První certifikační autorita, a.s.



Politika služby

I.CA RemoteSign

(vytváření elektronických podpisů na dálku)

Politika služby I.CA RemoteSign (vytváření elektronických podpisů 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 1.11

Copyright © První certifikační autorita, a.s.

OBSAH

1 Úvod 8
1.1 Přehled 9
1.2 Název a identifikace dokumentu 9
1.2.1 Politika vytváření podpisů 10
1.2.2 Podporované formáty a třídy podpisů, jejich omezení 10
1.2.3 Předávání parametrů podpisu 10
1.3 Participující subjekty 10
1.3.1 Poskytovatel služeb 10
1.3.2 Kontaktní místa 11
1.3.3 Spoléhající se strany 11
1.3.4 Třetí strany 11
1.3.5 Jiné participující subjekty 12
1.4 Použití Služby 12
1.4.1 Přípustné použití Služby 12
1.4.2 Omezení použití Služby 12
1.5 Správa politiky 12
1.5.1 Organizace spravující politiku nebo prováděcí směrnici 12
1.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici 12
1.5.3 Osoba rozhodující o souladu prováděcí směrnice s politikou služby 12
1.5.4 Postupy při schvalování prováděcí směrnice 12
1.6 Pojmy a zkratky 13
2 Odpovědnost za zveřejňování a úložiště informací a dokumentace 16
2.1 Úložiště informací a dokumentace 16
2.2 Zveřejňování informací a dokumentace 16
2.3 Periodicita zveřejňování informací 16
2.4 Řízení přístupu k jednotlivým typům úložišť 16
3 Životní cyklus služby – řešení 1 17
3.1 Uzavření smlouvy 17
3.2 Identifikace a autentizace ke Službě 17
3.2.1 Počáteční ověření identity 17
3.2.2 Ověření identity při prodloužení služby 17
3.2.3 Změna údajů 17
3.3 Zřízení Služby 17

3.3.1 Povinnosti Klienta a poskytovatele Služby 18
3.4 Aktivace Služby 18
3.5 Prodloužení Smlouvy 19
3.6 Konec platnosti Smlouvy 19
3.7 Zablokování a odblokování mobilní nebo PC aplikace 19
3.7.1 Zablokování 19
3.7.2 Odblokování 20
3.8 Používání Služby 20
4 Životní cyklus služby – řešení 2 21
4.1 Uzavření smlouvy 21
4.2 Identifikace a autentizace ke Službě 21
4.2.1 Počáteční ověření identity 21
4.2.2 Ověření identity při prodloužení služby 21
4.2.3 Změna údajů 21
4.3 Zřízení a aktivace Služby 21
4.3.1 Povinnosti Klienta a poskytovatele Služby 21
4.4 Aktivace Služby 22
4.5 Prodloužení poskytování Služby 22
4.6 Konec poskytování Služby 22
4.7 Aktivace a deaktivace požívání biometriky 23
4.8 Používání Služby 23
5 Postupy správy, řízení a provozu 24
5.1 Fyzická bezpečnost 24
5.1.1 Umístění a konstrukce 24
5.1.2 Fyzický přístup 24
5.1.3 Elektřina a klimatizace 24
5.1.4 Vlivy vody 24
5.1.5 Protipožární opatření a ochrana 24
5.1.6 Ukládání médií 25
5.1.7 Nakládání s odpady 25
5.1.8 Zálohy mimo budovu 25
5.2 Procesní bezpečnost 25
5.2.1 Důvěryhodné role 25
5.2.2 Počet osob požadovaných na zajištění jednotlivých činností 25
5.2.3 Identifikace a autentizace pro každou roli 26
5.2.4 Role vyžadující rozdělení povinností 26

5.3 Personální bezpečnost 26
5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost 26
5.3.2 Posouzení spolehlivosti osob 26
5.3.3 Požadavky na školení 27
5.3.4 Požadavky a periodicita doškolování 27
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi 27
5.3.6 Postihy za neoprávněné činnosti zaměstnanců 27
5.3.7 Požadavky na nezávislé dodavatele 27
5.3.8 Dokumentace poskytovaná zaměstnancům 27
5.4 Postupy zpracování auditních záznamů 28
5.4.1 Typy zaznamenávaných událostí 28
5.4.2 Periodicita zpracování záznamů 28
5.4.3 Doba uchování auditních záznamů 28
5.4.4 Ochrana auditních záznamů 28
5.4.5 Postupy pro zálohování auditních záznamů 28
5.4.6 Systém shromažďování auditních záznamů (interní nebo externí) 28
5.4.7 Postup při oznamování události subjektu, který ji způsobil 28
5.4.8 Hodnocení zranitelnosti 29
5.5 Uchovávání záznamů 29
5.5.1 Typy uchovávaných záznamů 29
5.5.2 Doba uchování záznamů 29
5.5.3 Ochrana úložiště záznamů 29
5.5.4 Postupy při zálohování záznamů 29
5.5.5 Požadavky na používání časových razítek při uchovávání záznamů 29
5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí) 29
5.5.7 Postupy pro získání a ověření uchovávaných informací 30
5.6 Obnova po havárii nebo kompromitaci 30
5.6.1 Postup ošetření incidentu nebo kompromitace 30
5.6.2 Poškození výpočetních prostředků, softwaru nebo dat 30
5.6.3 Schopnost obnovit činnost po havárii 30
5.7 Ukončení činnosti poskytovatele služeb 30
6 Řízení technické bezpečnosti 31
6.1 Kryptografie, soukromý klíč a jeho ochrana 31

6.2 Počítačová bezpečnost 31
6.2.1 Specifické technické požadavky na počítačovou bezpečnost 31
6.2.2 Hodnocení počítačové bezpečnosti 31
6.3 Technické řízení životního cyklu 32
6.3.1 Řízení vývoje systému pro poskytování služby 32
6.3.2 Řízení správy bezpečnosti 33
6.3.3 Řízení životního cyklu bezpečnosti 33
6.4 Řízení bezpečnosti sítě 33
6.5 Ochrana proti padělání a odcizení dat 33
7 Hodnocení shody a jiná hodnocení 34
7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení 34
7.2 Identita a kvalifikace hodnotitele 34
7.3 Vztah hodnotitele k hodnocenému subjektu 34
7.4 Hodnocené oblasti 34
7.5 Postup v případě zjištění nedostatků 34
7.6 Sdělování výsledků hodnocení 34
8 Ostatní obchodní a právní záležitosti 36
8.1 Poplatky 36
8.1.1 Poplatky za využívání služby 36
8.1.2 Poplatky za další služby 36
8.1.3 Postup při refundování 36
8.2 Finanční odpovědnost 36
8.2.1 Krytí pojištěním 36
8.2.2 Další aktiva 36
8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele 36
8.3 Důvěrnost obchodních informací 37
8.3.1 Rozsah důvěrných informací 37
8.3.2 Informace mimo rámec důvěrných informací 37
8.3.3 Odpovědnost za ochranu důvěrných informací 37
8.4 Ochrana osobních údajů 37
8.4.1 Politika ochrany osobních údajů 37
8.4.2 Informace považované za osobní údaje 37
8.4.3 Informace nepovažované za osobní údaje 37
8.4.4 Odpovědnost za ochranu osobních údajů 38
8.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním 38

8.4.6 Poskytování osobních údajů pro soudní či správní účely 38
8.4.7 Jiné okolnosti zpřístupňování osobních údajů.....38
8.5 Práva duševního vlastnictví.....38
8.6 Zastupování a záruky.....38
8.6.1 Zastupování a záruky I.CA 38
8.6.2 Zastupování a záruky kontaktního místa 38
8.6.3 Zastupování a záruky ostatních zúčastněných subjektů 39
8.7 Zřeknutí se záruk 39
8.8 Omezení odpovědnosti 39
8.9 Záruky a odškodnění.....39
8.10 Doba platnosti, ukončení platnosti.....40
8.10.1 Doba platnosti 40
8.10.2 Ukončení platnosti.....40
8.10.3 Důsledky ukončení a přetrvání závazků 40
8.11 Individuální upozorňování a komunikace se zúčastněnými subjekty.....40
8.12 Novelizace 40
8.12.1 Postup při novelizaci.....40
8.12.2 Postup a periodicita oznamování.....40
8.12.3 Okolnosti, při kterých musí být změněn OID.....41
8.13 Ustanovení o řešení sporů 41
8.14 Rozhodné právo.....41
8.15 Shoda s právními předpisy.....41
8.16 Další ustanovení 41
8.16.1 Rámcová dohoda 41
8.16.2 Postoupení práv 41
8.16.3 Oddělitelnost ustanovení 41
8.16.4 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv).....41
8.16.5 Vyšší moc.....42
8.17 Další opatření.....42
9 Závěrečná ustanovení.....43

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	26.02.2020	Generální ředitel společnosti První certifikační autorita, a.s.	První vydání.

1.01	27.08.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Vyznačení klasifikace, zapracována doporučení z auditu, upřesnění textu. Zapracována možnost použití služby i pro certifikáty vydané pro Slovenskou republiku.
1.02	31.08.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Oprava formální chyby.
1.03	02.12.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Doplnění možnosti používat i certifikáty vydané jiným poskytovatelem služeb vytvářejících důvěru.
1.04	23.11.2023	Generální ředitel společnosti První certifikační autorita, a.s.	Doplněny možnosti ověření identity žadatele prostřednictvím jiného kvalifikovaného certifikátu pro ověřování kvalifikovaného elektronického podpisu a distančně prostřednictvím ZealiD.
1.05	26.08.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace seznamu odkazovaných standardů, zohlednění požadavků ETSI TS 119 411-6. Revize textu.
1.06	22.11.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Doplněny další možností distančního ověření identity žadatele (NKČR, NIA).
1.07	15.01.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Doplněny možnosti ověření identity fyzické osoby na kontaktním místě o využití aplikace eDoklady a o ověřování listinného dokladu v ROB.
1.08	16.08.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace v souvislosti s S/MIME BR.
1.09	25.08.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Oprava formálních chyb.
1.10	12.09.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Oprava chyby v kapitole 1.2.
1.11	09.05.2026	Generální ředitel společnosti První certifikační autorita, a.s.	Zohlednění paralelně provozovaného nového technologického řešení služby vytváření elektronických podpisů na dálku. Přesun popisu identifikace a autentizace a informací o životním cyklu certifikátu do odpovídajících certifikačních politik.

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 I.CA RemoteSign, tedy vytváření elektronických podpisů na dálku (dále též Služba).

Dokument zohledňuje skutečnost, že jsou paralelně provozována dvě technologická řešení, původní a nově vytvořené, pokud se popis v závislosti na řešení liší, je to uvedeno buď ve tvaru **1:** *řešení 1* / **2:** *řešení 2*, nebo ve formě dvou kapitol, přičemž ta první má v názvu *xxxxx* – řešení 1, druhá potom *xxxxx* – řešení 2.

Služba je primárně určena k vytváření elektronických podpisů založených na kvalifikovaných certifikátech vydávaných společností I.CA, ale je možné ji využívat i k vytváření elektronických podpisů založených na kvalifikovaných certifikátech vydávaných jinými poskytovateli služeb vytvářejících důvěru (v současné době konkrétně společnost První certifikační autorita, s.r.o., dále též I.CA SK). Podmínkou je smluvní vztah mezi společností I.CA a těmito poskytovateli služeb vytvářejících důvěru a dále to, že soukromý klíč použitý k elektronickému podpisu byl vytvořen a je uložen v bezpečném kryptografickém zařízení nebo v zařízení typu QSCD, která jsou pod výhradní kontrolou I.CA.

V dalším textu jsou používány pojmy:

- certifikát pro podpis ve významu kvalifikovaný certifikát pro elektronické podpisy vydávaný podle legislativy ČR, resp. podle legislativy SR,
- mandátní certifikát ve významu kvalifikovaný mandátní certifikát vydávaný podle legislativy SR,
- pro všechny typy uvedené v předcházejících odrážkách souhrnně Certifikát.

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,
- zákonem Slovenské republiky č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),
- zákonem České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád),
- 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 elektronických podpisů na dálku, je poskytována všem Klientům, kteří potřebují vytvářet elektronický podpis dokumentů pro subjekt, který jim tyto dokumenty k podpisu předkládá (dále též třetí strana).

I.CA dále nijak neomezuje potenciální Klienty, poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

1.1 Přehled

Dokument **Politika služby I.CA RemoteSign (vytváření elektronických podpisů 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. 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 definuje procesy životního cyklu Služby až po ukončení poskytování Služby pro řešení 1.
- Kapitola 4 definuje procesy životního cyklu Služby až po ukončení poskytování Služby pro řešení 2.
- 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 RemoteSign ETSI TS 119 431-1 (dle též Směrnice1) a Prováděcí směrnice služby I.CA RemoteSign ETSI TS 119 431-2 (dále též Směrnice2).

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu:	Politika služby I.CA RemoteSign (vytváření elektronických podpisů na dálku), verze 1.11
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 podpisové klíče jsou uloženy v SCDev, nebo
	0.4.0.19431.1.1.3 (EU SSASC policy) - v případě, že podpisové klíče jsou uloženy v QSCD.

Pozn: V současné době je využívána možnost EU SSASC.

1.2.1 Politika vytváření podpisů

V rámci Služby je v každém okamžiku podporována jediná politika vytváření podpisů. Je implementována v rámci komponenty **1:** RSiCON / **2:** Orchestrátor umístěné v prostředí třetí strany, která zabezpečeně komunikuje s Klientem i s poskytovatelem Služby. Aplikovaná verze politiky vytváření podpisů je dána časem, kdy byl konkrétní elektronický podpis vytvořen.

1.2.2 Podporované formáty a třídy podpisů, 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. U formátů CAdES a PAdES je možné podepsat i dokument, který již nějaký podpis obsahuje.

CAdES

CAdES-B-B a CAdES-B-T dle normy ETSI EN 319 122-1, ve variantách interní a externí.

PAdES

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

Pro popředí viditelného podpisu 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.

Specifický formát podpisu pro E-recept (relevantní jen v případě řešení 1)

Formát je založen na XMLDSig.

1.2.3 Předávání parametrů podpisu

Definování parametrů podpisu je záležitostí již zmíněné komponenty **1:** RSiCON / **2:** Orchestrátor, která na straně poskytovatele vytvoří ve frontě příslušného Klienta požadavek na vytvoření elektronického podpisu obsahující mj. typ požadovaného podpisu (viz kapitola 1.2.2) datum a čas expirace požadavku, případně zašifrovaný náhled podepisovaného dokumentu nebo odkaz na něj (obojí může dešifrovat jen a pouze příslušný Klient), pokud možnost zobrazení před podpisem není realizována jinak, a kontrolní součet (hash) pro vytvoření podpisu. Podepisovaný dokument ani jeho náhled v otevřeném tvaru tady poskytovateli služby dostupné nejsou, má k dispozici pouze hash.

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 sloužící v případech fyzické přítomností Klienta nebo jeho zmocněnce (viz kapitola 3.1.2) se realizují prostřednictvím:

- veřejných registračních autorit I.CA, resp. I.CA SK, a
- klientských registračních autorit, a
- speciálních kontaktních míst orientovaných pouze na činnosti spojené se Službou,

přičemž registrační autority mohou být stacionární, nebo mobilní.

Kontaktní místa:

- přijímají žádosti o Službu poskytovanou podle této Politiky, 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, resp. I.CA SK uzavírat „Smlouvy o vydání certifikátu a využívání služby I.CA RemoteSign“ (dále též Smlouvy),
- zajišťují zpoplatňování služeb I.CA poskytovaných prostřednictvím kontaktních míst, pokud není stanoveno Smlouvou jinak.

Pokud proces probíhá za účasti NKČR (viz kapitola 3.1.2.4) jsou kontaktním místem distanční registračních autority (DRA) provozované NKČR. 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 DRA, pokud není stanoveno smlouvou jinak.

Oprávněným operátorem DRA mohou být pouze osoby definované notářským řádem, a to:

- notář – podle § 1/1 notářského řádu,
- notářský kandidát – podle § 23 nebo podle § 24/1 notářského řádu,
- notářský koncipient – podle § 19 notářského řádu.

Ve zvláštních případech může být řešení prostřednictvím klientských registračních autorit navázáno na personální oddělení konkrétní třetí strany.

1.3.3 Spoléhající se strany

Spoléhající se stranou je subjekt, který se spoléhá na elektronický podpis vytvořený v rámci Služby.

1.3.4 Třetí strany

Třetí stranou je subjekt, který má se společností I.CA uzavřenou smlouvu (Kontrakt) a který předkládá Klientům dokumenty k podpisu.

1.3.5 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 procesech vytváření elektronického podpisu ve prospěch konkrétní třetí strany a 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 protiprávní účely. Nesmí být např. použita pro vytváření elektronického podpisu jiného dokumentu, než který byl Klientovi k podpisu předložen třetí stranou.

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 osobou společnosti První certifikační autorita, a.s., v souvislosti s touto Politikou, resp. s odpovídajícími Směrnicemi, je výkonný ředitel I.CA. Platí kontaktní údaje uvedené v kapitole 2.2.

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., nebo jím pověřená osoba.

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

tab. 2 - Pojmy

Pojem	Vysvětlení
aktivační obálka	obálka, kterou Klient obdrží na kontaktním místě, na přední straně, resp. pod průhledným okénkem na přední straně je identifikační čárový kód obálky, uvnitř aktivační obálky je pod bezpečnostní přelepkou jiný, aktivační (QR nebo čárový) kód
aktivační kód	QR nebo čárový kód uvnitř aktivační obálky pod bezpečnostní přelepkou sloužící k aktivaci Služby pro konkrétního klienta
elektronický podpis	zaručený elektronický podpis, nebo kvalifikovaný elektronický podpis, nebo uznávaný elektronický dle platné právní úpravy pro služby vytvářející důvěru
elektronický podpis na dálku	elektronický podpis vytvořený soukromým klíčem, který je uložen v zařízení provozovaném I.CA, přičemž je pro tento klíč zajištěna výhradní kontrola jeho držitelem
identifikační kód	čárový kód na přední straně nebo pod průhledným okénkem aktivační obálky sloužící ke svázání klíčového páru s konkrétním klientem, identifikační kód je uveden i jako číslo, aby mohl být přetypován
Identita občana	elektronický doklad, primárně slouží pro bezpečné a jednoduché přihlašování do různých portálů veřejné správy
orgán dohledu	subjekt dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru
politika vytváření podpisu	soubor pravidel a omezení vztahujících se k vytvářeným elektronickým podpisům
Portál občana	webová služba, která umožňuje přístup k různým informacím a službám veřejné správy
právní úprava pro služby vytvářející důvěru	platné právní předpisy České republiky vztahující se ke službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
QR kód	Quick Response kód, prostředek pro automatizovaný sběr dat, zůstává čitelný i po odstranění značné části obrazce
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
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

tab. 3 - Zkratky

Zkratka	Vysvětlení
AdES	Advanced Electronic Signature, typ elektronického podpisu
CAdES	CMS Advanced Electronic Signature, typ elektronického podpisu
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	Global Data Protection Regulation, nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
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
NIA	Národní identitní autorita
NKČR	Notářská komora České republiky
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu

PAdES	PDF Advanced Electronic Signature, typ elektronického podpisu
PC	Personal Computer, osobní počítač
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, nebo pečetě (dle eIDAS)
ROB	Registr obyvatel
SCDev	Signature Creation Device, bezpečné zařízení pro tvorbu elektronického podpisu, nebo pečetě
SSASC	Server Signing Application Service Component
TS	Technical Specification, typ ETSI standardu
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
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 – neprodleně,
- 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 (viz kapitoly 2.2 a 2.3) 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 ŽIVOTNÍ CYKLUS SLUŽBY – ŘEŠENÍ 1

3.1 Uzavření smlouvy

Smlouva o zřízení a využívání Služby je uzavírána mezi I.CA a Klientem.

3.2 Identifikace a autentizace ke Službě

3.2.1 Počáteční ověření identity

Identifikace a autentizace ke službě je úzce svázána s identifikací a autentizací pro vydání Certifikátu.

3.2.1.1 Ověřování identity organizace

Popsáno v kapitole 3.2.2 Ověřování identity organizace příslušné certifikační politiky.

3.2.1.2 Ověřování identity fyzické osoby

Popsáno v kapitole 3.2.3 Ověřování identity fyzické osoby příslušné certifikační politiky.

3.2.2 Ověření identity při prodloužení služby

Prodloužení Služby probíhá automatizovaně. I.CA v roli třetí strany vloží Klientovi dotaz, zda chce vydat následný Certifikát a tak Službu prodloužit. Pokud Klient odpoví kladně (odpověď je opatřena elektronickým podpisem vytvořeným soukromým klíčem odpovídajícím Certifikátu, ke kterému má být vydán Certifikát následný), je Smlouva prodloužena do doby platnosti následného Certifikátu. Tím také Klient explicitně potvrzuje, že se jeho identifikační údaje kontrolované při počátečním ověření nezměnily.

3.2.3 Změna údajů

Pokud vzhledem ke změně údajů není možné vydat následný Certifikát, je Klient povinen absolvovat nové ověření identity.

3.3 Zřízení Služby

Postup zřízení Služby závisí na způsobu ověření identity Klienta (viz kapitola 3.1.2), při kterém:

- je uzavřena Smlouva,
- je vytvořena žádost o vydání příslušného Certifikátu,
- v závislosti na způsobu ověření identity Klienta:
  - je mu na kontaktním místě vydána aktivační obálka pro aktivaci Služby a mobilní aplikace, nebo
  - je mu zaslán jedinečný QR kód pro spuštění procesu aktivace Služby a mobilní aplikace,

- je vydán a zveřejněn Certifikát.

Další nakládání s uvedeným Certifikátem může být dáno smlouvou uzavřenou mezi konkrétní třetí stranou a I.CA (speciálním případem třetí strany je i I.CA).

3.3.1 Povinnosti Klienta a poskytovatele Služby

Klient je povinen zejména:

- seznámit se s touto Politikou, s příslušnou certifikační politikou 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 Certifikátu,
- poskytovat pravdivé a úplné informace pro zřízení Služby, resp. pro vydání Certifikátu,
- překontrolovat, zda údaje získané z předložených dokumentů jsou správné a odpovídají požadovaným údajům.

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.

3.4 Aktivace Služby

Aktivace Služby proběhne okamžitě po vydání Certifikátu Klientovi. Aby Klient mohl Službu využívat, musí provést instalaci mobilní nebo PC aplikace (v případě ověření identity Klienta distančním způsobem nebo na základě již vydaného kvalifikovaného certifikátu pro ověřování kvalifikovaného elektronického podpisu je instalace provázána s tvorbou žádosti). Jejím prostřednictvím získá přístup ke svému soukromému klíči. Jiný přístup k soukromému klíči konkrétního Klienta není možný.

3.5 Prodloužení Smlouvy

Před vypršením platnosti je Klient prostřednictvím mobilní nebo PC aplikace notifikován a dotázán, zda chce vydat Certifikát následný, tedy Certifikát s novým veřejným klíčem, ale se stejným obsahem v polích subject a subjectAlternativeName. Pokud Klient neodpoví kladně, Certifikát expiruje a platnost Smlouvy je ukončena, v opačném případě (odpověď je elektronicky podepsána soukromým klíčem odpovídajícím Certifikátu, ke kterému má být Certifikát následný) zůstává Smlouva v platnosti a Služba je Klientovi nadále poskytována.

Povinností držitele Certifikátu je uvědomit poskytovatele Služby o změnách ve smluvních údajích (a v polích subject a subjectAlternativeName Certifikátu).

3.6 Konec platnosti Smlouvy

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.

3.7 Zablokování a odblokování mobilní nebo PC aplikace

Mobilní nebo PC aplikace může být zablokována např. v případech ztráty nebo odcizení mobilního zařízení nebo PC.

3.7.1 Zablokování

Zablokování mobilní nebo PC aplikace znamená, že je převedena do stavu „blokovaná" a nadále ji není možné používat pro přístup k Certifikátu. Certifikát zůstává nadále v platnosti (je možné k němu přistupovat prostřednictvím jiné aktivované mobilní nebo PC aplikace téhož Klienta). Možnosti zablokování aplikace jsou:

- Prostřednictvím jiné aktivované mobilní nebo PC aplikace (téhož Klienta).
- Telefonicky na číslo +420 284 081 930, +420 284 081 931, +420 284 081 933. Pracovník technické podpory zjišťuje jméno, příjmení a akademický titul Klienta, identifikační číslo primárního dokladu, bydliště Klienta a dále se může zeptat na jakýkoliv další údaj neuvedený v Certifikátu, ale zadaný při žádosti o zřízení Služby. Pracovník technické podpory může při jakýchkoliv nejasnostech v odpovědích Klienta odkázat na jiný způsob zablokování prostředku pro elektronickou identifikaci.
- E-mailem na adresu podpora@ica.cz, e-mail musí být odeslán z e-mailové adresy zadané při zřizování služby. E-mail musí obsahovat tyto údaje:
  - Klient *akademický titul, jméno (jména) a příjmení*, datum narození *dd.mm.rrrr*, číslo primárního identifikačního dokladu *abcdefghij*, bydliště *ulice, číslo popisné, psč, město* žádá o zablokování zařízení pro přístup ke službě vytváření elektronického podpisu na dálku *identifikace mobilního zařízení*.

  V případě jakýchkoliv nejasností může být zablokování odmítnuto, o výsledku je Klient odpovědí na jeho e-mail vždy informován.

- Osobně na kontaktním místě, kdy musí být ke kontrole předloženy primární a sekundární doklad (sekundární nemusí být stejný jako při počátečním ověření identity dle kapitoly 3.1.1, ale musí obsahovat alespoň jeden z údajů dle kapitoly 3.1.1).

3.7.2 Odblokování

Odblokování mobilní nebo PC aplikace je možné pouze prostřednictvím jiné aktivované mobilní nebo PC aplikace (téhož Klienta). Pokud byla zadána časově omezená blokace, aplikace se automaticky odblokuje uplynutím času zvoleného při blokaci.

3.8 Používání Služby

Účelem služby je vytváření elektronických podpisů dokumentů na dálku. Dokumenty jsou zasílány třetími stranami, postup je následující:

- Třetí strana vloží do fronty požadavků v systému I.CA RemoteSign požadavek na vytvoření elektronického popisu dokumentu. Součástí požadavku je identifikace Klienta, který má dokument podepsat, zašifrované preview dokumentu (dešifrovat může pouze oprávněný Klient) a požadované parametry podpisu (podporovány jsou podpisy typů CAdES a PAdES).
- Klient si spustí mobilní nebo PC aplikaci a zadá heslo.
- Po ověření správnosti hesla se do aplikace stáhnou všechny požadavky na vytvoření elektronického podpisu.
- Klient si může v aplikaci prohlédnout detailní informace o požadavku včetně zobrazení podepisovaných dat, nebo jejich preview. Zavedená technické, personální, procedurální a kryptografická opatření zajišťující uložení soukromého klíče a přístup k němu umožňují podepisujícímu nést plnou záruku za vytvořený popis, a tedy za obsah podepsaného dokumentu.
- Pokud se Klient rozhodne konkrétní elektronický podpis vytvořit, stiskne tlačítko Podepsat a zadá heslo pro přístup k soukromému klíči. Tím, tedy vytvořením kvalifikovaného elektronického podpisu, dává Klient najevo svůj nepopiratelný souhlas s podepsaným obsahem.
- Pokud je heslo ke klíči správné, potom je s využitím soukromého klíče uloženého v bezpečném kryptografickém zařízení, případně v zařízení typu QSCD, vytvořen požadovaný elektronický podpis a je vrácen třetí straně

4 ŽIVOTNÍ CYKLUS SLUŽBY – ŘEŠENÍ 2

4.1 Uzavření smlouvy

Smlouva o zřízení Služby není uzavírána s každým Klientem zvlášť, primární smlouva je uzavřena mezi třetí stranou a I.CA.

4.2 Identifikace a autentizace ke Službě

4.2.1 Počáteční ověření identity

Identifikace a autentizace ke Službě je úzce svázána s identifikací a autentizací pro vydání Certifikátu.

4.2.1.1 Ověřování identity organizace

Popsáno v kapitole 3.2.2 Ověřování identity organizace příslušné certifikační politiky.

4.2.1.2 Ověřování identity fyzické osoby

Popsáno v kapitole 3.2.3 Ověřování identity fyzické osoby příslušné certifikační politiky.

4.2.2 Ověření identity při prodloužení služby

Prodloužení Služby probíhá automatizovaně tak, že třetí strana na základě souhlasu Klienta požádá o vydání Certifikátu následného, Klient má možnost následně vydaný Certifikát zneplatnit. Za správnost Klientových identifikačních údajů zodpovídá třetí strana.

4.2.3 Změna údajů

Pokud vzhledem ke změně údajů není možné vydat následný Certifikát, je Klient povinen absolvovat nové ověření identity, ale aktivace Služby zůstává v platnosti.

4.3 Zřízení a aktivace Služby

Předpokladem zřízení Služby je import dat o Klientovi do systému I.CA RemoteSign. Import může být proveden automaticky exportem z personálního systému Organizace, nebo může provést ručně pověřený zaměstnanec Organizace.

4.3.1 Povinnosti Klienta a poskytovatele Služby

Klient je povinen zejména:

- seznámit se s touto Politikou, s příslušnou certifikační politikou 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 Certifikátu,
- poskytovat pravdivé a úplné informace pro zřízení Služby, resp. pro vydání Certifikátu,
- překontrolovat, zda údaje získané z předložených dokumentů jsou správné a odpovídají požadovaným údajům.

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.

4.4 Aktivace Služby

Aktivace Služby proběhne okamžitě po vydání Certifikátu Klientovi. Aby Klient mohl Službu využívat, musí provést instalaci mobilní nebo PC aplikace. Jejím prostřednictvím získá přístup ke svému soukromému klíči. Jiný přístup k soukromému klíči konkrétního Klienta není možný.

4.5 Prodloužení poskytování Služby

Prodloužení služby probíhá automaticky vydáním následného kvalifikovaného certifikátu. Klient je o vydání následného certifikátu informován e-mailem a v případě nesouhlasu může tento certifikát revokovat.

4.6 Konec poskytování Služby

Konec poskytování Služby je vyvoláno ukončením vztahu mezi Klientem a Organizací, např. ukončením pracovního poměru. Na základě informace od Organizace jsou zablokovány všechny se Službou související přístupy, je revokován kvalifikovaný certifikát Klienta a následkem toho je mu poskytování Služby ukončeno.

4.7 Aktivace a deaktivace požívání biometriky

Přístup k soukromému klíči Klienta je chráněn Heslem/PINem, je ovšem možné toto doplnit o použití biometriky, tuto možnost je možné pouze v mobilní verzi klientské aplikace a předpokladem je, že Klient má biometriku v mobilním zařízení povolenou. Při povolování biometriky je vyžádáno zadání hesla/PINu a následně potvrzení použitím příslušné biometrické metody, kterou si aktivuje - podle konkrétního typu mobilního zařízení je možné použít buď otisk prstu (TouchID), nebo rozpoznávání tváře (FaceID).

4.8 Používání Služby

Účelem služby je vytváření elektronických podpisů dokumentů na dálku. Dokumenty jsou zasílány třetími stranami do komponenty Orchestrátor, postup je následující:

- Třetí strana vloží do fronty v systému I.CA RemoteSign požadavek na vytvoření elektronického popisu dokumentu (nebo množiny dokumentů). Součástí požadavku jsou jednoznačná identifikace Klienta, který má dokument podepsat, požadované parametry podpisu (podporovány jsou podpisy typů CAdES a PAdES) a příznak, zda bude povoleno zobrazení podepisovaných dokumentů.
- Na mobilní zařízení Klienta je zaslána notifikace s informací o novém požadavku na podpis - na PC zařízení notifikace doručována není.
- Klient si spustí mobilní nebo PC aplikaci.
- Do aplikace se stáhnou všechny požadavky na vytvoření elektronického podpisu.
- V aplikaci se zobrazí první požadavek k podpisu, pokud existuje.
- Klientovi se u požadavku na podpis zobrazí název dokumentu, hash dokumentu a možnost náhledu, pokud je povolený (parametr v požadavku na podpis). Pokud náhled u podepisovaného dokumentu v aplikaci povolený není, má Klient možnost si tento dokument zobrazit v interním systému Organizace a porovnat shodnost hashů (v aplikaci a interním systému). Jinak je kontrola integrity, tedy porovnání hashe předávaného ke vzdálenému vytvoření elektronického podpisu s hashem podepisovaného dokumentu je implementován také v komponentě Orchestrátor.
- Pokud se Uživatel rozhodne konkrétní elektronický podpis vytvořit, stiskne tlačítko "Potvrdit" a zadá Heslo/PIN pro přístup k soukromému klíči nebo pro přístup k Heslu/PINu použije biometriku.
- Pokud je Heslo/PIN pro přístup k soukromému klíči správné, je s využitím soukromého klíče uloženého v bezpečném kryptografickém zařízení vytvořen požadovaný elektronický podpis a podepsaný dokument je vrácen do systému Organizace. Vytvořením kvalifikovaného elektronického podpisu dává Klient najevo svůj nepopiratelný souhlas s podepsaným obsahem, protože zavedená technická, personální, procedurální a kryptografická opatření zajišťující uložení soukromého klíče a přístup k němu mu to umožňují.

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 přístroj.

5.1.6 Ukládání médií

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

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

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 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.

Všichni 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 uložených v kryptografickém modulu,
- obnovu těchto dat do kryptografického modulu.

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 okamžitě 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 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, 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,
- o dalším postupu rozhodne generální ředitel I.CA na základě rozhodnutí orgánu dohledu.

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.
- European Cybersecurity Certification Group Sub-group on Cryptography - Agreed Cryptographic Mechanisms.
- 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.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 403-1 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatele důvěryhodné služby – Část 1: Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodné služby.
- ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- 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.
- EN 301 549 Accessibility requirements for ICT products and services.
- 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. Spolupodílí se řízení počínaje managementem společnosti, přes vedoucí zaměstnance až po zaměstnance 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.

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

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

8 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 Poplatky

8.1.1 Poplatky za využívání služby

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

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 a jejích projevů,
- 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 uvedeným v tab. 1 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, Slovenské 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 RemoteSign (vytváření elektronických podpisů na dálku) vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem uvedeným v tab. 1.