První certifikační autorita, a.s.

Prováděcí směrnice

služby vytváření kvalifikovaných elektronických pečetí

na dálku

Verze 1.00

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	19.06.2018	Ředitel společnosti První certifikační autorita, a.s.	První vydání.

1 ÚVOD

Tento dokument stanoví zásady, které První certifikační autorita, a.s., (dále též I.CA) uplatňuje v souladu s platnými právními předpisy a mezinárodně uznávanými technickými normami při zajištění služby vytváření kvalifikovaných elektronických pečetí na dálku (dále též Služba).

Pozn.: Pokud jsou v dalším textu uváděny odkazy na standardy nebo zákony, jedná se vždy buď o uvedený standard nebo zákon, resp. standard či zákon, který ho nahrazuje. Pokud by byla tato politika v rozporu se standardy nebo zákony, které nahradí dosud platné, bude vydána její nová verze.

Zákonné 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),
- legislativou týkající se ochrany osobních údajů, v souladu se směrnicí č. 95/46/ES, resp. 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, po nabytí jeho platnosti 25.5.2018).

Služba společnosti První certifikační autorita, a.s., zajišťující vytváření kvalifikovaných elektronických pečetí na dálku je poskytována právnickým osobám (dále též Klient) na základě uzavřeného smluvního vztahu. I.CA dále nijak neomezuje potenciální Klienty, poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

1.1 Přehled

Dokument **Prováděcí směrnice služby vytváření kvalifikovaných elektronických pečetí na dálku** (dále též Směrnice) vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se ke Službě s přihlédnutím k platným standardům Evropské unie a k právu České republiky v dané oblasti. Dokument je rozdělen do devíti kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument, obecně popisuje subjekty, které participují na poskytování Služby a definuje přípustné využití Služby.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace ke Službě.
- Kapitola 4 definuje procesy životního cyklu Služby, technické parametry, až po ukončení poskytování služby.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání těchto záznamů a reakce po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost včetně počítačové a síťové ochrany.
- Kapitola 7 je zaměřena na problematiku hodnocení poskytované Služby.
- Kapitola 8 zahrnuje problematiku obchodní a právní, včetně ochrany osobních údajů.

- Kapitola 9 obsahuje závěrečná ustanovení.

1.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu:	Prováděcí směrnice služby vytváření kvalifikovaných elektronických pečetí na dálku, verze 1.00
OID politiky:	není přiřazeno

1.3 Participující subjekty

1.3.1 Poskytovatel služeb

Společnost První certifikační autorita, a.s., jako kvalifikovaný poskytovatel služeb vytvářejících důvěru.

1.3.2 Kontaktní místa

Kontaktními místy jsou určené registrační autority I.CA (nikoli všechny registrační autority), kde je na základě smlouvy o poskytování Služby mezi I.CA a Klientem osobě zastupující Klienta (dále též Osoba) vydán jednak prvotní autentizační komerční certifikát na aktivační kartu/token a dále vygenerována párová data a zprostředkováno vydání pečetícího certifikátu Klienta. Dále kontaktní místa:

- Poskytují potřebné informace, přijímají reklamace atd.
- Jsou oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti.

1.3.3 Spoléhající se strany

Spoléhající se stranou je subjekt, který se spoléhá na kvalifikovanou elektronickou pečeť vytvořenou Klientem v rámci Služby.

1.3.4 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, případně orgány dohledu a další, kterým to podle platné legislativy přísluší.

1.4 Použití služby

1.4.1 Přípustné použití služby

Službu provozovanou podle této Směrnice, resp. odpovídající Politiky služby vytváření kvalifikovaných elektronických pečetí na dálku (dále též Politika) lze využívat v procesech vytváření kvalifikované elektronické pečetě v souladu s platnou legislativou.

1.4.2 Omezení použití služby

Služba provozovaná podle této Směrnice nesmí být používána v rozporu s přípustným použitím popsaným v kapitole 1.4.1 a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující politiku nebo prováděcí směrnici

Tuto Směrnice, resp. jí odpovídající Politiku, spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s touto Směrnicí, resp. s odpovídající Politikou, je uvedena na internetové adrese (viz kapitola 2.2).

1.5.3 Osoba rozhodující o souladu prováděcí směrnice s politikou služby

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených ve Směrnici, resp. v odpovídající Politice, je ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování prováděcí směrnice

Pokud je potřebné provést změny v příslušné Směrnici a vytvořit její novou verzi, určuje ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze Směrnice předchází její schválení ředitelem společnosti První certifikační autorita, a.s.

1.6 Přehled použitých pojmů a zkratek

tab. 2 - Pojmy

Pojem	Vysvětlení
elektronická pečeť	v tomto dokumentu kvalifikovaná elektronická pečeť dle platné legislativy
legislativa pro služby vytvářející důvěru	nařízení eIDAS a aktuálně platná relevantní legislativa Evropské unie
orgán dohledu	orgán dohledu nad dodržováním legislativy pro služby vytvářející důvěru v ČR
smlouva	text smlouvy v elektronické nebo listinné podobě
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve

	znění pozdějších předpisů

tab. 3 - 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
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)
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
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování-Zavedení-Kontrola-Využití, Demingův cyklus, metoda neustálého zlepšování
QSealCD	kvalifikované zařízení pro tvorbu elektronických pečetí (v souladu s eIDAS)
TS	Technical Specification, typ ETSI standardu

UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
ZOOÚ	legislativa týkající se ochrany osobních údajů, v souladu se směrnicí č. 95/46/ES, resp. 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, po nabytí jeho platnosti 25.5.2018)

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

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

2.2 Zveřejňování informací a dokumentace

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

- adresa sídla společnosti:

  První certifikační autorita, a.s.

  Podvinný mlýn 2178/6

  190 00 Praha 9

  Česká republika
- internetová adresa http://www.ica.cz.

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

Na výše uvedené internetové adrese lze získat také informace o Službě.

Povolenými protokoly pro přístup k veřejným informacím jsou http a https. I.CA může bez udání důvodu přístup k některým informacím zrušit nebo pozastavit.

2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- politika Služby - po schválení a vydání nové verze,
- prováděcí směrnice Služby - neprodleně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb vytvářejících důvěru.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům I.CA, nebo subjektům definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

3 IDENTIFIKACE A AUTENTIZACE KE SLUŽBĚ

3.1 Počáteční ověření identity

Službu mohou využívat Klienti, kteří mají s I.CA uzavřenou platnou smlouvu o využívání této Služby (dále též Smlouva). Pravidla uvedená v následujících podkapitolách platí i pro vydání kvalifikovaného pečetícího certifikátu, který je ve Službě využíván.

3.1.1 Ověřování identity právnické osoby

Ověřování identity právnické osoby Klienta je prováděno před uzavřením Smlouvy, pokud ověření řádně neproběhne, není možné Smlouvu uzavřít. Pro ověření identity Klienta musí být předložen:

- originál nebo úředně ověřená kopie výpisu z obchodního nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny, resp. jiného dokladu stejné právní váhy, nebo
- vytištěný výtah z veřejně dostupných registrů, který předloží žadatel nebo jej vyhotoví operátor RA.

Tento dokument musí obsahovat úplné obchodní jméno, identifikační číslo (je-li přiřazeno), adresu sídla, jméno/jména osoby/osob oprávněné/oprávněných k zastupování (statutárních zástupců).

3.1.2 Pověřené osoby

Pověřené osoby Klienta oprávněné k využívání Služby (dála Osoby) jsou buď uvedeny ve Smlouvě, nebo jsou vybaveny plnou mocí k zastupování Klienta podepsanou statutárním zástupcem Klienta. Tyto Osoby jsou oprávněny požádat o vydání prvotního autentizačního komerčního certifikátu na aktivační kartě/tokenu a o vydání kvalifikovaného pečetícího certifikátu. Postup ověřování jejich identity je popsán dále.

3.1.3 Ověřování identity fyzické osoby

Primárním osobním dokladem pro občany ČR musí být platný občanský průkaz nebo cestovní pas. Primárním osobním dokladem pro cizince je platný cestovní pas, nebo jím v případě občanů členských států EU může být platný osobní doklad, sloužící k prokazování totožnosti na území příslušného státu.

Z tohoto dokladu jsou ověřovány následující údaje:

- celé občanské jméno,
- datum a místo narození, nebo rodné číslo, je-li v primárním dokladu uvedeno,
- číslo předloženého primárního osobního dokladu,
- adresa trvalého bydliště (je-li v primárním dokladu uvedena).

Sekundární osobní doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s primárním osobním dokladem a musí obsahovat alespoň jeden z následujících údajů:

- datum narození (nebo rodné číslo, je-li uvedeno),

- adresu trvalého bydliště,
- fotografii obličeje.

Údaje v sekundárním osobním dokladu sloužící k jednoznačné identifikaci Osoby musí být shodné s těmito údaji v primárním osobním dokladu.

Pokud Osoba není uvedena jako zástupce Klienta přímo ve Smlouvě musí předložit plnou mocí k zastupování Klienta podepsanou statutárním zástupcem Klienta.

3.2 Ověření identity při prodloužení služby

Prodloužení Služby probíhá automatizovaně.

3.3 Změna údajů

Pokud vzhledem ke změně údajů není možné provést prodloužení Služby, musí dojít k uzavření dodatku ke smlouvě a vydání nového autentizačního i pečetícího certifikátu.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS SLUŽBY

V následujících podkapitolách je popsán životní cyklus služby.

4.1 Uzavření smlouvy a zřízení služby

4.1.1 Proces uzavření smlouvy a odpovědnosti

Klient uzavírající smlouvu o využívání Služby (a kterému potom při návštěvě Osoby na kontaktním místu budou vydány prvotní autentizační komerční certifikát a kvalifikovaný pečetící certifikát je povinen zejména:

- seznámit se s touto Směrnicí, resp. s odpovídající Politikou a smluvně se zavázat jednat podle nich,
- poskytovat pravdivé a úplné informace pro uzavření Smlouvy,
- překontrolovat, zda údaje uvedené ve Smlouvě jsou správné a odpovídají požadovaným.

I.CA je povinna zejména:

- před uzavřením Smlouvy informovat Klienta o smluvních podmínkách,
- uzavírat s Klientem Smlouvu obsahující náležitosti požadované platnou legislativou a technickými standardy,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- činnosti spojené se Službou poskytovat v souladu s platnou legislativou, touto Směrnicí, resp. s Odpovídající Politikou a provozní dokumentací.

4.1.2 Povinnosti Klienta

Povinností Klientů (držitelů certifikátů) je zejména:

- dodržovat veškerá relevantní ustanovení Smlouvy,
- používat službu v souladu s ustanoveními kapitoly 1.4,
- nakládat s údaji pro identifikaci a autentizaci ke Službě (prvotní autentizační komerční certifikát, resp. jemu odpovídající soukromý klíč na aktivační kartě/tokenu, případně následný autentizační certifikát, resp. jemu odpovídající soukromý klíč uložený šifrovaně v konfiguračním souboru) tak, aby nemohlo dojít k jejímu zneužití,
- neprodleně uvědomit poskytovatele Služby o změnách údajů uvedených ve Smlouvě (a v certifikátu),
- neprodleně uvědomit poskytovatele Služby o podezření, že údaje pro identifikaci a autentizaci ke Službě byly zneužity.

4.1.3 Povinnosti Osoby

Povinností Osoby je v případě požadavku na ukončení Služby informovat o této skutečnosti I.CA a po vzájemné dohodě sjednanou formou smlouvu ukončit.

4.1.4 Zřízení služby

Zřízení služby probíhá na kontaktních místech, kterými jsou vybrané registrační autority I.CA. Osoba zastupující klienta ji navštíví, je provedeno ověření její identity - viz kapitola 3.1.3 - a potom vydán prvotní autentizační komerční certifikát na aktivační kartě/tokenu (je zde uložen včetně soukromého klíče) a pečetící kvalifikovaný certifikát, který je uložen na tutéž kartu/token. Soukromý klíč odpovídající pečetícímu certifikátu je vygenerován a uložen v zařízení typu QSealCD spravovaném poskytovatelem služby, do tohoto QSealCD je uložen i odpovídající certifikát.

4.2 Aktivace Služby

Aktivace Služby se provede spuštěním dodávané GUI utility s využitím aktivační karty/tokenu, utilita k jejímu vložení vyzve. Výsledným produktem aktivace Služby je nainstalování klientské aplikace (dále jen Aplikace), vygenerování klíčového páru a vystavení sekundárního autentizačního certifikátu a vytvoření konfiguračního souboru, který musí být následně načten do Aplikace. Soukromý klíč odpovídající sekundárnímu autentizačnímu certifikátu je zde uložen šifrovaně.

4.3 Tvorba kvalifikované elektronické pečetě

Vytváření pečetě iniciuje spisová služba (obecně volající aplikace) klienta. Klientská Aplikace vytvoří šifrovaný kanál k zařízení typu QSealCD, tímto kanálem předá žádost o vytvoření kvalifikované elektronické pečetě a vytvořená kvalifikované elektronická pečeť je stejným kanálem vrácena Aplikaci, která sestaví výsledný dokument opatřený pečetí. Pokud je požadován podpis opatřený kvalifikovaným časovým razítkem, je to provedeno v tomto okamžiku, následuje vrácení výsledného dokumentu spisové službě.

4.4 Automatické prodloužení služby

V pravidelných intervalech, pokud je automatické prodloužení zakotveno ve Smlouvě, je s určitým předstihem před vypršením platnosti pečetícího certifikátu provedeno:

- vygenerování nových párových dat pro sekundární autentizační certifikát,
- vygenerování nových párových dat pro vzdálené pečetění a vydán nový kvalifikovaný pečetící certifikát (soukromý klíč je vygenerován a uložen v zařícení typu QSealCD spravovaném poskytovatelem Služby).

Pokud došlo ke změně údajů v certifikátu a automatické prodloužení nemohlo proběhnout, je Klient prostřednictvím Osoby povinen dostavit se na kontaktní místo s doklady potřebnými pro počáteční ověření identity.

4.5 Účtování provedených operací

Všechny žádosti o kvalifikované elektronické pečetě jsou ukládány do databáze. V pravidelných intervalech jsou získávány záznamy o provedených operacích ze zařízení typu QSealCD, údaje jsou párovány se žádostmi a na základě toho je účtováno. Vedlejším efektem je, že pokud k operaci v QSealCD neexistuje odpovídající žádost, je situace řešena jako potenciální útok.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Management bezpečnosti je zaměřen především na:

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

Oblasti managementu provozní a fyzické bezpečnosti jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, této Směrnice, resp. odpovídající Politice a Plán pro zvládání krizových situací a plán obnovy, tak v upřesňujících interních dokumentech. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně uvedena 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.

5.1.1 Umístění a konstrukce

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

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

5.1.2 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.

5.1.3 Elektřina a klimatizace

V prostorách určených k výkonu Služby je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20°C ± 5°C. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

5.1.4 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.

5.1.5 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 jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

5.1.6 Ukládání 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.

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

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

Kopie provozních a pracovních záloh jsou uloženy na místě určeném ředitelem I.CA a popsaném v interní dokumentaci.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou v I.CA definovány důvěryhodné role. Postup jmenování zaměstnanců do důvěryhodných rolí, specifikace těchto rolí včetně odpovídajících činností a odpovědností jsou uvedeny v interní dokumentaci, zejména v dokumentech:

- „Systémová bezpečnostní politika“,
- „Příručka administrátora“.

Všichni zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, které 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“.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro procesy související s citlivými daty Klientů nutnými pro provoz Služby jsou definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

- inicializaci kryptografického modulu pro generování a ukládání citlivých dat nutných pro provoz Služby,
- zálohování těchto dat uložených v kryptografickém modulu,
- obnovu těchto dat do kryptografického modulu.

Pro provádění ostatních úloh není počet přítomných osob určen, musí však jít výhradně o pověřené pracovníky. Podrobné informace jsou uvedeny v interní dokumentaci:

- „Příručka administrátora“.

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci a autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné.

Pro vybrané činnosti využívají pracovníci v důvěryhodných rolích dvoufaktorovou autentizaci.

Problematika je upravena v interní dokumentaci, zejména:

- „Příručka administrátora“.

5.2.4 Role vyžadující rozdělení povinností

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou popsány v interním dokumentu:

- „Příručka administrátora“.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Zaměstnanci I.CA v důvěryhodných rolích jsou vybíráni a přijímáni na základě dále popsaných personálních 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 služeb vytvářejících důvěru Služby 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.

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

Pro vykonávání řídící 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.

5.3.2 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.

5.3.3 Požadavky na školení

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. Školení zahrnuje oblasti informační bezpečnosti, ochrany osobních údajů a další relevantní témata.

5.3.4 Požadavky a periodicita doškolování

Dvakrát za 12 měsíců jsou zaměstnancům I.CA poskytovány aktuální informace o vývoji v předmětných oblastech.

Pracovníci kontaktních míst jsou průběžně formou novinek a sdělení distribuovaných v rámci aplikačního vybavení registrační autority informováni o všech relevantních skutečnostech nutných pro správnou činnost kontaktního místa.

5.3.5 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.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem popsaným v interních dokumentech společnosti a řídícím se zákoníkem práce (tento proces

nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

Problematika je detailně popsána v interním dokumentu:

- „Pracovní řád“.

5.3.7 Požadavky na nezávislé dodavatele

I.CA může nebo musí některé činnosti zajišťovat smluvně, za činnost nezávislých dodavatelů plně odpovídá. 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 vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Postupy zpracování auditních záznamů

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“.

5.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované platnou legislativou pro služby vytvářející důvěru a příslušnými technickými standardy a normami.

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.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interním dokumentu:

- „Příručka administrátora“,

v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

Nestanoví-li relevantní legislativa jinak, jsou auditní záznamy uchovávány po dobu nejméně 10 let od jejich vzniku.

5.4.4 Ochrana auditních záznamů

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem zajišťujícím ochranu před jejich změnami, krádeží 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.

5.4.5 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.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů Služby interní.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s., prováděno v periodických intervalech jako součást analýzy rizik. Sledování zranitelnosti zařízení a programového vybavení souvisejících se službami vytvářejícími důvěru je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

Uchovávání záznamů, tj. informací a dokumentace, je u I.CA prováděno podle interní dokumentace, 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“.

5.5.1 Typy uchovávaných záznamů

I.CA uchovává níže uvedené záznamy (v elektronické nebo listinné podobě), které souvisejí s poskytovanou Službou, zejména:

- smlouvy s Klienty a jejich případné dodatky související se Službou,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování záznamů

Záznamy jsou uchovávány v souladu s ustanoveními kapitoly 5.4.3.

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště záznamů

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

Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací I.CA.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací.

5.5.5 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.

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

Záznamy jsou ukládány na místo určené ředitelem I.CA.

Samotná problematika přípravy a způsobu ukládání záznamů v elektronické i písemné podobě je upravena interními normami a směrnicemi. Shromažďování uchovávaných záznamů je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Obnova po havárii nebo kompromitaci

5.6.1 Postup ošetření incidentu nebo kompromitace

V případě výskytu těchto událostí 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“.

5.6.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz kapitola 5.6.1.

5.6.3 Schopnost obnovit činnost po havárii

Viz kapitola 5.6.1.

5.7 Ukončení činnosti poskytovatele služeb

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 na využívání Služby.
- ukončení činnosti poskytovatele služby vytvářející důvěru musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro

poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity služeb.

V případě bankrotu je postupováno v souladu s příslušnou legislativou.

V případě odnětí statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru dle platné legislativy:

- informace o odnětí statutu musí být písemně nebo elektronicky oznámena všem subjektům, které mají uzavřenou Smlouvu na využívání Služby,
- informace o odnětí statutu musí být zveřejněna v souladu s kapitolou 2.2,
- o dalším postupu rozhodne ředitel I.CA na základě rozhodnutí orgánu dohledu.

Problematika je podrobně popsána v interním dokumentu:

- „Ukončení služeb I.CA".

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Počítačová bezpečnost

6.1.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti komponent použitých pro poskytování Služby je definována platnou legislativou pro služby vytvářející důvěru, resp. v ní odkazovanými technickými standardy a normami. . 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“.

6.1.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti I.CA je založeno na požadavcích uvedených v mezinárodních a národních standardech, zejména:

- prEN 419241-1 Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements.
- prEN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.
- CEN/TS 419 261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 403 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatelů důvěryhodných služeb - Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation

- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.

6.2 Technické řízení životního cyklu

6.2.1 Řízení vývoje systému pro poskytování služby

Při vývoji systému je postupováno v souladu s interní dokumentací:

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

6.2.2 Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu se standardy, je prováděna v rámci periodických kontrol bezpečnostní shody podle platné legislativy a dále formou interních a externích 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.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

6.2.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu 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.

6.3 Řízení bezpečnosti sítě

V prostředí I.CA nejsou důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru umístěné na provozních pracovištích I.CA přímo dostupné z veřejné sítě Internet. Tyto systémy jsou chráněny komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System). Veškerá komunikace mezi klientskou částí aplikace a provozními pracovišti je vedena šifrovaně. Podrobnosti jsou popsány v interní dokumentaci:

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

6.4 Ochrana proti padělání a odcizení dat

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

7 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Periodicita hodnocení, včetně okolností pro provádění hodnocení, je dána platnou legislativou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, dle kterých je hodnocení prováděno.

Periodicita jiných hodnocení je dána příslušnými technickými standardy a normami.

7.2 Identita a kvalifikace hodnotitele

Identita (akreditovaný subjekt posuzování shody) a kvalifikace hodnotitele provádějícího hodnocení podle platné legislativy pro služby vytvářející důvěru, je dána touto legislativou a jí odkazovanými technickými standardy a normami.

Kvalifikace hodnotitele provádějícího jiná hodnocení je dána příslušnými technickými standardy a normami.

7.3 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 organizačně svázán.

7.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného platnou legislativou pro služby vytvářející důvěru jsou hodnocené oblasti konkretizovány touto legislativou, v ostatních případech jsou hodnocené oblasti dány technickými standardy a normami, podle kterých je hodnocení prováděno.

7.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů 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 její poskytování do doby, než budou tyto nedostatky odstraněny.

7.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům legislativy pro služby vytvářející důvěru a příslušných technických standardů a norem.

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána 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.

8 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 Poplatky

8.1.1 Poplatky za využívání služby

Poplatky za využívání Služby jsou upraveny ve Smlouvě uzavřené mezi I.CA a Klientem.

8.1.2 Poplatky za další služby

Není relevantní pro tento dokument.

8.1.3 Postup při refundování

Není relevantní pro tento dokument.

8.2 Finanční odpovědnost

8.2.1 Krytí pojištěním

Společnost První certifikační autorita, a.s., prohlašuje, že má 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.

8.2.2 Další aktiva

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..

8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

8.3 Důvěrnost obchodních informací

8.3.1 Rozsah důvěrných informací

Důvěrnými informacemi I.CA jsou veškeré informace, které nejsou označeny jako veřejné a nejsou zveřejňovány způsobem uvedeným v kapitole 2.2, zejména:

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

8.3.2 Informace mimo rámec důvěrných informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kapitole 2.2.

8.3.3 Odpovědnost za ochranu důvěrných informací

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

8.4 Ochrana osobních údajů

Problematika je podrobně popsána v interním dokumentu:

- „Ochrana osobních údajů v I.CA".

8.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

8.4.2 Informace považované za osobní údaje

Osobními informacemi jsou veškeré osobní údaje podléhající ochraně ve smyslu příslušných zákonných norem, tedy ZOOÚ.

Zaměstnanci I.CA, případně subjekty definované platnou legislativou 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.

8.4.3 Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které nespadají do působnosti příslušných zákonných norem, tedy ZOOÚ.

8.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

8.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Problematika oznamování o používání osobních údajů a souhlasu s jejich zpracováním je v I.CA řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

8.4.6 Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů pro soudní, resp. správní účely je v I.CA řešeno v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

8.4.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně podle požadavků příslušných zákonných norem, tedy ZOOÚ.

8.5 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.

8.6 Zastupování a záruky

8.6.1 Zastupování a záruky I.CA

I.CA zaručuje, že poskytuje:

- technickou podporu při provozu Služby, řešení nestandardních situací a poradenství související s provozem Služby prostřednictvím kontaktních údajů uvedených na adrese www.ica.cz,
- Službu vždy právně a technicky aktuální dle relevantních právních předpisů a technických standardů a norem.

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. odpovídající Politiky.

8.6.2 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

8.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., poskytuje pouze záruky, uvedené v kapitole 8.6.

8.8 Omezení odpovědnosti

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

8.9 Záruky a odškodnění

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení platné legislativy a dále takové záruky, které byly sjednány Smlouvou mezi společností První certifikační autorita, a.s., a uživatelem Služby. Smlouva nesmí být v rozporu s platnou legislativou a musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak platnou legislativou, tak příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služby,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, se kterými má platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo odpovědnosti, s výjimkou případů, kdy poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele,
- další možné náhrady škody vycházejí z ustanovení příslušné legislativy a o jejich výši může rozhodnout soud.

Společnost První certifikační autorita, a.s., **neodpovídá** za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování Služby Klientem, zejména za využívání v rozporu s podmínkami uvedenými v této Směrnici, resp. odpovídající Politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení,

Reklamaci 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 je povinna uvést:

- co nejvýstižnější 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, nebo 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.

8.10 Doba platnosti, ukončení platnosti

8.10.1 Doba platnosti

Tato Směrnice nabývá platnosti dnem uvedeným v kapitole 9 a platí minimálně po dobu poskytování Služby, nebo do nahrazení Směrnice novou verzí.

8.10.2 Ukončení platnosti

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této Směrnice je ředitel společnosti První certifikační autorita, a.s.

8.10.3 Důsledky ukončení a přetrvání závazků

Po ukončení platnosti této Směrnice, resp. odpovídající Politiky přetrvávají z ní vyplývající závazky I.CA, a to po dobu platnosti posledního podle ní vydaného Certifikátu.

8.11 Individuální upozorňování a komunikace se 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.

8.12 Novelizace

8.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interním dokumentu.

8.12.2 Postup a periodicita oznamování

Vydání nové verze Směrnice je vždy oznámeno formou zveřejňování informací.

8.12.3 Okolnosti, při kterých musí být změněn OID

OID není Směrnici přiřazen. V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

8.13 Ustanovení o řešení sporů

V případě, že Klient nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

- odpovědný pracovník kontaktního místa,
- odpovědný pracovník I.CA (nutné elektronické nebo listinné podání),

- ředitel I.CA (nutné elektronické nebo listinné podání).

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

8.14 Rozhodné právo

Obchodní činnost společnosti První certifikační autorita, a.s., se řídí právním řádem České republiky.

8.15 Shoda s právními předpisy

Systém poskytování služeb vytvářejících důvěru je provozován ve shodě s legislativními požadavky EU, České republiky a dále s relevantními mezinárodními standardy.

8.16 Další ustanovení

8.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

8.16.2 Postoupení práv

Není relevantní pro tento dokument.

8.16.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto směrnicí, resp. odpovídající Politikou, stanoví, že provádění některého povinného požadavku je nelegální, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a legální.

8.16.4 Zřeknutí se práv

Není relevantní pro tento dokument.

8.16.5 Vyšší moc

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývající ze 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.

8.17 Další opatření

Není relevantní pro tento dokument.

9 ZÁVĚREČNÁ USTANOVENÍ

Tato Prováděcí směrnice služby vytváření kvalifikovaných elektronických pečetí na dálku vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 19.6.2018.