

První certifikační autorita, a.s.



Certifikační politika

kořenové kvalifikované certifikační autority

(algoritmus RSA)

Certifikační politika kořenové kvalifikované certifikační autority (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 1.14

OBSAH

1	Úvod	11
1.1	Přehled	11
1.2	Název a jednoznačné určení 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	12
1.3.5	Jiné participující subjekty	12
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	Přehled použitých pojmů a zkratk.....	13
2	Odpovědnost za zveřejňování a za úložiště	18
2.1	Úložiště	18
2.2	Zveřejňování certifikačních informací	18
2.3	Čas nebo četnost zveřejňování	19
2.4	Řízení přístupu k jednotlivým typům úložišť	19
3	Identifikace a autentizace	20
3.1	Pojmenování	20
3.1.1	Typy jmen.....	20
3.1.2	Požadavek na významovost jmen	20
3.1.3	Anonymita nebo používání pseudonymu držitele certifikátu.....	20
3.1.4	Pravidla pro interpretaci různých forem jmen.....	20
3.1.5	Jedinečnost jmen.....	20
3.1.6	Uznávání, ověřování a poslání obchodních značek	20
3.2	Počáteční ověření identity	20
3.2.1	Ověřování vlastnictví soukromého klíče.....	20
3.2.2	Ověřování identity organizace	21

3.2.3	Ověřování identity fyzické osoby	21
3.2.4	Neověřované informace o držiteli certifikátu	21
3.2.5	Ověřování kompetencí.....	21
3.2.6	Kritéria pro interoperabilitu.....	21
3.3	Identifikace a autentizace při požadavku na výměnu klíče	22
3.3.1	Identifikace a autentizace při běžném požadavku na výměnu klíče	22
3.3.2	Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu.....	22
3.4	Identifikace a autentizace při požadavku na zneplatnění certifikátu.....	22
4	Požadavky na životní cyklus certifikátu.....	23
4.1	Žádost o vydání certifikátu	23
4.1.1	Kdo může požádat o vydání certifikátu	23
4.1.2	Registrační proces a odpovědnosti.....	23
4.2	Zpracování žádosti o certifikát.....	23
4.2.1	Provádění identifikace a autentizace	23
4.2.2	Schválení nebo zamítnutí žádosti o certifikát	23
4.2.3	Doba zpracování žádosti o certifikát	24
4.3	Vydání certifikátu.....	24
4.3.1	Úkony CA v průběhu vydávání certifikátu	24
4.3.2	Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou	24
4.4	Převzetí vydaného certifikátu	24
4.4.1	Úkony spojené s převzetím certifikátu	24
4.4.2	Zveřejňování certifikátů certifikační autoritou	24
4.4.3	Oznámení o vydání certifikátu certifikační autoritou jiným subjektům.....	24
4.5	Použití párových dat a certifikátu.....	25
4.5.1	Použití soukromého klíče a certifikátu držitelem certifikátu	25
4.5.2	Použití veřejného klíče a certifikátu spoléhající se stranou	25
4.6	Obnovení certifikátu	25
4.6.1	Podmínky pro obnovení certifikátu.....	25
4.6.2	Kdo může žádat o obnovení	25
4.6.3	Zpracování požadavku na obnovení certifikátu.....	26
4.6.4	Oznámení o vydání nového certifikátu držiteli certifikátu.....	26
4.6.5	Úkony spojené s převzetím obnoveného certifikátu	26
4.6.6	Zveřejňování obnovených certifikátů certifikační autoritou	26
4.6.7	Oznámení o vydání certifikátu certifikační autoritou jiným subjektům.....	26

4.7	Výměna veřejného klíče v certifikátu	26
4.7.1	Podmínky pro výměnu veřejného klíče v certifikátu	26
4.7.2	Kdo může žádat o výměnu veřejného klíče v certifikátu.....	26
4.7.3	Zpracování požadavku na výměnu veřejného klíče v certifikátu.....	26
4.7.4	Oznámení o vydání nového certifikátu držiteli certifikátu.....	26
4.7.5	Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem.....	27
4.7.6	Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou	27
4.7.7	Oznámení o vydání certifikátu certifikační autoritou jiným subjektům.....	27
4.8	Změna údajů v certifikátu	27
4.8.1	Podmínky pro změnu údajů v certifikátu	27
4.8.2	Kdo může požádat o změnu údajů v certifikátu.....	27
4.8.3	Zpracování požadavku na změnu údajů v certifikátu	27
4.8.4	Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu.....	27
4.8.5	Úkony spojené s převzetím certifikátu se změněnými údaji	27
4.8.6	Zveřejňování certifikátů se změněnými údaji certifikační autoritou	27
4.8.7	Oznámení o vydání certifikátu certifikační autoritou jiným subjektům.....	28
4.9	Zneplatnění a pozastavení platnosti certifikátu	28
4.9.1	Podmínky pro zneplatnění	28
4.9.2	Kdo může požádat o zneplatnění	28
4.9.3	Postup při žádosti o zneplatnění.....	28
4.9.4	Prodleva při požadavku na zneplatnění certifikátu.....	28
4.9.5	Doba zpracování žádosti o zneplatnění	28
4.9.6	Povinnosti spoléhajících se stran při kontrole zneplatnění	29
4.9.7	Periodicita vydávání seznamu zneplatněných certifikátů	29
4.9.8	Maximální zpoždění při vydávání seznamu zneplatněných certifikátů.....	29
4.9.9	Dostupnost ověřování stavu certifikátu on-line.....	29
4.9.10	Požadavky při ověřování stavu certifikátu on-line	29
4.9.11	Jiné možné způsoby oznamování zneplatnění	29
4.9.12	Zvláštní postupy při kompromitaci klíče	29
4.9.13	Podmínky pro pozastavení platnosti certifikátu	29
4.9.14	Kdo může požádat o pozastavení platnosti.....	29
4.9.15	Postup při žádosti o pozastavení platnosti.....	29

4.9.16	Omezení doby pozastavení platnosti	30
4.10	Služby ověřování stavu certifikátu	30
4.10.1	Funkční charakteristiky	30
4.10.2	Dostupnost služeb	30
4.10.3	Další charakteristiky služeb stavu certifikátu	30
4.11	Konec smlouvy o vydávání certifikátů	30
4.12	Úschova a obnova klíčů	30
4.12.1	Politika a postupy při úschově a obnově klíčů	30
4.12.2	Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace	30
5	Postupy správy, řízení a provozu	31
5.1	Fyzická bezpečnost	31
5.1.1	Umístění a konstrukce	31
5.1.2	Fyzický přístup	31
5.1.3	Elektřina a klimatizace	31
5.1.4	Vlivy vody	31
5.1.5	Protipožární opatření a ochrana	31
5.1.6	Ukládání médií	32
5.1.7	Nakládání s odpady	32
5.1.8	Zálohy mimo budovu	32
5.2	Procedurální postupy	32
5.2.1	Důvěryhodné role	32
5.2.2	Počet osob požadovaných pro zajištění jednotlivých činností	32
5.2.3	Identifikace a autentizace pro každou roli	33
5.2.4	Role vyžadující rozdělení povinností	33
5.3	Personální postupy	33
5.3.1	Požadavky na kvalifikaci, praxi a bezúhonnost	33
5.3.2	Posouzení spolehlivosti osob	33
5.3.3	Požadavky na školení	34
5.3.4	Požadavky a periodičita doškolování	34
5.3.5	Periodičita a posloupnost rotace pracovníků mezi různými rolemi	34
5.3.6	Postihy za neoprávněné činnosti	34
5.3.7	Požadavky na nezávislé dodavatele	34
5.3.8	Dokumentace poskytovaná zaměstnancům	34
5.4	Postupy zpracování auditních záznamů	35
5.4.1	Typy zaznamenávaných událostí	35
5.4.2	Periodičita zpracování záznamů	35

5.4.3	Doba uchování auditních záznamů.....	35
5.4.4	Ochrana auditních záznamů.....	35
5.4.5	Postupy pro zálohování auditních záznamů.....	36
5.4.6	System shromažďování auditních záznamů (interní nebo externí).....	36
5.4.7	Postup při oznamování události subjektu, který ji způsobil.....	36
5.4.8	Hodnocení zranitelnosti.....	36
5.5	Uchovávání záznamů.....	36
5.5.1	Typy uchovávaných záznamů.....	36
5.5.2	Doba uchování záznamů.....	36
5.5.3	Ochrana úložiště záznamů.....	37
5.5.4	Postupy při zálohování záznamů.....	37
5.5.5	Požadavky na používání časových razítek při uchovávání záznamů.....	37
5.5.6	System shromažďování uchovávaných záznamů (interní nebo externí).....	37
5.5.7	Postupy pro získání a ověření uchovávaných informací.....	37
5.6	Výměna klíče.....	37
5.7	Obnova po havárii nebo kompromitaci.....	38
5.7.1	Postup ošetření incidentu nebo kompromitace.....	38
5.7.2	Poškození výpočetních prostředků, programového vybavení nebo dat.....	38
5.7.3	Postup při kompromitaci soukromého klíče.....	38
5.7.4	Schopnost obnovit činnost po havárii.....	38
5.8	Ukončení činnosti CA nebo RA.....	38
6	Řízení technické bezpečnosti.....	40
6.1	Generování a instalace párových dat.....	40
6.1.1	Generování párových dat.....	40
6.1.2	Předávání soukromého klíče jeho držiteli.....	40
6.1.3	Předávání veřejného klíče vydavateli certifikátu.....	40
6.1.4	Poskytování veřejného klíče CA spoléhajícím se stranám.....	40
6.1.5	Délky klíčů.....	41
6.1.6	Parametry veřejného klíče a kontrola jeho kvality.....	41
6.1.7	Účely použití klíče (dle rozšíření key usage X.509 v3).....	41
6.2	Ochrana soukromého klíče a technologie kryptografických modulů.....	41
6.2.1	Řízení a standardy kryptografických modulů.....	41
6.2.2	Soukromý klíč pod kontrolou více osob (n z m).....	41
6.2.3	Úschova soukromého klíče.....	41

6.2.4	Zálohování soukromého klíče	41
6.2.5	Uchovávání soukromého klíče.....	41
6.2.6	Transfer soukromého klíče do nebo z kryptografického modulu	42
6.2.7	Uložení soukromého klíče v kryptografickém modulu	42
6.2.8	Postup aktivace soukromého klíče	42
6.2.9	Postup deaktivace soukromého klíče.....	42
6.2.10	Postup ničení soukromého klíče	42
6.2.11	Hodnocení kryptografických modulů.....	43
6.3	Další aspekty správy párových dat	43
6.3.1	Uchovávání veřejných klíčů	43
6.3.2	Doba funkčnosti certifikátu a doba použitelnosti párových dat	43
6.4	Aktivační data	43
6.4.1	Generování a instalace aktivačních dat	43
6.4.2	Ochrana aktivačních dat.....	43
6.4.3	Ostatní aspekty aktivačních dat	43
6.5	Řízení počítačové bezpečnosti.....	43
6.5.1	Specifické technické požadavky na počítačovou bezpečnost	43
6.5.2	Hodnocení počítačové bezpečnosti	43
6.6	Technické řízení životního cyklu.....	45
6.6.1	Řízení vývoje systému.....	45
6.6.2	Řízení správy bezpečnosti.....	45
6.6.3	Řízení životního cyklu bezpečnosti.....	46
6.7	Řízení bezpečnosti sítě	46
6.8	Označování časovými razítky.....	46
7	Profily certifikátu, seznamu zneplatněných certifikátů a OCSP.....	47
7.1	Profil certifikátu.....	47
7.1.1	Číslo verze	50
7.1.2	Rozšíření certifikátu.....	50
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	52
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.....	56
9	Ostatní obchodní a právní záležitosti.....	57
9.1	Poplatky	57
9.1.1	Poplatky za vydání nebo obnovení certifikátu	57
9.1.2	Poplatky za přístup k certifikátu	57
9.1.3	Zneplatnění nebo přístup k informaci o stavu certifikátu	57
9.1.4	Poplatky za další služby	57
9.1.5	Postup při refundování.....	57
9.2	Finanční odpovědnost.....	57
9.2.1	Krytí pojištěním.....	57
9.2.2	Další aktiva.....	57
9.2.3	Pojištění nebo krytí zárukou pro koncové uživatele	58
9.3	Důvěrnost obchodních informací.....	58
9.3.1	Rozsah důvěrných informací	58
9.3.2	Informace mimo rámec důvěrných informací	58
9.3.3	Odpovědnost za ochranu důvěrných informací.....	58
9.4	Ochrana osobních údajů	58
9.4.1	Politika ochrany osobních údajů	58
9.4.2	Informace považované za osobní údaje	58
9.4.3	Informace nepovažované za osobní údaje.....	58
9.4.4	Odpovědnost za ochranu osobních údajů.....	59
9.4.5	Oznámení o používání osobních údajů a souhlas s jejich zpracováním.....	59
9.4.6	Poskytování osobních údajů pro soudní či správní účely	59
9.4.7	Jiné okolnosti zpřístupňování osobních údajů.....	59
9.5	Práva duševního vlastnictví.....	59

9.6	Zastupování a záruky	59
9.6.1	Zastupování a záruky CA	59
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	60
9.6.5	Zastupování a záruky ostatních zúčastněných subjektů	60
9.7	Zřeknutí se záruk	60
9.8	Omezení odpovědnosti	60
9.9	Záruky a odškodnění	60
9.10	Doba platnosti, ukončení platnosti	60
9.10.1	Doba platnosti	60
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	61
9.12.1	Postup při novelizaci	61
9.12.2	Postup a periodicita oznamování	61
9.12.3	Okolnosti, při kterých musí být změněn OID	61
9.13	Ustanovení o řešení sporů	61
9.14	Rozhodné právo	61
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	Zřeknutí se práv	62
9.16.5	Vyšší moc	62
9.17	Další ustanovení	62
10	Závěrečná ustanovení	63

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.0	18.05.2015	Ředitel společnosti certifikační autorita, a.s.	První vydání.
1.10	01.02.2017	Ředitel společnosti certifikační autorita, a.s.	Úprava dle požadavků legislativy pro služby vytvářející důvěru.

1.11	06.04.2017	Ředitel společnosti certifikační autorita, a.s.	První	Zpřesnění formulací.
1.12	30.04.2018	Ředitel společnosti certifikační autorita, a.s.	První	Pravidelná revize textu, oprava formálních chyb.
1.13	30.04.2019	Ředitel společnosti certifikační autorita, a.s.	První	Pravidelná revize textu, oprava formálních chyb.
1.14	15.04.2020	Generální ředitel společnosti První certifikační autorita, a.s.		Pravidelná revize textu, oprava formálních chyb.

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 kořenovou certifikační autoritou (dále též Služba, Certifikát). Pro Službu poskytovanou podle této certifikační politiky (dále též CP) je využíván kryptografický algoritmus RSA (dále též 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 (eIDAS),
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

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

1.1 Přehled

Dokument **Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)**, dále též CP, vypracovaný společností První certifikační autorita, a. s., (dále též I.CA) se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu Certifikátů a striktně 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.

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

1.2 Název a jednoznačné určení dokumentu

Název tohoto dokumentu: Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA), verze 1.14

OID politiky: 1.3.6.1.4.1.23624.10.1.10.1.1

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA“)

Kořenová certifikační autorita (dále též 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 a pro OCSP respondér Autority.

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

1.3.2 Registrační autority (dále „RA“)

Na procesech životního cyklu Autoritou vydávaných Certifikátů se podílí speciální (neveřejná) 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 Autoritou podle této CP smějí být používány výhradně pro ověřování:

- elektronických značek/pečetí jí vydaných Certifikátů, seznamů zneplatněných certifikátů Autority (CRL) a OCSP odpovědí respondéru Autority,
- elektronických značek/pečetí certifikátů a seznamů zneplatněných certifikátů (CRL) vydaných podřízenými certifikačními autoritami a OCSP odpovědí vydaných OCSP respondéry podřízených certifikačních autorit.

1.4.2 Zakázané použití certifikátu

Certifikáty vydávané Autoritou 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 osoba společnosti První certifikační autorita, a.s., v souvislosti s touto CP, resp. s odpovídající CPS, je uvedena na internetové adrese - viz kapitola 2.2.

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených v 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 Přehled použitých pojmů a zkratk

tab. 2 - Pojmy

Pojem	Vysvětlení
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
elektronická značka	elektronická značka dle zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
elektronický podpis	zaručený elektronický podpis, nebo kvalifikovaný elektronický podpis, nebo uznávaný elektronický podpis dle právní úpravy pro služby vytvářející důvěru
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, případně svému OCSP respondéru
kvalifikovaná služba vytvářející důvěru	služba vytvářející důvěru, která splňuje požadavky stanovené v eIDAS
kvalifikovaný certifikát pro elektronický podpis	certifikát definovaný právní úpravou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů	prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II eIDAS
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
orgán dohledu	subjekt dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru
párová data	soukromý a jemu odpovídající veřejný klíč
písemná smlouva	text smlouvy v elektronické nebo listinné podobě
právní úprava pro služby vytvářející důvěru	platné právní předpisy České republiky vztahující se ke službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
smluvní partner	poskytovatel vybraných služeb vytvářejících důvěru, který zajišťuje na základě písemné smlouvy pro I.CA služby vytvářející důvěru nebo jejich části - nejčastěji se jedná o smluvní RA
soukromý klíč	jedinečná data pro vytváření elektronického podpisu/značky/pečetě
spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát
veřejný klíč	jedinečná data pro ověřování elektronického podpisu/značky/pečetě
vydávající, podřízená CA	pro účely tohoto dokumentu CA vydávající certifikáty koncovým uživatelům
zákon o ochraně	zákon České republiky č. 412/2005 Sb., o ochraně

utajovaných informací	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
BIH	Bureau International de l'Heure, (anglicky The International Time Bureau), Mezinárodní časová služba
bit	z anglického <i>binary digit</i> - číslice dvojkové soustavy - základní a současně nejmenší jednotka informace v číslicové technice
CA	certifikační autorita
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
ČR	Česká republika
ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátů
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
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
EZS	elektronická zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
GDPR	Global 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)
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.
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
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
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
MPSV	Ministerstvo práce a sociálních věcí
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
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
PUB	Publication, označení standardu FIPS
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu nebo pečetě
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)
sha, SHA	typ hashovací funkce
TS	Technical Specification, typ ETSI standardu
TSA	Time Stamp Authority, autorita časových razítek

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)
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., případně odkazy pro zjištění dalších informací, jsou:

- adresa sídla společnosti:
První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Praha 9
Česká republika
- internetová adresa <http://www.ica.cz>,
- sídla registračních autorit.

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

Na výše uvedené internetové adrese lze získat informace o:

- 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 a prováděcích směrnicích, vydaných a zneplatněných certifikátech 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 sloužících v procesech vydávání certifikátů koncovým uživatelům, vydávání seznamů zneplatněných certifikátů a poskytování informací o stavu certifikátů (dále též infrastrukturní certifikáty) 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.

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 infrastrukturního certifikátu, 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 procesu žádosti o certifikát se do vydávaných certifikátů přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokumentech.

3.1.5 Jedinečnost jmen

Autorita zaručuje jedinečnost polí subject a issuer v Certifikátu.

3.1.6 Uznávání, ověřování a posláním obchodních značek

Certifikáty vydávané 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 počáteční ověřování identity organizace žádající o vydání Certifikátu a pro ověřování identity zástupce této organizace.

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/značkou a držitel soukromého klíče tak prokazuje, že v době tvorby elektronické pečetě/značky soukromý klíč vlastnil.

3.2.2 Ověřování identity organizace

Musí být předložen originál nebo úředně ověřená kopie výpisu z obchodního nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny, resp. jiného dokladu stejné právní váhy.

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

3.2.3 Ověřování identity fyzické osoby

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

V procesu ověřování identity osoby zastupující I.CA 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 o 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

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

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Subjekty oprávněné podat žádost o zneplatnění Certifikátu jsou vyjmenovány v kapitole 4.9.2.

Žádost o zneplatnění Certifikátu musí být vždy písemná a podepsaná generálním ředitelem I.CA, nebo jím pověřenou osobou. Jejich identita musí být řádně ověřena primárním osobním dokladem. Pokud pověřená osoba není osobou ze zákona oprávněnou k zastupování společnosti I.CA, je dále požadována úředně ověřená plná moc k zastupování společnosti podepsaná statutárním zástupcem.

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 generální ředitel společnosti První certifikační autorita, a.s.

4.1.2 Registrační proces a odpovědnosti

Písemná žádost o vydání Certifikátu je předkládána vedení společnosti První certifikační autorita, a.s., generálním ředitelem I.CA a musí obsahovat název a OID této certifikační politiky, včetně uvedení požadovaného jména CA (tzv. commonName). Žádost musí být generálním ředitelem I.CA podepsána.

Držitel soukromého klíče, resp. držitel Certifikátu je povinen 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 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 CA a TSA 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 s příslušným obsahem pole subject, resp. issuer, 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 od 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 Certifikátu provádějí operátorky/operátoři, dále jen operátoři, CA:

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

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

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

V procesu vydávání Certifikátu je držitel Certifikátu, resp. zástupce I.CA žádající o vydání Certifikátu informován prostřednictvím pracovníka RA, resp. CA.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

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

4.4.2 Zveřejňování certifikátů certifikační autoritou

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

Certifikát kořenové certifikační autority a certifikáty podřízených certifikačních autorit související s kvalifikovanými službami vytvářejícími důvěru jsou předány orgánu dohledu.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

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

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností držitelů Certifikátů je zejména:

- dodržovat veškerá relevantní ustanovení smlouvy o poskytování této Služby,
- užívat soukromý klíč a odpovídající Certifikát vydaný podle této CP pouze pro účely stanovené v této CP a právní úpravou pro služby vytvářející důvěru,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v Certifikátu vydaném podle této CP, takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- neprodleně uvědomit poskytovatele Služby o skutečnostech, které vedou ke zneplatnění Certifikátu, zejména o:
 - podezření, že soukromý klíč byl zneužit, nebo
 - 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 certifikáty certifikačních autorit (internetová adresa uvedená v kapitole 2.2, pracoviště RA, důvěryhodný seznam ČR, internetová adresa orgánu dohledu, případně věstník příslušného orgánu dohledu) a ověřit kontrolní součet těchto certifikátů,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že Certifikáty nebyly zneplatněny.

4.6 Obnovení certifikátu

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

Služba obnovení Certifikátu není poskytována.

V případě této CP se vždy jedná o vydání nového Certifikátu s novým veřejným klíčem, kdy všechny informace musí být řádným způsobem ověřeny. Platí stejné požadavky jako v případě počátečního ověření identity - viz kapitola 3.2.

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 certifikátů certifikačních autorit není poskytována.

V případě této CP se vždy jedná o vydání nového certifikátu certifikační autority s novým veřejným klíčem, kdy všechny informace musí být řádným způsobem ověřeny. Platí stejné požadavky jako v případě počátečního ověření identity - viz kapitola 3.2.

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 stejný jako v Certifikátu, který je předmětem změny.

Služba změny údajů v Certifikátu není poskytována.

V případě této CP se vždy jedná o vydání nového Certifikátu s novým veřejným klíčem, kdy všechny informace musí být řádným způsobem ověřeny. Platí stejné požadavky jako v případě počátečního ověření identity - viz kapitola 3.2.

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

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 nebo příslušných technických standardech a normám.

4.9.2 Kdo může požádat o zneplatnění

Žádost o zneplatnění Certifikátu mohou podat:

- držitel Certifikátu (oprávněným žadatelem o zneplatnění Certifikátu je v tomto případě generální ředitel I.CA, nebo jím pověřený pracovník),
- 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 generálního ředitele I.CA nebo jím pověřeného pracovníka.

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 fyzické osoby oprávněné žádat zneplatnění Certifikátu a heslo pro zneplatnění Certifikátu. Pokud fyzická osoba oprávněná žádat zneplatnění Certifikátu heslo pro zneplatnění nezná, musí tuto skutečnost do písemné žádosti explicitně uvést.

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 vydaných dle této CP je vydáván po každém zneplatnění Certifikátu a dále v pravidelných intervalech, nejvýše jeden rok od vydání předchozího CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL je vždy vydán nejvýše jeden rok od vydání předchozího CRL.

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Služba ověřování stavu certifikátu podřízené certifikační autority s využitím protokolu OCSP je veřejně dostupná. Každý certifikát podřízené certifikační autority, vydaný podle této CP, obsahuje odkaz na příslušný OCSP respondér.

OCSP odpovědi vyhovují normám RFC 2560 a RFC 5019. Certifikát OCSP respondéru obsahuje rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 2560.

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, jiná služba oznamování zneplatnění certifikátu není poskytována.

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 vydaných Autoritou jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaných certifikátech.

Skutečnost, že Autorita poskytuje informace o stavu Certifikátu formou OCSP (služba OCSP), je uvedena v jí vydaných Certifikátech.

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 (platné 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 vydávání certifikátů

Po ukončení platnosti smlouvy o vydávání certifikátů přetrvávají z ní vyplývající závazky I.CA, a to po dobu platnosti posledního podle ní vydaného certifikátu.

4.12 Úschova a obnova klíčů

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

4.12.1 Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Viz kapitola 4.12.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Postupy správy, řízení a provozu jsou zaměřeny především na:

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

Postupy správy, řízení a provozu jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, Systémová bezpečnostní politika CA a TSA, Certifikační prováděcí směrnice, Plán pro zvládnutí 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 stoupačkou vodou. Provozní pracoviště jsou podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou

umístěny důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru, 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.

Papírová média, která je nutno dle právní úpravy pro služby vytvářející důvěru uchovávat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

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.

Všichni zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, které by mohly 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 OCSP respondéru kořenové certifikační autority,
- ničení soukromých klíčů veškerých certifikačních autorit a OCSP respondéru kořenové certifikační autority,
- zálohování soukromých klíčů certifikačních autorit, vydávajících kvalifikované certifikáty koncovým uživatelům, včetně kořenové certifikační autority,
- obnovu soukromých klíčů veškerých certifikačních autorit a jejich OCSP respondérů,
- aktivaci a deaktivaci soukromých klíčů veškerých certifikačních autorit a OCSP respondéru kořenové certifikační autority.

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 interní dokumentací.

5.3 Personální postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

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

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

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

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

Pro vykonávání řídicí 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 předemných 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 interní dokumentací a řídicím 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 Autority. Celý proces probíhá v souladu s právní úpravou pro služby vytvářející důvěru a s relevantními technickými standardy a normami, přičemž minimálně platí, že:

- je prováděno podle připraveného scénáře ve fyzicky zabezpečeném prostředí,
- dále:
 - je mu osobně přítomen auditor kvalifikovaný v souladu s platnými technickými standardy, nebo
 - je pořizován videozáznam a podle možnosti je generování přítomen notář, který o průběhu sepíše osvědčení,
- na základě osobní přítomnosti, nebo videozáznamu a případného osvědčení vystaví auditor, kvalifikovaný v souladu s platnými technickými standardy, zprávu, že Autorita při generování párových dat postupovala v souladu s připraveným scénářem a o opatřeních pro zajištění integrity a důvěrnosti.

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 interní dokumentací, 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 10 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, každá kopie je umístěna v jiné místnosti provozního pracoviště. Minimálně jedenkrát měsíčně se provádí uložení těchto auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

Auditní záznamy v papírové formě jsou umístěny mimo provozní prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je popsána interní dokumentací.

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 interní dokumentací.

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 typy záznamů (v elektronické nebo listinné podobě), které souvisejí s poskytovanými službami vytvářejícími důvěru, zejména:

- zprávu auditora o průběhu generování párových dat Autority,
- případný videozáznam průběhu generování párových dat Autority, resp. osvědčení notáře o průběhu generování párových dat Autority,
- záznamy související s životním cyklem Certifikátů,
- další záznamy potřebné pro vydávání Certifikátů,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování záznamů

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

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště záznamů

Prostory, ve kterých se uchovávané záznamy nacházejí, jsou zabezpečeny způsobem vycházejícím z požadavků provedené analýzy rizik a ze zákona o ochraně utajovaných informací.

Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

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

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

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

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

5.5.7 Postupy pro získání a ověření uchovávaných informací

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

V případě standardních situací (uplynutí platnosti certifikátů certifikačních autorit) je výměna s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) prováděna 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 příslušné platné certifikáty,
- bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese, pro zpřístupnění této informace je využít i seznam zneplatněných certifikátů,
- případně oznámí orgánu dohledu informaci o zneplatnění příslušného certifikátu s uvedením důvodu.

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

5.7.4 Schopnost obnovit činnost po havárii

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

5.8 Ukončení činnosti CA nebo RA

Pro ukončování činnosti Autority platí následující pravidla:

- ukončení činnosti Autority musí být písemně oznámeno orgánu dohledu a subjektům, které mají s I.CA uzavřenou smlouvu přímo se vztahující k poskytování služeb,
- ukončení činnosti Autority musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- pokud je součástí ukončení činnosti Autority ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně uvedení důvodu ukončení platnosti,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchování a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity služeb,

- po dobu platnosti i jen jediného certifikátu vydaného Autoritou musí Autorita či její nástupce v případě zániku zajistit alespoň služby zneplatňování Certifikátů a vydávání CRL,
- následně Autorita prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván podle pravidel této CP, a bude ukončena činnost i jí příslušné RA (kap. 1.3.2).

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

V případě odnětí statutu kvalifikovaného poskytovatele Služby:

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

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat Autority, které probíhá v souladu s právní úpravou pro služby vytvářející důvěru a s relevantními technickými standardy a normami ve vyhrazeném prostoru provozního pracoviště a o jehož průběhu je vyhotovena písemná zpráva, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 úroveň 3. Podrobnosti viz kapitola 5.4.1.

Generování párových dat OCSP respondérů Autority, které probíhá ve vyhrazeném prostoru provozního pracoviště, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 úroveň 3.

Generování párových dat podřízených certifikačních autorit, které probíhá v souladu s právní úpravou pro služby vytvářející důvěru a s relevantními technickými standardy a normami v zabezpečených vyhrazených prostorách provozních pracovišť, podle předem připraveného scénáře a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS PUB 140-2 úroveň 3.

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.

Veškeré požadavky na proces generování těchto párových dat jsou popsány interní dokumentací.

6.1.2 Předávání soukromého klíče jeho držiteli

Není relevantní pro tento dokument, soukromé klíče Autority, jejího OCSP respondéru a podřízených certifikačních autorit jsou uloženy v kryptografickém modulu.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Veřejný klíč je Autoritě doručen v žádosti (formát PKCS#10) o vydání Certifikátu.

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

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

- obdržení na RA,
- prostřednictvím internetových informačních adres I.CA a příslušného orgánu dohledu, případně prostřednictvím věstníku příslušného orgánu dohledu,
- každý žadatel o certifikát obdrží kořenový certifikát Autority při získání svého prvotního certifikátu.

6.1.5 Délky klíčů

Certifikační autority využívají asymetrický algoritmus RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) Autority je 4096 bitů, mohutnost klíčů (resp. parametrů daného algoritmu) jí vydávaných Certifikátů je minimálně 2048 bitů.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejného klíče Autority a jí vydávaných Certifikátů splňují požadavky uvedené v právní úpravě pro služby vytvářející důvěru, resp. v ní odkazovaných technických standardech nebo normách.

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 Autority, jejího OCSP respondéru a podřízených certifikačních autorit a uložení odpovídajících soukromých klíčů probíhá v kryptografickém modulu, který splňuje požadavky právní úpravy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3.

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

Pokud je pro činnosti spojené s kryptografickým modulem nezbytná přítomnost dvou členů vedení I.CA, pak každý z nich zná část pouze 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

Kryptografický modul použitý pro správu párových dat Autority, jejího OCSP respondéru a podřízených certifikačních autorit umožňuje zálohování soukromých klíčů. Soukromé klíče jsou zálohovány s využitím nativních prostředků kryptografického modulu v zašifrované podobě.

6.2.5 Uchovávání soukromého klíče

Po uplynutí doby platnosti soukromých klíčů Autority, jejího OCSP respondéru a podřízených certifikačních autorit jsou tyto včetně záloh zničeny.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Transfer soukromého klíče Autority z a do kryptografického modulu probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA.

Transfer soukromého klíče OCSP respondéru Autority z kryptografického modulu probíhá za přímé osobní účasti nejméně jednoho člena vedení I.CA.

Transfer soukromého klíče OCSP respondéru Autority do kryptografického modulu probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA.

Transfer soukromých klíčů podřízených certifikačních autorit vydávajících kvalifikované certifikáty koncovým uživatelům v souladu s legislativou pro služby vytvářející důvěru z a do kryptografického modulu probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA.

Transfer soukromých klíčů ostatních podřízených certifikačních autorit z kryptografického modulu probíhá za přímé osobní účasti nejméně jednoho člena vedení I.CA.

Transfer soukromých klíčů ostatních podřízených certifikačních autorit do kryptografického modulu probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA.

O provedeném transferu je vždy pořízen písemný záznam.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče Autority, jejího OCSP respondéru a podřízených certifikačních autorit jsou uloženy v kryptografickém modulu, splňujícím požadavky právní úpravy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3.

6.2.8 Postup aktivace soukromého klíče

Aktivace soukromých klíčů Autority, jejího OCSP respondéru a podřízených certifikačních autorit uložených v kryptografickém modulu je prováděna za přímé osobní účasti nejméně dvou členů vedení I.CA s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené aktivaci je pořízen písemný záznam.

6.2.9 Postup deaktivace soukromého klíče

Deaktivace soukromých klíčů Autority, jejího OCSP respondéru a podřízených certifikačních autorit uložených v kryptografickém modulu je prováděna za přímé osobní účasti nejméně dvou členů vedení I.CA s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené deaktivaci je pořízen písemný záznam.

6.2.10 Postup ničení soukromého klíče

Ničení soukromých klíčů Autority, jejího OCSP respondéru a podřízených certifikačních autorit uložených v kryptografickém modulu je realizováno nativními prostředky tohoto kryptografického modulu a za přímé osobní účasti nejméně dvou členů vedení I.CA podle přesně určeného postupu, který je upraven interní dokumentací. O provedeném ničení je pořízen písemný záznam.

Externí média, na kterých jsou uloženy zálohy výše uvedených soukromých klíčů, jsou rovněž zničena. Ničení, spočívající ve fyzické destrukci těchto nosičů, probíhá za přímé osobní účasti nejméně dvou členů I.CA podle přesně určeného postupu, který je upraven interní dokumentací. O provedeném ničení je pořízen písemný záznam.

6.2.11 Hodnocení kryptografických modulů

Kryptografický modul, sloužící ke generování párových dat a uložení soukromých klíčů Autority, jejího OCSP respondéru a podřízených certifikačních autorit splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3. Bezpečnost modulů je sledována po celou dobu jejich využívání.

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.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data Autority, jejího OCSP respondéru a podřízených certifikačních autorit jsou vytvářena v průběhu generování odpovídajících párových dat.

6.4.2 Ochrana aktivačních dat

Aktivační data Autority, jejího OCSP respondéru a podřízených certifikačních autorit jsou chráněna způsobem popsáným interní dokumentací.

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data soukromých klíčů Autority, jejího OCSP respondéru a podřízených certifikačních autorit nesmí přenášena nebo uchovávána v otevřené podobě. Veškeré aspekty jsou popsány interní dokumentací.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování služeb vytvářejících důvěru je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů a jejich periodicity, definována právní úpravou pro služby vytvářející důvěru, resp. v ní odkazovanými 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 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatelů důvěryhodných služeb - Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - 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.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ČSN 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.

Činnost Autority se dále řídí požadavky technických standardů a norem:

- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- 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 2560 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.
- 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.

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 ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.

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

Informační systém Autority je ve stavu off-line a není tedy propojen s žádnou externí sítí, ve stavu on-line je pouze OCSP respondér Autority. Ten je, stejně jako zbývající síťová infrastruktura provozního pracoviště, chráněn komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System). Detailní řešení řízení síťové bezpečnosti je popsáno interní dokumentací.

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 - Certifikát Autority

Pole	Obsah	Poznámka
version	v3 (0x2)	
serialNumber	jedinečné sériové číslo vydávaného certifikátu	
signatureAlgorithm	sha512WithRSAEncryption	
issuer		
commonName	I.CA Root CA/RSA MM/RRRR	MM/RRRR: měsíc a rok vydání certifikátu kořenové CA, uvedeno v certifikátu vydaném od data účinnosti politiky verze 1.10
organizationName	První certifikační autorita, a.s.	
country	CZ	
serialNumber	NTRCZ-26439395	položka je obsažena v certifikátu vydaném před datem účinnosti politiky verze 1.10
organizationIdentifier	NTRCZ-26439395	položka je obsažena v certifikátu vydaném od data účinnosti politiky verze 1.10
validity		
notBefore	datum vydání	UTC
notAfter	datum vydání + 25 let	UTC
subject		
commonName	I.CA Root CA/RSA MM/RRRR	MM/RRRR: měsíc a rok vydání certifikátu kořenové CA, uvedeno

		v certifikátu vydaném od data účinnosti politiky verze 1.10
organizationName	První certifikační autorita, a.s.	
country	CZ	
serialNumber	NTRCZ-26439395	položka je obsažena v certifikátu vydaném před datem účinnosti politiky verze 1.10
organizationIdentifier	NTRCZ-26439395	položka je obsažena v certifikátu vydaném od data účinnosti politiky verze 1.10
subjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	veřejný klíč (4096 bitů)	
extensions	rozšíření certifikátu	viz tab. 7
signature	elektronická značka, resp. zaručená elektronická pečeť Autority	

tab. 5 - Certifikát podřízené certifikační autority

Pole	Obsah	Poznámka
version	v3 (0x2)	
serialNumber	jedinečné sériové číslo vydávaného certifikátu	
signatureAlgorithm	sha256WithRSAEncryption	
issuer	vydavatel certifikátu	viz tab. 4
validity		
notBefore	datum vydání	UTC
notAfter	datum vydání+10 let	UTC
subject		
commonName	jméno podřízené certifikační autority	součástí je řetězec <i>MM/RRRR</i> : měsíc a rok vydání certifikátu podřízené

		certifikační autority
organizationName	První certifikační autorita, a.s.	
country	CZ	
serialNumber	NTRCZ-26439395	položka je obsažena v certifikátu vydaném před datem účinnosti politiky verze 1.10
organizationIdentifier	NTRCZ-26439395	položka je obsažena v certifikátu vydaném od data účinnosti politiky verze 1.10
subjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	veřejný klíč (minimálně 2048 bitů)	
extensions	rozšíření certifikátu	viz tab. 8
signature	elektronická značka, resp. zaručená elektronická pečeť Autority	

tab. 6 - Certifikát OCSP respondéru Autority

Pole	Obsah	Poznámka
version	v3 (0x2)	
serialNumber	jedinečné sériové číslo vydávaného certifikátu	
signatureAlgorithm	sha256WithRSAEncryption	
issuer	vydavatel certifikátu	viz tab. 4
validity		
notBefore	datum vydání	UTC
notAfter	datum vydání + maximálně 365 dnů, resp. 366 dnů v případě přestupného roku	UTC
subject		
commonName	jméno OCSP respondéru*	
organizationName	První certifikační autorita, a.s.	
countryName	CZ	
serialNumber	NTRCZ-26439395	položka je obsažena v certifikátu

		vydaném podle politiky verze 1.0
organizationIdentifier	NTRCZ-26439395	položka je obsažena v certifikátu vydaném podle politiky verze 1.10 a vyšší
subjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	veřejný klíč (minimálně 2048 bitů)	
extensions	rozšíření certifikátu	viz tab. 9
signature	elektronická značka, resp. zaručená elektronická pečeť Autority	

* Obsahující jméno (commonName) Autority 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. 7 - Rozšíření certifikátu Autority

Rozšíření	Obsah	Poznámka
certificatePolicies		nekritické
policyIdentifier	2.5.29.32.0 (anyPolicy)	
userNotice	Tento kvalifikovaný systémový certifikát byl vydán podle zákona 227/2000 Sb. v platném znění/This qualified system certificate was issued according to Act No. 227/2000 Coll.	položka je obsažena v certifikátu vydaném před datem účinnosti politiky verze 1.10
basicConstraints		kritické
cA	True	
keyUsage	keyCertSign, cRLSign	kritické
subjectKeyIdentifier		nekritické
keyIdentifier	hash veřejného klíče Autority	

tab. 8 - Rozšíření certifikátu podřízené certifikační autority

Rozšíření	Obsah	Poznámka
certificatePolicies		nekritické

policyIdentifier	2.5.29.32.0 (anyPolicy)	
userNotice	Tento kvalifikovaný systémový certifikát byl vydán podle zákona 227/2000 Sb. v platném znění/This qualified system certificate was issued according to Act No. 227/2000 Coll.	položka je obsažena v certifikátu vydaném před datem účinnosti politiky verze 1.10
basicConstraints		kritické
cA	True	
pathLenConstraint	0	
keyUsage	keyCertSign, cRLSign	kritické
subjectKeyIdentifier		nekritické
keyIdentifier	hash veřejného klíče této podřízené certifikační autority	
authorityKeyIdentifier		nekritické
keyIdentifier	hash veřejného klíče Autority	
CRLDistributionPoints*	http://qcrlp1.ica.cz/rcaRR_rsa.crl http://qcrlp2.ica.cz/rcaRR_rsa.crl http://qcrlp3.ica.cz/rcaRR_rsa.crl	nekritické
authorityInformationAccess		nekritické
id-ad-ocsp*	http://ocsp.ica.cz/rcaRR_rsa	URI (http) na OCSP respondér kořenové CA
id-ad-calssuers*	http://r.ica.cz/rcaRR_rsa.cer	URI (http) na certifikát kořenové CA

* RR - poslední dvě číslice roku vydání certifikátu Autority.

tab. 9 - Rozšíření certifikátu OCSP respondéru Autority

Rozšíření	Obsah	Poznámka
certificatePolicies		nekritické
policyIdentifier	viz kap. 1.2	
userNotice	Tento kvalifikovaný systémový certifikát byl vydán podle zákona 227/2000 Sb. v platném znění/This qualified system certificate was issued according to Act No. 227/2000 Coll.	položka je obsažena v certifikátu vydaném podle politiky verze 1.0
authorityInformationAccess		nekritické

id-ad-calssuers*	http://r.ica.cz/rcaRR_rsa.cer	URI (http) na certifikát kořenové CA
basicConstraints		nekritická
cA	False	
keyUsage	digitalSignature	kritické
extendedKeyUsage	id-kp-OCSPSigning	kritické
id-pkix-ocsp-nocheck	NULL	nekritické
subjectKeyIdentifier		nekritické
keyIdentifier	hash veřejného klíče OCSP respoděru Authority	
authorityKeyIdentifier		nekritické
keyIdentifier	hash veřejného klíče Authority	

* *RR* - poslední dvě číslice roku vydání certifikátu 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

Autorita vydává certifikáty s tvary jmen, vyhovujícími 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

OID tohoto dokumentu/politiky je uveden v kapitole 1.2. V certifikátech certifikačních autorit je uvedeno speciální označení politiky anyPolicy, jehož OID je 2.5.29.32.0. OID politiky OCSP respoděru Autority je uvedeno v kapitole 1.2.

7.1.7 Použití rozšíření Policy Constraints

Není relevantní pro Certifikáty vydávané dle této CP.

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. 10 - Profil CRL¹

Pole	Obsah
version	v2(0x1)
signatureAlgorithm	sha512WithRSAEncryption
issuer	vydavatel CRL
thisUpdate	datum vydání
nextUpdate	datum vydání + maximálně 365 dní
revokedCertificates	seznam zneplatněných certifikátů
crlEntries	
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu - viz tab. 11
crlExtensions	
crlExtensions	rozšíření CRL - viz tab. 11
signature	elektronická značka nebo zaručená elektronická pečeť vydavatele CRL (Authority)

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X509 verze 2.

7.2.2 Rozšíření CRL a záznamů v CRL

tab. 11 - Rozšíření CRL²

Položka	Obsah	Poznámka
crlEntryExtensions		
CRLReason	důvod zneplatnění certifikátu; důvod certificateHold je nepřipustný, nepoužívá se	nekritické, volitelné
crlExtensions		
authorityKeyIdentifier		

¹ I.CA si vyhrazuje právo upravit množinu a obsah polí CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft)

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

keyIdentifier	hash veřejného klíče vydavatele CRL (Authority)	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. Pro certifikáty nevydané příslušnou CA je vrácena odpověď unAuthorized. Jako přenosový protokol je používáno pouze http.

Bližší podrobnosti jsou uvedeny v odpovídající certifikační prováděcí směrnici.

7.3.1 Číslo verze

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

7.3.2 Rozšíření OCSP

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

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita nebo okolnosti hodnocení

Periodicita hodnocení, včetně okolností pro provádění hodnocení, je dána právní úpravou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, dle kterých je hodnocení prováděno.

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

Periodicita jiných hodnocení je dána příslušnými technickými standardy a normami.

8.2 Identita a kvalifikace hodnotitele

Identita (akreditovaný subjekt posuzování shody) a kvalifikace hodnotitele provádějícího hodnocení podle právní úpravy pro služby vytvářející důvěru, je dána touto právní úpravou a jí odkazovanými technickými standardy a normami.

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

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

8.3 Vztah hodnotitele k hodnocenému subjektu

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

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

8.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného právní úpravou pro služby vytvářející důvěru jsou hodnocené oblasti konkretizovány touto právní úpravou.

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

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

8.5 Postup v případě zjištění nedostatků

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

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům právní úpravy pro služby vytvářející důvěru a příslušných technických standardů a norem, v případě hodnocení požadované programem Microsoft Trusted Root Certificate Program potom požadavkům společnosti Microsoft.

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

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

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Provozovatelem všech certifikačních autorit a OCSP respondéru, jejichž certifikáty byly vydány dle této CP, je společnost První certifikační autorita, a.s. Poplatky za vydávání certifikátů kořenovou certifikační autoritou nejsou účtovány.

9.1.2 Poplatky za přístup k certifikátu

Přístup elektronickou cestou k certifikátům vydaným dle této CP I.CA nezpoblatňuje.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) nebo stavech certifikátů (OCSP) vydaných dle této CP I.CA nezpoblatňuje.

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 osobní údaje podléhající ochraně ve smyslu příslušných právních předpisů.

Zaměstnanci I.CA, případně subjekty definované platnou právní úpravou přicházející do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního, nebo jiného obdobného poměru, nebo po provedení příslušných prací.

9.4.3 Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které nespádají 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 systémů poskytujících služby vytvářející důvěru jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče příslušné certifikátům Autority pouze k tvorbě elektronické pečeti/značky vydávaných Certifikátů a seznamů zneplatněných certifikátů Autority,
- Autoritou vydávané Certifikáty splňují náležitosti požadované příslušnými technickými standardy a normami, resp. právní úpravou pro služby vytvářející důvěru,
- zneplatní Certifikáty vydané Autoritou, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

9.6.2 Zastupování a záruky RA

Není relevantní pro tento dokument, viz bod 1.3.2.

9.6.3 Zastupování a záruky držitele certifikátu

Držitel Certifikátu postupuje v souladu s právní úpravou pro služby vytvářející důvěru a relevantními technickými standardy a normami a ručí za správnost jím uváděných informací v celém životním cyklu využívání poskytované služby vytvářející důvěru.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle této CP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované právní úpravou pro služby vytvářející důvěru a 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 řešeno v politikách autorit vydávajících certifikáty koncovým uživatelům.

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

Všechny zúčastněné subjekty jsou organizačními částmi I.CA a komunikace mezi nimi se řídí interními pravidly I.CA.

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným interní dokumentací.

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 právní úpravou pro služby vytvářející důvěru.

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

9.13 Ustanovení o řešení sporů

Všechny zúčastněné subjekty jsou organizačními částmi I.CA a řešení sporů mezi nimi se řídí interními pravidly I.CA.

9.14 Rozhodné právo

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

9.15 Shoda s platnými právními předpisy

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

9.16 Různá ustanovení

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto CP, stanoví, že provádění některého povinného požadavku je protiprávní, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a v souladu s platnou právní úpravou.

9.16.4 Zřeknutí se práv

Není relevantní pro tento dokument.

9.16.5 Vyšší moc

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

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

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