

První certifikační autorita, a.s.



Prováděcí směrnice

kvalifikované služby ověřování platnosti

kvalifikovaných elektronických podpisů a pečeti

Prováděcí směrnice kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečeti 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 1.14

OBSAH

| | | |
|-------|--|----|
| 1 | Úvod | 5 |
| 1.1 | Přehled | 5 |
| 1.1.1 | Identifikace poskytovatele služeb vytvářejících důvěru | 6 |
| 1.1.2 | Podporované politiky služby ověřování podpisů | 6 |
| 1.2 | Komponenty služby ověřování podpisů | 6 |
| 1.2.1 | Participující subjekty | 6 |
| 1.2.2 | Architektura systému | 7 |
| 1.3 | Pojmy a zkratky | 9 |
| 1.3.1 | Pojmy | 9 |
| 1.3.2 | Zkratky | 10 |
| 1.4 | Zásady a postupy | 11 |
| 1.4.1 | Organizace spravující dokumentaci | 11 |
| 1.4.2 | Kontaktní osoba | 11 |
| 1.4.3 | Dokumentace související se službou | 11 |
| 1.4.4 | Úložiště informací | 12 |
| 2 | Řízení a provoz služby | 13 |
| 2.1 | Postupy organizace | 13 |
| 2.1.1 | Spolehlivost externí organizace | 13 |
| 2.1.2 | Oddělení povinností | 13 |
| 2.1.3 | Finanční odpovědnost | 14 |
| 2.1.4 | Řešení sporů | 14 |
| 2.1.5 | Záruky a odpovědnosti | 14 |
| 2.2 | Lidské zdroje | 16 |
| 2.2.1 | Požadavky na kvalifikaci, zkušenosti a bezúhonnost | 16 |
| 2.2.2 | Posouzení spolehlivosti osob | 16 |
| 2.2.3 | Příprava pro výkon role, školení, dokumentace | 16 |
| 2.2.4 | Administrativní a řídicí postupy zaměstnanců a vedoucích zaměstnanců | 17 |
| 2.2.5 | Periodicita a posloupnost rotace pracovníků mezi různými rolemi | 17 |
| 2.2.6 | Postihy za neoprávněné činnosti zaměstnanců | 17 |
| 2.3 | Správa aktiv | 17 |
| 2.3.1 | Obecné požadavky | 17 |
| 2.3.2 | Správa médií | 17 |

| | | |
|--------|---|----|
| 2.4 | Řízení přístupu..... | 18 |
| 2.4.1 | Počáteční ověření identity | 18 |
| 2.4.2 | Autentizace ke službě QVerify | 18 |
| 2.5 | Kryptografická opatření | 18 |
| 2.6 | Fyzická bezpečnost a bezpečnost prostředí | 18 |
| 2.6.1 | Umístění a konstrukce | 19 |
| 2.6.2 | Fyzický přístup | 19 |
| 2.6.3 | Elektřina a klimatizace | 19 |
| 2.6.4 | Vlivy vody | 19 |
| 2.6.5 | Protipožární opatření a ochrana | 19 |
| 2.7 | Bezpečnost provozu..... | 19 |
| 2.7.1 | Relevantní standardy..... | 20 |
| 2.7.2 | Řízení vývoje a provozu | 21 |
| 2.7.3 | Řízení změn | 21 |
| 2.7.4 | Řízení bezpečnosti | 22 |
| 2.7.5 | Ochrana proti padělání a odcizení | 22 |
| 2.7.6 | Hodnocení zranitelnosti | 22 |
| 2.7.7 | Vyšší moc..... | 22 |
| 2.7.8 | Další opatření | 23 |
| 2.8 | Síťová bezpečnost | 23 |
| 2.9 | Ošetření incidentů | 23 |
| 2.10 | Shromažďování důkazů | 23 |
| 2.10.1 | Auditní záznamy (logy) | 24 |
| 2.10.2 | Uchovávání informací a dokumentace | 25 |
| 2.11 | Havarijní plánování | 26 |
| 2.12 | Ukončení činnosti a plány ukončení činnosti | 26 |
| 2.13 | Shoda | 27 |
| 2.13.1 | Rozhodné právo a shoda s právními předpisy | 27 |
| 2.13.2 | Hodnocení | 27 |
| 2.13.3 | Ochrana osobních údajů..... | 28 |
| 2.13.4 | Citlivost obchodních informací | 29 |
| 3 | Signature validation service design Koncept služby ověřování podpisů..... | 30 |
| 3.1 | Požadavky procesu ověřování podpisů | 31 |
| 3.2 | Požadavky protokolu ověřování podpisu | 31 |
| 3.3 | Rozhraní | 32 |

| | | |
|-------|--|----|
| 3.3.1 | Komunikační kanál | 32 |
| 3.3.2 | Vztah mezi poskytovatelem služby a jinými poskytovateli služeb vytvářejících důvěru..... | 32 |
| 3.4 | Požadavky na zprávu o ověření | 32 |
| 4 | Závěrečná ustanovení..... | 33 |

tab. 1 - Vývoj dokumentu

| Verze | Datum vydání | Schválil | Poznámka |
|-------|--------------|---|--|
| 1.00 | 1.11.2016 | Ředitel společnosti První certifikační autorita, a.s. | První vydání. |
| 1.10 | 13.1.2017 | Ředitel společnosti První certifikační autorita, a.s. | Rozšíření o kvalifikované elektronické pečeti. |
| 1.11 | 15.3.2017 | Ředitel společnosti První certifikační autorita, a.s. | Opraveny formální chyby. |
| 1.12 | 30.1.2018 | Ředitel společnosti První certifikační autorita, a.s. | Rozšíření o formáty s časových razítkem, zpracování připomínek auditora, aktualizace seznamu standardů. |
| 1.13 | 27.1.2020 | Generální ředitel společnosti První certifikační autorita, a.s. | Aktualizace seznamu standardů. |
| 1.14 | 14.4.2022 | Generální ředitel společnosti První certifikační autorita, a.s. | Změna struktury dokumentu v souladu s ETSI TS 119 441. Doplněn seznam formátů ověřovaných elektronických podpisů a pečeti. Revize textu. |

1 ÚVOD

Tento dokument, Prováděcí směrnice kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí (dále též Směrnice), rozpracovává zásady uvedené v dokumentu Politika kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí (dále též Politika), které První certifikační autorita, a.s., uplatňuje v souladu s platnými právními předpisy a mezinárodně uznávanými technickými normami při zajištění provozu kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí v souladu s relevantní právní úpravou (dále též služba QVerify, Služba). Služba QVerify nesmí být provozována v rozporu s výše uvedeným a pro jakékoliv nelegální účely.

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.

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),
- zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- 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.

1.1 Přehled

Dokument **Prováděcí směrnice kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí** vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se ke službě ověřování platnosti kvalifikovaných elektronických podpisů a pečetí s přihlédnutím k platným standardům Evropské unie a k právu České republiky v dané oblasti. Dokument je rozdělen do tří kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 poskytuje základní informace o společnosti První certifikační autorita, a.s., o Službě, tedy o participujících subjektech, architektuře a dokumentaci a uvádí seznam zkratk a pojmů.
- Kapitola 2 popisuje prostředí, ve kterém je Služba provozována, tedy mj. otázky finančního zabezpečení a pojištění, způsob řešení sporů, omezení odpovědnosti poskytovatele, záležitosti personální, fyzické a síťové bezpečnosti, řešení incidentů, zaznamenávání událostí, havarijního plánování a hodnocení shody s právními předpisy.
- Kapitola 3 popisuje koncept služby, mj. blíže popisuje klientskou a serverovou část, proces a protokol ověřování podpisů, komunikaci v rámci Služby a zprávu o ověření podpisu.

1.1.1 Identifikace poskytovatele služeb vytvářejících důvěru

Služba QVerify je poskytována společností První certifikační autorita, a.s., která je kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle nařízení eIDAS. Jako takový poskytovatel je uvedena v důvěryhodném seznamu České republiky vedeném Ministerstvem vnitra České republiky – viz https://tsl.gov.cz/publ/TSL_CZ.pdf.

Základní adresy (dále též informační adresy), na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s., případně odkazy pro zjištění dalších informací, jsou:

- adresa sídla společnosti:
První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Praha 9
Česká republika
- internetová adresa <http://www.ica.cz>,
- ID datové schránky I.CA je a69fvfb.

Elektronická adresa, která slouží pro kontakt veřejnosti s I.CA, je info@ica.cz.

1.1.2 Podporované politiky služby ověřování podpisů

Služba QVerify ověřující kvalifikované elektronické podpisy a kvalifikované elektronické pečete vyhovuje politice ověřování podpisů s OID:

0.4.0.19441.1.2

definované dle kapitoly 4.2.2 standardu ETSI TS 119 441.

1.2 Komponenty služby ověřování podpisů

1.2.1 Participující subjekty

1.2.1.1 Klient služby

Klientem Služby (dále jen Klient) může být fyzická osoba, právnická osoba nebo organizační složka státu, která uzavřela se společností První certifikační autorita, a.s., smlouvu o poskytování Služby (dále též Smlouva).

1.2.1.2 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, případně orgány dohledu a další, kterým to podle relevantní právní úpravy přísluší.

1.2.1.3 Komunikace mezi zúčastněnými subjekty

Pro individuální oznámení a komunikaci se zúčastněnými subjekty může I.CA využít jimi dodané e-mailové adresy, poštovní adresy, telefonní čísla, osobní jednání atd.

Komunikovat s I.CA lze taktéž způsoby uvedenými na internetové informační adrese.

1.2.2 Architektura systému

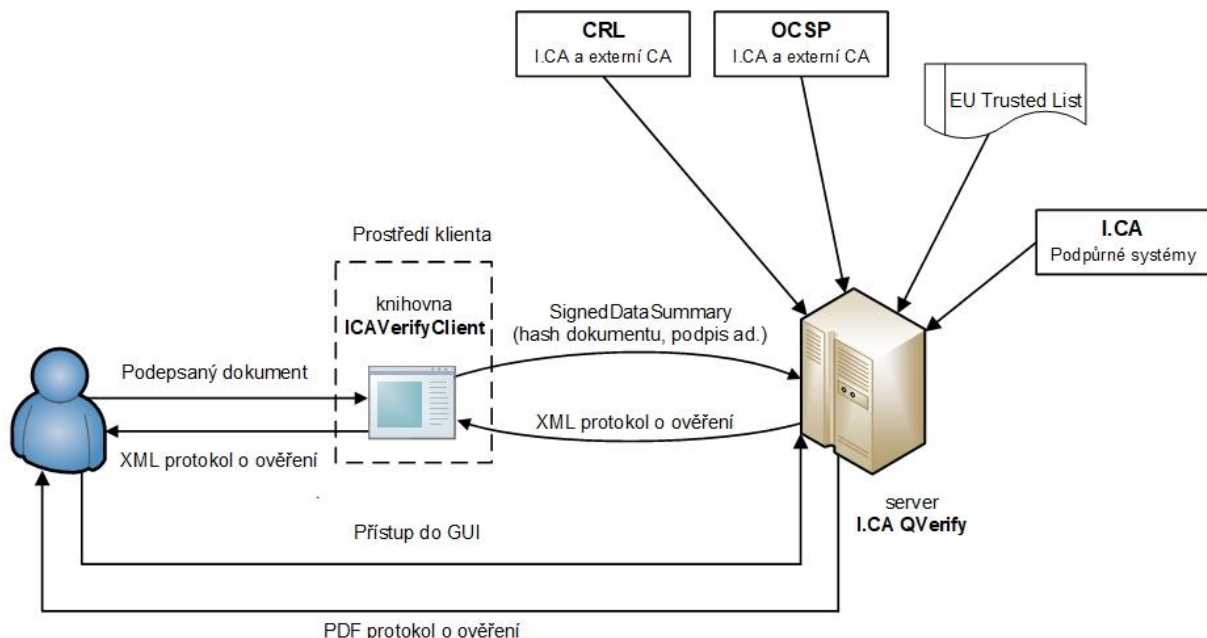
Architektura Služby je v základě tvořena klientskou komponentou a serverovou částí – bližší popis obou je uveden v kapitole 3.

Ověřovaná data nejsou v systému ukládána. Pro důvěrnost dat dále platí:

- Při přenosu dat je používán SSL protokol.
- Při zpracování požadavku na ověření na serveru se s ověřovanými daty pracuje pouze v paměti a nejsou v žádném kroku fyzicky uložena do souboru (ani dočasně) nebo databáze. Po procesu ověření jsou data z paměti vymazána.

Celý proces ověření je logován.

Graficky je architektura Služby znázorněna na obr.1 dále.



obr. 1 - Architektura služby QVerify

1.2.2.1 Životní cyklus služby QVerify

1.2.2.1.1 Žádost o uzavření smlouvy

O uzavření Smlouvy může požádat fyzická osoba, právnická osoba nebo organizační složka státu, obecně jakýkoli subjekt (Klient).

1.2.2.1.2 Proces uzavření smlouvy a odpovědnosti

Klient hodlající využívat Službu je povinen zejména:

- seznámit se s touto Směrnicí, resp. s Politikou příslušnou této Směrnicí a smluvně se zavázat jednat podle ní,

- poskytovat pravdivé a úplné informace pro uzavření Smlouvy,
- překontrolovat, zda údaje uvedené ve Smlouvě jsou správné a odpovídají požadovaným údajům.

I.CA je povinna zejména:

- před uzavřením Smlouvy informovat Klienta o smluvních podmínkách,
- uzavírat s Klientem Smlouvu obsahující náležitosti požadované relevantní právní úpravou a technickými standardy,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 1.4.3,
- činnosti spojené se Službou poskytovat v souladu s relevantními právními předpisy, touto Směrnicí a jí příslušnou Politikou, Systémovou bezpečnostní politikou – důvěryhodné systémy a provozní dokumentací.

1.2.2.1.3 Definování technických parametrů implementace služby QVerify

Technické parametry konkrétní implementace Služby jsou uvedeny ve Smlouvě.

1.2.2.1.4 Testovací prostředí

Pokud byly vzájemně dohodnuty technické parametry implementace Služby, je přistoupeno, v případě požadavku Klienta, k instalaci služby TQVerify, tj. testovací verze Služby do testovacího prostředí Klienta.

Účelem testování je potvrzení předpokládaných výsledků ověřování platnosti elektronických podpisů a pečetí, výkonových parametrů, propustnosti atd.

1.2.2.1.5 Produkční prostředí

Pokud bylo dosaženo předpokládaných a požadovaných výsledků služby TQVerify, je přistoupeno, po akceptaci protokolu o testování, k instalaci služby QVerify do produkčního prostředí Klienta.

1.2.2.1.6 Provoz služby QVerify

Po úspěšné instalaci Služby do produkčního prostředí Klienta je na základě podpisu předávacího protokolu zahájen rutinní provoz.

Povinností obou smluvních stran je zejména:

- dodržovat veškerá relevantní ustanovení Smlouvy,
- užívat autentizační certifikát výhradně k autentizaci k předmětné službě,
- užívat Službu podle této Směrnice, resp. Politiky příslušné této Směrnicí pouze pro účely stanovené zde a v relevantní právní úpravě,
- neprodleně uvědomit poskytovatele služeb vytvářejících důvěru o skutečnostech, které mohou ohrozit řádné využívání Služby.

1.2.2.1.7 Změny při provozování a využívání služby QVerify

Jakékoli změny v provozování a využívání Služby musí nastat změnou smluvních podmínek, a to vztupně číslovanými dodatky Smlouvy podepsanými Klientem.

Technické parametry klientské komponenty, tj. přepis do jiného programovacího jazyka, jiné parametry atd., mohou být upraveny po definování smluvních podmínek Smlouvou (např. ceny a doby úprav).

1.2.2.1.8 Ukončení poskytování služby QVerify

Viz kapitola 2.12.

1.2.2.1.9 Úschova dat pro ověřování platnosti elektronických podpisů a pečetí

Doba, po kterou jsou uchovávány soubory potřebné pro ověření platnosti kvalifikovaných elektronických podpisů a pečetí, činí minimálně 10 let.

1.3 Pojmy a zkratky

1.3.1 Pojmy

| Pojem | Vysvětlení |
|---------------------------------------|---|
| autentizační certifikát | v tomto dokumentu komerční certifikát použitý pro autentizaci ke službě QVerify |
| certifikát | v tomto dokumentu kvalifikovaný certifikát pro elektronické podpisy nebo pečetě |
| elektronický podpis | zaručený elektronický podpis, resp. uznávaný elektronický podpis, resp. kvalifikovaný elektronický podpis dle právní úpravy |
| kvalifikovaná elektronická pečeť | zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť dle právní úpravy |
| orgán dohledu | orgán dohledu nad kvalifikovanými poskytovateli služeb vytvářejících důvěru |
| právní úprava | platné právní předpisy ČR a nařízení eIDAS |
| Smlouva | text smlouvy v elektronické nebo listinné podobě |
| spoléhající se strana | subjekt spoléhající se při své činnosti na výsledek ověření platnosti elektronického podpisu a kvalifikované elektronické pečeti |
| zákon o ochraně utajovaných informací | zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů |
| zákoník práce | zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů |

1.3.2 Zkratky

| Pojem | Vysvětlení |
|-------|--|
| 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 |
| 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 |
| 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) |
| I.CA | První certifikační autorita, a.s. |
| 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 |
| PCO | pult centrální ochrany |
| PDCA | Plan-Do-Check-Act, Plánování – Zavedení – Kontrola – Využití, Demingův cyklus, metoda neustálého zlepšování |
| TS | Technical Specification, typ ETSI standardu |

| | |
|------|---|
| UPS | Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení |
| ZOOÚ | právní úprava týkající se ochrany osobních údajů |

1.4 Zásady a postupy

1.4.1 Organizace spravující dokumentaci

Veškerou dokumentaci vztahující se ke Službě spravuje společnost První certifikační autorita, a.s.

1.4.1.1 Doba platnosti a ukončení platnosti

Tato Směrnice nabývá platnosti a účinnosti dle kapitoly 4 1 a platí minimálně po dobu poskytování Služby, nebo do nahrazení této Směrnice její novou verzí. Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této Směrnice, je generální ředitel společnosti První certifikační autorita, a.s.

1.4.1.2 Postup při oznamování změn

Vydání nové verze Směrnice je vždy oznámeno formou zveřejňování informací.

1.4.1.3 Okolnosti, při kterých musí být změněn OID

OID není přidělen, v případě jakýchkoliv změn je zvýšena verze dokumentu.

1.4.1.4 Práva duševního vlastnictví

Tato Směrnice, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systému poskytujícího Službu jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

1.4.2 Kontaktní osoba

Kontaktní osoba společnosti První certifikační autorita, a.s. je uvedena na internetové adrese společnosti.

1.4.3 Dokumentace související se službou

Tato prováděcí směrnice služby QVerify ověřující kvalifikované elektronické podpisy a kvalifikované elektronické pečete doplňuje a rozpracovává zásady uvedené v dokumentu Politika kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí (OID 1.3.6.1.4.1.23624.12.1.200.1.0), přičemž platí:

- Název a identifikace dokumentu: Prováděcí směrnice kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí, verze 1.14
- OID dokumentu: není přidělen

Podmínky pro zřízení a využívání Služby a veškerá veřejná dokumentace se Službou spojená jsou vystaveny na webu společnosti (www.ica.cz) a jsou nedílnou součástí smlouvy s Klientem.

Pro pravidelně aktualizovanou analýzu rizik Služby je používán nástroj RAMSES. Výsledky jsou dokumentovány v interní dokumentaci, mj.:

- „Politika bezpečnosti informací – důvěryhodné systémy“,
- „Rozsah ISMS – důvěryhodné systémy“,
- „Analýz rizik – důvěryhodné systémy – Závěrečná zpráva“,
- „Výběr protopatření – důvěryhodné systémy“.

1.4.4 Úložiště informací

Společnost První certifikační autorita, a.s., zřizuje a provozuje úložiště informací a dokumentace.

1.4.4.1 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- Směrnice, resp. Politika – po schválení a vydání nové verze,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb vytvářejících důvěru.

1.4.4.2 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům I.CA, nebo subjektům definovaným právní úpravou. Přístup k těmto informacím je řízen pravidly popsány v interní dokumentaci, zejména:

- „Příručka administrátora“,
- „Dílčí spisový a skartační plán pro agendy certifikačních služeb“.

2 ŘÍZENÍ A PROVOZ SLUŽBY

Tato kapitola je zaměřena na:

- systém poskytované Služby,
- veškeré procesy podporující poskytování této Služby.

Oblasti řízení jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, Systémová bezpečnostní politika – důvěryhodné systémy, Plán pro zvládnutí krizových situací a plán obnovy, tak v upřesňujících interních dokumentech. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

2.1 Postupy organizace

Služba QVerify je poskytována na základě uzavřeného smluvního vztahu. I.CA nijak neomezuje potenciální Klienty, poskytování Služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

Poplatky za využívání Služby jsou upraveny ve Smlouvě.

2.1.1 Spolehlivost externí organizace

I.CA může nebo musí některé činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se např. o zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými politikami, relevantními částmi interní dokumentace I.CA, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou uplatňovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva. Za činnost dodavatelů I.CA plně odpovídá.

2.1.2 Oddělení povinností

Pro vybrané činnosti jsou v I.CA definovány důvěryhodné role, které jsou spolu s odpovídajícími činnostmi a odpovědnostmi popsány v interní dokumentaci, zejména v dokumentech:

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

Činnosti související se Službou nevyžadují, aby byly vykonávány za účasti více než jedné osoby. Podrobné informace jsou uvedeny v interní dokumentaci:

- „Příručka administrátora“.

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci (jméno, certifikát) a autentizaci (heslo, soukromý klíč) k těm komponentám, které jsou pro jejich činnost nezbytné. Problematika je upravena v interní dokumentaci, zejména:

- „Příručka administrátora“.

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou popsány v interní dokumentaci:

- „Příručka administrátora“.

2.1.3 Finanční odpovědnost

2.1.3.1 Krytí pojištěním

Společnost První certifikační autorita, a.s., prohlašuje, že má platně uzavřené pojištění podnikatelských rizik takovým způsobem, aby byly pokryty případné finanční škody.

Společnost První certifikační autorita, a.s., sjednala pro všechny zaměstnance pojištění odpovědnosti za škody způsobené zaměstnavateli v rozsahu určeném představenstvem společnosti.

2.1.3.2 Další aktiva a záruky

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiná finanční zajištění na poskytování služeb vytvářejících důvěru s ohledem na riziko vzniku odpovědnosti za škodu.

Podrobné informace o aktivech společnosti První certifikační autorita, a.s., je možno získat z Výroční zprávy společnosti První certifikační autorita, a.s. zveřejněné v obchodním rejstříku.

2.1.4 Řešení sporů

V případě, že uživatel Služby nesouhlasí s návrhem na vyřešení sporu, může použít následující stupně odvolání:

- odpovědný pracovník I.CA (nutné elektronické nebo listinné podání),
- generální ředitel I.CA (nutné elektronické nebo listinné podání).

Uvedený postup dává nesouhlasící straně možnost prosazovat svůj názor rychlejším způsobem než soudní cestou.

2.1.5 Záruky a odpovědnosti

2.1.5.1 Záruky a odpovědnosti I.CA:

I.CA zaručuje, že poskytuje:

- technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem Smlouvy prostřednictvím kontaktních údajů uvedených na www.ica.cz,
- Službu vždy právně a technicky aktuální, tj. v souladu s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud subjekt využívající Službu neporušil povinnosti plynoucí mu ze Smlouvy a této Směrnice, resp. Politiky příslušné této Směrnici.

2.1.5.2 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované touto Směrnicí, resp. Politikou příslušnou této Směrnicí, podle které byla Služba poskytována. Dále neodpovídá za škody vzniklé v důsledku porušení povinností I.CA z důvodu vyšší moci.

2.1.5.3 Odpovědnost za škodu, náhrada škody

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení právních předpisů a dále takové záruky, které byly sjednány Smlouvou. Tato Smlouva nesmí být v rozporu s právní úpravou a musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak relevantními právními předpisy, tak příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti Smlouvy.

Společnost První certifikační autorita, a.s., **neodpovídá:**

- za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání Služby, zejména za využívání v rozporu s podmínkami uvedenými v této Směrnicí, resp. v Politice příslušné této Směrnicí, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení.

Reklamací je možné podat těmito způsoby:

- e-mailem na adresu reklamace@ica.cz,
- prostřednictvím datové schránky I.CA,
- doporučenou poštovní zásilkou na adresu sídla společnosti,
- osobně v sídle společnosti.

Reklamující osoba (pověřená osoba ve Smlouvě) je povinna uvést:

- co nejdůležitější popis závady,
- bližší popis reklamované služby,
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne I.CA nejpozději do tří pracovních dnů od doručení reklamace a vyrozumí o tom reklamujícího (formou elektronické pošty, prostřednictvím datové schránky, jedná-li se o orgán státní správy, nebo poštovní doporučenou zásilkou), pokud se strany nedohodnou jinak.

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do třiceti dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

Další možné náhrady škody vycházejí z ustanovení relevantních právních předpisů a o jejich výši může rozhodnout soud.

2.2 Lidské zdroje

2.2.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Zaměstnanci I.CA v důvěryhodných rolích jsou vybíráni a přijímáni na základě těchto kritérií:

- naprostá občanská bezúhonnost – prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z rejstříku trestů, nebo čestné prohlášení),
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně tři roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně pět let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně jeden rok v oblasti poskytování certifikačních/důvěryhodných služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Ostatní zaměstnanci I.CA podílející se na zajištění certifikačních služeb včetně služby QVerify jsou přijímáni na základě následujících kritérií:

- vysokoškolské vzdělání v rámci akreditovaného bakalářského, resp. magisterského studijního programu, nebo středoškolské vzdělání,
- základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.
- Popis konkrétní činnosti zaměstnance je definován pracovní smlouvou.

Pro vykonávání řídicí funkce musí mít vedoucí zaměstnanci zkušenosti získané praxí nebo odbornými školeními s ohledem na důvěryhodnost Služby, znalost bezpečnostních postupů s odpovědností za bezpečnost a zkušenosti s bezpečností informací a hodnocením rizik.

Dokud nejsou dokončeny veškeré vstupní kontroly zaměstnance, není mu umožněn logický ani fyzický přístup k důvěryhodným systémům.

2.2.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích I.CA jsou:

- sami tito zaměstnanci,
- osoby, které tyto zaměstnance znají,
- veřejné zdroje informací.

Zaměstnanci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, ty jsou aktualizovány při periodických pohovorech s nadřízeným pracovníkem v průběhu pracovního poměru.

2.2.3 Příprava pro výkon role, školení, dokumentace

Zaměstnanci I.CA jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samostudia a metodickým vedením již zaškoleným pracovníkem. Běžná doba na zaškolení je jeden měsíc. Školení zahrnuje oblasti informační bezpečnosti, ochrany osobních údajů a další relevantní témata.

Dvakrát za dvanáct měsíců jsou zaměstnancům poskytovány aktuální informace o vývoji v předmětných oblastech.

Zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, který by mohly ohrozit nestrannost operací I.CA.

Postup jmenování zaměstnanců do důvěryhodných rolí a specifikace těchto rolí jsou uvedeny v interní dokumentaci:

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

Zaměstnanci I.CA mají k dispozici, kromě Politiky a Směrnice, bezpečnostní a provozní dokumentace, veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

2.2.4 Administrativní a řídicí postupy zaměstnanců a vedoucích zaměstnanců

Zaměstnanci jsou povinni vykonávat administrativní a řídicí postupy a procesy, které jsou v souladu s postupy I.CA v oblasti řízení informační bezpečnosti.

Pro vykonávání řídicí funkce musí mít vedoucí zaměstnanci zkušenosti získané praxí nebo odbornými školeními s ohledem na důvěryhodnost Služby, znalost bezpečnostních postupů s odpovědností za bezpečnost a zkušenosti s bezpečností informací a hodnocením rizik.

2.2.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti v mimořádných případech jsou zaměstnanci I.CA motivováni k získávání znalostí potřebných pro zastávání jiné role v I.CA.

2.2.6 Postihy za neoprávněné činnosti zaměstnanců

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem popsaným v interních dokumentech společnosti a řídicím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

Problematika je detailně popsána v interní dokumentaci:

- „Pracovní řád“.

2.3 Správa aktiv

2.3.1 Obecné požadavky

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

2.3.2 Správa médií

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

je umístěno provozní pracoviště, na místě určeném výkonným ředitelem I.CA a popsaném v interní dokumentaci:

- „Příprava uchovávaných informací“,
- „Záloha dat provozních systémů“.

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

2.4 Řízení přístupu

Řízení přístupu k důvěryhodným systémům, na kterých je služba QVerify provozována, je založeno na existenci důvěryhodných rolí v souladu se standardem CEN/TS 419261:2015 Security requirements for trustworthy systems managing certificates and time-stamps.

V následujících podkapitolách je popsán způsob řízení přístupu v rámci QVerify.

2.4.1 Počáteční ověření identity

Službu QVerify mohou využívat subjekty, které mají s I.CA uzavřenou platnou smlouvu o využívání této služby (dále též Smlouva).

Pověřené osoby subjektu oprávněného k využívání služby QVerify jsou uvedeny ve Smlouvě. Tím jsou tyto osoby oprávněny podat žádosti o autentizační certifikát ke službě QVerify.

2.4.2 Autentizace ke službě QVerify

Autentizace ke službě QVerify je možná pouze prostřednictvím autentizačního certifikátu. Je realizována v rámci klientské komponenty instalované v prostředí Klienta.

2.5 Kryptografická opatření

Kryptografické klíče související se službou QVerify jsou uloženy v kryptografickém modulu hodnoceném podle ISO/IEC 15408 EAL4+.

2.6 Fyzická bezpečnost a bezpečnost prostředí

Problematika fyzické bezpečnosti je detailně popsána v interní dokumentaci, zejména:

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

2.6.1 Umístění a konstrukce

Objekty provozního pracoviště jsou umístěny v geograficky odlišných lokalitách, které jsou dále jiné než ředitelství společnosti, obchodní a vývojová pracoviště, pracoviště registračních autorit a obchodních míst.

Zařízení určená k výkonu služby QVerify jsou umístěna ve vyhrazených prostorách provozních pracovišť. Tyto prostory jsou zabezpečené obdobně, jako zabezpečené oblasti kategorie „Důvěrné“ podle zákona o ochraně utajovaných informací.

2.6.2 Fyzický přístup

Požadavky na fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozních pracovišť jsou uvedeny v interní dokumentaci společnosti. Ochrana objektů je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a případně speciálním systémem pro sledování pohybu osob a dopravních prostředků.

2.6.3 Elektřina a klimatizace

V prostorách určených k výkonu služby QVerify je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí $20\text{ °C} \pm 5\text{ °C}$. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

2.6.4 Vlivy vody

Všechny kritické systémy provozních pracovišť jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště jsou podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

2.6.5 Protipožární opatření a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení, určená k výkonu služby QVerify, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

2.7 Bezpečnost provozu

Úroveň bezpečnosti komponent použitých v rámci služby, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů, a jejich periodicity je definována právní úpravou pro služby vytvářející důvěru, resp. v ní odkazovaných technických standardech a normách. Detailně je řešení popsáno v interní dokumentaci, zejména:

- „Plán pro zvládání krizových situací a plán obnovy“,
- „Obnova komponenty provozního pracoviště“,
- „Přemístění provozního pracoviště“,
- „Záloha dat provozních systémů“,

- „Příprava uchovávaných informací“,
- „Příručka administrátora“,
- „Řízení fyzického přístupu do místností I.CA“.

2.7.1 Relevantní standardy

Vývoj a provoz systému QVerify se řídí požadavky uvedenými v mezinárodních a národních standardech, zejména:

- CEN/TS 419261:2015 Security requirements for trustworthy systems managing certificates and time-stamps.
- ETSI TS 119 441 V 1.1.1 (2018-08) Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.
- ČSN ETSI EN 319 403-1 V.2.3.1 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatele důvěryhodné služby - Část 1: Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodné služby.
- ETSI EN 319 403-1 V.2.3.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI TS 119 312 V1.3.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ETSI TS 119 101 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation.
- ČSN ETSI EN 319 401 V2.2.1 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.
- ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 102-1 V1.1.1 Elektronické podpisy a infrastruktury (ESI) – Postupy pro vytváření a ověřování platnosti digitálních podpisů AdES – Část 1: Vytváření a ověřování platnosti
- ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.
- ETSI TS 103 171 V.2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.
- ETSI TS 103 172 V.2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.
- ETSI TS 103 173 V.2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile.
- ČSN ETSI EN 319 122-1 V1.1.1 Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy CAdES – Část 1: Stavební bloky a základní podpisy CAdES.
- ETSI EN 319 122-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

- ČSN ETSI EN 319 132-1 V1.1.1 Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy XAdES – Část 1: Stavební bloky a základní podpisy XAdES
- ETSI EN 319 132-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.
- ČSN ETSI EN 319 142-1 V1.1.1 Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy PAdES – Část 1: Stavební bloky a základní podpisy PAdES.
- ETSI EN 319 142-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.
- ETSI TS 103 174 V2.2.1 (2013-06) Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile.
- ČSN ETSI EN 319 162 V1.1.1 Elektronické podpisy a infrastruktury (ESI) – Přidružené zásobníky podpisu (ASiC) – Část 1: Stavební bloky a základní zásobníky ASiC.
- ETSI EN 319 162 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers.
- ČSN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
- ČSN EN 301 549 V3.1.1 Požadavky přístupnosti na výrobky a služby ICT.
- EN 301 549 Accessibility requirements for ICT products and services.
- ČSN ISO/IEC 17021-1 Posuzování shody – Požadavky na orgány poskytující služby auditů a certifikace systémů managementu – Část 1: Požadavky.
- ISO/IEC 17021-1:2015 Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements.
- ČSN ISO/IEC 17065 Posuzování shody – Požadavky na orgány certifikující produkty, procesy a služby.
- ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services.

2.7.2 Řízení vývoje a provozu

Při vývoji a provozování systému QVerify je postupováno v souladu s interní dokumentací:

- „Změnové řízení“,
- „Metodika vývoje“,
- „Příručka administrátora“.

2.7.3 Řízení změn

Postup je realizován řízeným procesem popsaným v interní dokumentaci:

- „Změnové řízení“.

2.7.4 Řízení bezpečnosti

Řízení bezpečnosti informací, včetně kontroly souladu s technickými standardy a normami, je prováděno v rámci periodických kontrol služeb vytvářejících důvěru a dále formou auditů systému řízení bezpečnosti informací (ISMS).

Bezpečnost informací se v I.CA řídí těmito normami:

- ČSN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.
- ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.
- ČSN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací.

Řízení životního cyklu bezpečnosti je v I.CA je prováděno procesním přístupem typu „Plánování–Zavedení–Kontrola–Využití“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování – stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou,
- implementace a provoz – účelné a systematické prosazení vybraných bezpečnostních opatření,
- monitorování a přehodnocování – zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení společnosti k posouzení,
- údržba a zlepšování – provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení organizace.

2.7.5 Ochrana proti padělání a odcizení

Opatření proti padělání a odcizení dat jsou součástí celého systému řízení bezpečnosti informací nejen Služby, ale všech důvěryhodných systémů I.CA. Spolupodílí se řízení počínaje managementem společnosti, přes vedoucí zaměstnance až po zaměstnance v důvěryhodných rolích s příslušnými oprávněními.

2.7.6 Hodnocení zranitelnosti

Zranitelnost je, jako součást penetračního testování, skenována každé čtvrtletí – viz kapitola 2.8. Sledování zranitelnosti zařízení a programového vybavení souvisejících se Službou je popsáno v interní dokumentaci:

- „Příručka administrátora“.

2.7.7 Vyšší moc

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývajících ze smluvních vztahů s klientem vzniklých na základě zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či

občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu, popř. výpadku komunikačního spojení.

2.7.8 Další opatření

Provozní prostředí operačních a databázových systémů je udržováno v souladu s doporučeními výrobců, jsou aplikovány relevantní záplaty a případné neaplikování je zaznamenáno a zdůvodněno. Podrobnosti jsou popsány v interní dokumentaci:

- „Příručka administrátora“.

Při vývoji systému jsou využívány prověřené protokoly a knihovny, tato skutečnost je prověřována každoročními audity.

2.8 Síťová bezpečnost

V prostředí I.CA nejsou prostředky poskytující službu QVerify přímo dostupné z veřejné sítě Internet. Informační systém je mimo jiné chráněn komerčním produktem typu firewall. Veškerá komunikace mezi klientskou částí QVerify a provozním pracovištěm je vedena šifrovaně. Důvěryhodný systém podporující poskytování služby QVerify neukládá a nezpracovává důvěrné informace (s výjimkou kryptografických klíčů uložených v kryptografickém modulu – viz kapitola 2.5.

Penetrační testování je jednou ročně prováděno specializovanou externí firmou, v ostatních případech je využíváno k tomu účelu zakoupeného programového vybavení.

Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

- „Příručka administrátora“,
- „Firewall – provozní pracoviště“.

2.9 Ošetření incidentů

V případě incidentu postupuje I.CA v souladu s interním plánem pro zvládání krizových situací a plánem obnovy a případně s další relevantní interní dokumentací:

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

2.10 Shromažďování důkazů

I.CA jako kvalifikovaný poskytovatel služeb vytvářejících důvěru jednak vytváří, uchovává a zpracovává auditní záznamy a dále uchovává relevantní informace, obojí v souladu s požadavky relevantní právní úpravy a navazujících technických standardů.

2.10.1 Auditní záznamy (logy)

Problematika spojená s vytvářením, zpracováním a uchováváním auditních logů je detailně řešena v interní dokumentaci, zejména:

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

2.10.1.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované právní úpravou.

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje integritu těchto dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

Všechny záznamy v auditním souboru obsahují následující parametry:

- datum (rok, měsíc, den) a čas (hodina, minuta, sekunda) události,
- typ události,
- identitu entity, která je za akci odpovědná,
- úspěšnost /neúspěšnost auditované události.

2.10.1.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní dokumentaci:

- „Příručka administrátora“,

v případě bezpečnostního incidentu okamžitě.

2.10.1.3 Doba uchování auditních záznamů

Nestanoví-li relevantní právní předpisy jinak, jsou auditní záznamy uchovávány po dobu nejméně deseti let od jejich vzniku.

2.10.1.4 Ochrana auditních záznamů

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem zajišťujícím ochranu před jejich změnami, odcizením a zničením (ať již úmyslným nebo neúmyslným).

Elektronické auditní záznamy jsou ukládány ve dvou kopiích, každá kopie je umístěna v jiné místnosti provozního pracoviště. Minimálně jedenkrát měsíčně se provádí uložení těchto auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

Auditní záznamy v papírové formě jsou umístěny mimo provozní prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci.

2.10.1.5 Postupy pro zálohování auditních záznamů

Zálohování elektronických auditních záznamů probíhá obdobným způsobem, jako zálohování ostatních elektronických informací. Zálohování auditních záznamů v papírové formě prováděno není.

2.10.2 Uchovávání informací a dokumentace

Informace a dokumentace jsou ukládány na místo určené výkonným ředitelem I.CA.

Shromažďování uchovávaných informací je evidováno.

Uchovávané informace a dokumentace jsou přístupné:

- zaměstnancům I.CA, pokud je to k jejich činnosti vyžadováno
- oprávněným dohledovým a kontrolním subjektům a orgánům činným v trestním řízení, pokud je to právními předpisy vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

Uchovávání informací a dokumentace je popsáno v interní dokumentaci, zejména:

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

Shromažďování uchovávaných informací je evidováno.

Uchovávané informace a dokumentace jsou umístěny v lokalitách k tomu určených a jsou přístupné:

- zaměstnancům I.CA, pokud je to k jejich činnosti vyžadováno
- oprávněným dohledovým a kontrolním subjektům a orgánům činným v trestním řízení, pokud je to právními předpisy vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

2.10.2.1 Typy informací a dokumentace, které se uchovávají

I.CA uchovává níže uvedené informace a dokumentaci (v elektronické nebo listinné podobě), které souvisejí s poskytovanou službou QVerify, zejména:

- dokumenty a záznamy související se Službou,
- záznamy o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentaci.

2.10.2.2 Doba uchování uchovávaných informací a dokumentace

Informace vztahující se ke Službě jsou uchovávány po celou dobu existence I.CA.

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací – viz kapitola 2.10.2.

2.10.2.3 Ochrana úložiště uchovávaných informací a dokumentace

Prostory, ve kterých se uchovávají informace a dokumentace nacházejí, jsou zabezpečeny způsobem vycházejícím z požadavků provedené analýzy rizik a ze zákona o ochraně utajovaných informací.

Postupy při ochraně úložiště uchovávaných informací a dokumentace jsou upraveny interní dokumentací – viz kapitola 2.10.2.

2.10.2.3.1 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací – viz kapitola 2.10.2.

2.10.2.4 Požadavky na používání časových razítek při uchovávání záznamů

V případě, že jsou využívána časová razítka, jedná se o kvalifikovaná elektronická časová razítka vydávaná I.CA.

2.11 Havarijní plánování

V případě výskytu incidentu, kompromitace dat, poškození výpočetních prostředků, programového vybavení nebo dat postupuje I.CA v souladu s interním plánem pro zvládání krizových situací a plánem obnovy a případně s další relevantní interní dokumentací:

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

2.12 Ukončení činnosti a plány ukončení činnosti

V případě, že dojde k ukončení poskytování Služby, bez ohledu na to, zda k tomu došlo na popud I.CA či Klienta, budou data získaná klientskou komponentou uchováována po dobu minimálně 10 let, a to v elektronické podobě. V případě požadavku mohou být Klientovi zpřístupněna. Jde o zpoplatněnou službu nad rámec smluvního vztahu.

Pro ukončování činnosti kvalifikovaného poskytovatele služby vytvářející důvěru platí následující pravidla:

- ukončení činnosti kvalifikovaného poskytovatele služby vytvářející důvěru musí být písemně oznámeno orgánu dohledu a všem subjektům, které mají uzavřenou Smlouvu,
- ukončení činnosti poskytovatele služby vytvářející důvěru musí být zveřejněno na internetové adrese podle kapitoly 1.1.1,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchování a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity služeb,

V případě bankrotu je pokračováno v souladu s relevantní právní úpravou.

V případě odnětí statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru dle relevantní právní úpravy:

- informace o odnětí statutu musí být písemně nebo elektronicky oznámena všem subjektům, které mají uzavřenou Smlouvu,
- informace o odnětí statutu musí být zveřejněna v souladu s kapitolou 1.1.1,
- o dalším postupu rozhodne generální ředitel I.CA na základě rozhodnutí orgánu dohledu.

Postup při ukončování činnosti je popsán v interní dokumentaci:

- „Ukončení činnosti služeb I.CA“.

2.13 Shoda

2.13.1 Rozhodné právo a shoda s právními předpisy

Obchodní činnost společnosti První certifikační autorita, a.s., se řídí právním řádem České republiky. Systém poskytování služeb vytvářejících důvěru je provozován ve shodě s právními požadavky EU, České republiky a dále s relevantními mezinárodními standardy.

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté tímto dokumentem, stanoví, že provádění některého povinného požadavku je protiprávní, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a v souladu s platnou právní úpravou.

2.13.2 Hodnocení

2.13.2.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Periodicita hodnocení podle eIDAS, včetně okolností pro provádění hodnocení, je striktně dána požadavky tohoto nařízení, auditní perioda nepřekračuje dva roky.

2.13.2.2 Identita a kvalifikace hodnotitele

Kvalifikace externího auditora provádějícího hodnocení podle eIDAS je dána požadavky tohoto nařízení.

2.13.2.3 Vztah hodnotitele k hodnocenému subjektu

V případě interního hodnotitele platí, že tento není ve vztahu podřízenosti vůči organizační jednotce, která zajišťuje provoz Služby.

V případě externího hodnotitele platí, že se jedná o subjekt, který není s I.CA majetkově ani personálně svázán.

2.13.2.4 Hodnocené oblasti

V případě, že je prováděno hodnocení požadované právní úpravou, jsou hodnocené oblasti konkretizovány touto právní úpravou, v ostatních případech jsou hodnocené oblasti dány standardy, podle kterých je hodnocení prováděno.

2.13.2.5 Postup v případě zjištění nedostatků

Se zjištěními prováděných hodnocení je seznámen bezpečnostní manažer I.CA, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat Službu, přeruší I.CA Službu do doby, než budou tyto nedostatky odstraněny.

2.13.2.6 Sdělování výsledků hodnocení

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

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

Sdělování výsledků hodnocení podléhá požadavkům právní úpravy.

2.13.3 Ochrana osobních údajů

2.13.3.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných právních předpisů, tedy zejména ZOOÚ a GDPR.

2.13.3.2 Informace považované za osobní údaje

Osobními údaji jsou veškeré informace podléhající ochraně ve smyslu příslušných právních předpisů.

Zaměstnanci I.CA, případně subjekty definované relevantní právní úpravou, přicházející do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního, nebo jiného obdobného poměru, nebo po provedení příslušných prací.

2.13.3.3 Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které nespádají do působnosti příslušných právních předpisů.

2.13.3.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný generální ředitel I.CA.

2.13.3.5 Oznamování o používání osobních údajů a souhlas s jejich zpracováním

Problematika oznamování o používání důvěrných informací a souhlasu s používáním citlivých informací je v I.CA řešena v souladu s požadavky příslušných právních předpisů.

2.13.3.6 Poskytování osobních údajů pro soudní či správní účely

Poskytování citlivých informací pro soudní, resp. správní účely je v I.CA řešeno v souladu s požadavky příslušných právních předpisů.

2.13.3.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně podle požadavků příslušných právních předpisů.

2.13.4 Citlivost obchodních informací

2.13.4.1 Výčet citlivých informací

Citlivými a důvěrnými informacemi I.CA jsou veškeré informace, které nejsou označeny jako veřejné, zejména:

- veškeré soukromé klíče, sloužící v procesu poskytování Služby,
- obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

2.13.4.2 Informace mimo rámec citlivých informací

Za veřejné se považují pouze informace označené jako veřejné.

2.13.4.3 Odpovědnost za ochranu citlivých informací

Žádný zaměstnanec I.CA, který přijde do styku s citlivými a důvěrnými informacemi, je nesmí bez souhlasu generálního ředitele I.CA poskytnout třetí straně.

3 SIGNATURE VALIDATION SERVICE DESIGN KONCEPT SLUŽBY OVĚŘOVÁNÍ PODPISŮ

Služba QVerify je poskytována v režimu 24/7 s propustností počtu ověření za minutu definovaným ve smlouvě o využívání Služby.

Integrita vstupních dat při přenosu je řešena na úrovni datové struktury webové služby (vstupem je hash ověřovaných dat a hash z podpisu nebo pečete) a jejich kontrolou na serveru.

Služba QVerify ověřuje elektronické podpisy a pečete ve formátech:

- XAdES dle ETSI TS 103 171 v úrovni shody B, T a LT,
- PAdES dle ETSI TS 103 172 v úrovni shody B, T, LT a LTA,
- CAdES dle ETSI TS 103 173 v úrovni shody B, T a LT,
- CAdES dle ETSI EN 319 122-1 v úrovni shody B-B, B-T, B-LT a B-LTA,
- XAdES dle ETSI EN 319 132-1 v úrovni shody B-B, B-T a B-LT,
- PAdES dle ETSI EN 319 142-1 v úrovni shody B-B, B-T, B-LT a B-LTA,
- ASiC-E CAdES dle ETSI TS 103 174 v úrovni shody B, T a LT,
- ASiC-E XAdES dle ETSI TS 103 174 v úrovni shody B, T a LT,
- ASiC-S with CAdES dle ETSI TS 103 174 v úrovni shody B, T a LT,
- ASiC-S with XAdES dle ETSI TS 103 174 v úrovni shody B, T a LT,
- ASiC-S with CAdES dle ETSI EN 319 162 v úrovni shody B-B, B-T a B-LT,
- ASiC-S with XAdES dle ETSI EN 319 162 v úrovni shody B-B, B-T a B-LT.

Kompletní názvy standardů jsou uvedeny v kapitole 2.7.1.

Funkčnost procesu ověřování kvalifikovaných elektronických podpisů a pečetí je předmětem testování v průběhu vývoje i při jakékoliv změně. O provedeném testu je vždy proveden záznam ve formě protokolu, který je spolu s testovacími scénáři uložen v interním systému společnosti.

Klientská komponenta je realizována v Javě 32b a 64b a .NET v prostředí Windows. Zajišťuje:

1. Autentizaci uživatele ke službě (komerční technologický certifikát I.CA).
2. Výpočet hashe z podepsaných dat, získání podpisové struktury.
3. Zaslání dat k ověření ze strany Klienta na server I.CA.
4. Přijetí výsledku ověření ve formě XML podepsaného protokolu.

Kompletní ověření je prováděno na serveru v interním prostředí I.CA. Pomocí klientské komponenty I.CA umístěné a volané z prostředí Klienta dojde k výpočtu hashe z podepsaných dat a získání podpisové struktury. Tato data jsou zaslána na server I.CA, kde proběhne vlastní ověření. Znamená to, že podepsaný dokument (tj. data v dokumentu, tedy obsah dokumentu), jehož podpis se ověřuje, nikdy neopustí prostředí Klienta.

Komponenta mimo parsování podpisu a zajištění potřebných dat pro ověření zajišťuje komunikaci s interním systémem I.CA; za její aktuálnost (právní i technickou) a integritu odpovídá I.CA. Komponenta neumožňuje komunikaci s jiným poskytovatelem než I.CA,

Serverová část zajišťuje:

1. Provedení vstupních kontrol.
2. Provedení ověření jednotlivých podpisů a pečetí (tj. dvojic podpisová struktura + hash).
3. Sestavení odpovědi s výsledkem ověření.
4. Uložení dat pro kontrolní účely.
5. Předání výsledku ověření v XML struktuře aplikaci Klienta.
6. Zalogování procesu ověření.
7. Záznam o využití služby.
8. Konec zpracování.

Kompletní ověření je prováděno na serveru v interním prostředí I.CA. Nejdříve dojde k provedení vstupních kontrol (správnost a aktuálnost komponenty, autentizace, oprávnění k čerpání služby) a ověření jednotlivých podpisů nebo pečetí (dvojic podpisová struktura a hash) a časových razítek (pokud jsou v dokumentu či podpisu přítomna).

Je sestavena odpověď v xml struktuře a on-line odeslána https protokolem zpět Klientovi. XML data jsou podepsána externím CADES podpisem. XML protokol je identifikován jednoznačným číslem generovaným vzestupně. Číslo protokolu je jednoznačné v rámci celé Služby.

Data nutná pro ověření jsou uložena pro případné kontrolní účely.

3.1 Požadavky procesu ověřování podpisů

Vlastní ověřování kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí je prováděno v souladu s aktuální verzí dokumentu Politika ověřování podpisu I.CA QVerify. OID dokumentu je:

- 1.3.6.1.4.1.23624.20.x.y,

kde x.y je aktuální číslo verze a podverze dokumentu, který reflektuje požadavky relevantních standardů.

OID je ve zprávě o ověření uveden, ověřování podle politiky jiné prováděno není.

3.2 Požadavky protokolu ověřování podpisu

Případná podrobná zpráva o ověření kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti obsahuje ověřovací status konzistentní s odpovědí na tento požadavek.

Odpověď na požadavek o ověření kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečeti podpisu obsahuje mj. OID politiky této služby.

3.3 Rozhraní

3.3.1 Komunikační kanál

Veškerá komunikace mezi klientskou a serverovou částí probíhá šifrovaně a přímo mezi Klientem a poskytovatelem Služby. Každý klient je jednoznačně identifikován prostřednictvím autentizačního certifikátu, který je mu vydán po uzavření Smlouvy.

3.3.2 Vztah mezi poskytovatelem služby a jinými poskytovateli služeb vytvářejících důvěru

Služba QVerify je záležitostí pouze komunikace mezi Klientem a poskytovatele Služby. Z tohoto pohledu není otázka vztahu mezi poskytovatelem Služby a jinými poskytovateli služeb vytvářejících důvěru relevantní.

3.4 Požadavky na zprávu o ověření

Výstupem z procesu ověřování kvalifikovaných elektronických podpisů a kvalifikovaných elektronických pečetí prostřednictvím Služby jsou dva formáty zprávy, a to:

- Zpráva ve formátu, který byl používán před vydáním standardů ETSI TS 119 441 a standardů souvisejících. Zpráva v tomto formátu je vydávána proto, že Klienti jsou na něj zvyklí.
- Zpráva ve formátu plně kompatibilním s aktuálními verzemi technických standardů.

Oba formáty zpráv jsou opatřeny zaručeným elektronickým podpisem.

4 ZÁVĚREČNÁ USTANOVENÍ

Tato prováděcí nabývá platnosti dnem uvedeným v tab. 1 a účinnosti dnem uvedení příslušné Politiky na důvěryhodném seznamu.