První certifikační autorita, a.s.



Politika

služby I.CA RemoteSeal

(vytváření elektronických pečetí na dálku)

Politika služby I.CA RemoteSeal (vytváření elektronických pečetí na dálku) 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 1.04

Copyright © První certifikační autorita, a.s.

OBSAH

1 Úvod 8
1.1 Přehled 8
1.2 Název a identifikace dokumentu 9
1.2.1 Politika vytváření pečetí (podpisů) 9
1.2.2 Podporované formáty a třídy pečetě, jejich omezení 9
1.2.3 Předávání parametrů pečetě 10
1.2.4 Architektura Služby 10
1.3 Participující subjekty 12
1.3.1 Poskytovatel služeb 12
1.3.2 Kontaktní místa 12
1.3.3 Spoléhající se strany 12
1.3.4 Jiné participující subjekty 12
1.4 Použití služby 13
1.4.1 Přípustné použití služby 13
1.4.2 Omezení použití služby 13
1.5 Správa politiky 13
1.5.1 Organizace spravující politiku nebo prováděcí směrnici 13
1.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici 13
1.5.3 Osoba rozhodující o souladu prováděcí směrnice s politikou služby 13
1.5.4 Postupy při schvalování prováděcí směrnice 13
1.6 Pojmy a zkratky 14
1.6.1 Pojmy 14
1.6.2 Zkratky 14
2 Odpovědnost za zveřejňování a úložiště informací a dokumentace 17
2.1 Úložiště informací a dokumentace 17
2.2 Zveřejňování informací a dokumentace 17
2.3 Periodicita zveřejňování informací 17
2.4 Řízení přístupu k jednotlivým typům úložišť 17
3 Identifikace a autentizace ke službě 18
3.1 Počáteční ověření identity 18
3.1.1 Ověřování identity organizace 18
3.1.2 Ověřování identity fyzické osoby 18
3.1.3 Ověřování e-mailové adresy 19

3.2 Ověření identity při prodloužení služby 19
3.3 Změna údajů 19
3.4 Identifikace a autentizace při požadavku na zneplatnění Certifikátu 19
4 Požadavky na životní cyklus služby 21
4.1 Uzavření smlouvy 21
4.2 Zřízení Služby 21
4.2.1 Registrační proces a odpovědnosti 21
4.3 Aktivace Služby 22
4.4 Správa Služby 22
4.5 Prodloužení Smlouvy 22
4.6 Konec platnosti Smlouvy 23
4.7 Zneplatnění Certifikátu a pozastavení platnosti Certifikátu 23
4.7.1 Podmínky pro zneplatnění 23
4.7.2 Kdo může požádat o zneplatnění Certifikátu 25
4.7.3 Postup při podání žádosti o zneplatnění 26
4.7.4 Prodleva při požadavku na zneplatnění certifikátu 27
4.8 Používání Služby 27
4.9 Dodatečná bezpečnostní opatření 27
5 Postupy správy, řízení a provozu 28
5.1 Fyzická bezpečnost 28
5.1.1 Umístění a konstrukce 28
5.1.2 Fyzický přístup 28
5.1.3 Elektřina a klimatizace 28
5.1.4 Vlivy vody 28
5.1.5 Protipožární opatření a ochrana 28
5.1.6 Ukládání médií 29
5.1.7 Nakládání s odpady 29
5.1.8 Zálohy mimo budovu 29
5.2 Procesní bezpečnost 29
5.2.1 Důvěryhodné role 29
5.2.2 Počet osob požadovaných na zajištění jednotlivých činností 29
5.2.3 Identifikace a autentizace pro každou roli 30
5.2.4 Role vyžadující rozdělení povinností 30
5.3 Personální bezpečnost 30
5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost 30
5.3.2 Posouzení spolehlivosti osob 30

5.3.3 Požadavky na školení 31
5.3.4 Požadavky a periodicita doškolování 31
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi 31
5.3.6 Postihy za neoprávněné činnosti zaměstnanců 31
5.3.7 Požadavky na nezávislé dodavatele 31
5.3.8 Dokumentace poskytovaná zaměstnancům 31
5.4 Postupy zpracování auditních záznamů 32
5.4.1 Typy zaznamenávaných událostí 32
5.4.2 Periodicita zpracování záznamů 32
5.4.3 Doba uchování auditních záznamů 32
5.4.4 Ochrana auditních záznamů 32
5.4.5 Postupy pro zálohování auditních záznamů 32
5.4.6 Systém shromažďování auditních záznamů (interní nebo externí) 32
5.4.7 Postup při oznamování události subjektu, který ji způsobil 32
5.4.8 Hodnocení zranitelnosti 33
5.5 Uchovávání záznamů 33
5.5.1 Typy uchovávaných záznamů 33
5.5.2 Doba uchování záznamů 33
5.5.3 Ochrana úložiště záznamů 33
5.5.4 Postupy při zálohování záznamů 33
5.5.5 Požadavky na používání časových razítek při uchovávání záznamů 33
5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí) 33
5.5.7 Postupy pro získání a ověření uchovávaných informací 34
5.6 Obnova po havárii nebo kompromitaci 34
5.6.1 Postup ošetření incidentu nebo kompromitace 34
5.6.2 Poškození výpočetních prostředků, softwaru nebo dat 34
5.6.3 Schopnost obnovit činnost po havárii 34
5.7 Ukončení činnosti poskytovatele služeb 34
6 Řízení technické bezpečnosti 35
6.1 Kryptografie, soukromý klíč a jeho ochrana 35
6.2 Počítačová bezpečnost 35
6.2.1 Specifické technické požadavky na počítačovou bezpečnost 35
6.2.2 Hodnocení počítačové bezpečnosti 35

6.3 Technické řízení životního cyklu 36
6.3.1 Řízení vývoje systému pro poskytování služby 36
6.3.2 Řízení správy bezpečnosti 37
6.3.3 Řízení životního cyklu bezpečnosti 37
6.4 Řízení bezpečnosti sítě 37
6.5 Ochrana proti padělání a odcizení dat 37
7 Hodnocení shody a jiná hodnocení 38
7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení 38
7.2 Identita a kvalifikace hodnotitele 38
7.3 Vztah hodnotitele k hodnocenému subjektu 38
7.4 Hodnocené oblasti 38
7.5 Postup v případě zjištění nedostatků 38
7.6 Sdělování výsledků hodnocení 38
8 Ostatní obchodní a právní záležitosti 40
8.1 Poplatky 40
8.1.1 Poplatky za využívání služby 40
8.1.2 Poplatky za další služby 40
8.1.3 Postup při refundování 40
8.2 Finanční odpovědnost 40
8.2.1 Krytí pojištěním 40
8.2.2 Další aktiva 40
8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele 40
8.3 Důvěrnost obchodních informací 41
8.3.1 Rozsah důvěrných informací 41
8.3.2 Informace mimo rámec důvěrných informací 41
8.3.3 Odpovědnost za ochranu důvěrných informací 41
8.4 Ochrana osobních údajů 41
8.4.1 Politika ochrany osobních údajů 41
8.4.2 Informace považované za osobní údaje 41
8.4.3 Informace nepovažované za osobní údaje 41
8.4.4 Odpovědnost za ochranu osobních údajů 42
8.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním 42
8.4.6 Poskytování osobních údajů pro soudní či správní účely 42
8.4.7 Jiné okolnosti zpřístupňování osobních údajů 42
8.5 Práva duševního vlastnictví 42

8.6 Zastupování a záruky 42
8.6.1 Zastupování a záruky I.CA 42
8.6.2 Zastupování a záruky kontaktního místa 42
8.6.3 Zastupování a záruky ostatních zúčastněných subjektů 43
8.7 Zřeknutí se záruk 43
8.8 Omezení odpovědnosti 43
8.9 Záruky a odškodnění 43
8.10 Doba platnosti, ukončení platnosti 44
8.10.1 Doba platnosti 44
8.10.2 Ukončení platnosti 44
8.10.3 Důsledky ukončení a přetrvání závazků 44
8.11 Individuální upozorňování a komunikace se zúčastněnými subjekty 44
8.12 Novelizace 44
8.12.1 Postup při novelizaci 44
8.12.2 Postup a periodicita oznamování 44
8.12.3 Okolnosti, při kterých musí být změněn OID 45
8.13 Ustanovení o řešení sporů 45
8.14 Rozhodné právo 45
8.15 Shoda s právními předpisy 45
8.16 Další ustanovení 45
8.16.1 Rámcová dohoda 45
8.16.2 Postoupení práv 45
8.16.3 Oddělitelnost ustanovení 45
8.16.4 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv) 45
8.16.5 Vyšší moc 46
8.17 Další opatření 46
9 Závěrečná ustanovení 47

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	19.10.2022	Generální ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.01	26.08.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace seznamu odkazovaných standardů, zohlednění požadavků ETSI TS 119 411-6. Revize textu.
1.02	16.08.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace v souvislosti s S/MIME BR.
1.03	25.08.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Oprava formálních chyb.
1.04	12.09.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Oprava chyby v kapitole 1.2.

1 ÚVOD

Tento dokument stanoví zásady, které První certifikační autorita, a.s., (dále též I.CA) uplatňuje v souladu s platnými právními předpisy a mezinárodně uznávanými technickými normami při zajištění služby vytváření kvalifikovaných elektronických pečetí na dálku (I.CA RemoteSeal, dále též Služba). Dokument zároveň uvádí postupy pro uživatele Služby (dále též Klient) vztahující se k vydání a správě příslušného kvalifikovaného certifikátu (dále též Certifikát). Klientem je právnická osoba, nebo organizační složka státu.

Právní požadavky na Službu jsou definovány:

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

Pozn.: Pokud jsou v dalším textu uváděny odkazy na standardy nebo právní předpisy, jedná se vždy buď o uvedený standard nebo právní předpis, resp. standard či právní předpis, který ho nahrazuje. Pokud by byla tato politika v rozporu se standardy nebo právními předpisy, které nahradí dosud platné, bude vydána její nová verze.

Služba společnosti První certifikační autorita, a.s., zajišťující vytváření kvalifikovaných elektronických pečetí na dálku je poskytována všem Klientům na základě uzavřeného smluvního vztahu. První certifikační autorita, a.s., dále nijak neomezuje potenciální Klienty, poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

1.1 Přehled

Dokument **Politika služby vytváření kvalifikovaných elektronických pečetí na dálku** (dále též Politika) vypracovaný společností První certifikační autorita, a.s., se zabývá skutečnostmi, vztahujícími se ke Službě s přihlédnutím k platným standardům Evropské unie a k právu České republiky v dané oblasti a obsahuje i informace vyplývající z požadavků na definování politiky vytváření podpisů (resp. pečetí). Dokument je rozdělen do devíti kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument, obecně popisuje subjekty, které participují na poskytování Služby a definuje přípustné využití Služby.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace ke Službě.
- Kapitola 4 definuje procesy životního cyklu Služby až po ukončení poskytování služby.
- 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 včetně počítačové a síťové ochrany.
- Kapitola 7 je zaměřena na problematiku hodnocení poskytované Služby.
- Kapitola 8 zahrnuje problematiku obchodní a právní, včetně ochrany osobních údajů.
- Kapitola 9 obsahuje závěrečná ustanovení.

Bližší podrobnosti o Službě poskytované podle této Politiky jsou uvedeny ve dvou prováděcích směrnicích (dále též Směrnice), jejichž existence je vyžadována standardy ETSI TS 119 431-1 a ETSI TS 119 431-2 (viz kapitola 6.1.2), a to Prováděcí směrnice služby I.CA RemoteSeal ETSI TS 119 431-1 (dle též Směrnice1) a Prováděcí směrnice služby I.CA RemoteSeal ETSI TS 119 431-2 (dále též Směrnice2).

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu:	Politika služby vytváření kvalifikovaných elektronických pečetí na dálku, verze 1.04
Podporovaná OID:	**0.4.0.19431.2.1.2** (eu-advanced-x509, AdES založený na X.509 certifikátech), a **0.4.0.19431.1.1.2** (Normalized SSASC policy) - v případě, že pečetící klíče jsou uloženy v SCDev, nebo **0.4.0.19431.1.1.3** (EU SSASC policy) - v případě, že pečetící klíče jsou uloženy v QSCD.

1.2.1 Politika vytváření pečetí (podpisů)

V rámci Služby je v každém okamžiku podporována jediná politika vytváření pečetí. Je implementována v rámci komponenty RSeC umístěné v prostředí Klienta, která zabezpečeně komunikuje s poskytovatelem Služby. Aplikovaná verze politiky je dána časem, kdy byla konkrétní elektronická pečeť vytvořena.

1.2.2 Podporované formáty a třídy pečetě, jejich omezení

Služba podporuje následující formáty. Znaky „-B“ na konci názvu formátu znamenají, že se jedná o formát bez časového razítka, „-T“ je formát s časovým razítkem.

CAdES

CAdES-B-B a CAdES-B-T dle normy ETSI EN 319 122, ve variantách interní a externí.

Na vstupu bude volba hash algoritmu podpisu (SHA256/SHA384/SHA512).

PAdES

PAdES-B-B a PAdES-B-T dle normy ETSI EN 319 142, ve variantách neviditelný a viditelný.

Pro popředí viditelné pečetě je možné si vybrat ze tří variant:

- pouze text (který tak zaplní celý obdélník pro viditelnou reprezentaci podpisu),
- pouze obrázek (který tak zaplní celý obdélník pro viditelnou reprezentaci podpisu),
- text i obrázek (kdy se obdélník pro viditelnou reprezentaci rozdělí na levou a pravou polovinu. V levé polovině bude obrázek, v pravé text).

Ke všem těmto variantám popředí je možné volitelně specifikovat obrázek na pozadí, který se vždy roztáhne do celého obdélníku pro viditelnou reprezentaci.

Na vstupu bude volba hash algoritmu podpisu (SHA256/SHA384/SHA512).

XAdES

XAdES-B a XAdES-T dle normy ETSI TS 103 171, ve variantě „enveloped“, přičemž na vstupu budou:

- XML dokument, který bude kompletně použit jako vstup pečetěných dat,
- určení ID elementu, do nějž bude jako poslední child element přidán element Signature obsahující nově vytvořenou kvalifikovanou elektronickou pečeť,
- definice požadovaných transformací, digest metody a mimetype odkazovaných dat pro element Reference s id="xadesReference",
- volba hash algoritmu podpisu (SHA256/SHA384/SHA512).

ASiC-E XAdES

ASiC-E XAdES-B a ASiC-E XAdES-T dle normy ETSI TS 103 174, přičemž:

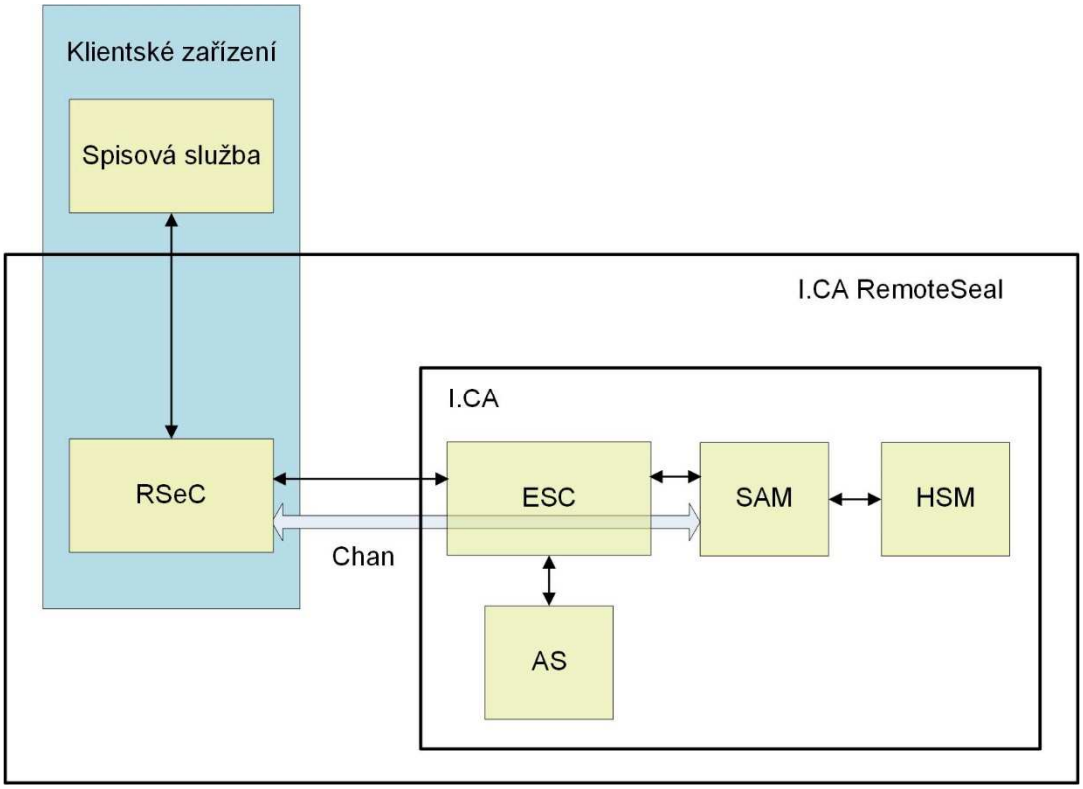
- je možné právě jeden datový objekt opatřit právě jednou kvalifikovanou elektronickou pečetí,
- není podporováno rozšíření stávajícího ASiC-E souboru o další pečeť, ani několik pečetí v rámci jednoho ASiC-E souboru,
- pro soubory typu .txt, .pdf, .xml a .png je implicitně doplněn příslušný mimetype odpovídající dané příponě; tuto implicitní volbu je možné v rozhraní explicitně přenastavit na jiný mimetype, popř. lze explicitní cestou nastavit mimetype pro ostatní (implicitně nepodporované) typy datových objektů,
- samotná XAdES pečeť uvnitř ASiC-E kontejneru obsahuje pouze minimální nezbytně nutnou množinu podepisovaných a nepodepisovaných atributů vyžadovanou danou ETSI normou,
- na vstupu bude volba hash algoritmu podpisu (SHA256/SHA384/SHA512).

1.2.3 Předávání parametrů pečetě

Definování parametrů pečetě (PAdES/CAdES/XAdES/ASiC-E XAdES atd.) je záležitostí klientské aplikace, obvykle spisové služby, volající již zmíněnou komponentu RSeC. Ta potom sestaví požadavek na vytvoření elektronické pečetě jednoho nebo více dokumentů a odešle ho poskytovateli Služby.

1.2.4 Architektura Služby

Architektura služby I.CA RemoteSeal (vytváření elektronických pečetí na dálku) je zobrazena na následujícím obrázku:



V obrázku architektury jsou použity tyto pojmy a zkratky:

Pojem / zkratka	**Popis**
AS	Authorization Server, aplikační server, který zajišťuje ověření autentizace koncového uživatele (držitele klíče) a vytváření datové struktury pro SAM, která autorizuje použití příslušného soukromého klíče pro opatření odpovídajících dat elektronickou pečetí
ESC	Evolved Signature Core, základní aplikační server provozovaný I.CA, přes který probíhá veškeré komunikace týkající se pečetění z klientských komponent
HSM	Hardware Security Module, povinná součást QSCD, fyzické zařízení, které generuje párová data Klientů, udržuje databázi soukromých klíčů a realizuje pečetě po úspěšné identifikaci a autentizaci Klienta
Chan	kanál umožňující bezpečnou komunikaci aplikace RSeC s modulem SAM
RSeC	Remote Seal Connector, klientská komponenta určená pro strojové pečetění dokumentů a pro integraci do spisové služby nebo jiného systému, který potřebuje autonomně vytvářet kvalifikované pečetě; existuje ve více variantách pro snadnou integraci do různých systémů

	komponenta vytvořená v I.CA, ale provozovaná v prostředí třetí strany, sloužící mj. pro zasílání požadavků na pečetě do fronty na serveru ESC, a naopak dostávající z ESC pečetě formátů AdES
SAM	Signature Activation Module, povinná součást QSCD pro vzdálenou pečeť, která zajišťuje kontrolu přístupu k soukromým pečetícím klíčům
Spisová služba	aplikace Klienta, která vyžaduje opatření dokumentů elektronickou pečetí

Obdobnou funkcionalitu, tedy vytváření elektronických pečetí na dálku, ale napřímo, nikoliv přes komponentu RSec navázanou na spisovou služby Klienta, poskytuje také autonomní aplikace RemoteSealProFi.

1.3 Participující subjekty

1.3.1 Poskytovatel služeb

Společnost První certifikační autorita, a.s., jako kvalifikovaný poskytovatel služeb vytvářejících důvěru.

1.3.2 Kontaktní místa

Kontaktní místa:

- přijímají žádosti o Službu poskytovanou podle této Politiky,
- zřizují Službu včetně vydání kvalifikovaného Certifikátu,
- poskytují potřebné informace, přijímají reklamace atd.,
- jsou oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela, nebo zčásti výkon své činnosti,
- jsou zmocněna jménem I.CA uzavírat Smlouvy,
- zajišťují zpoplatňování služeb I.CA poskytovaných prostřednictvím kontaktních míst, pokud není stanoveno smlouvou jinak.

1.3.3 Spoléhající se strany

Spoléhající se stranou je subjekt, který se spoléhá na kvalifikovanou elektronickou pečeť vytvořenou v rámci Služby.

1.3.4 Jiné participující subjekty

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

1.4 Použití služby

1.4.1 Přípustné použití služby

Službu provozovanou podle této Politiky lze využívat v procesu vytváření kvalifikované elektronické pečetě, vždy v souladu s platnou právní úpravou.

1.4.2 Omezení použití služby

Služba provozovaná podle této Politiky nesmí být používána v rozporu s přípustným použitím popsaným v kapitole 1.4.1 a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující politiku nebo prováděcí směrnici

Tuto Politiku, resp. jí odpovídající Směrnice, spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici

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

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

1.5.3 Osoba rozhodující o souladu prováděcí směrnice s politikou služby

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených ve Směrnicích s touto Politikou, je generální ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování prováděcí směrnice

Pokud je potřebné provést změny v některé Směrnici 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 Směrnice předchází její schválení generálním ředitelem společnosti První certifikační autorita, a.s.

1.6 Pojmy a zkratky

1.6.1 Pojmy

Pojem	Vysvětlení
bezpečné kryptografické prostředí	zařízení typu QSCD (skládající se ze SAM a HSM) a databáze certifikovaným způsobem zašifrovaných soukromých klíčů (šifrovací klíč je spravován zařízením QSCD), obojí provozováno ve fyzicky zabezpečeném prostředí
elektronická pečeť	kvalifikovaná elektronická pečeť dle platné právní úpravy pro služby vytvářející důvěru
elektronická pečeť na dálku	elektronická pečeť vytvořená soukromým klíčem, který je uložen v bezpečném kryptografickém prostředí, přičemž je pro tento klíč zajištěna kontrola oprávněné organizace nad využíváním Služby a použitím klíče
orgán dohledu	subjekt dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru
politika vytváření pečetě (podpisu)	soubor pravidel o omezení vztahujících se k vytvářeným elektronickým pečetím (podpisům)
právní úprava pro služby vytvářející důvěru	platné právní předpisy České republiky vztahující se ke službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru	služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru, definovaná právní úpravou pro služby vytvářející důvěru
smlouva	text smlouvy v elektronické nebo listinné podobě
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
soukromý klíč	jedinečná data pro vytváření elektronické pečetě
veřejný klíč	jedinečná data pro ověřování elektronické pečetě
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

1.6.2 Zkratky

Zkratka	Vysvětlení
AdES	Advanced Electronic Signature, typ elektronického podpisu/pečetě
ASiC-E	Associated Signature Container – Extended, kontejnerová struktura pro svázání podepisovaných/pečetěných dat a externího podpisu/pečeti do jednoho soboru – kontejneru

CAdES	CMS Advanced Electronic Signature, typ elektronického podpisu/pečetě
ČR	Česká republika
ČSN	označení českých technických norem
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EU	Evropská unie
EZS	elektronická zabezpečovací signalizace
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)
HSM	Hardware Security Module
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
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
ISMS	Information Security Management System, systém řízení bezpečnosti informací
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
PAdES	PDF Advanced Electronic Signature, typ elektronického podpisu/pečetě
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování–Zavedení–Kontrola–Využití, Demingův cyklus, metoda neustálého zlepšování

QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu/pečetě
SAM	Signature Activation Module,
SCDev	Secure Cryptographic Device, bezpečné kryptografické zařízení
S/MIME BR	dokument „Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" organizace CA/Browser Forum
TS	Technical Specification, typ ETSI standardu
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
XAdES	XML Advanced Electronic Signature, typ elektronického podpisu/pečetě
ZOOÚ	aktuální právní úprava týkající se ochrany osobních údajů

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

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

2.2 Zveřejňování informací a dokumentace

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

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Česká republika
- internetová adresa http://www.ica.cz.

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 také informace o Službě.

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

2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- politika Služby – po schválení a vydání nové verze,
- prováděcí směrnice Služby – po schválení a vydání nové verze,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb vytvářejících důvěru.

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 platnou právní úpravou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

3 IDENTIFIKACE A AUTENTIZACE KE SLUŽBĚ

3.1 Počáteční ověření identity

Službu mohou využívat Klienti, kteří mají s I.CA uzavřenou platnou Smlouvu. Pravidla uvedená v následujících podkapitolách platí i pro vydání kvalifikovaného certifikátu (Certifikátu), který je integrální součástí Služby.

3.1.1 Ověřování identity organizace

Pro ověření identity Klienta musí být předložen:

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

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

3.1.2 Ověřování identity fyzické osoby

Oprávněná osoba Klienta, dále též Osoba, je buď uvedena ve Smlouvě, nebo je vybavena úředně ověřenou plnou mocí k zastupování Klienta podepsanou statutárním zástupcem Klienta. Tato Osoba je oprávněna požádat o vydání prvotního autentizačního komerčního certifikátu na čipové kartě Starcos 3.5 a vyšší a automaticky se stává správcem služby pečetění daného Klienta.

V procesu ověřování identity Osoby jsou vyžadovány dva doklady, primární a sekundární, obsahující údaje uvedené níže v této kapitole.

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

Z tohoto dokladu jsou ověřovány následující údaje:

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

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

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

Údaje v sekundárním osobním dokladu sloužící k jednoznačné identifikaci osoby zastupující Organizaci musí být shodné s těmito údaji v primárním osobním dokladu.

3.1.3 Ověřování e-mailové adresy

Ověření e-mailové adresy je prováděno dvěma způsoby, a to kontrolou příslušnosti adresy k registrované DNS doméně (validating authority over mailbox via domain) nebo ověřením držitele e-mailové adresy pomocí obsahu zasílaného e-mailu (validating control over mailbox via email). Užití příslušné ověřovací metody odvisí od typu smluvního vztahu s klientem.

3.1.3.1 Ověřování proti registrované DNS doméně

Metoda ověření e-mailové adresy vůči registrované DNS doméně je určena pro firemní zákazníky, kde smluvní partner má kontrolu nad příslušnou DNS doménou. V takovém případě se ověřuje příslušnost doménové části e-mailové adresy vůči interně udržovanému seznamu registrovaných podnikových domén (podnik má s I.CA uzavřenou smlouvu a kontrola nad DNS doménou byla ověřena).

3.1.3.2 Ověřování adresy pomocí obsahu zasílaného ověřovacího e-mailu

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

3.2 Ověření identity při prodloužení služby

Prodloužení Služby probíhá automatizovaně v určitém předstihu před vypršením platnosti Certifikátu původního a provést ho může jen a pouze oprávněná osoba Klienta, tedy Osoba.

3.3 Změna údajů

Pokud vzhledem ke změně údajů není možné provést prodloužení Služby, musí dojít k uzavření dodatku ke smlouvě a vydání nového autentizačního i pečetícího certifikátu.

3.4 Identifikace a autentizace při požadavku na zneplatnění Certifikátu

Subjekty oprávněné podat žádost o zneplatnění Certifikátu jsou vyjmenovány v kapitole 4.7.2.

V případě **osobního předání žádosti o zneplatnění Certifikátu na kontaktním místě** musí být žádost o zneplatnění Certifikátu písemná a podepsaná osobou, která je buď oprávněna jednat za Klienta ze zákona, nebo je uvedena ve Smlouvě, nebo má pověření jednat za Klienta podepsané osobou jednat za Klienta ze zákona. Identita osoby musí být řádně ověřena (viz kapitola 3.1.2).

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

- prostřednictvím formuláře na webových stránkách společnosti (s využitím hesla pro zneplatnění Certifikátu),

- prostřednictvím elektronické zprávy, která je opatřena elektronickým podpisem/pečetí, kde:
  - elektronický podpis/pečeť musí být vytvořen soukromým klíčem příslušným k zneplatňovanému Certifikátu,
  - zpráva musí být odeslána na adresu revoke@ica.cz,
- prostřednictvím nepodepsané elektronické zprávy:
  - která obsahuje heslo pro zneplatnění,
  - zpráva musí být odeslána na adresu revoke@ica.cz,
- prostřednictvím datové schránky I.CA (s využitím hesla pro zneplatnění Certifikátu).

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

Údaje, které musí žádost o zneplatnění Certifikátu obsahovat, jsou uvedeny v kapitole 4.7.3.

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

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS SLUŽBY

V následujících podkapitolách je popsán životní cyklus služby.

4.1 Uzavření smlouvy

Před zřízením Služby musí být podepsána Smlouva o zřízení a využívání Služby mezi I.CA a Klientem, identita Klienta musí být ověřena v souladu s ustanoveními kapitoly 3.1.1. Následně může Osoba navštívit kontaktní místo a zažádat o zřízení Služby. Identita Osoby je ověřována v souladu s ustanoveními kapitola 3.1.2

4.2 Zřízení Služby

Zřízení služby probíhá na kontaktních místech, kterými jsou vybrané registrační autority I.CA. Osoba s potřebnými doklady kontaktní místo navštíví a po ověření její identity v souladu s ustanoveními kapitoly 3.1.2 je jí vydán osobní autentizační komerční certifikát na čipovou kartu Starcos 3.5 nebo vyšší. Osoba se tímto automaticky stává správcem služby pečetění pro daného Klienta.

Následně je pracovníkem kontaktního místa provedeno zřízení služby I.CA RemoteSeal včetně vydání Certifikátu pro daného Klienta, přičemž klíčový pár příslušející tomuto Certifikátu je generován QSCD zařízením služby I.CA RemoteSeal a soukromý klíč je dále uložen a spravován v příslušném bezpečném kryptografickém prostředí.

V rámci vydání Certifikátu Osoba podepisuje dokumentaci související s vydáním Certifikátu, přičemž tato může být podepsána:

- klasicky vlastnoručním podpisem na papírový dokument, nebo
- bezpapírově/elektronicky pomocí osobního autentizačního komerčního certifikátu Osoby.

4.2.1 Registrační proces a odpovědnosti

Osoba zastupující Klienta je povinna zejména:

- seznámit se s touto Politikou a s Certifikační politikou vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku (algoritmus RSA) a smluvně se zavázat jednat podle nich,
- seznámit se se Smlouvou,
- dodržovat veškerá ustanovení Smlouvy,
- používat Službu v souladu s ustanoveními kapitoly 1.4,
- nakládat s údaji pro identifikaci a autentizaci ke Službě tak, aby nemohlo dojít k jejímu zneužití,
- neprodleně vyrozumět poskytovatele Služby o podezření, že údaje pro identifikaci a autentizaci ke Službě byly zneužity a požádat o zneplatnění Certifikátů,
- neprodleně uvědomit poskytovatele Služby o změnách údajů uvedených ve Smlouvě (a v Certifikátu),
- poskytovat pravdivé a úplné informace pro zřízení Služby, resp. pro vydání Certifikátů,

- překontrolovat, zda údaje získané z předložených dokumentů jsou správné a odpovídají požadovaným údajům,
- zvolit vhodné heslo pro zneplatnění Certifikátu (minimální/maximální délka hesla 4/32 znaků, povolené znaky 0..9, A..Z, a..z),
- v případě požadavku na ukončení Služby je povinností Osoby informovat o této skutečnosti I.CA a po vzájemné dohodě sjednanou formou smlouvu ukončit.

Poskytovatel Služby je povinen zejména:

- před uzavřením Smlouvy informovat Klienta o smluvních podmínkách,
- uzavírat s Klientem Smlouvu obsahující náležitosti požadované platnou právní úpravou a technickými standardy,
- v procesu zřizování Služby ověřit všechny ověřitelné údaje podle předložených dokladů,
- vydat Certifikát obsahující věcně správné údaje na základě informací, které jsou poskytovateli Služby k dispozici v době vydávání tohoto Certifikátu,
- zveřejnit certifikáty vydávající certifikační autority a kořenové CA,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- činnosti spojené se Službou poskytovat v souladu s platnou právní úpravou, touto Politikou, odpovídající certifikační politikou, certifikační prováděcí směrnicí, Celkovou bezpečnostní politikou, Systémovou bezpečnostní politikou – důvěryhodné systémy a s provozní dokumentací.

4.3 Aktivace Služby

Organizace Klienta si může Službu aktivovat na více zařízeních, pro každou instanci (účet) je vytvořen přístupový soubor a heslo k němu. Instanci vytváří Osoba prostřednictvím aplikace RemoteSealProFi (dále též Aplikace), v průběhu vytváření je vyžadováno zadání jména instance (pro interní identifikaci v rámci Klienta) a nastavení hesla. Po dokončení je po výběru adresáře přístupový soubor sloužící pro autentizaci vůči Službě uložen.

4.4 Správa Služby

Správa klientské aplikace Služby je prováděna v Aplikace. Jejím prostřednictvím Osoba jednak spravuje klientskou komponentu pro strojové pečetění dokumentů, tj. přidává, ruší, blokuje, odblokovává a přejmenovává uživatelské účty a dále řídí vydání následného pečetícího certifikátu.

4.5 Prodloužení Smlouvy

S předstihem před koncem platnosti aktuálního pečetícího certifikátu (třicet, deset a pět dnů) je Osoba informována o blížícím se konci platnosti Certifikátu pomocí automaticky odesílaného e-mailu, informace je také Osobě zobrazována po přihlášení se do Aplikace. Pro vydání následného certifikátu musí Osoba provést následující kroky:

- přihlásit se do aplikace RemoteSealProFi,
- otevřít správu Certifikátu,

- stisknout tlačítko „Obnovit certifikát“.

Aplikace zajistí vytvoření žádosti o následný certifikát a zobrazí detail žádosti o vydání následného certifikátu. Dále:

- Osoba stiskne tlačítko „Podepsat“ a zadá své heslo ke Službě,
- Služba následně zajistí vydání následného Certifikátu a po jeho vydání naplánuje jeho odložené nasazení (patnáct dní, resp. počet dní zbývajících do konce platnosti původního pečetícího certifikátu); Osoba může interval odložení v Aplikaci změnit).

Osoba si může po vydání Certifikátu v aplikaci zobrazit informace o novém Certifikátu, uložit si nový Certifikátu do souboru a vidět přesný čas plánovaného nasazení nového Certifikátu.

4.6 Konec platnosti Smlouvy

Platnost Smlouvy končí, pokud Klient Certifikát pro vydávání pečetí zneplatní a tento je uveden na CRL. Další možné způsoby ukončení smluvního vztahu jsou definovány Smlouvou.

4.7 Zneplatnění Certifikátu a pozastavení platnosti Certifikátu

Ke zneplatnění Certifikátu dojde vždy při ukončení smlouvy o poskytování Služby (např. Osoba nepodepíše žádost o vydání následného certifikátu a tomu vyprší platnost).

Kromě toho je možné požádat o zneplatnění certifikátu. Žádosti o zneplatnění Certifikátu přijímá I.CA nepřetržitě prostřednictvím formuláře na webových stránkách společnosti. Nepřetržitě je možné podat žádost o zneplatnění Certifikátu také prostřednictvím e-mailu, datové schránky a listovní zásilky. Takto podaná žádost je přijata nejpozději následující pracovní den po jejím doručení.

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

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

4.7.1 Podmínky pro zneplatnění

4.7.1.1 Důvody zneplatnění uživatelského certifikátu

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

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

5. I.CA získá důkaz, že na metodu pro ověření vlastnictví domény nebo kontroly nad mailovou adresou pro kteroukoliv mailovou adresu v Certifikátu nelze spoléhat (CRLReason #4, superseded).

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

6. Certifikát nevyhovuje požadavkům na kryptografické algoritmy a jejich požadovaným parametrům (kvalitě, viz kapitoly 6.1.5 a 6.1.6) (CRLReason #4, superseded),
7. I.CA získá důkaz, že Certifikát byl zneužit (CRLReason #9, privilegeWithdrawn),
8. I.CA je vyrozuměna, že držitel Certifikátu porušil jednu nebo více ze svých důležitých povinností plynoucích ze smlouvy o vydání Certifikátu nebo smlouvy o podmínkách používání Certifikátu (CRLReason #9, privilegeWithdrawn),
9. I.CA je vyrozuměna o okolnostech indikujících, že e-mailová adresa plně kvalifikované jméno domény uvedené v certifikátu není dále právně přípustné (tj. soud nebo arbitráž odňaly registrantovi právo používat e-mailovou adresu nebo doménové jméno, zrušily relevantní smlouvu, smlouva o licenci nebo službě mezi registrantem doménového jména a žadatelem o certifikát byla zrušena, nebo se registrantovi doménového jména nepodařilo e-mailovou adresu nebo doménové jméno udržet v aktivním stavu) CRLReason #5, cessationOfOperation),
10. I.CA je vyrozuměna, že došlo ke podstatným změnám informací obsažených v Certifikátu (CRLReason #9, privilegeWithdrawn),
11. I.CA je vyrozuměna, že Certifikát nebyl vydán v souladu s S/MIME BR, CP nebo CPS (CRLReason #4, superseded),
12. I.CA zjistí, že některá informace v Certifikátu je nepřesná nebo zavádějící (CRLReason #9, privilegeWithdrawn),
13. oprávnění I.CA vydávat Certifikáty podle S/MIME BR a této CP vypršelo, bylo zneplatněno, nebo ukončeno a I.CA nepřipravila způsob, jak udržovat CRL/OCSP úložiště (nespecifikováno – unspecified(0); tento kód se v CRL u položky neuvádí),
14. zneplatnění je vyžadováno CP nebo CPS (nespecifikováno – unspecified(0); tento kód se v CRL u položky neuvádí),
15. CRLReason #1, keyCompromise v případech, že:
    - je I.CA je vyrozuměna o předvedené nebo prokázané metodě pro kompromitaci soukromého klíče držitele Certifikátu,
    - nebo je jasný důkaz, že konkrétní metoda použitá pro generování soukromého klíče obsahovala chybu.

4.7.1.2 Důvody zneplatnění certifikátu Autority

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

1. Autorita požádá písemně o zneplatnění,
2. Autorita oznámila kořenové certifikační autoritě, že původní žádost o její certifikát byla neoprávněná a že zpětně neudělí autorizaci,
3. kořenová certifikační autorita je vyrozuměna, že soukromý klíč Autority byl kompromitován, nebo nadále nesplňuje požadavky na kryptografické algoritmy a požadované parametry (kvalitu, viz kapitola 6.1.5 a 6.1.6),
4. kořenová certifikační autorita je vyrozuměna, certifikát Autority byl zneužit,

5. kořenová CA je vyrozuměna, že certifikát Autority nebyl vydán v souladu s S/MIME BR, příslušnou CP nebo CPS, nebo nesplňuje jejich požadavky,
6. I.CA zjistí, že některá informace v certifikátu Autority je nepřesná nebo zavádějící
7. kořenová CA nebo Autorita ukončily z nějakého důvodu činnost a nepřevedly podporu zneplatňování na jinou CA,
8. právo kořenové CA nebo Autority vydávat certifikáty podle podmínek S/MIME BR nebo CP vypršelo, nebo bylo odvoláno či ukončeno a kořenová CA nezajistila pro Autoritu pokračující správu úložiště CRL/OCSP,
9. zneplatnění je vyžádáno CP a/nebo CPS kořenové CA.

4.7.2 Kdo může požádat o zneplatnění Certifikátu

Žádost o zneplatnění Certifikátu mohou podat:

- poskytovatel Služby (oprávněným žadatelem o zneplatnění Certifikátu je v tomto případě generální ředitel I.CA, nebo jím pověřený člen představenstva):
  - v případě, že Certifikát byl vydán na základě nepravdivých údajů,
  - pokud zjistí, že při vydání Certifikátu nebyly splněny požadavky platné právní úpravy pro služby vytvářející důvěru,
  - dozví-li se prokazatelně, že Certifikát byl použit v rozporu s omezením definovaným v kapitole 1.4.2,
  - dozví-li se prokazatelně, že držitel Certifikátu zanikl, nebo pokud údaje, na jejichž základě byl Certifikát vydán, pozbyly pravdivosti,
  - pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném certifikátu,
  - pokud prokazatelně zjistí, že soukromý klíč, patřící k veřejnému klíči uvedenému v Certifikátu, byl kompromitován (došlo ke kompromitace autentizačních údajů k tomuto soukromému klíči),
  - dojde k ukončení smlouvy o poskytování Služby podle této Politiky,
- orgán dohledu, případně další subjekty definované platnou právní úpravou pro služby vytvářející důvěru.

Žádost o zneplatnění Certifikátu mohou dále podat:

- držitel Certifikátu (Klient) prostřednictvím Osoby,
- subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování Služby podle této Politiky,
- subjekt pověřený jednáním za právního nástupce původního subjektu (Organizace), jemuž byl Certifikát vydán,
- prostřednictvím oprávněného pracovníka subjekty, jimž to umožňuje platná právní úprava.

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

Kromě toho další strany (např. orgán dohledu, orgány činné v trestním řízení, spoléhající se strany, dodavatelé aplikačního SW) mohou zasílat hlášení o problému s Certifikátem informující Autoritu o dostatečných důvodech pro zneplatnění Certifikátu – viz kapitola 4.7.3.

4.7.3 Postup při podání žádosti o zneplatnění

Pro žádost o zneplatnění Certifikátu podávanou Klientem (jeho držitelem) platí:

- V případě osobního předání žádosti o zneplatnění Certifikátu na kontaktním místě (RA) musí žádost obsahovat sériové číslo Certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“), jméno, popř. jména a příjmení fyzické osoby oprávněné žádat zneplatnění certifikátu a heslo pro zneplatnění certifikátu. Pokud fyzická osoba oprávněná žádat zneplatnění Certifikátu heslo pro zneplatnění nezná, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla primárního osobního dokladu předloženého při žádosti o vydání Certifikátu, nebo čísla nového primárního osobního dokladu, pokud byl původní nahrazen novým. Tímto osobním dokladem se musí pracovníkovi RA prokázat. V případě, že je žádost oprávněná, pracovník RA certifikát zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. V případě, že žádost o zneplatnění Certifikátu nelze akceptovat (nesprávné heslo pro zneplatnění, neprokazatelná identita fyzické osoby oprávněné žádat zneplatnění Certifikátu), pokusí se pracovník RA v součinnosti s touto fyzickou osobou tyto skutečnosti napravit a pokud to z libovolného důvodu nebude možné, žádost o zneplatnění Certifikátu bude zamítnuta. Žadatel o zneplatnění Certifikátu je vždy o výsledku informován prostřednictvím pracovníka RA.
- V případě předání žádosti o zneplatnění Certifikátu elektronickou cestou jsou přípustné následující možnosti:
  - Prostřednictvím formuláře na internetové informační adrese. Datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. O kladném vyřízení je žadatel informován.
  - Elektronická zpráva opatřená elektronickou pečetí – tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

    Zadam o zneplatneni certifikatu cislo = xxxxxxx,

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

    Zpráva musí být opatřena elektronickou pečetí vytvořenou soukromým klíčem příslušným k veřejnému klíči ve zneplatňovaném Certifikátu.
  - Elektronicky podepsaná či ve zvláštních případech nepodepsaná zpráva odeslaná definovanou osobou pověřenou za Organizaci vystupovat ve smluvním vztahu s I.CA:

    Zadam o zneplatneni certifikatu cislo = xxxxxxx,

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

  Pokud žádost splňuje požadavky jedné z výše uvedených možností, odpovědný pracovník Certifikát v systému CA neprodleně zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. O kladném vyřízení je žadatel informován.
- V případě použití doporučené listovní zásilky pro podání žádosti o zneplatnění Certifikátu musí být žádost v následujícím tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

Heslo pro zneplatneni = yyyyyy,

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

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.

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

4.7.4 Prodleva při požadavku na zneplatnění certifikátu

Požadavek na zneplatnění Certifikátu musí být podán bezodkladně.

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

4.8 Používání Služby

Postup opatřování dokumentů kvalifikovanou elektronickou pečetí je následující:

- spisová služba předá komponentě RSeC přístupový soubor, heslo, seznam dokumentů, které mají být opatřeny elektronickou pečetí a požadované parametry pečetí (viditelný nebo neviditelný, formát, s nebo bez časového razítka) – předáním vyjadřuje klient nepopiratelný souhlas s obsahem dokumentu, který bude opatřen elektronickou pečetí,
- komponenta RSeC připraví datové struktury dle požadavků norem (včetně hashů pečetěných souborů, kompletní soubory nejsou poskytovateli Služby předávány) a autorizuje použití soukromého klíče uloženého v HSM modulu,
- komponenta RSeC získá zpět vytvořenou pečetící strukturu včetně případného časového razítka,
- komponenta RSeC sestaví kompletní dokumenty opatřené elektronickou pečetí a předá je zpět spisové službě.

4.9 Dodatečná bezpečnostní opatření

Pro jednotlivé instance/účty je možné nastavit doplňkové zabezpečení určující, odkud může daný účet Službu kontaktovat (omezení na určitou VPN mezi Klientem a I.CA, zabezpečení komunikace konkrétním certifikátem atd.).

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Postupy správy, řízení a provozu jsou zaměřeny především na:

- systém poskytované Služby,
- veškeré procesy podporující poskytování Služby.

Postupy správy, řízení a provozu jsou řešeny jak v dokumentu Celková bezpečnostní politika, tak dále v Systémové bezpečnostní politice – důvěryhodné systémy, Směrnicích, Plánu pro zvládání krizových situací a plánu obnovy a v upřesňující interní dokumentaci. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Objekty provozního pracoviště jsou umístěny v geograficky odlišných lokalitách, které jsou dále jiné než ředitelství společnosti, obchodní a vývojová pracoviště, pracoviště kontaktních a obchodních míst.

Zařízení určená k výkonu Služby jsou umístěna 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 společnosti. 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 určených k výkonu Služby je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20 °C ± 5 °C. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

5.1.4 Vlivy vody

Všechny kritické systémy provozních pracovišť 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

umístěna zařízení určená k výkonu Služby, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroje.

5.1.6 Ukládání médií

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

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

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

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

Zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, který by mohl ohrozit nestrannost operací I.CA. Postup jmenování zaměstnanců do důvěryhodných rolí a specifikace těchto rolí jsou uvedeny v interní dokumentaci.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro procesy související s citlivými daty Klientů nutnými pro provoz Služby jsou definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

- inicializaci kryptografického modulu pro generování a ukládání citlivých dat nutných pro provoz Služby,
- zálohování těchto dat,
- obnovu těchto dat.

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 a autentizaci 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 bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

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

- naprostá občanská bezúhonnost – prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z rejstříku trestů, nebo čestné prohlášení),
- 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 certifikačních/důvěryhodných služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

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

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

Popis konkrétní činnosti zaměstnance je definován pracovní smlouvou.

Dokud nejsou dokončeny veškeré vstupní kontroly zaměstnance, není mu umožněn logický ani fyzický přístup k systémům pro výkon Služby.

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

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích I.CA jsou:

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

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

5.3.3 Požadavky na školení

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

5.3.4 Požadavky a periodicita doškolování

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

Pro pracovníky kontaktních míst je minimálně jednou za tři roky pořádáno školení zaměřené na procesy spojené s činností kontaktního místa.

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 zaměstnanců

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem popsaným v interních dokumentech společnosti a řídícím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

5.3.7 Požadavky na nezávislé dodavatele

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

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci I.CA mají k dispozici, kromě Politiky a Směrnice služby, bezpečnostní a provozní dokumentaci, 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 platnou právní úpravou pro služby vytvářející důvěru a příslušnými technickými standardy a normami.

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 těchto 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 10 let od jejich vzniku.

5.4.4 Ochrana auditních záznamů

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

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

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

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů Služby 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 Službou je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

Uchovávání záznamů, tj. informací a dokumentace, je u I.CA prováděno podle interní dokumentace.

5.5.1 Typy uchovávaných záznamů

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

- smlouvy s Klienty a jejich případné dodatky související se Službou,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování záznamů

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 interními normami a směrnicemi. 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 Obnova po havárii nebo kompromitaci

5.6.1 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.

5.6.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz kapitola 5.6.1.

5.6.3 Schopnost obnovit činnost po havárii

Viz kapitola 5.6.1.

5.7 Ukončení činnosti poskytovatele služeb

Pro ukončování činnosti kvalifikovaného poskytovatele služby vytvářející důvěru platí následující pravidla:

- ukončení činnosti kvalifikovaného poskytovatele služby vytvářející důvěru musí být písemně oznámeno orgánu dohledu a všem subjektům, které mají uzavřenou Smlouvu na využívání Služby.
- ukončení činnosti poskytovatele služby vytvářející důvěru musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity služeb.

V případě odnětí statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru dle platné právní úpravy:

- informace o odnětí statutu musí být písemně nebo elektronicky oznámena všem subjektům, které mají uzavřenou Smlouvu na využívání Služby,
- informace o odnětí statutu musí být zveřejněna v souladu s kapitolou 2.2,
- na základě rozhodnutí orgánu dohledu o dalším postupu rozhodne generální ředitel I.CA, případně jím pověřená osoba.

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Kryptografie, soukromý klíč a jeho ochrana

V rámci služba je zásadně využívána kryptografie RSA. Délka klíčů odpovídá požadavkům ETSI TS 119 312.

Párová data klientů Služby jsou generována a soukromé klíče uloženy v kryptografickém modulu, případně v zařízení typu QSCD pod výhradní kontrolou I.CA. Přístup k soukromým klíčů je chráněn kryptografickým protokolem, který zajišťuje, že přístup ke klíči má pouze jeho oprávněný majitel.

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

Soukromé klíče klientů jsou zálohovány v zašifrované podobě, která zajišťuje stejnou úroveň ochrany jako kryptografické zařízení.

6.2 Počítačová bezpečnost

6.2.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti komponent použitých pro poskytování Služby je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů, a jejich periodicity, definována platnou právní úpravou pro služby vytvářející důvěru, resp. v ní odkazovanými technickými standardy a normami.

6.2.2 Hodnocení počítačové bezpečnosti

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

- ČSN EN 419241-1 Důvěryhodné systémy podporující podpisový server – Část 1: Obecné bezpečnostní požadavky systému.
- EN 419241-1 Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements.
- ČSN EN 419241-2 Důvěryhodné systémy podporující podpisový server – Část 2: Profil ochrany pro zařízení QSCD pro serverový podpis.
- EN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.
- ČSN EN 419221-5 – Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografické modul pro důvěryhodné služby.
- EN 419221-5 – Protection Profiles for TSP Cryptographic Modules – Part 5 - Cryptographic Module for Trust Services.
- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.

- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation.
- ETSI TS 119 432 Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation.
- ETSI EN 319 102-1 Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.
- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.
- EN 319 142 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures.
- ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.
- ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile.
- 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.
- EN 301 549 Accessibility requirements for ICT products and services.
- ČSN ETSI EN 319 403-1 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatele důvěryhodné služby – Část 1: Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodné služby.
- ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI TS 119 411-6 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation.
- ČSN EN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.

6.3 Technické řízení životního cyklu

6.3.1 Řízení vývoje systému pro poskytování služby

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.3.2 Řízení správy bezpečnosti

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

Bezpečnost informací se v I.CA řídí těmito normami:

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

6.3.3 Řízení životního cyklu bezpečnosti

Řízení životního cyklu bezpečnosti je v I.CA je 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 organizace.

6.4 Řízení bezpečnosti sítě

V prostředí I.CA nejsou důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru umístěné na provozních pracovištích I.CA přímo dostupné z veřejné sítě Internet. Tyto systémy jsou chráněny komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System). Veškerá komunikace mezi klientskou částí aplikace a provozními pracovišti je vedena šifrovaně. Podrobnosti jsou popsány v interní dokumentaci.

6.5 Ochrana proti padělání a odcizení dat

Opatření proti padělání a odcizení dat jsou součástí celého systému řízení bezpečnosti informací nejen Služby, ale všech systémů I.CA. Na jejich naplnění se spolupodílí management společnosti, vedoucí zaměstnanci i zaměstnanci v důvěryhodných rolích s příslušnými oprávněními.

7 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

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

Periodicita jiných hodnocení je dána příslušnými technickými standardy a normami.

7.2 Identita a kvalifikace hodnotitele

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

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

7.3 Vztah hodnotitele k hodnocenému subjektu

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

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

7.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného platnou právní úpravou pro služby vytvářející důvěru jsou hodnocené oblasti konkretizovány touto právní úpravou, v ostatních případech jsou hodnocené oblasti dány technickými standardy a normami, podle kterých je hodnocení prováděno.

7.5 Postup v případě zjištění nedostatků

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

7.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům platné právní úpravy pro služby vytvářející důvěru a příslušných technických standardů a norem.

O průběhu a výsledku auditu je sepsána zpráva, jejíž součástí je vyhodnocení shody auditovaných postupů s požadavky odpovídajících norem/specifikací. V případě nalezených

nedostatků je kvantifikována jejich míra vlivu na plnění kvality služeb a navrženo odpovídající nápravné opatření.

Konečnou auditní zprávu podepisuje bezpečnostní manažer, který o výsledcích auditu následně informuje členy bezpečnostního výboru na zasedání bezpečnostního výboru. V případě nalezení závažných nedostatků (významná neshoda) informuje bezpečnostní manažer členy bezpečnostního výboru v nejbližším možném termínu.

8 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 Poplatky

8.1.1 Poplatky za využívání služby

Poplatek za využívání Služby je určen počtem vytvořených elektronických pečetí a paušálem za odběrové pásmo. Poplatky za vydání certifikátů, resp. za vydání čipové karty nejsou účtovány samostatně.

8.1.2 Poplatky za další služby

Není relevantní pro tento dokument.

8.1.3 Postup při refundování

Není relevantní pro tento dokument.

8.2 Finanční odpovědnost

8.2.1 Krytí pojištěním

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

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

8.2.2 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., uveřejněné v obchodním rejstříku.

8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

8.3 Důvěrnost obchodních informací

8.3.1 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 kryptografické informace sloužící v procesu poskytování Služby,
- obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

8.3.2 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.

8.3.3 Odpovědnost za ochranu důvěrných informací

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

8.4 Ochrana osobních údajů

8.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných právních norem, tedy zejména GDPR a ZOOÚ. Informace o zásadách ochrany osobních údajů klientů je uvedena v dokumentu „Zásady nakládání s osobními údaji klientů“ vystaveném na webu společnosti – viz kapitola 2.2.

8.4.2 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.

8.4.3 Informace nepovažované za osobní údaje

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

8.4.4 Odpovědnost za ochranu osobních údajů

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

8.4.5 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.

8.4.6 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.

8.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

8.5 Práva duševního vlastnictví

Tato Politika, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systému poskytujícího Službu, jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

8.6 Zastupování a záruky

8.6.1 Zastupování a záruky I.CA

I.CA zaručuje, že poskytuje:

- technickou podporu při provozu Služby, řešení nestandardních situací a poradenství související s provozem Služby prostřednictvím kontaktních údajů uvedených na adrese www.ica.cz,
- Službu vždy právně a technicky aktuální dle relevantních právních předpisů a technických standardů a norem.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud subjekt využívající Službu neporušil povinnosti plynoucí mu ze Smlouvy a této Politiky.

8.6.2 Zastupování a záruky kontaktního místa

Kontaktní místo:

- přejímá závazek za správnost poskytovaných služeb,
- nevyřídí kladně žádost, pokud Klient odmítá sdělit potřebné údaje, nebo není oprávněn k podání žádosti o Službu,
- odpovídá za vyřizování připomínek a stížností.

8.6.3 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

8.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., poskytuje pouze záruky, uvedené v kapitole 8.6.

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

8.9 Záruky a odškodnění

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

Společnost První certifikační autorita, a.s.:

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

Společnost První certifikační autorita, a.s., **neodpovídá** za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování Služby Klientem, zejména za využívání v rozporu s podmínkami uvedenými v této Politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení.

Reklamaci je možné podat těmito způsoby:

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

Reklamující osoba je povinna uvést:

- co nejvýstižnější popis závady,
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne I.CA nejpozději do tří pracovních dnů od doručení reklamace a vyrozumí o tom reklamujícího (formou elektronické pošty, nebo doporučenou zásilkou), pokud se strany nedohodnou jinak.

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

Další možné náhrady škody vycházejí z ustanovení příslušných právních předpisů a o jejich výši může rozhodnout soud.

8.10 Doba platnosti, ukončení platnosti

8.10.1 Doba platnosti

Tato Politika nabývá platnosti dnem dle kapitoly 9 a platí minimálně po dobu poskytování Služby, nebo do nahrazení Politiky novou verzí.

8.10.2 Ukončení platnosti

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

8.10.3 Důsledky ukončení a přetrvání závazků

Po ukončení platnosti této Politiky přetrvávají z ní vyplývající závazky I.CA, a to po dobu platnosti poslední Smlouvy, podle které je Služba poskytována.

8.11 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.

8.12 Novelizace

8.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interním dokumentu.

8.12.2 Postup a periodicita oznamování

Vydání nové verze Politiky je vždy oznámeno formou zveřejňování informací.

8.12.3 Okolnosti, při kterých musí být změněn OID

OID není Politice přiřazen, Politika pokrývá požadavky politik viz kapitola 1.2. V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

8.13 Ustanovení o řešení sporů

V případě, že Klient nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

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

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

8.14 Rozhodné právo

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

8.15 Shoda s právními předpisy

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

8.16 Další ustanovení

8.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

8.16.2 Postoupení práv

Není relevantní pro tento dokument.

8.16.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto Politikou, 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.

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

Není relevantní pro tento dokument.

8.16.5 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.

8.17 Další opatření

Není relevantní pro tento dokument.

9 ZÁVĚREČNÁ USTANOVENÍ

Tato Politika služby I.CA RemoteSeal (vytváření elektronických pečetí na dálku) vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem uvedeným v tab. 1.