

První certifikační autorita, a.s.



Certifikační politika

vydávání kvalifikovaných certifikátů SK

pro vzdálené podepisování

(algoritmus RSA)

Certifikační politika vydávání kvalifikovaných certifikátů SK pro elektronické podpisy (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 1.00

OBSAH

1	Úvod	10
1.1	Přehled	10
1.2	Název a identifikace dokumentu.....	11
1.3	Participující subjekty	11
1.3.1	Certifikační autority (dále „CA“)	11
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	12
1.4.1	Přípustné použití certifikátu	12
1.4.2	Zakázané použití certifikátu	13
1.5	Správa politiky.....	13
1.5.1	Organizace spravující dokument	13
1.5.2	Kontaktní osoba	13
1.5.3	Osoba rozhodující o souladu CPS s certifikační politikou	13
1.5.4	Postupy při schvalování CPS.....	13
1.6	Pojmy a zkratky.....	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 posílání obchodních značek	20
3.2	Počáteční ověření identity	20
3.2.1	Ověřování vlastnictví soukromého klíče.....	20
3.2.2	Ověřování identity organizace	20

3.2.3	Ověřování identity fyzické osoby	21
3.2.4	Neověřované informace vztahující se k 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	21
3.3.1	Identifikace a autentizace při běžném požadavku na výměnu klíče	21
3.3.2	Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu.....	21
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	23
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	25
4.6.4	Oznámení o vydání nového certifikátu držiteli certifikátu.....	25
4.6.5	Úkony spojené s převzetím obnoveného certifikátu	25
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.....	26
4.7.6	Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou	26
4.7.7	Oznámení o vydání certifikátu certifikační autoritou jiným subjektům	26
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	27
4.9	Zneplatnění a pozastavení platnosti certifikátu	27
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	28
4.9.7	Periodicita vydávání seznamu zneplatněných certifikátů	28
4.9.8	Maximální zpoždění při vydávání seznamu zneplatněných certifikátů	28
4.9.9	Dostupnost ověřování stavu certifikátu on-line.....	28
4.9.10	Požadavky při ověřování stavu certifikátu on-line	28
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	29
4.10	Služby ověřování stavu certifikátu	29
4.10.1	Funkční charakteristiky	29
4.10.2	Dostupnost služeb	29
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	32
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 periodicita doškolování	34
5.3.5	Periodicita 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	Periodicita 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	Systém 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	Systém 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	42
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.....	43
6.2.10	Postup ničení soukromého klíče	43
6.2.11	Hodnocení kryptografických modulů.....	43
6.3	Další aspekty správy párových dat	44
6.3.1	Uchovávání veřejných klíčů	44
6.3.2	Doba funkčnosti certifikátu a doba použitelnosti párových dat	44
6.4	Aktivační data	44
6.4.1	Generování a instalace aktivačních dat	44
6.4.2	Ochrana aktivačních dat	44
6.4.3	Ostatní aspekty aktivačních dat	44
6.5	Řízení počítačové bezpečnosti.....	44
6.5.1	Specifické technické požadavky na počítačovou bezpečnost	44
6.5.2	Hodnocení počítačové bezpečnosti	45
6.6	Technické řízení životního cyklu.....	47
6.6.1	Řízení vývoje systému.....	47
6.6.2	Řízení správy bezpečnosti.....	47
6.6.3	Řízení životního cyklu bezpečnosti.....	47
6.7	Řízení bezpečnosti sítě	48
6.8	Označování časovými razítky.....	48
7	Profily certifikátu, seznamu zneplatněných certifikátů a OCSP	49
7.1	Profil certifikátu.....	49
7.1.1	Číslo verze	55
7.1.2	Rozšíření certifikátu.....	55
7.1.3	Objektové identifikátory algoritmů.....	58
7.1.4	Tvary jmen.....	60
7.1.5	Omezení jmen	60
7.1.6	Objektový identifikátor certifikační politiky.....	61
7.1.7	Použití rozšíření Policy Constraints	61
7.1.8	Syntaxe a sémantika kvalifikátorů politiky	61
7.1.9	Zpracování sémantiky kritického rozšíření Certificate Policies	61
7.2	Profil seznamu zneplatněných certifikátů.....	61

7.2.1	Číslo verze	62
7.2.2	Rozšíření CRL a záznamů v CRL	62
7.3	Profil OCSP	62
7.3.1	Číslo verze	62
7.3.2	Rozšíření OCSP	62
8	Hodnocení shody a jiná hodnocení	63
8.1	Periodicita nebo okolnosti hodnocení	63
8.2	Identita a kvalifikace hodnotitele.....	63
8.3	Vztah hodnotitele k hodnocenému subjektu	63
8.4	Hodnocené oblasti	63
8.5	Postup v případě zjištění nedostatků.....	63
8.6	Sdělování výsledků hodnocení.....	64
9	Ostatní obchodní a právní záležitosti.....	65
9.1	Poplatky	65
9.1.1	Poplatky za vydání nebo obnovení certifikátu	65
9.1.2	Poplatky za přístup k certifikátu	65
9.1.3	Zneplatnění nebo přístup k informaci o stavu certifikátu	65
9.1.4	Poplatky za další služby	65
9.1.5	Postup při refundování.....	65
9.2	Finanční odpovědnost.....	65
9.2.1	Krytí pojištěním.....	65
9.2.2	Další aktiva.....	65
9.2.3	Pojištění nebo krytí zárukou pro koncové uživatele	66
9.3	Důvěrnost obchodních informací.....	66
9.3.1	Rozsah důvěrných informací	66
9.3.2	Informace mimo rámec důvěrných informací	66
9.3.3	Odpovědnost za ochranu důvěrných informací.....	66
9.4	Ochrana osobních údajů	66
9.4.1	Politika ochrany osobních údajů	66
9.4.2	Informace považované za osobní údaje	66
9.4.3	Informace nepovažované za osobní údaje.....	67
9.4.4	Odpovědnost za ochranu osobních údajů.....	67
9.4.5	Oznámení o používání osobních údajů a souhlas s jejich zpracováním.....	67
9.4.6	Poskytování osobních údajů pro soudní či správní účely	67
9.4.7	Jiné okolnosti zpřístupňování osobních údajů.....	67
9.5	Práva duševního vlastnictví.....	67

9.6	Zastupování a záruky	67
9.6.1	Zastupování a záruky CA	67
9.6.2	Zastupování a záruky RA	68
9.6.3	Zastupování a záruky držitele certifikátu	68
9.6.4	Zastupování a záruky spoléhajících se stran	68
9.6.5	Zastupování a záruky ostatních zúčastněných subjektů	68
9.7	Zřeknutí se záruk	68
9.8	Omezení odpovědnosti	68
9.9	Záruky a odškodnění	69
9.10	Doba platnosti, ukončení platnosti	69
9.10.1	Doba platnosti	69
9.10.2	Ukončení platnosti	69
9.10.3	Důsledky ukončení a přetrvání závazků	69
9.11	Individuální upozorňování a komunikace se zúčastněnými subjekty	69
9.12	Novelizace	69
9.12.1	Postup při novelizaci	69
9.12.2	Postup a periodicita oznamování	69
9.12.3	Okolnosti, při kterých musí být změněn OID	69
9.13	Ustanovení o řešení sporů	70
9.14	Rozhodné právo	70
9.15	Shoda s platnými právními předpisy	70
9.16	Různá ustanovení	70
9.16.1	Rámcová dohoda	70
9.16.2	Postoupení práv	70
9.16.3	Oddělitelnost ustanovení	70
9.16.4	Vymáhání (poplatky za právní zastoupení a zřeknutí se práv)	70
9.16.5	Vyšší moc	70
9.17	Další ustanovení	70
10	Závěrečná ustanovení	71

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	27.8.2022	Generální ředitel společnosti První certifikační autorita, a.s.	První vydání.

1 ÚVOD

Tento dokument stanoví zásady, které První certifikační autorita, a.s., (dále též I.CA), kvalifikovaný poskytovatel služeb vytvářejících důvěru, uplatňuje při poskytování kvalifikované služby vytvářející důvěru vydávání kvalifikovaných certifikátů SK pro vzdálené podepisování (dále též Služba, Certifikát). Jedná se o dva typy certifikátů analogické s:

- kvalifikovanými certifikáty SK pro elektronické podpisy – dále jen certifikáty pro elektronické podpisy, a
- kvalifikovanými mandátními certifikáty SK – dále jen mandátní certifikáty.

Pro Službu poskytovanou podle této certifikační politiky (dále též CP) je využíván algoritmus RSA.

Právní požadavky na Službu jsou definovány:

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

Služba je poskytována všem koncovým uživatelům na základě uzavřeného smluvního vztahu. I.CA nijak neomezuje potenciální koncové uživatele, poskytování Služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

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

1.1 Přehled

Dokument **Certifikační politika vydávání kvalifikovaných certifikátů SK pro vzdálené podepisování (algoritmus RSA)** vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu vydávaných Certifikátů a dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC 3647, s přihlédnutím k platným technickým standardům a normám Evropské unie a k právu České republiky a Slovenské republiky v dané oblasti (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k ní irelevantní). Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem, obecně popisuje subjekty participující na poskytování této Služby a definuje přípustné využívání vydávaných Certifikátů.

- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání Certifikátu, resp. zneplatnění Certifikátu, včetně definování typů a obsahů používaných jmen ve vydávaných Certifikátech.
- Kapitola 4 definuje procesy životního cyklu jí vydávaných Certifikátů, tzn. žádost o vydání a vlastní vydání Certifikátu, žádost o zneplatnění a vlastní zneplatnění Certifikátu, služby související s ověřováním stavu Certifikátu, ukončení poskytování Služby atd.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání těchto záznamů a reakce po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.
- Kapitola 7 definuje profil vydávaných Certifikátů a seznamů zneplatněných certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytované Služby.
- Kapitola 9 zahrnuje problematiku obchodní a právní.

Bližší podrobnosti o naplnění polí a rozšíření Certifikátů vydávaných podle této CP a o jejich správě mohou být uvedeny v odpovídající certifikační prováděcí směrnici (dále CPS) a také v dokumentu Politika služby I.CA RemoteSign (vytváření elektronického podpisu na dálku), dále též Politika_RSIGN.

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu: Certifikační politika vydávání kvalifikovaných certifikátů SK pro vzdálené podepisování (algoritmus RSA), verze 1.00

1.2.1 Certifikáty pro elektronické podpisy

OID politiky: 1.3.6.1.4.1.23624.10.1.93.1.0

1.2.2 Mandátní certifikáty

OID politiky: 1.3.6.1.4.1.23624.10.1.94.1.0

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA“)

Kořenová certifikační autorita společnosti První certifikační autorita, a.s., vydala ve dvoustupňové struktuře certifikačních autorit, v souladu s platnou právní úpravou a s požadavky technických standardů a norem, certifikát podřízené certifikační autoritě (dále

těž Autorita) provozované I.CA. Tato Autorita vydává Certifikáty dle této CP a certifikáty pro vlastní OCSP respondér.

1.3.2 Registrační autority (dále „RA“)

Poskytování služeb společnosti První certifikační autorita, a.s., se realizuje prostřednictvím registračních autorit (stacionárních nebo mobilních) - v terminologii služby vytváření elektronického podpisu na dálku je požíván termín kontaktní místa – které jsou:

- v případě **certifikátů pro elektronický podpis** buď veřejné (poskytují služby veřejnosti), nebo klientské (poskytují služby svým zákazníkům),
- v případě **mandátních certifikátů** vyhrazené.

Tyto registrační autority:

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

1.3.3 Držitelé certifikátů

Držitelem vydávaného Certifikátu může být fyzická osoba 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 právní úpravy pro služby vytvářející důvěru přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP lze využívat pouze v procesech ověřování elektronického podpisu v souladu s právní úpravou pro služby vytvářející důvěru.

1.4.2 Zakázané použití certifikátu

Certifikáty vydávané podle této CP nesmějí být používány v rozporu s přípustným použitím popsáním 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 související s touto CP, je generální ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování CPS

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

1.6 Pojmy a zkratky

tab. 2 – Pojmy

Pojem	Vysvětlení
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 kvalifikovaná elektronická pečeť dle právní úpravy pro služby vytvářející důvěru
elektronická značka	elektronická značka dle právní úpravy pro služby vytvářející důvěru
elektronický dokument	číselně kódovaný dokument, uchovávaný na fyzickém nosiči, přenášený nebo zpracovávaný pomocí technických prostředků v elektronické, magnetické, optické nebo jiné formě
elektronický podpis	kvalifikovaný 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
kvalifikovaný certifikát pro elektronický podpis nebo pro elektronickou pečeť	certifikát definovaný právní úpravou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů, resp. pečeti	prostředek pro vytváření elektronických podpisů, resp. pečeti, který splňuje požadavky stanovené v příloze II eIDAS
mandant	osoba nebo orgán veřejné moci, za které nebo jejichž jménem mandatář jedná
mandatář	fyzická osoba, oprávněná ze zákona nebo na základě zákona jednat za jinou osobu nebo orgán veřejné moci nebo jejich jménem, nebo osoba, která vykonává činnost nebo funkci podle zvláštního předpisu
mandát	potvrzení o platnosti práva jednat za jinou osobu nebo orgán veřejné moci nebo jejich jménem
mandátní certifikát	kvalifikovaný certifikát pro elektronický podpis vydaný fyzické osobě oprávněné ze zákona nebo na základě zákona jednat za jinou osobu nebo orgán veřejné moci nebo jejich jménem, nebo osobě, která vykonává činnost nebo funkci podle zvláštního předpisu
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
pečetící osoba	právnícká osoba, která vytváří elektronickou pečeť
písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
podřízená CA	CA vydávající certifikáty koncovým uživatelům
právní úprava pro služby vytvářející důvěru	platné právní předpisy vztahující se ke službám vytvářejícím důvěru
služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru	služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru definovaná eIDAS
smluvní partner	subjekt zajišťující na základě písemné smlouvy pro I.CA služby vytvářející důvěru nebo jejich části – nejčastěji se jedná o smluvní RA
softcard	programová emulace čipové karty pro přístup k soukromému klíči uloženému v HSM
soukromý klíč	jedinečná data pro vytváření elektronického podpisu/pečeti
spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát

DUAL	obchodní produkt I.CA, obsahující dvojici certifikátů: <ul style="list-style-type: none"> ▪ kvalifikovaný certifikát pro elektronický podpis, ▪ komerční certifikát – vydaný výhradně na základě smluvního vztahu mezi I.CA a koncovým uživatelem
veřejný klíč	jedinečná data pro ověřování elektronického podpisu/pečetě
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

tab. 3 – Zkratky

Zkratka	Vysvětlení
ASCII	American Standard Code for Information Interchange, kódová tabulka definující znaky anglické abecedy a jiné znaky používané v informatice
BIH	Bureau International de l'Heure, (anglicky The International Time Bureau), Mezinárodní časová služba
bit	z anglického <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
CP	certifikační politika
CPS	certifikační prováděcí směrnice
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátu
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	General Data Protection Regulation, nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
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
IT	Information Technology, informační technologie
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
MPSV	Ministerstvo práce a sociálních věcí České republiky
NBÚ SR	Národný bezpečnostný úrad Slovenskej republiky
NTR	National Trade Register, obchodní rejstřík
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
OSVČ	osoba samostatně výdělečně činná
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
PTC	Publicly-Trusted Certificate, certifikát, jehož certifikát kořenový je

	distribuován jako důvěryhodná kotva v běžně dostupném aplikačním programovém vybavení
PUB	Publication, označení standardu FIPS
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu nebo pečetě (dle eIDAS)
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
STN	označení slovenských technických norem
TS	Technical Specification, typ ETSI standardu
TSA	Time-Stamping Authority, autorita časových razítek
TSS	Time-Stamp Server, server časových razítek
TSU	Time-Stamp Unit, jednotka vydávající časová razítka
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., jsou:

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

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

Na výše uvedené internetové adrese lze získat informace o:

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

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

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

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

2.3 Čas nebo četnost zveřejňování

I.CA zveřejňuje informace s následující periodicitou:

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

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení.

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

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

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

3.1.2 Požadavek na významovost jmen

V procesu vydávání Certifikátu je vždy vyžadována významovost všech ověřitelných jmen, uvedených v položkách pole subject, resp. rozšíření subjectAlternativeName. Podporované položky tohoto pole a rozšíření jsou uvedeny v kapitole 7.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Certifikáty vydávané podle této CP nepodporují anonymitu, ani používání pseudonymu.

3.1.4 Pravidla pro interpretaci různých forem jmen

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

3.1.5 Jedinečnost jmen

Autorita zaručuje jedinečnost pole subject v Certifikátu příslušného držitele tohoto Certifikátu.

3.1.6 Uznávání, ověřování a posílání obchodních značek

Certifikáty vydané podle této CP neobsahují žádné obchodní značky.

3.2 Počáteční ověření identity

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

3.2.1 Ověřování vlastnictví soukromého klíče

Vzhledem k tomu, že soukromý klíč je generován a uložen v zařízení typu QSCD provozovaném I.CA, není jeho vlastnictví ověřováno.

3.2.2 Ověřování identity organizace

Postup je popsán v dokumentu Politika_RSign, v kapitole Ověřování identity právnické osoby.

3.2.3 Ověřování identity fyzické osoby

Postup je popsán v dokumentu Politika_RSIGN, v kapitole Ověřování identity fyzické osoby.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Neověřovanými informacemi v případě **certifikátu pro elektronické podpisy** je generationQualifier (generační kvalifikátor), v případě **mandátního certifikátu** musí být všechny informace ověřeny.

3.2.5 Ověřování kompetencí

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

Vzhledem k tomu, že soukromý klíč je generován a uložen v zařízení typu QSCD provozovaném I.CA, není jeho vlastnictví ověřováno.

V případě **mandátního certifikátu** dále mandatář prokazuje oprávnění jednat za mandanta nebo jeho jménem, jednat jako orgán veřejné moci nebo oprávnění vykonávat činnost podle zvláštního předpisu nebo vykonávat funkci podle zvláštního předpisu v souladu s požadavky na udělení daného oprávnění, které jsou uvedeny v seznamu oprávnění vedeném NBÚ SR.

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

Identifikace a autentizace při běžném požadavku na výměnu klíče (vydání následného Certifikátu) není prováděna, výměna klíče probíhá automaticky a elektronickou cestou v určitém minimálním předstihu před vypršením platnosti Certifikátu původního (uživatel služby vytváření elektronických podpisů na dálku, tj. držitel Certifikátu, je dotázán, zda chce vydat Certifikát následný). Držitel Certifikátu je plně odpovědný za hlášení případných změn, tato povinnost je mj. uvedena ve smlouvě o poskytování služby vytváření elektronického podpisu na dálku.

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

Ke zneplatnění Certifikátu dojde vždy při ukončení smlouvy o poskytování služby vytváření elektronických podpisů na dálku (Klient neodpoví kladně na dotaz, zda chce vydat následný Certifikát). Kromě toho je zneplatnění možné i způsoby popsány v dokumentu Politika_RSIGN, v kapitolách Zneplatnění Certifikátu a Podání žádosti o zneplatnění.

O zneplatnění Certifikátu mohou požádat prostřednictvím oprávněného pracovníka subjekty, jimž to umožňuje platná právní úprava.

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

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

O vydání Certifikátu žádá fyzická osoba, která uzavírá smlouvu o poskytování Služby (Smlouvu).

4.1.2 Registrační proces a odpovědnosti

Postup je popsán v dokumentu Politika_RSIGN, v kapitole Registrační proces a odpovědnosti.

4.2 Zpracování žádosti o certifikát

4.2.1 Provádění identifikace a autentizace

Při vydávání **prvotního Certifikátu** jsou identifikace a autentizace prováděny podle dokumentu Politika_RSIGN, kapitoly Ověřování identity fyzické osoby a případně Ověřování identity právnické osoby. Pro vydávání **následného Certifikátu** platí kapitola 3.3.1.

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

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

- kontrolu údajů v předkládaných dokladech,
- vizuální kontrolu formální správnosti údajů.

Ověřování kompetencí a kontroly formální správnosti údajů jsou prováděny i programovým vybavením systému RA.

Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu, a tedy uzavírání smlouvy o poskytování služby vytváření elektronického podpisu na dálku je ukončen, v opačném případě je postupováno v souladu s ustanoveními kapitoly 4.3.

4.2.3 Doba zpracování žádosti o certifikát

Po kladném rozhodnutí o vydání Certifikátu je I.CA povinna neprodleně Certifikát vydat. Přibližné časové údaje pro vydání Certifikátu, není-li smluvně ošetřeno jinak, jsou v následujícím seznamu:

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

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání **prvotního** Certifikátu 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.

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, a tedy uzavírání Smlouvy, je ukončen.

Vydání **následného Certifikátu** probíhá automaticky, bez zásahu operátora CA, na základě kladné odpovědi Klienta na dotaz, zda chce následný Certifikát vydat.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

V procesu vydávání **prvotního Certifikátu** je držitel Certifikátu buď informován prostřednictvím pracovníka RA, nebo v průběhu aktivace služby vytváření elektronických podpisů na dálku. Certifikát je následně zveřejněn, další nakládání s ním může být dáno smlouvou mezi konkrétní třetí stranou a I.CA.

Vydání **následného Certifikátu** probíhá automatizovaně, pouze na základě kladné odpovědi držitele Certifikátu na dotaz, zda chce následný Certifikát vydat. V případě kladné odpovědi je vydán Certifikát zveřejněn, další nakládání s ním může být dáno smlouvou mezi konkrétní třetí stranou a I.CA. Klient je plně odpovědný za aktuálnost údajů v Certifikátu.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání Certifikátu, je tento zveřejněn. Držitel Certifikát převezme Certifikát okamžikem aktivace aplikace na mobilním zařízení.

4.4.2 Zveřejňování certifikátů certifikační autoritou

I.CA zajistí zveřejnění jí vydaných Certifikátů.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Oznámení o vydání Certifikátu může být, v závislosti na smlouvě mezi konkrétní třetí stranou a I.CA, oznamováno této třetí straně. Jiným subjektům vydání Certifikátu oznamováno není.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností Klientů jsou uvedeny v dokumentu Politika_RSIGN, v kapitole Registrační proces a odpovědnosti.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje (např. www.ica.cz, web orgánu dohledu, pracoviště RA, příslušný důvěryhodný seznam) certifikáty certifikačních autorit související s Certifikátem vydaným podle této CP, ověřit hodnoty jejich otisků a jejich platnost,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že Certifikát je platný,
- dodržovat veškerá ustanovení této CP, dokumentu Politika_RSIGN a právní úpravy pro služby vytvářející důvěru, vztahující se k povinnostem spoléhající se strany.

4.6 Obnovení certifikátu

Službou obnovení Certifikátu je podle této CP míněno vydání následného 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.

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 nebo rozšíření subjectAlternativeName Certifikátu, jehož veřejný klíč je předmětem výměny.

Proces vydání nového Certifikátu probíhá automatizovaně, další podrobnosti jsou uvedeny v dokumentu Politika_RSIGN, v kapitole Prodloužení Smlouvy.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Postup je popsán v dokumentu Politika_RSIGN, v kapitole Prodloužení Smlouvy.

4.7.2 Kdo může žádat o výměnu veřejného klíče v certifikátu

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

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Požadavek na výměnu veřejného klíče v Certifikátu je zpracován okamžitě po kladné odpovědi držitele Certifikátu na dotaz, zda chce vydat Certifikát následný.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Uvedeno v kapitole 4.3.2.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Uvedeno v kapitole 4.4.1.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Uvedeno v kapitole 4.4.2.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Uvedeno v kapitole 4.4.3.

4.8 Změna údajů v certifikátu

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

Služba změny údajů Certifikátu není poskytována.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

4.8.5

4.8.6 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

4.8.7 Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

4.8.8 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Zneplatnění Certifikátu je nedílnou součástí zrušení služby vytváření elektronických podpisů na dálku, postup je popsán v dokumentu Politika_RSIGN, v kapitolách Zneplatnění Certifikátu a Podání žádosti o zneplatnění.

Službu pozastavení platnosti Certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění

Viz kap. 4.9.

4.9.2 Kdo může požádat o zneplatnění

Viz kap. 4.9.

4.9.3 Postup při žádosti o zneplatnění

Viz kap. 4.9.

4.9.4 Prodleva při požadavku na zneplatnění certifikátu

Viz kap. 4.9.

4.9.5 Doba zpracování žádosti o zneplatnění

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

4.9.6 Povinnosti spoléhajících se stran při kontrole zneplatnění

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

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je vydáván neprodleně po kladném zpracování žádosti o zneplatnění Certifikátu. Nedojde-li ke zneplatnění Certifikátu, je nový CRL vydáván zpravidla v intervalu 8 hodin, nejvýše však 24 hodin od vydání předchozího CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

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

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Služba ověřování stavu Certifikátu s využitím protokolu OCSP je veřejně dostupná. Každý Certifikát, vydaný podle této CP, obsahuje odkaz na příslušný OCSP respondér.

OCSP odpovědi vyhovují normám RFC 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.

4.9.12 Zvláštní postupy při kompromitaci klíče

Postup pro zneplatnění Certifikátu v případě kompromitace soukromého klíče není odlišný od výše popsání postupu pro zneplatnění Certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

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

4.9.14 Kdo může požádat o pozastavení platnosti

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

4.9.15 Postup při žádosti o pozastavení platnosti

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

4.9.16 Omezení doby pozastavení platnosti

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

4.10 Služby ověřování stavu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných Certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaných Certifikátech.

Skutečnost, že Autorita poskytuje informace o stavu Certifikátu formou 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 (CRL), a dále dostupnost služby OCSP.

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

Konec Smlouvy je svázán s koncem platnosti Certifikátu. Pokud:

- Klient neodsouhlasí obnovu Certifikátu, Certifikát expiruje, nebo
- Klient Certifikát zneplatní a tento je uveden na CRL, platnost Smlouvy končí.

4.12 Úschova a obnova klíčů

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

4.12.1 Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Viz kapitola 4.12.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Postupy správy, řízení a provozu jsou zaměřeny především na:

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

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

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

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

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

5.1.2 Fyzický přístup

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

5.1.3 Elektřina a klimatizace

V prostorách, kde jsou umístěny důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru, je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí $20\text{ °C} \pm 5\text{ °C}$. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

5.1.4 Vlivy vody

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

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěny důvěryhodné systémy určené k podpoře služeb 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 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 popsáném v interní dokumentaci.

5.2 Procedurální postupy

5.2.1 Důvěryhodné role

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

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 jim příslušných OCSP respondérů,
- ničení soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů, včetně jejich záloh,
- zálohování a obnovu soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů,

- aktivaci a deaktivaci soukromých klíčů veškerých certifikačních autorit a jim příslušných OCSP respondérů.

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

5.2.3 Identifikace a autentizace pro každou roli

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

Pro vybrané činnosti využívají pracovníci v důvěryhodných rolích dvoufaktorovou autentizaci.

5.2.4 Role vyžadující rozdělení povinností

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

5.3 Personální postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

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

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

Ostatní zaměstnanci I.CA podílející se na zajištění 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 předmětných oblastech.

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

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

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

5.3.6 Postihy za neoprávněné činnosti

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem popsáním v interní dokumentaci 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 certifikačních autorit. Celý proces generování párových dat certifikačních autorit probíhá v souladu s právní úpravou pro služby vytvářející důvěru a s relevantními technickými standardy a normami. Generování je vždy prováděno podle připraveného scénáře ve fyzicky zabezpečeném prostředí a pod kontrolou více osob v důvěryhodných rolích.

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

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

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

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

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní dokumentaci, v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

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

5.4.4 Ochrana auditních záznamů

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

Elektronické auditní záznamy jsou ukládány ve dvou kopiích, 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 v interní dokumentaci.

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

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

5.5 Uchovávání záznamů

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

5.5.1 Typy uchovávaných záznamů

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

- zprávy/protokoly o průběhu generování párových dat certifikačních autorit,
- videozáznam průběhu generování párových dat podřízené certifikační autority vydávající certifikáty typu SSL,
- 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 dokumentaci.

5.5.2 Doba uchování záznamů

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

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště záznamů

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

Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

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

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

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

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

5.5.7 Postupy pro získání a ověření uchovávaných informací

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

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

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

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

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup ošetření incidentu nebo kompromitace

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

5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče

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

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

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

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, všem držitelům platných Certifikátů a subjektům, které mají s I.CA uzavřenou smlouvu přímo se vztahující k poskytování služeb vytvářejících důvěru,
- 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,

V případě odnětí statutu kvalifikovaného poskytovatele Služby:

- informace musí být písemně nebo elektronicky oznámena všem držitelům platných Certifikátů a subjektům, které mají s I.CA uzavřenou smlouvu přímo se vztahující k poskytování služeb vytvářejících důvěru,
- informace musí být zveřejněna v souladu s kapitolou 2.2 a na všech pracovištích registračních autorit; součástí informace bude i sdělení, že 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.

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

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit a jejich OCSP respondérů, které probíhá v zabezpečených vyhrazených prostorách provozních pracovišť v souladu s požadavky kapitol 5.2 a 5.4.1, je prováděno v kryptografických modulech, které splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN.

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 výše uvedených párových dat jsou popsány interní a externí dokumentací.

Generování párových dat vztahujících se k Certifikátům probíhá v zařízení typu QSCD umístěném v zabezpečených vyhrazených prostorách provozního pracoviště.

6.1.2 Předávání soukromého klíče jeho držiteli

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

Pro soukromé klíče Certifikátů není relevantní – soukromé klíče jsou uloženy v kryptografickém modulu, který je pod výhradní kontrolou I.CA.

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

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Veřejné klíče certifikačních autorit a jejich OCSP respondérů jsou příslušné certifikační autoritě doručovány v žádosti (formát PKCS#10) o vydání certifikátu.

Pro veřejné klíče koncových uživatelů není relevantní, veřejný klíč byl jako součást párových dat vygenerován v kryptografickém modulu pod výhradní kontrolou I.CA. Veřejný klíč jako součást vydaného Certifikátu je okamžitě po vydání zveřejněn, další nakládání s Certifikátem může záviset na smlouvě mezi konkrétní třetí stranou a I.CA.

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

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

- obdržením na RA,
- prostřednictvím internetových informačních adres I.CA, příslušného orgánu dohledu, resp. prostřednictvím věstníku tohoto orgánu dohledu,

6.1.5 Délky klíčů

Pro Službu poskytovanou podle této CP je výhradně využíván asymetrický algoritmus RSA. Mohutnost klíče kořenové certifikační autority I.CA je 4096 bitů, mohutnost klíčů v jí vydávaných certifikátech je minimálně 2048 bitů. Mohutnost klíčů v Certifikátech vydávaných podle této CP je minimálně 2048 bitů.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky uvedené v právní úpravě pro služby vytvářející důvěru, resp. v ní odkazovaných technických standardech nebo normách. Tyto klíče jsou generovány a kontrolovány příslušným technickým a programovým vybavením.

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

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

Možnosti použití klíče jsou uvedeny v rozšíření certifikátu.

6.2 Ochrana soukromého klíče a technologie kryptografických modulů

6.2.1 Řízení a standardy kryptografických modulů

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

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

Generování párových dat a uložení soukromých klíčů příslušných Certifikátům probíhá v kryptografickém modulu uvedeném na unijním seznamu jako zařízení typu QSCD.

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

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

6.2.3 Úschova soukromého klíče

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

6.2.4 Zálohování soukromého klíče

Soukromé klíče certifikačních autorit a jejich OCSP respondérů chráněné kryptografickými moduly jsou zálohovány v zašifrované podobě, která zajišťuje stejnou úroveň ochrany jako kryptografické zařízení.

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

Soukromé klíče koncových uživatelů chráněné kryptografickým modulem jsou zálohovány v zašifrované podobě, která zajišťuje stejnou úroveň ochrany jako kryptografické zařízení.

6.2.5 Uchovávání soukromého klíče

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

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

Soukromé klíče koncových uživatelů nejsou nikde uchovávány, po uplynutí doby platnosti jsou zničeny přístupové údaje k těmto klíčům umožňující jejich dešifrování a následné použití.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou generovány v kryptografických modulech (jako neexportovatelné) a nelze je z kryptografického modulu (provozovaném v certifikovaném režimu) exportovat v žádném tvaru¹. Import soukromého klíče CA do kryptografického modulu není prováděn.

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

Soukromé klíče koncových uživatelů jsou generovány v kryptografickém modulu (jako neexportovatelné) a nelze je z kryptografického modulu (provozovaného v certifikovaném režimu) exportovat v žádném tvaru². Import soukromého klíče CA do kryptografického modulu není prováděn.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou uloženy v kryptografických modulech splňujících požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN.

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

Soukromé klíče koncových uživatelů jsou uloženy v kryptografickém modulu uvedeném na unijním seznamu jako zařízení typu QSCD.

6.2.8 Postup aktivace soukromého klíče

Aktivace soukromých klíčů (umožnění jejich použití) certifikačních autorit a jejich OCSP respondérů v kryptografických modulech je prováděna:

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

² Výjimkou je zašifrovaná záloha, kterou lze použít pouze v kryptografickém modulu (resp. v HA/LB modulech), kde byl klíč vygenerován.

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

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

Aktivace soukromých klíčů (umožnění jejich použití) koncových uživatelů v kryptografickém modulu je prováděna pomocí softcard – předložením softcard a hesla.

6.2.9 Postup deaktivace soukromého klíče

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

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

Deaktivace soukromých klíčů koncových uživatelů je provedena ukončením smlouvy, zneplatnění příslušného certifikátu, nebo vydáním certifikátu následnému k certifikátu, jehož soukromý klíč má být deaktivován.

6.2.10 Postup ničení soukromého klíče

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

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

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

Ničení soukromých klíčů koncových uživatelů uložených v kryptografickém modulu pod kontrolu I.CA spočívá ve zrušení přístupových údajů, bez kterých není možné klíč uložený v zašifrovaném tvaru dešifrovat a následně použít. K tomu dojde po ukončení platnosti smlouvy, po zrušení příslušného certifikátu, nebo po vygenerování certifikátu následného.

6.2.11 Hodnocení kryptografických modulů

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

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

Kryptografické moduly, ve kterých jsou koncovým uživatelům generována párová data a jsou uloženy odpovídající soukromé klíče jsou uvedeny na unijním seznamu jako zařízení typu QSCD.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

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

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

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

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

Aktivační data soukromých klíčů koncových uživatelů (softcard) jsou vytvářena před generováním nebo v průběhu generování příslušných párových dat

6.4.2 Ochrana aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit a jejich OCSP respondérů (čipová karta nebo softcard) jsou chráněna nastaveným heslem.

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

Aktivační data soukromých klíčů koncových uživatelů (softcard) jsou chráněna nastaveným heslem.

6.4.3 Ostatní aspekty aktivačních dat

Není relevantní pro tento dokument.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti komponent použitých pro poskytování služeb vytvářejících důvěru je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů, a jejich periodicity, definována 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.
- ČSN ETSI EN 319 412-1 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 1: Přehled a společné datové struktury.
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ČSN ETSI EN 319 412-2 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám.
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ČSN ETSI EN 319 412-3 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 3: Profil certifikátu pro certifikáty vydávané právnickým osobám.
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ČSN ETSI EN 319 412-4 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 4: Profil certifikátu pro certifikáty webových stránek.
- ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

- ČSN ETSI EN 319 412-5 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 5: Prohlášení „QC Statements“.
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- ČSN EN 419 221-5 Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografický modul pro důvěryhodné služby.
- EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services.
- ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.
- ČSN EN ISO/IEC 15408-2 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty.
- ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.
- ČSN EN ISO/IEC 15408-3 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk.
- ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.
- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ČSN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací, resp. STN ISO/IEC 27006 Informačné technológie. Bezpečnostné metódy. Požiadavky na orgány poskytujúce audit a certifikáciu systémov manažérstva informačnej bezpečnosti.
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.
- ISO 3166-1 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.
- ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- RFC 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.

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, resp. STN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky, resp. STN ISO/IEC 27001 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací, resp. STN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.

6.6.3 Řízení životního cyklu bezpečnosti

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

- vybudování - stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou,
- implementace a provoz - účelné a systematické prosazení vybraných bezpečnostních opatření,
- monitorování a přehodnocování - zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení společnosti k posouzení,
- údržba a zlepšování - provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení společnosti.

6.7 Řízení bezpečnosti sítě

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

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

7.1.1 Certifikát pro elektronické podpisy

tab. 4 – Základní pole Certifikátu

Pole	Obsah
version	v3 (0x2)
serialNumber	jedinečné sériové číslo Certifikátu
signatureAlgorithm	minimálně sha256withRSAEncryption
issuer	vydavatel Certifikátu
validity	
notBefore	počátek platnosti Certifikátu (UTC)
notAfter	počátek platnosti + maximálně 365 dnů, resp. 366 dnů v případě přestupného roku (UTC)
subject	viz tab. 5
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	minimálně 2048 bitů
extensions	viz tab. 8
signature	elektronická značka, resp. zaručená elektronická pečeť vydavatele Certifikátu

tab. 5 - Pole subject

Všechny položky³ pole subject jsou převzaty ze žádosti o Certifikát s výjimkou položek vytvářených Autoritou. Povinné položky musí být v žádosti obsaženy.

Položka	Poznámka
countryName**	povinná, kód státu (ISO 3166), jediný výskyt
givenName	povinná v případě neuvedení položky pseudonym, jediný výskyt
surName	povinná v případě neuvedení položky pseudonym, jediný výskyt

³ I.CA si vyhrazuje právo upravit množinu a obsah položek pole subject, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

pseudonym	povinná v případě neuvedení položek givenName a surName, jediný výskyt
serialNumber (1)	vytváří Autorita v procesu vydávání prvotního Certifikátu, jednoznačná identifikace držitele Certifikátu v systému Autority (ICA - xxxxxxxx), využívána též při automatizovaném vydávání následného certifikátu
serialNumber (2)	volitelná, jedna z možností: <ul style="list-style-type: none"> ▪ IDCss-nnnnnnnn, ▪ PASss-nnnnnnnn, ▪ PNOss-yyyyyyyyyy (vyhrazeno pouze pro občany Slovenské republiky), kde: <ul style="list-style-type: none"> ▪ ss je kód státu (ISO 3166) – vydávající doklad, ▪ nnnnnnnn je číslo dokladu, ▪ yyyyyyyyyy rodné číslo
serialNumber (3)	volitelná a pokud je v položce serialNumber (2) uvedeno rodné číslo, jedna z možností: <ul style="list-style-type: none"> ▪ IDCss-nnnnnnnn, ▪ PASss-nnnnnnnn, kde: <ul style="list-style-type: none"> ▪ ss je kód státu (nemusí odpovídat countryName), ▪ nnnnnnnn je číslo dokladu
commonName*	povinná, jediný výskyt, musí zahrnovat obsah položek givenName a surName
initials	volitelná, jediný výskyt
emailAddress	v prvotním Certifikátu nesmí být položka uvedena
name	v prvotním Certifikátu nesmí být položka uvedena
generationQualifier	volitelná, jediný výskyt
organizationName	zaměstnanec Organizace: povinná, jediný výskyt fyzická osoba podnikající: volitelná, jediný výskyt fyzická osoba nepodnikající: nesmí být uvedena
organizationIdentifier	volitelný a pouze v případě uvedení atributu organizationName, jediný výskyt: <ul style="list-style-type: none"> ▪ NTRss-id, (National Trade Register, tzn. IČ) kde: <ul style="list-style-type: none"> ▪ ss je kód státu (ISO 3166) registrace zaměstnavatele nebo fyzické osoby podnikající (nemusí být shodná

	s countryName), <ul style="list-style-type: none"> ▪ id je identifikační číslo organizace v příslušném registru
organizationalUnitName	volitelná, možný vícenásobný výskyt
title	volitelná, možný vícenásobný výskyt
stateOrProvinceName**	volitelná, jediný výskyt
localityName**	volitelná, jediný výskyt první Certifikát: pokud bude uvedena, musí být také uvedeny položky streetAddress a postalCode
streetAddress**	volitelná, jediný výskyt první Certifikát: pokud bude uvedena, musí být také uvedeny položky localityName a postalCode
postalCode**	volitelná, jediný výskyt první Certifikát: pokud bude uvedena, musí být také uvedeny položky localityName a streetAddress

* Jméno, pod kterým subjekt Certifikátu (držitel soukromého klíče) běžně vystupuje, položka může obsahovat i ověřené tituly držitele Certifikátu.

** Položky countryName, stateOrProvinceName, localityName, streetAddress a postalCode se vztahují k údajům ověřeným v procesu ověřování identity fyzické osoby (viz kapitola 3.2.3).

7.1.2 Mandátní certifikát

tab. 6 - Základní pole Certifikátu

Pole	Obsah
version	v3 (0x2)
serialNumber	jedinečné sériové číslo Certifikátu
signatureAlgorithm	minimálně sha256withRSAEncryption
issuer	vydavatel Certifikátu
validity	
notBefore	počátek platnosti Certifikátu (UTC)
notAfter	počátek platnosti + maximálně 365 dnů, resp. 366 dnů v případě přestupného roku (UTC)
subject	viz tab. 7
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	minimálně 2048 bitů
extensions	viz tab. 9
signature	elektronická značka, resp. zaručená elektronická pečeť

	vydavatele Certifikátu
--	------------------------

tab. 7 - Pole subject

Všechny položky⁴ pole subject jsou převzaty ze žádosti o Certifikát s výjimkou položek vytvářených Autoritou. Povinné položky musí být v žádosti obsaženy.

	Položka	Poznámka
Mandatář	commonName	povinná, složená z položek givenName a surName a doplněných o text OPRÁVNENIE a číslo oprávnění, tedy: <ul style="list-style-type: none"> ▪ givenName surName OPRÁVNENIE xxxx kde xxxx je konkrétní číslo oprávnění
	givenName	Povinná
	surName	Povinná
	title	Volitelná
	serialNumber (1)	vytváří Autorita v procesu vydávání prvotního Certifikátu, jednoznačná identifikace držitele Certifikátu v systému Autority (ICA - xxxxxxxx), využívána též při automatizovaném vydávání následného certifikátu
	serialNumber (2)	povinná, jedna z možností: <ul style="list-style-type: none"> ▪ IDCss-nnnnnnnn, ▪ PASss-nnnnnnnn, ▪ PNOss-yyyyyyyyyy (vyhrazeno pouze pro občany Slovenské republiky), ▪ IDCss-DDD-nnnnnnnn, kde: <ul style="list-style-type: none"> ▪ ss je kód státu ((ISO 3166), ▪ nnnnnnnn je číslo dokladu, ▪ yyyyyyyyyy rodné číslo, ▪ DDD je specifikace typu identifikační karty
	serialNumber (3)	volitelná a pokud je v položce serialNumber (2) uvedeno rodné číslo, jedna ze dvou možností: <ul style="list-style-type: none"> ▪ IDCss-nnnnnnnn,

⁴ I.CA si vyhrazuje právo upravit množinu a obsah položek pole subject, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

		<ul style="list-style-type: none"> ▪ PASss-nnnnnnnn, kde: <ul style="list-style-type: none"> ▪ ss je kód státu (nemusí odpovídat countryName), ▪ nnnnnnn je číslo dokladu
Zaměstnavatel	serialNumber (4)	povinná, identifikační údaj zaměstnavatele mandátáře (resp. mandatář u této organizace vykonává činnost nebo funkci podle zvláštního předpisu): <ul style="list-style-type: none"> ▪ NTRss-id, (National Trade Register, tzn. IČ), kde: <ul style="list-style-type: none"> ▪ ss je kód státu (ISO 3166), ▪ id je identifikační číslo organizace v příslušném registru
	organizationName	povinná, zaměstnavatel mandátáře (resp. mandatář u této organizace vykonává činnost nebo funkci podle zvláštního předpisu) v případě, že mandatář poskytuje služby jako fyzická osoba, uvede se jméno a příjmení tak, jak je uvedeno v registru
	organizationIdentifier	povinná, identifikační údaj zaměstnavatele mandátáře (resp. mandatář u této organizace vykonává činnost nebo funkci podle zvláštního předpisu): <ul style="list-style-type: none"> ▪ NTRss-id, (National Trade Register, tzn. IČ), kde: <ul style="list-style-type: none"> ▪ ss je kód státu (ISO 3166), ▪ id je identifikační číslo organizace v příslušném registru
	organizationalUnitName	volitelná, název dílčího organizačního členění
	countryName*	povinná, kód státu (ISO 3166), jediný výskyt
	stateOrProvinceName*	volitelná, jediný výskyt
	localityName*	volitelná, jediný výskyt prvotní Certifikát: pokud bude uvedena, musí být také uvedeny položky streetAddress a postalCode
	streetAddress*	volitelná, jediný výskyt prvotní Certifikát: pokud bude uvedena, musí

		být také uvedeny položky <code>localityName</code> a <code>postalCode</code>
	<code>postalCode*</code>	volitelná, jediný výskyt prvotní Certifikát: pokud bude uvedena, musí být také uvedeny položky <code>localityName</code> a <code>streetAddress</code>
Mandant**	<code>givenName</code>	fyzická osoba: povinná ostatní: nesmí být uvedena
	<code>surName</code>	fyzická osoba: povinná ostatní: nesmí být uvedena
	<code>serialNumber (5)</code>	fyzická osoba: povinná, jedna z možností: <ul style="list-style-type: none"> ▪ <code>IDC<i>ss</i>-<i>nnnnnnnn</i></code>, ▪ <code>PAS<i>ss</i>-<i>nnnnnnnn</i></code>, ▪ <code>PNO<i>ss</i>-<i>yyyyyyyyyy</i></code> (vyhrazeno pouze pro občany Slovenské republiky), ▪ <code>IDC<i>ss</i>-<i>DDD</i>-<i>nnnnnnnn</i></code>, kde: <ul style="list-style-type: none"> ▪ <i>ss</i> je kód státu (ISO 3166), ▪ <i>nnnnnnnn</i> je číslo dokladu, ▪ <i>yyyyyyyyyy</i> rodné číslo, ▪ <i>DDD</i> je specifikace typu identifikační karty pro jiné držitele certifikátu, než fyzické osoby nesmí být položka uvedena
	<code>serialNumber (6)</code>	volitelná a pokud je v položce <code>serialNumber (5)</code> uvedeno rodné číslo, jedna z možností: <ul style="list-style-type: none"> ▪ <code>IDC<i>ss</i>-<i>nnnnnnnn</i></code>, ▪ <code>PAS<i>ss</i>-<i>nnnnnnnn</i></code>, ▪ <code>IDC<i>ss</i>-<i>DDD</i>-<i>nnnnnnnn</i></code>, kde: <ul style="list-style-type: none"> ▪ <i>ss</i> je kód státu ((ISO 3166), ▪ <i>nnnnnnnn</i> je číslo dokladu, ▪ <i>DDD</i> je specifikace typu identifikační karty
	<code>serialNumber (7)</code>	povinná v případě zaměstnance nebo právnické osoby/orgánu veřejné moci: <ul style="list-style-type: none"> ▪ <code>NTR<i>ss</i>-<i>id</i></code>, (National Trade Register, tzn. IČ),

		<p>kde:</p> <ul style="list-style-type: none"> ▪ <i>ss</i> je kód státu (ISO 3166), ▪ <i>id</i> je identifikační číslo organizace v příslušném registru
	organizationName	<p>povinná položka v případě fyzické osoby – zaměstnance nebo právnické osoby/orgánu veřejné moci:</p> <ul style="list-style-type: none"> ▪ MANDANT <i>zaměstnavatel mandanta</i>; např. MANDANT Firma, a.s.
	organizationIdentifier	<p>povinná v případě zaměstnance nebo právnické osoby/orgánu veřejné moci:</p> <ul style="list-style-type: none"> ▪ NTR<i>ss-id</i>, (National Trade Register, tzn. IČ), <p>kde:</p> <ul style="list-style-type: none"> ▪ <i>ss</i> je kód státu (ISO 3166), ▪ <i>id</i> je identifikační číslo organizace v příslušném registru

* Položky countryName, stateOrProvinceName, localityName, streetAddress a postalCode se vztahují k údajům ověřeným v procesu ověřování identity fyzické osoby (viz kapitola 3.2.3).

** Obsah položek, které se vztahují k mandantovi je vždy uvozen řetězcem MANDANT následovaným mezerou, např. MANDANT Jan Poslušný.

7.1.3 Číslo verze

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

7.1.4 Rozšíření certifikátu

7.1.4.1 Certifikát pro elektronické podpisy

tab. 8 – Rozšíření⁵ Certifikátu

Rozšíření	Obsah	Poznámka
certificatePolicies		nekritické
.policyInformation (1)		
policyIdentifier	viz kapitola 1.2	OID politiky I.CA
policyQualifiers		
cPSuri	http://www.ica.cz	

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

.policyInformation (2)		
policyIdentifier	1.3.158.36061701.0.0.0.1.2.2	OID politiky NBÚ SR
policyQualifiers		
userNotice	EN: This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014. SK: Kvalifikovaný certifikát pre elektronický podpis v súlade s nariadením (EU) č. 910/2014.	vydavateľ môže text položky zmeniť dle požadavku právni úpravy Slovenské republiky
.policyInformation (3)		
policyIdentifier	OID (QCP-n-qscd): 0.4.0.194112.1.2	OID politiky ETSI (soukromý klíč je generován a uložen na QSCD)
QCStatements		nekritické
	0.4.0.1862.1.1	Id-etsi-qcs-QcCompliance
	0.4.0.1862.1.4	Id-etsi-qcs-QcSSCD
	0.4.0.1862.1.5	id-etsi-qcs-QcPDS; odkaz (URI, https) na zprávu pro uživatele (PDS)
	0.4.0.1862.1.6 = 0.4.0.1862.1.6.1	id-etsi-qcs-QcType = id-etsi-qct-esign
CRLDistributionPoints*	http://qcrlp1.ica.cz/qcaRR_rsa.crl http://qcrlp2.ica.cz/qcaRR_rsa.crl http://qcrlp3.ica.cz/qcaRR_rsa.crl	nekritické
authorityInformationAccess		nekritické
id-ad-ocsp*	http://ocsp.ica.cz/qcaRR_rsa	
id-ad-caIssuers*	{ http://q.ica.cz/qcaRRsk_rsa.p7c http://q.ica.cz/qcaRR_rsa.cer }	
basicConstraints		nekritické
cA	False	
keyUsage	<ul style="list-style-type: none"> ▪ DUAL: <ul style="list-style-type: none"> - digitalSignature, nonRepudiation, 	kritické, povinné <ul style="list-style-type: none"> ▪ DUAL – vytváří Autorita,

	<ul style="list-style-type: none"> ▪ ostatní: na základě obsahu žádosti o Certifikát jedna z možností: <ul style="list-style-type: none"> - nonRepudiation, - digitalSignature, nonRepudiation, - digitalSignature, nonRepudiation a keyEncipherment*** 	<ul style="list-style-type: none"> ▪ ostatní – v případě absence tohoto rozšíření v žádosti bude doplněno: <ul style="list-style-type: none"> - digitalSignature, nonRepudiation
extendedKeyUsage	na základě obsahu žádosti o Certifikát jedna ze možností: <ul style="list-style-type: none"> ▪ id-kp-emailProtection, ▪ ms-Document_Signing, ▪ id-kp-emailProtection a ms-Document_Signing 	nekritické, povinné v případě absence tohoto rozšíření v žádosti bude doplněno: <ul style="list-style-type: none"> ▪ id-kp-emailProtection
subjectKeyIdentifier	hash veřejného klíče (subjectPublicKey) v Certifikátu	nekritické
authorityKeyIdentifier		nekritické
keyIdentifier	hash veřejného klíče Authority	
subjectAlternativeName		nekritické
otherName**	I.CA_User_ID(1.3.6.1.4.1.23624.4.6): xxxxxxx	
otherName	MPSV_IK (1.3.6.1.4.1.11801.2.1): číselný identifikátor dodávaný MPSV	volitelné
rfc822Name	e-mail adresa	volitelné, možný vícenásobný výskyt
nsComment	identifikační číslo QSCD	nekritické, volitelné – vkládá Autorita v případě ověření generování a uložení soukromého klíče na QSCD čipovou kartu typu Starcos
I.CA_TWAIN_ID: 1.3.6.1.4.1.23624.4.3	číslo žádosti o Certifikát	nekritické
I.CA_CERT_INTERCONNECTION:	v případě vydávání více typů certifikátů jednomu subjektu (vazba	nekritické

1.3.6.1.4.1.23624.4.7	subjektu k vydávaným certifikátům)	
-----------------------	------------------------------------	--

- * *RR* – poslední dvě číslice roku vydání certifikátu Autority.
- ** Jedná se o vybraný podřetězec z položky serialNumber pole subject vytvářené Autoritou (viz tab. 5).
- *** Poslední možnost (obsahující nastavení bitu keyEncipherment) pro keyUsage nelze použít při generování a uložení soukromého klíče na čipové kartě Starcos 3.5 a vyšší.

7.1.4.2 Mandátní certifikát

tab. 9 - Rozšíření⁶ Certifikátu

Rozšíření	Obsah	Poznámka
CertificatePolicies		nekritické
.policyInformation (1)		
policyIdentifier	viz kapitola 1.2	OID politiky I.CA
policyQualifiers		
cPSuri	http://www.ica.cz	
.policyInformation (2)		
policyIdentifier	1.3.158.36061701.0.0.0.1.2.2	OID politiky NBÚ SR
policyQualifiers		
userNotice	EN: This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014. SK: Kvalifikovaný certifikát pre elektronicky podpis v súlade s nariadením (EU) č. 910/2014.	vydavatel může text položky změnit dle požadavku právní úpravy Slovenské republiky
.policyInformation (3)		
policyIdentifier	1.3.158.36061701.1.1.xxxx	OID politiky pro příslušného mandatáře, xxxx – konkrétní číslo oprávnění
userNotice*	EN: Authorization xxxx N, SK: Opravenie xxxx N	xxxx – konkrétní číslo oprávnění N – konkrétní název oprávnění
.policyInformation (4)		
policyIdentifier	OID (QCP-n-qscd): 0.4.0.194112.1.2	OID politiky ETSI (soukromý klíč je generován a uložen

⁶ I.CA si vyhrazuje právo upravit množinu a obsah rozšíření Certifikátu, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

		na QSCD)
QCStatements		Nekritické
	0.4.0.1862.1.1	Id-etsi-qcs-QcCompliance
	0.4.0.1862.1.4	Id-etsi-qcs-QcSSCD; uvedeno v případě, kdy soukromý klíč je generován a uložen na QSCD
	0.4.0.1862.1.5	id-etsi-qcs-QcPDS; odkaz (URI, https) na zprávu pro uživatele (PDS)
	0.4.0.1862.1.6 = 0.4.0.1862.1.6.1	id-etsi-qcs-QcType = id-etsi-qct-esign
CRLDistributionPoints**	http://qcrlp1.ica.cz/qcaRR_rsa.crl http://qcrlp2.ica.cz/qcaRR_rsa.crl http://qcrlp3.ica.cz/qcaRR_rsa.crl	Nekritické
authorityInformationAccess		Nekritické
id-ad-ocsp**	http://ocsp.ica.cz/qcaRR_rsa	
id-ad-calssuers**	{http://q.ica.cz/qcaRRsk_rsa.p7c http://q.ica.cz/qcaRR_rsa.cer }	
basicConstraints		Nekritické
cA	False	
keyUsage	na základě obsahu žádosti o Certifikát jedna z možností: <ul style="list-style-type: none"> ▪ nonRepudiation, ▪ digitalSignature, nonRepudiation, ▪ digitalSignature, nonRepudiation a keyEncipherment**** 	kritické, povinné v případě absence tohoto rozšíření v žádosti bude doplněno: <ul style="list-style-type: none"> ▪ digitalSignature, nonRepudiation
extendedKeyUsage	na základě obsahu žádosti o Certifikát jedna z možností: <ul style="list-style-type: none"> ▪ id-kp-emailProtection, ▪ ms-Document_Signing, ▪ id-kp-emailProtection a ms-Document_Signing 	nekritické, povinné v případě absence tohoto rozšíření v žádosti bude doplněno: <ul style="list-style-type: none"> ▪ id-kp- emailProtection
subjectKeyIdentifier	hash veřejného klíče	nekritické

	(subjectPublicKey) v Certifikátu	
authorityKeyIdentifier		Nekritické
keyIdentifier	hash veřejného klíče Autority	
subjectAlternativeName		Nekritické
otherName***	I.CA_User_ID(1.3.6.1.4.1.23624.4.6) : xxxxxxxx	
otherName	MPSV_IK (1.3.6.1.4.1.11801.2.1): číselný identifikátor dodávaný MPSV	Volitelné
rfc822Name	e-mail adresa	volitelné, možný vícenásobný výskyt
nsComment	identifikační číslo QSCD	nekritické, volitelné – v případě ověření generování a uložení soukromého klíče na QSCD čipovou kartu typu Starcos
I.CA_CERT_INTERCONNECTION: 1.3.6.1.4.1.23624.4.7	v případě vydávání více typů certifikátů jednomu subjektu (vazba subjektu k vydávaným certifikátům)	Nekritické

- * Anglická verze je nepovinná, uvádí se, pokud je obsažena v seznamu oprávnění.
- ** RR – poslední dvě číslice roku vydání certifikátu Autority.
- *** Jedná se o vybraný podřetězec z položky serialNumber pole subject vytvářené Autoritou (viz tab. 5).
- **** Poslední možnost (obsahující nastavení bitu keyEncipherment) pro keyUsage nelze použít při generování a uložení soukromého klíče na čipové kartě Starcos 3.5 a vyšší.

7.1.5 Objektové identifikátory algoritmů

V procesu poskytování služeb vytvářejících důvěru jsou využívány algoritmy v souladu s příslušnými technickými standardy a normami.

7.1.6 Tvary jmen

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

7.1.7 Omezení jmen

Není relevantní pro Certifikáty vydávané koncovým uživatelům.

7.1.8 Objektový identifikátor certifikační politiky

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

- OID certifikační politiky I.CA, dle které je Certifikát vydán,
- OID politiky NBÚ SR,
- OID příslušné certifikační politiky určené normou ETSI EN 319 411-2, resp. ČSN ETSI EN 319 411-2 pro certifikát vydávaný fyzické osobě s ohledem na uložení soukromého klíče a deklarující, že Certifikát je v souladu s eIDAS.

7.1.9 Použití rozšíření Policy Constraints

Není relevantní pro Certifikáty vydávané koncovým uživatelům.

7.1.10 Syntaxe a sémantika kvalifikátorů politiky

Viz rozšíření Certifikátu v kapitole 7.1.2 výše.

7.1.11 Zpracování sémantiky kritického rozšíření Certificate Policies

Není relevantní pro tento dokument – není označeno jako kritické.

7.2 Profil seznamu zneplatněných certifikátů

tab. 10 - Profil CRL⁷

Pole	Obsah
version	v2(0x1)
signatureAlgorithm	minimálně sha256withRSAEncryption
issuer	vydavatel CRL
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate*	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu – viz tab. 8
crlExtensions	rozšíření CRL – viz tab. 11
signature	elektronická značka, resp. zaručená elektronická pečeť vydavatele CRL

⁷ I.CA si vyhrazuje právo upravit množinu a obsah polí CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

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

7.2.1 Číslo verze

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

7.2.2 Rozšíření CRL a záznamů v CRL

tab. 11 - Rozšíření CRL⁸

Rozšíření	Obsah	Poznámka
crlEntryExtensions		
CRLReason	důvod zneplatnění certifikátu důvod certificateHold je nepřipustný, nepoužívá se při zneplatnění certifikátu podřízené CA je uveden jiný důvod, než unspecified (0)	nekritické, volitelné
crlExtensions		
authorityKeyIdentifier		
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. 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 I.CA si vyhrazuje právo upravit množinu a obsah rozšíření CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami (např. společnost Microsoft).

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 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 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 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 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

Účtování poplatků za využívání služby je dáno smlouvou s konkrétní třetí stranou (formou může být paušální poplatek za určité časové období, placení za každé úspěšné vytvoření podpisu apod.).

9.1.2 Poplatky za přístup k certifikátu

Přístup elektronickou cestou k Certifikátům vydaným podle 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) a o stavech certifikátů vydaných Autoritou 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 informace podléhající ochraně ve smyslu příslušných právních předpisů.

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

9.4.3 Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které 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 důvěryhodných 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 certifikačních autorit pouze pro vydávání certifikátů koncovým uživatelům (vyjma kořenové certifikační autority I.CA), vydávání seznamů zneplatněných certifikátů a k vydávání certifikátů OCSP respondérů,
- použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,
- Certifikáty vydávané koncovým uživatelům splňují náležitosti požadované právní úpravou pro služby vytvářející důvěru a příslušnými technickými standardy a normami,
- zneplatní vydané Certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

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

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

Držitel Certifikátu vydaného podle této CP uplatňuje záruku vždy u RA, která zpracovala jeho žádost o vydání tohoto Certifikátu.

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

Záruky zahrnují:

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

9.6.2 Zastupování a záruky RA

Podrobný popis je uveden v dokumentu Politika_RSIGN, v kapitole Zastupování a záruky kontaktního místa (RA je zde uvedena jako kontaktní místo).

9.6.3 Zastupování a záruky držitele certifikátu

Podrobný popis je uveden ve smlouvě o poskytování služby vytváření elektronických podpisů na dálku.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle této CP a případně podle dokumentu Politika_RSIGN.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

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

9.8 Omezení odpovědnosti

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

9.9 Záruky a odškodnění

Uvedeno podrobně v dokumentu Politika_RSIGN, kapitola Záruky a odškodnění.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

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

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

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

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

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

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

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interní dokumentaci.

9.12.2 Postup a periodicita oznamování

Vydání nové verze CP je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněn OID

OID politiky musí být změněn v případě, že se zásadně sníží záruky za důvěryhodnost Certifikátu s významným účinkem na akceptovatelnost tohoto Certifikátu v souladu s právní úpravou pro služby vytvářející důvěru.

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

9.13 Ustanovení o řešení sporů

Uvedeno podrobně v dokumentu Politika_RSIGN, kapitola Ustanovení o řešení sporů.

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, České republiky a Slovenské 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 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv)

Není relevantní pro tento dokument.

9.16.5 Vyšší moc

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

9.17 Další ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

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