První certifikační autorita, a.s.



Prováděcí směrnice

služby I.CA RemoteSign

(ETSI TS 119 431-1)

Prováděcí směrnice služby I.CA RemoteSign (ETSI TS 119 431-1) je veřejným dokumentem, který je vlastnictvím společnosti První certifikační autorita, a.s., a byl vypracován jako nedílná součást komplexní bezpečnostní dokumentace. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu majitele autorských práv.

Verze 1.04

Copyright © První certifikační autorita, a.s.

OBSAH

1 Úvod 5
1.1 Požadavky prováděcí směrnice 5
1.1.1 Právní požadavky 5
1.1.2 Identifikace důvěryhodného poskytovatele Služby 6
1.1.3 Organizace spravující prováděcí směrnici 6
1.1.4 Kontaktní osoba organizace spravující prováděcí směrnici 6
1.1.5 Osoba rozhodující o souladu prováděcí směrnice s politikou služby 6
1.1.6 Postupy při schvalování prováděcí směrnice 6
1.1.7 Přípustné použití služby 6
1.1.8 Omezení použití služby 6
1.1.9 Dokumentace vztahující se ke Službě 7
1.1.10 Postupy při ukončení služby 8
1.2 Název a identifikace dokumentu 8
1.2.1 Podporovaná politika pro vytváření podpisu 8
1.3 Zúčastněné strany 8
1.4 Pojmy a zkratky 9
2 Odpovědnost za zveřejňování a úložiště informací a dokumentace 12
2.1 Úložiště informací a dokumentace 12
2.2 Zveřejňování informací a dokumentace 12
2.3 Periodicita zveřejňování informací 12
2.4 Řízení přístupu k jednotlivým typům úložišť 12
3 Inicializace podpisového klíče 13
3.1 Generování podpisového klíče 13
3.1.1 Generování podpisového klíče – řešení 1 13
3.1.2 Generování podpisového klíče – řešení 2 13
3.2 Propojení prostředku elektronické identifikace s konkrétním Klientem 13
3.2.1 Propojení prostředku elektronické identifikace s konkrétním Klientem – řešení 1 13
3.2.2 Propojení prostředku elektronické identifikace s konkrétním Klientem – řešení 2 14
3.3 Propojení certifikátu 14
3.4 Zajišťování prostředků elektronické identifikace 14
4 Požadavky na životní cyklus podpisového klíče 15
4.1 Aktivace tvorby podpisu na dálku 15

4.1.1 Aktivace tvorby podpisu na dálku – řešení 1 15
4.1.2 Aktivace tvorby podpisu na dálku – řešení 2 15
4.2 Rušení podpisového klíče 15
4.3 Úschova a obnova podpisového klíče 15
5 Postupy správy, řízení a provozu 16
5.1 Obecné informace 16
5.2 Fyzická bezpečnost 16
5.3 Procesní bezpečnost 16
5.4 Personální bezpečnost 17
5.5 Postupy zpracování auditních záznamů 17
5.6 Uchovávání záznamů 17
5.7 Obnova po havárii nebo kompromitaci 17
5.8 Ukončení činnosti poskytovatele Služby 17
6 Technická bezpečnost 19
6.1 Řízení systémů a jejich bezpečnosti 19
6.2 Systémy a jejich provozování 19
6.2.1 Přiřazení rolí 19
6.2.2 Provozní dokumentace 19
6.2.3 Synchronizace času 19
6.3 Řízení počítačové bezpečnosti 19
6.4 Řízení bezpečnosti životního cyklu 20
6.5 Řízení bezpečnosti sítě 20
7 HodocenÍ shody a jiná hodnocení 21
7.1.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení 21
7.1.2 Identita a kvalifikace hodnotitele 21
7.1.3 Vztah hodnotitele k hodnocenému subjektu 21
7.1.4 Hodnocené oblasti 21
7.1.5 Postup v případě zjištění nedostatků 21
7.1.6 Sdělování výsledků hodnocení 21
8 Ostatní obchodní a právní záležitosti 22
8.1 Poplatky 22
8.2 Finanční odpovědnost 22
8.3 Důvěrnost obchodních informací 22
8.4 Ochrana osobních údajů 22
8.5 Práva duševního vlastnictví 22
8.6 Zastupování a záruky 22

8.7 Zřeknutí se záruk 22
8.8 Omezení odpovědnosti 22
8.9 Záruky a odškodnění 22
8.10 Doba platnosti, ukončení platnosti 23
8.11 Individuální upozorňování a komunikace se zúčastněnými subjekty 23
8.12 Novelizace 23
8.13 Ustanovení o řešení sporů 23
8.14 Rozhodné právo 23
8.15 Shoda s právními předpisy 23
9 Další ustanovení 24
9.1 Organizační záležitosti 24
9.2 Smluvní požadavky a podmínky 24
10 Právní předpisy, technické normy a standardy 25
11 Závěrečná ustanovení 27

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	31.08.2022	Generální ředitel společnosti První certifikační autorita, a.s.	Vyznačení klasifikace dokumentu. Zapracována možnost použití služby i pro certifikáty vydané pro Slovenskou republiku.
1.02	23.11.2023	Generální ředitel společnosti První certifikační autorita, a.s.	Zapracováno využití nového HW a SW (Entrust), revize textu.
1.03	22.11.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Revize dokumentu, aktualizace odkazované dokumentace.
1.04	09.05.2026	Generální ředitel společnosti První certifikační autorita, a.s.	Revize dokumentu, aktualizace odkazované dokumentace, zohlednění druhého technologického řešení služby.

1 ÚVOD

Tento dokument, Prováděcí směrnice služby I.CA RemoteSign (ETSI TS 119 431-1) - dále též Směrnice1 – stanoví zásady, které První certifikační autorita, a.s., (dále též I.CA) uplatňuje při poskytování služby I.CA RemoteSign, tj. vytváření elektronických podpisů na dálku – dále též Služba, z pohledu požadavků standardu ETSI TS 119 431-1 [11], tj. z pohledu správy a řízení bezpečného zařízení pro vytváření elektronických podpisů. Tato verze zohledňuje vytvoření druhé technologické varianty Služby, pokud se někde text závislosti na variantě 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 v první řadě popsána dokumentem Politika služby I.CA RemoteSign (vytváření elektronických podpisů 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 RemoteSign (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 byl tento dokument v rozporu se standardy nebo právními předpisy, které nahradí dosud platné, bude vydána jeho 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, v platném znění [1],
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce [18],
- 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) [19],
- právní úpravou týkající se ochrany osobních údajů, v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

Služba společnosti První certifikační autorita, a.s., zajišťující vytváření elektronických podpisů na dálku je poskytována ve prospěch konkrétní třetí se strany, a to všem koncovým uživatelům (dále jen „Klientům"), kteří potřebují elektronický podpis pro tuto stranu vytvářet na základě uzavřeného smluvního vztahu.

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 osobou společnosti První certifikační autorita, a.s., v souvislosti s touto Směrnicí1 je výkonný ředitel I.CA. Platí kontaktní údaje uvedené v kapitole 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 elektronického podpisu ve prospěch konkrétní třetí se strany 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 protiprávní účely.

1.1.9 Dokumentace vztahující se ke Službě

Dokumentace společnosti I.CA je tvořena následujícími okruhy:

Okruh	Dokument	Důvěrnost*
Dokumentace ISMS	Rozsah ISMS – důvěryhodné systémy	I.CA – Jen pro vnitřní potřebu
	Politika bezpečnosti informací – důvěryhodné systémy	I.CA – Jen pro vnitřní potřebu
	Přístupy k posuzování a ošetřování rizik bezpečnosti informací – důvěryhodné systémy	I.CA – Jen pro vnitřní potřebu
	Analýza rizik – důvěryhodné systémy Závěrečná zpráva	I.CA – Důvěrné
	Výběr protiopatření – důvěryhodné systémy	I.CA – Důvěrné
	Prohlášení o aplikovatelnosti – důvěryhodné systémy	I.CA – Důvěrné
	Zbytková rizika – důvěryhodné systémy	I.CA – Důvěrné
	Plán ošetření rizik – důvěryhodné systémy	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	Celková bezpečnostní politika a Systémová bezpečnostní politika – důvěryhodné systémy	I.CA – Jen pro vnitřní potřebu
Certifikační politiky a certifikační prováděcí směrnice	certifikační politiky pro vydávané typy certifikátů a společná certifikační prováděcí směrnice – 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 podepisováním na dálku	Politika služby I.CA RemoteSign, dokument dle zvyklostí I.CA, hlavní dokument, se kterým se musí Klient seznámit, součástí jsou také	Veřejný dokument
	Prováděcí směrnice služby I.CA RemoteSign (ETSI TS 119 341-1) - tento dokument	Veřejný dokument

	Prováděcí směrnice služby I.CA RemoteSign (ETSI TS 119 341-2)	Veřejný dokument

* Klasifikační stupně informací používané v I.CA.

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 kapitole 5.7 Ukončení činnosti poskytovatele služeb. Problematika je detailně rozpracována v interní dokumentaci:

- „Ukončení činnosti služeb I.CA“.

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu: Prováděcí směrnice služby I.CA RemoteSign (ETSI TS 119 431-1), verze 1.04

OID dokumentu: není přiřazeno

1.2.1 Podporovaná politika pro vytváření podpisu

Uvedeno v Politice.

1.3 Zúčastněné strany

Procesu Služby, tj. vytváření elektronických podpisů na dálku, se účastní:

- Klient služby, fyzická osoba (dále též Klient), která:
  - má buď s I.CA uzavřenou platnou "Smlouvu o vydání a používání kvalifikovaného certifikátu pro elektronický podpis a službě I.CA RemoteSign", dále též Smlouva, nebo na základě jeho souhlasu jeho jménem vůči I.CA vystupuje třetí strana a potřebné je řešeno smlouvou uzavřenou mezi touto třetí stranou a I.CA,
  - je držitel certifikátu veřejného klíče pro ověřování elektronických podpisů (kvalifikovaný certifikát pro elektronický podpis vydaný pro Českou republiku, kvalifikovaný certifikát pro elektronický podpis vydaný pro Slovenskou republiku nebo kvalifikovaný mandátní certifikát vydaný pro Slovenskou republiku), jemuž příslušný soukromý klíč byl generován a je používán v zařízení typu QSCD provozovaném I.CA,
  - prostřednictvím aplikace na svém mobilním zařízení nebo PC iniciuje vytvoření elektronického podpisu dokumentu, který mu byl k podpisu předložen třetí stranou (viz dále).
- Třetí strana, právnická osoba, která:
  - má s I.CA uzavřenou smlouvu o poskytování Služby definovaným Klientům,
  - prostřednictvím aplikace na zařízení pod svojí kontrolou předkládá Klientům dokumenty k podpisu (k vytvoření elektronického podpisu),

- třetích stran může být ve službě více, speciálním případem třetí strany může být i I.CA sama, v tomto případě samozřejmě smlouva o poskytování Služby definovaným klientům uzavřena není.

- I.CA jako důvěryhodný poskytovatel Služby:
  - je kvalifikovaným poskytovatelem služeb vytvářejících důvěru dle 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 [16],
  - 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 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
párová data	soukromý a jemu odpovídající veřejný klíč
právní úprava pro služby vytvářející důvěru	platné právní předpisy České republiky a Slovenské 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
soukromý klíč	jedinečná data pro vytváření elektronického podpisu
veřejný klíč	jedinečná data pro ověřování elektronického podpisu

tab. 3 - Zkratky

Pojem	Vysvětlení
CA	Certification Authority, certifikační autorita
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
ČSN	označení českých technických norem
EC	Elliptic Curves, eliptické křivky
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
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
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)
HSM	Hardware Security Module, fyzické zařízení, které generuje párová data Klientů, udržuje databázi soukromých klíčů a realizuje podpisy po úspěšné identifikaci a autentizaci Klienta
ISMS	Information Security Management System, systém řízení bezpečnosti informací
NKČR	Notářská komora České republiky
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
PC	Personal Computer, osobní počítač

QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu/pečetě
RA	registrační autorita
RSA	šifra s veřejným klíčem pro podepisování a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)
SCDev	Secure Cryptographic Device, bezpečné kryptografické zařízení
TS	Technical Specification, typ ETSI standardu
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 viz kapitola 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 Celkové bezpečnostní politice.

3 INICIALIZACE PODPISOVÉHO KLÍČE

3.1 Generování podpisového klíče

Podpisové klíče Klientů jsou generovány a používány v zařízení typu QSCD, které je uvedeno na unijním seznamu těchto zařízení a přítomnost na zmíněném seznamu je periodicky kontrolována.

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 používán buď algoritmus RSA s délkou klíče 4096 bitů, nebo algorimus ECC s délkou klíče minimálně 256 bitů.

3.1.1 Generování podpisového klíče – řešení 1

Párová data jsou generována předem, součástí generování je vytvoření aktivačních obálek. Propojení konkrétního klíčového páru s konkrétním Klientem je prováděno při zřízení Služby pro tohoto Klienta prostřednictvím zmíněné aktivační obálky. Aktivační obálka je jediným možným způsobem přístupu k soukromému klíči uloženému v zařízení typu QSCD, bez instalování aplikace na mobilní zařízení nebo PC s využitím aktivační obálky není možné soukromý klíč k provedení jakékoliv kryptografické operace použít.

3.1.2 Generování podpisového klíče – řešení 2

Generování párových dat Klienta je iniciováno tímto Klientem. Nutnou podmínkou je, že Klient má nainstalovanou mobilní nebo PC aplikaci pro vzdálené podepisování a tedy vytvořeny identifikační údaje pro přístup k zařízení typu QSCD (a tedy k vygenerovanému soukromém klíči).

3.2 Propojení prostředku elektronické identifikace s konkrétním Klientem

3.2.1 Propojení prostředku elektronické identifikace s konkrétním Klientem – řešení 1

Prostředkem elektronické identifikace jsou v případě Služby identifikační a autentizační údaje pro přístup k soukromý klíči Klienta uloženému v zařízení typu QSCD. Přístupové údaje k tomuto klíči jsou uloženy v aktivační bezpečnostní obálce, která je Klientovi předána po řádném ověření totožnosti (viz Politika) v průběhu procesu zřizování Služby.

3.2.2 Propojení prostředku elektronické identifikace s konkrétním Klientem – řešení 2

Prostředkem elektronické identifikace jsou v případě Služby identifikační a autentizační údaje pro přístup k soukromému klíči Klienta uloženému v zařízení typu QSCD. Přístupové údaje k tomuto klíči jsou vytvářeny v průběhu aktivace Služby Klientem a standardně jsou chráněny heslem / PINem, Klient má ale možnost přejít na idetifikaci biometrickou, případně se zase k používání hesla / PINu vrátit.

3.3 Propojení certifikátu

Propojení soukromého klíče s certifikátem odpovídajícího veřejného klíče Klienta je zaručeno tím, že páry klíčů jsou generovány v zařízení typu QSCD pod výhradní kontrolou I.CA.

3.4 Zajišťování prostředků elektronické identifikace

Není relevantní, prostředky elektronické identifikace ve fyzické podobě nejsou vydávány a tedy ani distribuovány Klientům.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS PODPISOVÉHO KLÍČE

4.1 Aktivace tvorby podpisu na dálku

4.1.1 Aktivace tvorby podpisu na dálku – řešení 1

Klient na závěr procesu uzavírání Smlouvy obdrží tzv. aktivační obálku, na jejíž přední straně, resp. pod průhledným okénkem na přední straně je vytisknut tzv. identifikační kód, uvnitř obálky je pod bezpečnostní přelepkou vytisknut tzv. aktivační kód. Identifikační kód slouží k svázání klíčového páru s konkrétním Klientem. Aktivační kód slouží Klientovi pro zřízení přístupu ke Službě z určitého zařízení a pro vytvoření si pro ně autentizačních údajů. V případě prvního zařízení Klienta se jedná o tzv. aktivaci Služby.

Aktivaci tvorby elektronického podpisu v rámci Služby provádí Klient. Jeho unikátní identifikační a autentizační údaje jsou přeneseny z aplikace nainstalované na jeho mobilním zařízení nebo PC do zařízení typu QSCD. Pro zabezpečení Služby je využíván proprietární protokol popsaný v interním materiálu dokumentu uloženém v interním informačním systému:

- „I.CA RemoteSign – kompletní analýza“.

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

4.1.2 Aktivace tvorby podpisu na dálku – řešení 2

Aktivace Služby je integrální součástí procesu zahrnujícího mj. vydání kvalifikovaného certifikátu, v rámci kterého jsou zároveň vytvořeny identifikační údaje pro přístup k soukromému klíči, resp. k jeho užití v zařízení typu QSCD.

Pro zabezpečení Služby je využíván standardní protokol definovaný v ETSI TS 119 432 [13]. Zmíněný protokol zajišťuje, aby bylo zamezeno útočníkovi s vysokým potenciálem útoku Službu narušit.

4.2 Rušení podpisového klíče

Rušení soukromých klíčů odpovídajících zneplatněným nebo expirovaným certifikátům je realizováno nativními prostředky zařízení typu QSCD.

4.3 Úschova a obnova podpisového klíče

Zařízení typu QSCD použité pro správu párových dat Klientů umožňuje zálohování soukromých klíčů. Soukromé klíče jsou zálohovány s využitím nativních prostředků těchto zařízení v zašifrované podobě. Zašifrovaná záloha je použitelná pouze v příslušném zařízení. Zálohování a obnovu databáze soukromých klíčů provádějí pracovníci v důvěryhodných rolích – popsáno v interní dokumentaci:

- „Příručka administrátora".

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 Systémové bezpečnostní politice – důvěryhodné systémy, 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“,
- „HSM nShield Postupy generování klíčů a certifikátů CA a OCSP“,
- „HSM nShield Connect 5c Postupy generování klíčů a certifikátů CA a OCSP“,
- „HSM nShield Connect XC CMTS Postupy instalace a správy“,
- „HSM nShield Connect 5c CMTS Postupy instalace a správy“.
- „Směrnice pro pracovníky RA I.CA“,
- „Směrnice pro pracovníky DRA NKČR“,
- „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“,
- „Zálohování 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“,
- „Zálohování 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 TECHNICKÁ BEZPEČNOST

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“.

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. Popis je rozpracován v interní dokumentaci:

- „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, v platném znění.

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

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

[15] European Cybersecurity Certification Group Sub-group on Cryptography - Agreed Cryptographic Mechanisms.

[16] ČSN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky.

[17] 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.

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

[19] Zákon 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).

11 ZÁVĚREČNÁ USTANOVENÍ

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