První certifikační autorita, a.s.



Prováděcí směrnice

služby I.CA RemoteSign

(ETSI TS 119 431-2)

Prováděcí směrnice služby I.CA RemoteSign (ETSI TS 119 431-2) 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 4
1.1 Přehled 4
1.1.1 Identifikace důvěryhodného poskytovatele služby 4
1.1.2 Podporovaná politika pro vytváření podpisu 4
1.2 Prostředí komponent aplikace pro vytváření podpisů 5
1.2.1 Zúčastněné strany Služby 5
1.2.2 Architektura služby 5
1.3 Pojmy a zkratky 9
1.3.1 Pojmy 9
1.3.2 Zkratky 9
1.4 Zásady a postupy 10
1.4.1 Organizace spravující dokumentaci důvěryhodného poskytovatele Služby 10
1.4.2 Kontaktní osoba 10
1.4.3 Dokumentace vztahující se ke Službě 11
2 Řízení a provoz důvěryhodných služeb 13
2.1 Interní postupy organizace 13
2.1.1 Spolehlivost organizace 13
2.1.2 Oddělení povinností 13
2.2 Lidské zdroje 13
2.3 Správa aktiv 13
2.3.1 Obecné požadavky 13
2.3.2 Manipulace s médii 14
2.4 Řízení přístupu 14
2.5 Kryptografická opatření 14
2.6 Fyzická bezpečnost a bezpečnost prostředí 14
2.7 Bezpečnost provozu 15
2.8 Síťová bezpečnost 15
2.9 Ošetření incidentů 15
2.10 Shromažďování důkazů 15
2.11 Řízení kontinuity činností 16
2.12 Ukončení činnosti a plány ukončení činnosti důvěryhodného poskytovatele služeb 16
2.13 Shoda 16
3 Technické požadavky na komponenty Služby 17

3.1 Rozhraní 17
3.1.1 Rozhraní – řešení 1 17
3.1.2 Rozhraní – řešení 2 17
3.2 Tvorba elektronického podpisu AdES 17
4 Právní předpisy, technické normy a standardy 18
5 Závěrečná ustanovení 19

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 RemoteSign (ETSI TS 119 431-2) 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), dle požadavků standardu ETSI TS 119 431-2 [12]. 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 dokument Prováděcí směrnice služby I.CA RemoteSign (ETSI TS 119 431-1) - dále též Směrnice1 a tento dokument – 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 Přehled

1.1.1 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.

1.1.2 Podporovaná politika pro vytváření podpisu

Uvedeno v Politice.

1.2 Prostředí komponent aplikace pro vytváření podpisů

1.2.1 Zúčastněné strany Služby

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 poskytování Služby, 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 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 [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.

1.2.2 Architektura služby

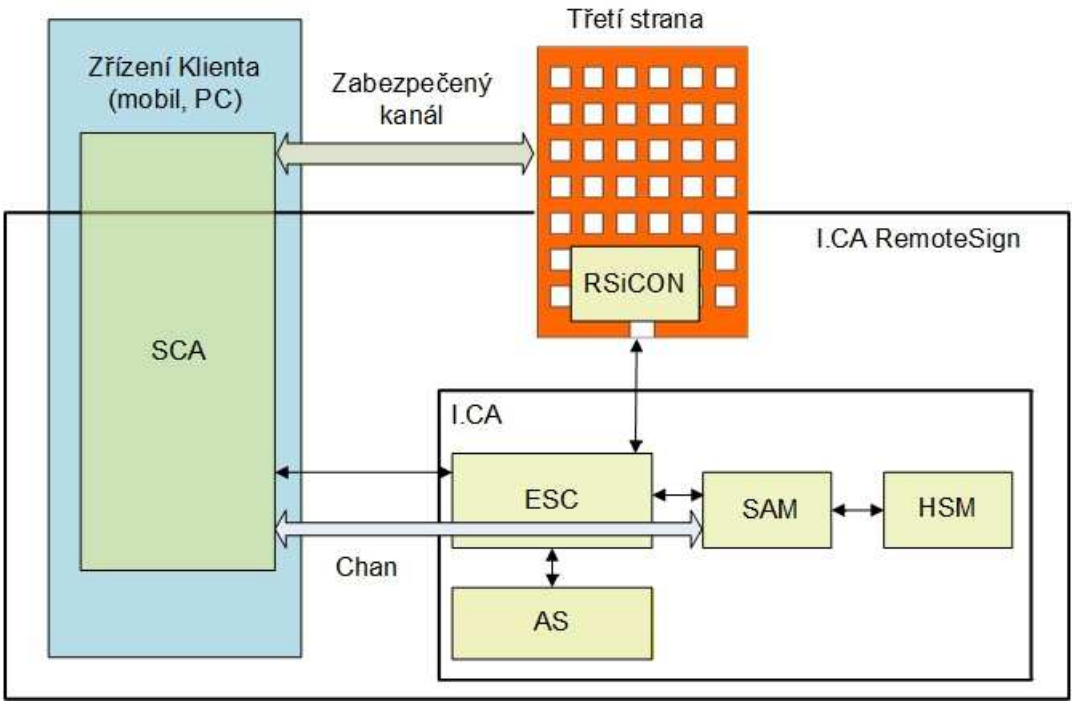
Následující dvě podkapitoly obsahují schematický popis obou řešení architektury Služby. Podrobné popisy včetně mapování jednotlivých funkčních požadavků relevantních standardů na funkcionality komponent tohoto řešení jsou uvedeny v interní dokumentaci:

- Analytická dokumentace I.CA RemoteSign, I.CA RemoteSeal“.

1.2.2.1 Architektura služby – řešení 1

Architektura služby je popsána na následujícím obrázku, jsou v něm použity tyto pojmy a zkratky:

Pojem / zkratka	**Popis**
Zabezpečený kanál	jakýkoliv zabezpečený kanál pro komunikaci mezi systémy třetí strany a Klientem (smart mobilní aplikace, např. smart banking, webový portál, telefonické spojení na definované číslo, nebo osobní jednání Klienta u třetí strany
RSiCON	Remote Sign Connector, aplikace vytvořená v I.CA, ale provozovaná v prostředí třetí strany, sloužící mj. pro zasílání požadavků na podpis do fronty na serveru ESC a naopak dostávající z ESC podpisy AdES
SCA	Secure Application, aplikace komunikující bezpečným způsobem s dalšími komponentami systému, mj. zprostředkovávající zobrazení podepisovaných dat, komunikaci se SAM nebo autorizující použití podepisovacího klíče
Chan	kanál umožňující bezpečnou komunikace aplikace SCA s modulem SAM
ESC	Evolved Signature Core, hlavní server systému na straně I.CA, na které je mj. udržována fronta požadavků na podpis dokumentů zaslaných třetí stranou prostřednictvím RSiCON, která je přístupná Klientovi v aplikaci SCA
SAM	Signature Activation Module, povinná součást QSCD pro vzdálený podpis, která zajišťuje kontrolu přístupu k soukromým podpisovým klíčům
HSM	Hardware Security Module, certifikované fyzické zařízení, které generuje párová data Klientů, udržuje databázi soukromých klíčů a realizuje podpisy po úspěšné identifikaci a autentizaci Klienta
AS	Authorization Server, aplikační server, který zajišťuje ověření autentizace koncového uživatele (držitele klíče) a vytváření datové struktury pro SAM, která autorizuje použití příslušného soukromého klíče pro opatření odpovídajících dat elektronickým podpisem



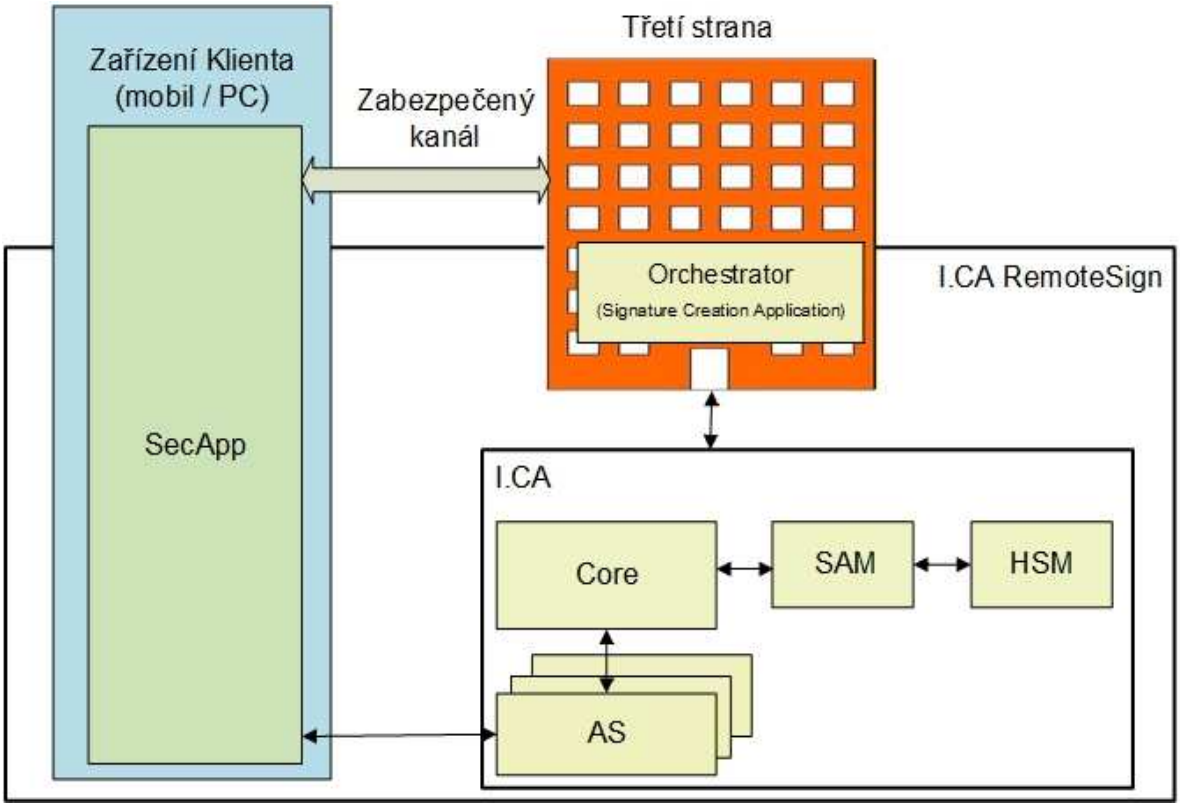
Třetí strana připravuje Klientovi dokumenty k podpisu a zařazuje je do fronty na serveru ESC. O dokumentech připravených k podpisu je Klient informován zabezpečeným kanálem. Prostřednictvím aplikace ESC má do fronty požadavků přístup a má možnost vybrat ten dokument, který si přeje podepsat. Klient má k dispozici možnost náhledu jednotlivých dokumentů (I.CA obsah/náhled podepisovaných dokumentů v čitelné podobě k dispozici nemá). Server ESC sestaví data k podepsání (obsahující podepisované atributy) a předá je aplikaci SCA na mobilním zařízení nebo PC Klienta. Po odsouhlasení operace (požadavku na podpis dokumentu) Klientem předá aplikace SCA příslušná data zabezpečeným kanálem aplikaci SAM. SAM prověří integritu dat ve vztahu ke Klientovi a jeho zařízení a následně předá data k podpisu do HSM, kde je nakonec připravená datová struktura podepsána Klientovým soukromým klíčem. Podepsaná struktura je vrácena serveru ESC, který ji pošle aplikaci RSiCON na straně třetí strany.

1.2.2.2 Architektura služby – řešení 2

Architektura služby je popsána na následujícím obrázku. V obrázku jsou použity tyto pojmy a zkratky:

Pojem / zkratka	**Popis**
Zabezpečený kanál	jakýkoliv zabezpečený kanál pro komunikaci mezi systémy třetí strany a Klientem (smart mobilní aplikace, např. smart banking, webový portál, telefonické spojení na definované číslo, nebo osobní jednání Klienta u třetí strany
Orchestrator	aplikace vytvořená I.CA, provozovaná v prostředí třetí strany, sloužící mj. pro zasílání požadavků na podpis do fronty na serveru Core a naopak dostávající z Core podpisy AdES

SecApp	Secure Application, aplikace komunikující bezpečným způsobem s dalšími komponentami systému, mj. zprostředkovávající zobrazení podepisovaných dat nebo autorizující použití podepisovacího klíče
Core	hlavní server systému na straně I.CA, na které je mj. udržována fronta požadavků na podpis dokumentů zaslaných třetí stranou prostřednictvím komponenty Orchestrator, která je přístupná Klientovi v aplikaci SCA
SAM	Signature Activation Module, povinná součást QSCD pro vzdálený podpis, která zajišťuje kontrolu přístupu k soukromým podpisovým klíčům
HSM	Hardware Security Module, certifikované fyzické zařízení, které generuje párová data Klientů a realizuje podpisy po úspěšné identifikaci a autentizaci Klienta
AS	Authorization Server, aplikační server, který zajišťuje ověření autentizace koncového uživatele (držitele klíče) a vytváření datové struktury pro SAM, která autorizuje použití příslušného soukromého klíče pro opatření odpovídajících dat elektronickým podpisem, může existovat více instancí v závislosti na konkrétní třetí straně



Třetí strana připravuje Klientovi dokumenty k podpisu a zařazuje je do fronty na serveru Orchestrator. O dokumentech připravených k podpisu je Klient informován zabezpečeným kanálem. Prostřednictvím komponenty Orchestrator jsou mu zprostředkovány požadavky na

podpis dokumentů. Pokud je v požadavku více dokumentů, podepisují se jako sada dokumentů, nelze zvolit podepsání jednotlivých dokumentů ze sady. Klient může mít k dispozici možnost náhledu jednotlivých dokumentů (I.CA obsah/náhled podepisovaných dokumentů v čitelné podobě k dispozici nemá), pokud nemá možnost si náhled zobrazit v jiném systému třetí strany. Server Orchestrator sestaví data k podepsání (obsahující podepisované atributy) a předá je aplikaci SecApp na mobilním zařízení nebo PC Klienta. Po odsouhlasení operace (požadavku na podpis dokumentu) Klientem předá aplikace SecApp příslušná data aplikaci SAM. SAM prověří integritu dat ve vztahu ke Klientovi a jeho zařízení a následně předá data k podpisu do HSM, kde je nakonec připravená datová struktura podepsána Klientovým soukromým klíčem. Podepsaná hash je vrácena komponentě Orchestrator, který složí výsledná podepsaná data a předá je třetí straně.

1.3 Pojmy a zkratky

1.3.1 Pojmy

Pojem	Vysvětlení
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
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
soukromý klíč	jedinečná data pro vytváření elektronického podpisu
veřejný klíč	jedinečná data pro ověřování elektronického podpisu

1.3.2 Zkratky

Zkratka	Vysvětlení
AdES	Advanced Electronic Signature, zaručený elektronický podpis
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
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
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	Signature Creation Device, zařízení pro tvorbu elektronického podpisu
TS	Technical Specification, typ ETSI standardu
TSA	Time Stamping Authority, autorita časových razítek
TSP	Trusted Service Provider, důvěryhodný poskytovatel služeb
TSS	Time Stamp Server, server vytvářející časová razítka

1.4 Zásady a postupy

1.4.1 Organizace spravující dokumentaci důvěryhodného poskytovatele Služby

Veškerou dokumentaci důvěryhodného poskytovatele Služby včetně této Směrnice2 spravuje společnost První certifikační autorita, a.s.

1.4.2 Kontaktní osoba

Kontaktní osobou společnosti První certifikační autorita, a.s., v souvislosti s touto Směrnicí2 je výkonný ředitel I.CA. Platí kontaktní údaje uvedené v kapitole 1.1.2.

1.4.3 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)	Veřejný dokument

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

* Klasifikační stupně informací používané v I.CA.

Veřejné dokumenty jsou k dispozici na webových stránkách I.CA.

2 ŘÍZENÍ A PROVOZ DŮVĚRYHODNÝCH SLUŽEB

2.1 Interní postupy organizace

2.1.1 Spolehlivost organizace

Popsáno v Politice, konkrétně v kapitole Požadavky na nezávislé dodavatele.

2.1.2 Oddělení povinností

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

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

2.2 Lidské zdroje

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

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Řízení bezpečnosti informací“,
- „Příručka administrátora“,
- „Kontrolní činnost, bezúhonnost a odbornost“,
- „Pracovní řád“.

2.3 Správa aktiv

2.3.1 Obecné požadavky

Hlavní požadavky na správu aktiv jsou popsány v interní dokumentaci:

- „Celková bezpečnostní politika“,
- „Řízení bezpečnosti informací“,
- „Zálohování dat provozních systémů“,
- „Pořizování, správa a likvidace majetku I.CA“,
- „Evidence licenčního software“,
- „Příručka administrátora".

2.3.2 Manipulace s médii

Popsáno v Politice, konkrétně v kapitole Ukládání médií. Popis je rozpracován v interní dokumentaci:

- „Příručka administrátora“.

2.4 Řízení přístupu

Řízení fyzického přístupu je popsáno v Politice, konkrétně v kapitole Fyzický přístup. Popis je rozpracován v interní dokumentaci:

- „Řízení fyzického přístupu do místností I.CA“,
- „Kamerový systém – provozní pracoviště“,
- projekty fyzické bezpečnosti jednotlivých provozních pracovišť.

Řízení logického přístupu je založeno na systému rolí. Popis je rozpracován v interní dokumentaci:

- „Příručka administrátora“.

2.5 Kryptografická opatření

Kryptografická opatření jsou nasazována:

- podle požadavků příslušné právní úpravy a souvisejících technických standardů,
- na základě pravidelně opakované analýzy rizik důvěryhodných systémů.

Šifrovaně je vedena veškerá komunikace s klientskými místy (registračními autoritami).

Kryptografické algoritmy jsou vybírány dle doporučení standardů ETSI TS 119 312 [14], resp. ENISA [15].

2.6 Fyzická bezpečnost a bezpečnost prostředí

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.

2.7 Bezpečnost provozu

Popsáno v Politice, konkrétně v kapitolách Procesní bezpečnost, Personální bezpečnost, Technické řízení životního cyklu a Ochrana proti padělání a odcizení dat. Popis je rozpracován v interní dokumentaci:

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

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

2.8 Síťová bezpečnost

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

- „Systémová bezpečnostní politika – důvěryhodné systémy“,
- „Řízení bezpečnosti informací“,
- „Firewall – provozní pracoviště",
- „HSM nShield Connect XC CMTS Postupy instalace a správy“,
- „HSM nShield Connect 5c CMTS Postupy instalace a správy“,
- „Správa TSMC",
- „Příručka administrátora“.

2.9 Ošetření incidentů

Popsáno v Politice, konkrétně v kapitole Postup ošetření incidentu nebo kompromitace. Popis je rozpracován v interní dokumentaci:

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

2.10 Shromažďování důkazů

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

- „Řízení fyzického přístupu do místností I.CA“,

- „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“.

2.11 Řízení kontinuity činností

Popsáno v politice, konkrétně v kapitole Postup ošetření incidentu nebo kompromitace. Popis je rozpracován v interní dokumentaci:

- „Plán pro zvládání krizových situací a plán obnovy“.

2.12 Ukončení činnosti a plány ukončení činnosti důvěryhodného poskytovatele služeb

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

- „Ukončení činnosti služeb I.CA“.

2.13 Shoda

Popsáno v Politice, konkrétně v kapitole Hodnocení shody a jiná hodnocení. Popis je rozpracován v interní dokumentaci:

- „Řízení bezpečnosti informací“.

3 TECHNICKÉ POŽADAVKY NA KOMPONENTY SLUŽBY

3.1 Rozhraní

3.1.1 Rozhraní – řešení 1

Služba využívá pro interakci mezi Klientem a komponentami pod kontrolou I.CA proprietární kryptografický protokol popsaný v interním materiálu uložen ve vnitřním informačním systému:

- „I.CA RemoteSign – kompletní analýza“.

Zmíněný protokol splňuje požadavky relevantního technického standardu (ETSI TS 119 432 [13]) a zajišťuje, aby bylo zamezeno Službu narušit i útočníkovi s vysokým potenciálem útoku.

Zmíněný kryptografický protokol umožňuje vytvořit zabezpečený komunikační kanál mezi Klientem a komponentou SAM, která je předřazena kryptografickému modulu HSM (viz obrázek v kapitole 1.2.2).

Dokument, který má být podepsán, prezentuje Klientovi třetí strana, v jejíž prospěch je tento dokument podepisován. Klient má k dispozici vždy alespoň jednu možnost náhledu dokumentu předkládaného k podpisu. Aplikace RSiCON při zakládání transakce buď vytvoří náhled dokumentu ve tvaru PDF, nebo do preview bloku vloží odkaz na podepisovaná data.

3.1.2 Rozhraní – řešení 2

Služba využívá pro interakci mezi Klientem a komponentami pod kontrolou I.CA standardizovaný protokol splňující požadavky technického standardu (ETSI TS 119 432 [13]), který zajišťuje, aby bylo zamezeno Službu narušit i útočníkovi s vysokým potenciálem útoku.

Zmíněný kryptografický protokol umožňuje vytvořit zabezpečený komunikační kanál mezi Klientem a komponentou SAM, která je předřazena kryptografickému modulu HSM (viz obrázek v kapitole 1.2.2).

Dokument, který má být podepsán, prezentuje Klientovi třetí strana, v jejíž prospěch je tento dokument podepisován. Klient může mít k dispozici možnost náhledu dokumentu předkládaného k podpisu, pokud tato možnost není realizovaná jinými systémy třetí strany.

3.2 Tvorba elektronického podpisu AdES

Veškerá komunikace v rámci Služby je vedena šifrovaně, použité kryptografické algoritmy jsou v souladu s doporučeními ETSI TS 119 312 [14], resp. ENISA [15].

Pro tvorbu elektronického podpisu na dálku je výhradně využit kryptografický algoritmus RSA (uvedeno v Politice), každý Klient má v systému.

Identifikační a autentizační údaje Klienta pro přístup k soukromého klíči uloženému v zařízení typu QSCD spravovaném I.CA jsou přenášeny prostřednictvím výše uvedeného **1:** proprietárního protokolu **2:** standardizovaného protokolu, který zajišťuje jejich, integritu a zaručuje, že tyto údaje nejsou v prostředí I.CA nikdy ukládány. Stejný protokol zaručuje, že podepsán je ten dokument, který Klient k podepsání vybral.

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

[18] 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).

5 ZÁVĚREČNÁ USTANOVENÍ

Tato Prováděcí směrnice služby I.CA RemoteSign (EN 119 431-2) vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem uvedeným v tab. 1.