První certifikační autorita, a.s.

Prováděcí směrnice

služby I.CA RemoteSeal

(ETSI TS 119 431-2)

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 119 431-2) - dále též Směrnice2, stanovuje zásady, které První certifikační autorita, a.s., (dále též I.CA), uplatňuje při zajištění služby I.CA RemoteSeal, tj. vytváření elektronických pečetí na dálku (dále též Služba), z pohledu požadavků standardu ETSI TS 119 431-2 [12].

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 dokument Prováděcí směrnice služby I.CA RemoteSeal (ETSI TS 119 431-1) - dále též Směrnice1 a tento dokument (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 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 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.

1.2 Prostředí komponent aplikace pro vytváření pečetí

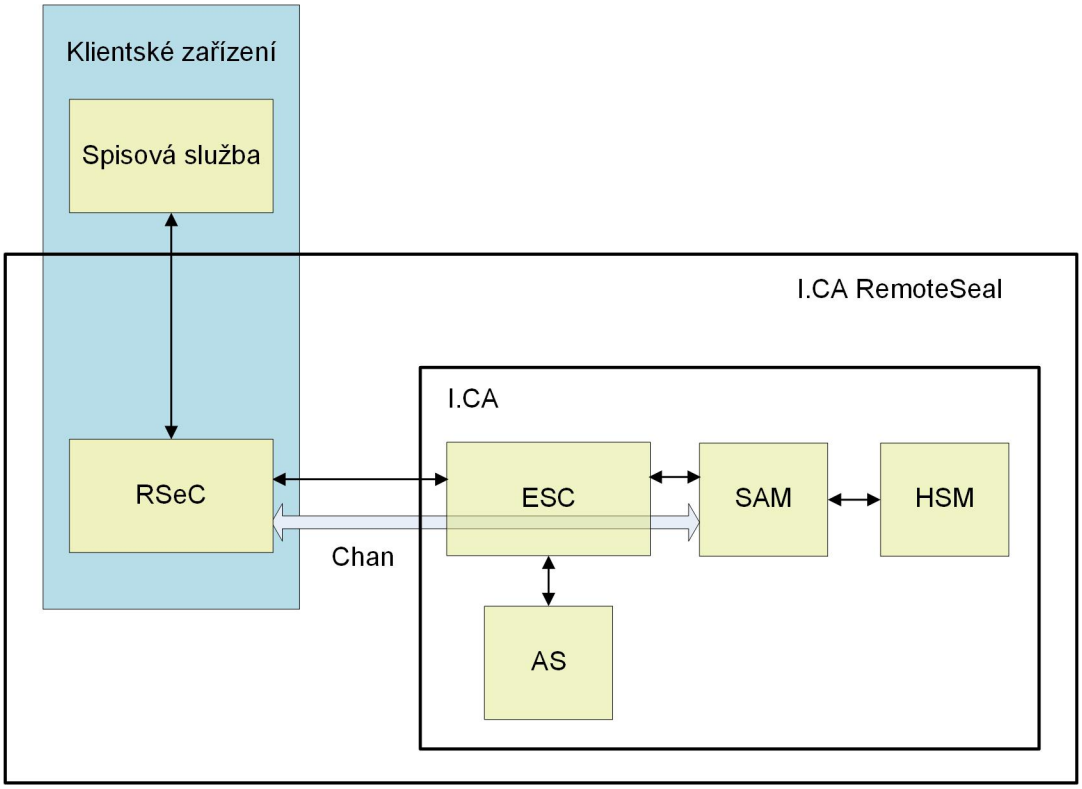
1.2.1 Zúčastněné strany

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 [15],
  - 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

Architektura Služby je zobrazena na následujícím obrázku:



V obrázku architektury jsou použity tyto pojmy a zkratky:

Pojem / zkratka	**Popis**
AS	Authorization Server, aplikační server, který zajišťuje ověření autentizace koncového uživatele (držitele klíče) a vytváření datové struktury pro SAM, která autorizuje použití příslušného soukromého klíče pro opatření odpovídajících dat elektronickou pečetí
ESC	Evolved Signature Core, základní aplikační server provozovaný I.CA přes který probíhá veškeré komunikace týkající se pečetění z klientských komponent
HSM	Hardware Security Module, povinná součást QSCD, fyzické zařízení, které generuje párová data Klientů, udržuje databázi soukromých klíčů a realizuje pečetě po úspěšné identifikaci a autentizaci Klienta
Chan	kanál umožňující bezpečnou komunikaci aplikace RSeC s modulem SAM

RSeC	Remote Seal Connector, klientská komponenta určená pro strojové pečetění dokumentů a pro integraci do spisové služby nebo jiného systému, který potřebuje autonomně vytvářet kvalifikované pečetě; existuje ve více variantách pro snadnou integraci do různých systémů komponenta vytvořená v I.CA, ale provozovaná v prostředí třetí strany, sloužící mj. pro zasílání požadavků na pečetě do fronty na serveru ESC, a naopak dostávající z ESC pečetě formátů AdES
SAM	Signature Activation Module, povinná součást QSCD pro vzdálenou pečeť, která zajišťuje kontrolu přístupu k soukromým pečetícím klíčům
Spisová služba	aplikace Klienta, která vyžaduje opatření dokumentů elektronickou pečetí

Postup opatřování dokumentů kvalifikovanou elektronickou pečetí je následující:

- spisová služba předá komponentě RSeC přístupový soubor, heslo, seznam dokumentů, které mají být opatřeny elektronickou pečetí a požadované parametry pečetí (viditelný nebo neviditelný, formát, s nebo bez časového razítka),
- komponenta RSeC připraví datové struktury dle požadavků norem, autorizuje použití soukromého klíče uloženého v HSM modulu,
- komponenta RSeC získá zpět vytvořenou pečetící strukturu včetně případného časového razítka,
- komponenta RSeC sestaví kompletní podepsané dokumenty a předá je zpět spisové službě.

1.3 Pojmy a zkratky

1.3.1 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	platné právní předpisy České republiky vztahující se ke

vytvářející důvěru	službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
soukromý klíč	jedinečná data pro vytváření elektronické pečetě
veřejný klíč	jedinečná data pro ověřování elektronické pečetě

1.3.2 Zkratky

Zkratka	Vysvětlení
AdES	Advanced Electronic Signature, typ elektronického podpisu/pečetě
ASiC-E	Associated Signature Container – Extended, kontejnerová struktura pro svázání podepisovaných/pečetěných dat a externího podpisu/pečeti do jednoho soboru – kontejneru
CAdES	CMS Advanced Electronic Signature, typ elektronického podpisu/pečetě
ČR	Česká republika
ČSN	označení českých technických norem
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EU	Evropská unie
EZS	elektronická zabezpečovací signalizace
GDPR	General Data Protection Regulation, nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
HSM	Hardware Security Module
http	Hypertext Transfer Protocol, protokol pro výměnu textových dokumentů ve formátu html
https	Hypertext Transfer Protocol Secure, protokol pro zabezpečenou výměnu textových dokumentů ve formátu html
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory

ISMS	Information Security Management System, systém řízení bezpečnosti informací
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
PAdES	PDF Advanced Electronic Signature, typ elektronického podpisu/pečetě
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování–Zavedení–Kontrola–Využití, Demingův cyklus, metoda neustálého zlepšování
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu/pečetě
SAM	Signature Activation Module
SCDev	Secure Cryptographic Device, bezpečné kryptografické zařízení
TS	Technical Specification, typ ETSI standardu
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
XAdES	XML Advanced Electronic Signature, typ elektronického podpisu/pečetě
ZOOÚ	aktuální právní úprava týkající se ochrany osobních údajů

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 osoba společnosti První certifikační autorita, a.s., v souvislosti s touto Směrnicí2, je uvedena na internetové adrese (viz kapitola 1.1.1).

1.4.3 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), prováděcí směrnice dle požadavků normy ETSI TS 119 341-1	Veřejný dokument
	Prováděcí směrnice služby I.CA RemoteSeal (ETSI TS 119 341-2) - tento dokument – prováděcí směrnice dle požadavků normy ETSI TS 119 341-2	Veřejný dokument

* na konci názvu dokumentu je vždy text " - důvěryhodné systémy"

** klasifikační stupně informací používané v I.CA

Všechny 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“,
- „Příprava uchovávaných informací“,
- „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 kontaktními místy (registračními autoritami).

Kryptografické algoritmy a protokoly jsou vybírány dle doporučení standardů ETSI TS 119 312 [14], resp. ETSI TS 119 432 [13].

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“,
- „Firewall – provozní pracoviště",
- „HSM/nShield XC“,
- „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“,
- „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“.

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

Služba využívá pro interakci mezi Klientem a komponentami pod kontrolou I.CA proprietární kryptografický protokol popsaný v interní dokumentaci:

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

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).

3.2 Tvorba elektronického pečetě AdES

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

Pro tvorbu elektronické pečetě na dálku je výhradně využit kryptografický algoritmus RSA (uvedeno v Politice), každý Klient má v systému právě jeden aktivní pečetící (soukromý) klíč.

Identifikační a autentizační údaje Klienta pro přístup k soukromému klíči uloženému v bezpečném kryptografickém prostředí jsou přenášeny prostřednictvím výše uvedeného proprietárního protokolu, který zajišťuje jejich důvěrnost, integritu a zaručuje, že tyto údaje nejsou v prostředí I.CA nikdy ukládány. Stejný proprietární protokol zaručuje, že je podepsán ten a jedině 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 (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] 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] ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.

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

[17] Signature Activation Module – Product description ENTRUST.

5 ZÁVĚREČNÁ USTANOVENÍ

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