První certifikační autorita, a.s.

Prováděcí směrnice

služby I.CA RemoteSeal

(ETSI TS 119 431-1)

Verze 1.00

OBSAH

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 ÚVOD

Tento dokument, Prováděcí směrnice služby I.CA RemoteSeal (ETSI TS 119 431-1) - dále též Směrnice1, stanovuje zásady, které První certifikační autorita, a.s., (dále též I.CA) uplatňuje při poskytování služby I.CA RemoteSeal, tj. vytváření kvalifikovaných elektronických pečetí na dálku – dále též Služba, z pohledu požadavků standardu ETSI TS 119 431-1 [12], tj. z pohledu správy a řízení bezpečného zařízení pro vytváření elektronických pečetí (podpisů).

Služba je v první řadě popsána dokumentem Politika služby I.CA RemoteSeal (vytváření elektronických pečetí na dálku) - dále též Politika. Ta je vytvořena dle zvyklostí I.CA týkajících se dokumentování služeb vytvářejících důvěru a respektuje v maximální možné míře strukturu definovanou standardem RFC 3647. Na Politiku navazuje tento dokument (Směrnice1) a dále Prováděcí směrnice služby I.CA RemoteSeal (ETSI TS 119 431-2) - dále též Směrnice2.

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 prováděcí směrnice v rozporu se standardy nebo právními předpisy, které nahradí dosud platné, bude vydána její nová verze.

1.1 Požadavky prováděcí směrnice

1.1.1 Právní požadavky

Právní požadavky na Službu jsou definovány:

- nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS) [12]1],
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- legislativou týkající se ochrany osobních údajů, v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

Služba společnosti První certifikační autorita, a.s., zajišťující vytváření kvalifikovaných elektronických pečetí na dálku je poskytována na základě uzavřeného smluvního vztahu všem koncovým uživatelům – právnickým osobám – (dále jen „Klientům"), kteří potřebují elektronické pečetě vytvářet.

1.1.2 Identifikace důvěryhodného poskytovatele Služby

Důvěryhodným poskytovatelem Služby je společnost První certifikační autorita, a.s., která je kvalifikovaným poskytovatelem služeb vytvářejících důvěru dle nařízení eIDAS. Základní údaje o společnosti jsou:

- adresa sídla společnosti:

  První certifikační autorita, a.s.

Podvinný mlýn 2178/6

190 00 Praha 9

Česká republika

- IČ 26439395,
- internetová adresa http://www.ica.cz,
- elektronická adresa info@ica.cz,
- ID datové schránky a69fvfb.

1.1.3 Organizace spravující prováděcí směrnici

Tuto Směrnici1 spravuje společnost První certifikační autorita, a.s.

1.1.4 Kontaktní osoba organizace spravující prováděcí směrnici

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s touto Směrnicí1, je uvedena na internetové adrese (viz kapitola 1.1.2).

1.1.5 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 v Politice s touto Směrnicí1, je generální ředitel společnosti První certifikační autorita, a.s.

1.1.6 Postupy při schvalování prováděcí směrnice

Pokud je potřebné provést změny v této Směrnici1 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 Směrnice1 předchází její schválení ředitelem společnosti První certifikační autorita, a.s.

1.1.7 Přípustné použití služby

Službu provozovanou podle Politiky lze využívat v procesech vytváření kvalifikovaných elektronických pečetí a v souladu s platnou právní úpravou.

1.1.8 Omezení použití služby

Služba provozovaná podle Politiky nesmí být používána v rozporu s přípustným použitím popsaným v kapitole 1.1.7 a dále pro jakékoliv nelegální účely.

1.1.9 Dokumentace vztahujícím se ke Službě

Dokumentace společnosti I.CA je tvořena následujícími okruhy:

Okruh	Dokument	Důvěrnost**
Dokumentace ISMS	Rozsah ISMS*	I.CA – Jen pro vnitřní potřebu
	Politika bezpečnosti informací*	I.CA – Jen pro vnitřní potřebu
	Přístupy k posuzování a ošetřování rizik bezpečnosti informací*	I.CA – Jen pro vnitřní potřebu
	Analýza rizik – důvěryhodné systémy Závěrečná zpráva	I.CA – Důvěrné
	Výběr protiopatření*	I.CA – Důvěrné
	Prohlášení o aplikovatelnosti*	I.CA – Důvěrné
	Zbytková rizika*	I.CA – Důvěrné
	Plán ošetření rizik*	I.CA – Důvěrné
	Zbytková rizika – důvěryhodné systémy – Manažerské shrnutí	I.CA – Jen pro vnitřní potřebu
	Dokumentace ISMS – důvěryhodné systémy – Konfigurační manuál	I.CA – Důvěrné
Bezpečnostní politiky	Systémová bezpečnostní politika – důvěryhodné systémy	I.CA – Jen pro vnitřní potřebu
	systémové bezpečnostní politiky jednotlivých systémů	I.CA – Jen pro vnitřní potřebu
Certifikační politiky a certifikační prováděcí směrnice	certifikační politiky pro vydávané typy certifikátů a společná certifikační prováděcí směrnice (pro každý typ kryptografie, tj. RSA i EC) - viz webové stránky společnosti	Veřejný dokument
Interní směrnice	směrnice pokrývající různé oblasti činnosti důvěryhodných systémů, např. „Řízení fyzického přístupu do místností I.CA", „Příručka administrátora", „Přemístění provozního pracoviště" atd.	I.CA – Jen pro vnitřní potřebu, resp. I.CA – Důvěrné

Dokumentace související s pečetěním na dálku	Politika služby vytváření kvalifikovaných elektronických pečetí na dálku, dokument dle zvyklostí I.CA, hlavní dokument, se kterým se musí Klient seznámit	Veřejný dokument
	Prováděcí směrnice služby I.CA RemoteSeal (ETSI TS 119 341-1) - tento dokument – prováděcí směrnice dle požadavků normy ETSI TS 119 341-1	Veřejný dokument
	Prováděcí směrnice služby I.CA RemoteSeal (ETSI TS 119 341-2), prováděcí směrnice dle požadavků normy ETSI TS 119 341-2	Veřejný dokument

* na konci názvu dokumentu je text „ – důvěryhodné systémy"

** klasifikační stupně informací používané v I.CA

Všechny veřejné dokumenty jsou k dispozici na webových stránkách I.CA.

1.1.10 Postupy při ukončení služby

Ukončení činnosti je popsáno v Politice, konkrétně v kapitola 5.7 Ukončení činnosti poskytovatele služeb. Problematika je detailně popsána v interní dokumentaci:

- „Ukončení činnosti služeb I.CA“.

1.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu: Prováděcí směrnice služby I.CA RemoteSeal (ETSI TS 119 431-1), verze 1.00

OID dokumentu: není přiřazeno

1.2.1 Podporovaná politika pro vytváření pečetí

Služba podporuje politiky:

- **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 klíč je uložen v SCDev, nebo
- **0.4.0.19431.1.1.3** (EU SSASC policy) - v případě, že pečetící klíč je uložen v QSCD.

1.3 Zúčastněné strany

Zúčastněnými stranami jsou:

- Právnická osoba, nebo organizační složka státu (dále též Klient), která:
  - má s I.CA uzavřenou platnou smlouvu o využívání Služby (dále též Smlouva),
  - prostřednictvím oprávněné osoby (dále též Osoba) požádala o zřízení Služby a v rámci toho o vydání prvotního autentizačního certifikátu na čipovou kartu a o vydání kvalifikovaného certifikátu pro elektronickou pečeť, jehož je držitelem, přičemž odpovídající soukromý klíč byl vygenerován v zařízení typu QSCD (provozuje I.CA) a zůstává uložen v bezpečném kryptografickém prostředí,
- I.CA jako důvěryhodný poskytovatel Služby:
  - je kvalifikovaným poskytovatelem služeb vytvářejících důvěru dle nařízení eIDAS [1],
  - provozuje a spravuje důvěryhodné systémy pro podporu Služby,
  - má pro oblast důvěryhodných systémů zavedený a certifikovaný systém řízení bezpečnosti informací (ISMS) v souladu s normou ČSN ISO/IEC 27001 [18],
  - je autorem aplikací pro podporu Služby,
  - při své činnosti v nezbytně nutné míře využívá služeb třetích stran.
- Případně další subjekty, jako jsou orgány dohledu, zejména orgány činné v trestním řízení a další subjekty, kterým to umožňuje platná právní úprava.

1.4 Přehled použitých pojmů a zkratek

1.4.1 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 nebo zaručená 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 Klienta nad využíváním Služby a použitím klíče
párová data	soukromý a jemu odpovídající veřejný klíč
právní úprava pro služby vytvářející důvěru	platné právní předpisy České republiky vztahující se ke službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
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 v I.CA
soukromý klíč	jedinečná data pro vytváření elektronické pečetě
veřejný klíč	jedinečná data pro ověřování elektronické pečetě

1.4.2 Zkratky

Pojem	Vysvětlení
CA	Certification Authority, certifikační autorita
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
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
EN	European Standard, typ ETSI standardu
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EU	Evropská unie
http	Hypertext Transfer Protocol, protokol pro výměnu textových dokumentů ve formátu html
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
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
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
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení

	pro tvorbu kvalifikovaného elektronického podpisu/pečetě
RSA	šifra s veřejným klíčem pro podepisování/pečetění a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)
SAM	Signature Activation Module, povinná součást QSCD pro vzdálenou pečeť, která zajišťuje kontrolu přístupu k soukromým pečetícím klíčům
SCDev	Secure Cryptographic Device, bezpečné kryptografické zařízení
TS	Technical Specification, typ ETSI standardu
TSA	Time Stamping Authority, autorita časových razítek
TSMC	Time Source Master Clock, zdroj přesného času
TSP	Trusted Service Provider, důvěryhodný poskytovatel služeb
TSS	Time Stamp Server, server vytvářející časová razítka

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 uvedeny v kapitole 1.1.2.

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 platnými právními předpisy. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci, zejména:

- „Operátor CA“,
- „Směrnice pro pracovníky RA I.CA“,
- „Řízení bezpečnosti informací“,
- „Příručka administrátora“,
- „Bezpečnostní incidenty“,
- „HSM/nShield XC“,
- „Správa TSS“,
- „Správa TSMC“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

3 INICIALIZACE PEČETÍCÍHO KLÍČE

3.1 Generování pečetícího klíče

Pečetící klíče Klientů jsou generovány a spravovány v bezpečném kryptografickém prostředí. Součástí bezpečného kryptografického prostředí je zařízení typu QSCD uvedené na unijním seznamu QSCD. Přítomnost užitého QSCD zařízení na unijním seznamu QSCD je pravidelně ověřována.

Postup kontroly je popsán v interní dokumentaci:

- „Personalizace QSCD".

Generování probíhá v zabezpečených vyhrazených prostorách provozního pracoviště, v místnosti zabezpečené obdobně jako místnosti určené pro zpracování informací stupně utajení „Důvěrné" podle zákona č. 412/2005 Sb. - popsáno v interní dokumentaci:

- „Projekt fyzické bezpečnosti Provodov",
- „Projekt fyzické bezpečnosti Zlín – 9. patro SPUR".

Pro generování je výhradně používán algoritmus RSA s délkou klíče minimálně 2048 bitů. Párová data jsou generována během procesu zřízení Služby.

3.2 Propojení prostředku elektronické identifikace s konkrétním Klientem

Přístupové údaje ke Službě Klient získá prostřednictvím Osoby po řádném ověření totožnosti (viz Politika) v průběhu procesu zřizování Služby. Pro autentizaci ke Službě slouží:

- čipová karta s autentizačním osobním komerčním certifikátem
- PIN k čipové kartě

Ověřený Klient prostřednictvím aplikace RemoteSealProFi a autentizačního certifikátu aktivuje svůj účet a získá možnost vygenerovat přístupový soubor a zvolit přístupové heslo pro každou instanci komponenty RSeC. Přístupový soubor a heslo slouží k autentizaci a následné autorizaci volající aplikace k použití soukromého klíče Klienta.

3.3 Propojení certifikátu

Propojení soukromého klíče s odpovídajícím certifikátem veřejného klíče Klienta probíhá na kontaktním místě v rámci procesu zřizování Služby. Po řádném ověření totožnosti Klienta je mj. vyplněna a certifikační autoritě odeslána žádost o vydání certifikátu a následně je certifikát vydán.

3.4 Zajišťování prostředků elektronické identifikace

Prostředkem elektronické identifikace Klienta v rámci Služby jsou identifikační a autentizační údaje pro přístup k jeho soukromému klíči uloženému v bezpečném kryptografickém prostředí. Zmíněné údaje Klient získá po aktivaci Služby viz kapitola 3.2.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS PEČETÍCÍHO KLÍČE

4.1 Zřízení Služby a vytvoření pečetícího klíče

Po uzavření Smlouvy mezi Klientem a společností I.CA navštíví Osoba kontaktní místo, kde pro Klienta získá prvotní autentizační (komerční) certifikát na čipové kartě, v zařízení pro vytváření elektronických pečetí jsou vygenerována párová data a k nim je certifikační autoritou I.CA vydán certifikát pro ověřování elektronických pečetí. Certifikát je vystaven a zaslán na zadanou mailovou adresu.

4.2 Aktivace Služby

„Aktivace služby na straně Klienta se provádí prostřednictvím aplikace RemoteSealProfi (aplikace pro správu pečetění v rámci organizace Klienta). Nedílnou součástí aktivačního procesu je i provedení aktivace uživatelského účtu (viz bod 4.2.1) a aktivace komponenty RSeC (viz bod 4.2.2).

4.2.1 Aktivace uživatelského účtu

Pro aktivaci uživatelského účtu je nutná čipová karta s autentizačním komerčním certifikátem obdržená při zřizování služby (a znalost PINu k této kartě). Ve volbě přidání uživatelského profilu je vyžádáno vložení čipové karty, zadání PINu a následně je vyžadována volba hesla, kterým se bude uživatel společně s čipovou kartou autentizovat pro autorizaci ke správě pečetění dané organizace prostřednictvím aplikace RemoteSealProFi.

4.2.2 Aktivace komponenty RSeC pro autentizaci vůči Službě

Aktivace komponenty RSeC (v rámci organizace Klienta může existovat několik instancí) znamená vytvoření příslušného přístupového souboru a hesla. Pro identifikaci v rámci prostředí Klienta je instance pojmenována.

4.3 Rušení pečetícího klíče

Rušení pečetícího klíče znamená zrušení přístupových údajů k němu.

4.4 Úschova a obnova pečetícího klíče

Soukromé pečetící klíče Klientů jsou uloženy v bezpečném kryptografické prostředí, ve formě bezpečným a certifikovaným způsobem šifrovaných záznamů databáze. Jejich úschova a obnova je úschovou a obnovou databáze, které provádějí pracovníci v důvěryhodných rolích – popsáno v interní dokumentaci:

- „Příručka administrátora".

4.5 Proprietární protokol

Pro zabezpečení Služby je využíván proprietární protokol popsaný v interní dokumentaci:

- „Analytická dokumentace I.CA RemoteSign, I.CA RemoteSeal".

Tento proprietární protokol zajišťuje, aby bylo zamezeno Službu narušit i útočníkovi s vysokým potenciálem útoku.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

5.1 Obecné informace

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 v Politice, Plánu pro zvládání krizových situací a plánu obnovy a v upřesňující interní dokumentaci. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

5.2 Fyzická bezpečnost

Popsáno v Politice, konkrétně v kapitole Fyzická bezpečnost. Popis je rozpracován v interní dokumentaci:

- „Řízení fyzického přístupu do místností I.CA“,
- „Požární bezpečnost“,
- „Kontrolní činnost, bezúhonnost a odbornost“,
- „Bezpečnostní incidenty“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Kamerový systém – provozní pracoviště“,
- projekty fyzické bezpečnosti jednotlivých provozních pracovišť.

5.3 Procesní bezpečnost

Popsáno v Politice, konkrétně v kapitole Procesní bezpečnost. Popis je rozpracován v interní dokumentaci:

- „Systémová bezpečnostní politika - důvěryhodné systémy“,
- „Řízení bezpečnosti informací“,
- „Příručka administrátora“,
- „Hierarchická struktura - Postupy generování klíčů a certifikátů CA“,
- „HSM/nShield XC“,
- „Směrnice pro pracovníky RA I.CA“,
- „Operátor CA“.

5.4 Personální bezpečnost

Popsáno v Politice, konkrétně v kapitole Personální bezpečnost. Popis je rozpracován v interní dokumentaci:

- „Kontrolní činnost, bezúhonnost a odbornost“,
- „Pracovní řád“.

5.5 Postupy zpracování auditních záznamů

Popsáno v Politice, konkrétně v kapitole Postupy zpracování auditních záznamů. Popis je rozpracován v interní dokumentaci:

- „Příručka administrátora“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

5.6 Uchovávání záznamů

Popsáno v Politice, konkrétně v kapitole Uchovávání záznamů. Popis je rozpracován v interní dokumentaci:

- „Řízení fyzického přístupu do místností I.CA“,
- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“,
- „Příručka administrátora“,
- „Dokumenty agendy certifikačních služeb“,
- „Dílčí spisový a skartační řád pro agendy certifikačních služeb“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

5.7 Obnova po havárii nebo kompromitaci

Popsáno v Politice, konkrétně v kapitole Obnova po havárii nebo kompromitaci. Popis je rozpracován v interní dokumentaci:

- „Plán pro zvládání krizových situací a plán obnovy“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Bezpečnostní incidenty“.

5.8 Ukončení činnosti poskytovatele Služby

Popsáno v Politice, konkrétně v kapitole Ukončení činnosti poskytovatele služeb. Popis je rozpracován v interní dokumentaci:

- „Ukončení činnosti služeb I.CA“.

6 TECHNICKÉ BEZPEČNOSTI

6.1 Řízení systémů a jejich bezpečnosti

Popsáno v Politice, konkrétně v kapitole Procesní bezpečnost. Popis je rozpracován v interní dokumentaci:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Řízení bezpečnosti informací“,
- „Příručka administrátora“.

6.2 Systémy a jejich provozování

6.2.1 Přiřazení rolí

Popsáno v Politice, konkrétně v kapitole Důvěryhodné role. Popis je rozpracován v interní dokumentaci:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Řízení bezpečnosti informací“,
- „Příručka administrátora“.

6.2.2 Provozní dokumentace

Popsáno v Politice, konkrétně v kapitole Dokumentace poskytovaná zaměstnancům.

6.2.3 Synchronizace času

Čas důvěryhodných systémů“ je synchronizován způsobem popsaným v interní dokumentaci:

- „Příručka administrátora“,
- „Správa TSMC“,
- „Správa TSS“.

6.3 Řízení počítačové bezpečnosti

Důvěryhodné systémy podporující poskytování Služby provádějí monitorování a zaznamenávání relevantních událostí – popsáno v Politice, konkrétně v kapitole Postupy zpracování auditních záznamů. Vybrané události jsou monitorovacím systémem okamžitě hlášeny příslušným administrátorům. Popis je rozpracován v interní dokumentaci:

- „Příručka administrátora“.

6.4 Řízení bezpečnosti životního cyklu

Poskytování Služby je prováděno prostřednictvím důvěryhodných systémů, pro zajištění jejich provozu a správy jsou definovány důvěryhodné role. Popis, včetně řízení elektronických médií a aplikace bezpečnostních patchů, je rozpracován v interní dokumentaci:

- „Řízení bezpečnosti informací“,
- „Kontrolní činnost, bezúhonnost a odbornost“,
- „Příručka administrátora“.
- „Metodika vývoje".
- „Změnové řízení“.

Soulad s požadavky standardů je pravidelně ověřován (zavedený a certifikovaný systém ISMS).

6.5 Řízení bezpečnosti sítě

Popsáno v Politice, konkrétně v kapitole Řízení bezpečnosti sítě. Popis je rozpracován v interní dokumentaci:

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Příručka administrátora“,
- „Firewall – provozní pracoviště“,
- „Plán pro zvládání krizových situací a plán obnovy“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“.

7 HODOCENÍ SHODY A JINÁ HODNOCENÍ

7.1.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Popsáno v Politice, konkrétně v kapitole Periodicita hodnocení nebo okolnosti pro provedení hodnocení.

7.1.2 Identita a kvalifikace hodnotitele

Popsáno v Politice, konkrétně v kapitole Identita a kvalifikace hodnotitele.

7.1.3 Vztah hodnotitele k hodnocenému subjektu

Popsáno v Politice, konkrétně v kapitole Vztah hodnotitele k hodnocenému subjektu.

7.1.4 Hodnocené oblasti

Popsáno v Politice, konkrétně v kapitole Hodnocené oblasti.

7.1.5 Postup v případě zjištění nedostatků

Popsáno v Politice, konkrétně v kapitole Postup v případě zjištění nedostatků.

7.1.6 Sdělování výsledků hodnocení

Popsáno v Politice, konkrétně v kapitole Sdělování výsledků hodnocení.

8 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 Poplatky

Popsáno v Politice, konkrétně v kapitole Poplatky.

8.2 Finanční odpovědnost

Popsáno v Politice, konkrétně v kapitole Finanční odpovědnost.

8.3 Důvěrnost obchodních informací

Popsáno v Politice, konkrétně v kapitole Důvěrnost obchodních informací.

8.4 Ochrana osobních údajů

Popsáno v Politice, konkrétně v kapitole Ochrana osobních údajů.

- „Ochrana osobních údajů v I.CA“,
- „Řízení bezpečnosti informací“.

8.5 Práva duševního vlastnictví

Popsáno v Politice, konkrétně v kapitole Práva duševního vlastnictví

8.6 Zastupování a záruky

Popsáno v Politice, konkrétně v kapitole Zastupování a záruky.

8.7 Zřeknutí se záruk

Popsáno v Politice, konkrétně v kapitole Zřeknutí se záruk.

8.8 Omezení odpovědnosti

Popsáno v Politice, konkrétně v kapitole Omezení odpovědnosti.

8.9 Záruky a odškodnění

Popsáno v Politice, konkrétně v kapitole Záruky a odškodnění.

8.10 Doba platnosti, ukončení platnosti

Popsáno v Politice, konkrétně v kapitole Doba platnosti, ukončení platnosti.

8.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

Popsáno v Politice, konkrétně v kapitole Individuální upozorňování a komunikace se zúčastněnými subjekty.

8.12 Novelizace

Popsáno v Politice, konkrétně v kapitolách Postup při novelizaci a Postup a periodicita oznamování (postup pro Politiku platí analogicky i pro tuto Směrnici1). Dále platí, že OID není Směrnici1 přiřazen, Směrnice1 pokrývá požadavky politiky – viz kapitola 1.2. V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze, v případě zásadních změn v poskytování Služby musí změněno OID pokryté politiky.

8.13 Ustanovení o řešení sporů

Popsáno v Politice, konkrétně v kapitole Ustanovení o řešení sporů.

8.14 Rozhodné právo

Popsáno v Politice, konkrétně v kapitole Rozhodné právo.

8.15 Shoda s právními předpisy

Popsáno v Politice, konkrétně v kapitole Shoda s právními předpisy.

9 DALŠÍ USTANOVENÍ

9.1 Organizační záležitosti

I.CA má dostatečné finanční zdroje pro poskytování Služby a má uzavřena potřebná pojištění – viz výroční zpráva společnosti První certifikační autorita, a.s.

První certifikační autorita, a.s., která je důvěryhodným poskytovatelem Služby, je kvalifikovaným poskytovatelem služeb vytvářejících důvěru dle nařízení eIDAS. I.CA nijak neomezuje potenciální Klienty, poskytování Služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením. Má uzavřeny bilaterální smlouvy se subdodavateli. Definováním a dodržováním oddělení rolí v průběhu procesu omezuje příležitosti k neoprávněné nebo neúmyslné změně nebo zneužití aktiv.

9.2 Smluvní požadavky a podmínky

Popsáno v kapitolách 1.1.2, 1.1.7 a 1.1.8, 1.2.1, 1.3 tohoto dokumentu a v Politice, konkrétně v kapitolách Použití služby, Požadavky na životní cyklus Služby, Doba uchování auditních záznamů, Hodnocení shody a jiná hodnocení, Omezení odpovědnosti, Ustanovení o řešení sporů a Shoda s právními předpisy.

Politika a Směrnice1 i Směrnice2 jsou elektronicky přístupné na webu společnosti.

10 PRÁVNÍ PŘEDPISY, TECHNICKÉ NORMY A STANDARDY

[1] Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS).

[2] CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.

[3] ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.

[4] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[5] ČSN EN 419241-1 Důvěryhodné systémy podporující podpisový server – Část 1: Obecné bezpečnostní požadavky systému.

[6] EN 419 241-1 Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements.

[7] ČSN EN 419241-2 Důvěryhodné systémy podporující podpisový server - Část 2: Profil ochrany pro zařízení QSCD pro serverový podpis.

[8] EN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.

[9] ČSN EN 419221-5 Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografický modul pro důvěryhodné služby.

[10] EN 419221-5 Protection Profiles for TSP Cryptographic Modules – Part 5 - Cryptographic Module for Trust Services.

[11] 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.

[12] 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.

[13] EN 319 142 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures.

[14] ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.

[15] ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile.

[16] ETSI TS 119 432 Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation.

[17] ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[18] ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky.

[19] Prováděcí nařízení komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

[20] zákon České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

11 ZÁVĚREČNÁ USTANOVENÍ

Tato Prováděcí směrnice služby I.CA RemoteSeal (EN 119 431-1) vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem uvedeným v tab. 1.