a odpovídající Certifikát pouze pro účely stanovené v této CP,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v Certifikátu takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- neprodleně uvědomit poskytovatele Služby o skutečnostech, které vedou ke zneplatnění Certifikátu, zejména o:
  - podezření, že soukromý klíč byl zneužit, a
  - neplatnosti či nepřesnosti údajů v Certifikátu,

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

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny získat z bezpečného zdroje (www.ica.cz, pracoviště RA, případně z příslušného důvěryhodného seznamu) certifikáty certifikačních autorit související s Certifikátem vydaným podle této CP, ověřit hodnoty jejich otisků a jejich platnost.

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 s jiným veřejným klíčem, ale s totožným obsahem položek uvedených v poli subject Certifikátu, jehož veřejný klíč je předmětem výměny.

Služba výměny veřejného klíče v Certifikátu není poskytována.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.2 Kdo může žádat o výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Viz kapitola 4.7.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Viz kapitola 4.7.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.7.

4.8 Změna údajů v certifikátu

Službou změny údajů v Certifikátu je podle této CP míněno vydání nového Certifikátu s minimálně jednou změnou v obsahu položek uvedených v poli subject 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.

Služba změny údajů v Certifikátu není poskytována.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Zneplatnění Certifikátu znamená, že do doby vydání Certifikátu nového je služba OCSP respondéru příslušné Autority pozastavena.

Službu pozastavení platnosti Certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění

Certifikát musí být zneplatněn mj. na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče, odpovídajícího veřejnému klíči tohoto Certifikátu,
- technický obsah nebo formát Certifikátu představují neakceptovatelné riziko (např. daný kryptografický/podepisovací algoritmus nebo délka klíče),
- v případech, kdy nastanou skutečnosti uvedené v právní úpravě pro služby vytvářející důvěru, příslušných technických standardech a normám (např. neplatnost údajů v Certifikátu).

4.9.2 Kdo může požádat o zneplatnění

Žádost o zneplatnění Certifikátu mohou podat:

- držitel Certifikátu (oprávněným žadatelem o zneplatnění Certifikátu vydaného I.CA je v tomto případě osoba zastupující I.CA při vydání Certifikátu),
- případně orgán dohledu nebo další subjekty definované právní úpravou pro služby vytvářející důvěru.

4.9.3 Postup při žádosti o zneplatnění

Zneplatnění Certifikátu probíhá za osobní účasti osoby zastupující I.CA při vydání Certifikátu.

Písemná žádost o zneplatnění Certifikátu musí obsahovat sériové číslo Certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“), jméno Autority, která Certifikát vydala, 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 primárního osobního dokladu předloženého při žádosti o vydání Certifikátu, nebo čísla nového primárního osobního dokladu, pokud byl původní nahrazen novým. Tímto primárním osobním dokladem se musí prokázat.

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

Pokud žádost požadavky splňuje, odpovědný pracovník Certifikát v systému CA neprodleně zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku. CRL obsahující sériové číslo zneplatněného Certifikátu musí být vydán neprodleně po zneplatnění tohoto Certifikátu.

4.9.6 Povinnosti spoléhajících se stran při kontrole zneplatnění

Spoléhající se strany jsou povinny postupovat v souladu s kapitolou 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je vydáván po každém zneplatnění certifikátu vydaného příslušnou certifikační autoritou a dále v pravidelných intervalech, nejvýše čtyřiadvacet, zpravidla osm hodin (v případě podřízené certifikační autority vydávající certifikáty typu SSL/TLS), nebo nejvýše jeden rok, zpravidla půl roku (v případě kořenové certifikační autority TLS) 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

Není relevantní pro tento dokument, stav Certifikátu není ověřován on-line.

4.9.10 Požadavky při ověřování stavu certifikátu on-line

Viz kapitola 4.9.9.

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 formou zveřejňování informací.

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 (platný 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.

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

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 vydání certifikátu

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

4.12 Úschova a obnova klíčů

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

4.12.1 Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Viz kapitola 4.12.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Postupy správy, řízení a provozu jsou zaměřeny především na:

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

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

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

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

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

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

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

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

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 se službami vytvářejícími důvěru je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

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

5.5.1 Typy uchovávaných záznamů

I.CA uchovává níže uvedené záznamy (v elektronické nebo listinné podobě), které souvisejí se Službou, zejména:

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

5.5.2 Doba uchování záznamů

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

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště záznamů

Prostory, ve kterých se uchovávané záznamy nacházejí, jsou zabezpečeny 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 výrobním 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 na své internetové informační adrese, pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,
- oznámí orgánu dohledu informaci o zneplatnění příslušného certifikátu s uvedením důvodu.

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

Pravidla pro ukončování činnosti podřízených certifikačních autorit a jim příslušných RA jsou uvedena v CP, dle kterých se řídí jimi vydávané certifikáty.

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 těchto 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.

6.1.2 Předávání soukromého klíče jeho držiteli

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

Služba generování párových dat 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 4096 bitů, mohutnost klíčů OCSP respondérů certifikačních autorit 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.

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.

6.2.5 Uchovávání soukromého klíče

Soukromé klíče certifikačních autorit a jejich OCSP respondérů nejsou nikde uchovávány, po uplynutí doby platnosti jsou zničeny.

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

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.

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.

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.

6.2.9 Postup deaktivace soukromého klíče

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

Deaktivace soukromých klíčů pracovníků podílejících se na vydávání Certifikátů je provedena vyjmutím čipové karty ze snímače.

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.

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

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.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

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

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit 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.

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.

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 Služby je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů a jejich periodicity, definována relevantními 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.
- 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.
- 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 vydávaného Certifikátu – nejméně 64 bitů z generátoru náhodných čísel (používaného pro kryptosystémy) větší než nula
signatureAlgorithm	minimálně sha256WithRSAEncryption
issuer	vydavatel Certifikátu
validity	
notBefore	počátek platnosti Certifikátu (UTC)
notAfter	OCSP respondér kořenové CA TLS: notBefore + maximálně 365 dnů, resp. 366 dnů v případě přestupného roku (UTC) OCSP respondér podřízené CA vydávající certifikáty typu SSL/TSL: notBefore + maximálně 180 dnů (UTC)
subject	
countryName	CZ
organizationName	První certifikační autorita, a.s.
organizationIdentifier	NTRCZ-26439395
commonName	jméno OCSP respondéru*
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	minimálně 2048 bitů
extensions	viz tab. 5
signature	zaručená elektronická pečeť vydavatele Certifikátu

* Obsahuje jméno Autority (commonName) vydávající certifikát OCSP respondéru, následované řetězcem „ OCSP responder“.

7.1.1 Číslo verze

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

7.1.2 Rozšíření certifikátu

tab. 5 - Rozšíření Certifikátu[2]

Rozšíření	Obsah	Poznámka
basicConstraints		kritické, povinné
cA	False	
keyUsage	digitalSignature	kritické, povinné
extendedKeyUsage	id-kp-OCSPSigning	kritická, povinná
id-pkix-ocsp-nocheck	NULL	nekritické, povinné
subjectKeyIdentifier	hash veřejného klíče OCSP respondéru Autority	nekritické, povinné
authorityKeyIdentifier		nekritická, povinná
keyIdentifier	hash veřejného klíče Autority	

7.1.3 Objektové identifikátory algoritmů

V procesu poskytování služeb vytvářejících důvěru 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 dle této CP.

7.1.6 Objektový identifikátor certifikační politiky

Objektový identifikátor certifikační politiky je uveden v kapitole 1.2.

7.1.7 Použití rozšíření Policy Constraints

Není relevantní pro Certifikáty vydávané dle této CP.

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

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, není označeno jako kritické.

7.2 Profil seznamu zneplatněných certifikátů

tab. 6 - Profil CRL[3]

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. 7
crlExtensions	rozšíření CRL – viz tab. 7
signature	zaručená elektronická pečeť vydavatele CRL

* V případě certifikátu kořenové CA TLS thisUpdate + maximálně 365 dní, v případě certifikátu podřízené CA vydávající certifikáty typu SSL/TLS 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. 7 - Rozšíření CRL[4]

Rozšíření	Obsah	Poznámka
crlEntryExtensions		
CRLReason	důvod zneplatnění certifikátu	nekritické, volitelné

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

[4] 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

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; při zneplatnění certifikátu podřízené CA je uveden jiný důvod, než unspecified (0). 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

Hodnocení shody je popsáno v certifikační politice konkrétní služby využívající OCSP respondér.

8.1 Periodicita nebo okolnosti hodnocení

Viz kapitola 8.

8.2 Identita a kvalifikace hodnotitele

Viz kapitola 8.

8.3 Vztah hodnotitele k hodnocenému subjektu

Viz kapitola 8.

8.4 Hodnocené oblasti

Viz kapitola 8.

8.5 Postup v případě zjištění nedostatků

Viz kapitola 8.

8.6 Sdělování výsledků hodnocení

Viz kapitola 8.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Provozovatelem OCSP respondérů vydávajících Autorit je společnost První certifikační autorita, a.s., poplatky za vydávání certifikátů OCSP respondérů nejsou účtovány. Služba obnovení certifikátu OCSP respondéru 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 služeb vytvářejících důvěru 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.

9.3 Důvěrnost obchodních informací

9.3.1 Rozsah důvěrných informací

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

- veškeré soukromé klíče, sloužící v procesu poskytování služeb vytvářejících důvěru,
- 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.

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 Služby, jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče certifikačních autorit pouze pro vydávání certifikátů koncovým uživatelům (vyjma kořenové certifikační autority I.CA), vydávání seznamů jimi vydaných zneplatněných certifikátů a k vydávání certifikátů jejich OCSP respondérů,
- použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,
- certifikáty splňují náležitosti požadované příslušnými technickými standardy a normami,
- zneplatní certifikáty OCSP respondérů, pokud byla žádost o jejich zneplatnění podána způsobem definovaným v této CP.

9.6.2 Zastupování a záruky RA

Určená RA:

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost o Certifikát, pokud se nepodařilo ověřit některou z položek žádosti, nebo žadatel není oprávněn k podání žádosti o Certifikát.

9.6.3 Zastupování a záruky držitele certifikátu

Není relevantní pro tento dokument.

9.6.4 Zastupování a záruky spoléhajících se stran

Záruky spoléhajících se stran jsou popsány v certifikační politice konkrétní služby využívající OCSP respondér.

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 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

Není relevantní pro tento dokument, je uvedeno v certifikační politice konkrétní služby využívající OCSP respondér.

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

Komunikace mezi subjekty, které jsou organizačnímu částmi I.CA, se řídí interními pravidly I.CA.

Způsob komunikace se spoléhajícími se stranami je vždy uveden v certifikační politice konkrétní služby využívající OCSP respondér.

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interní dokumentaci.

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

Řešení sporů mezi organizačnímu částmi I.CA se řídí interními pravidly I.CA.

Řešení sporů se spoléhajícími se stranami je vždy popsáno v certifikační politice konkrétní služby využívající OCSP respondér.

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 poskytováním Služby provozován ve shodě s právními předpisy EU a České republiky a dále s relevantními mezinárodními standardy.

9.16 Různá ustanovení

Vždy popsáno v certifikační politice konkrétní certifikační služby využívající OCSP respondér.

9.16.1 Rámcová dohoda

Viz kapitola 9.16.

9.16.2 Postoupení práv

Viz kapitola 9.16.

9.16.3 Oddělitelnost ustanovení

Viz kapitola 9.16.

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

Viz kapitola 9.16.

9.16.5 Vyšší moc

Viz kapitola 9.16.

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

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