První certifikační autorita, a.s.

Prováděcí směrnice

kvalifikované služby ověřování platnosti

kvalifikovaných elektronických podpisů a pečetí

Verze 1.12

OBSAH

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 pečetě.
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, zapracování připomínek auditora, aktualizace seznamu standardů.

1 ÚVOD

Tento dokument stanoví zásady, 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 („QVerify“).

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 prováděcí směrnice v rozporu se standardy nebo zákony, které nahradí dosud platné, bude vydána její nová verze.

Zákonné požadavky na službu QVerify 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,
- zákonem č. 101/2000 Sb., o ochraně osobních údajů, v platném znění, kterým se řídí zpracování osobních údajů v souladu se směrnicí č. 95/46/ES.

Služba QVerify provozovaná společností První certifikační autorita, a.s., zajišťující ověřování elektronických podpisů a pečetí koncovým uživatelům a spoléhajícím se stranám (dále jen „Klient“) je poskytována všem Klientům na základě uzavřeného smluvního vztahu. I.CA nijak neomezuje potenciální Klienty, poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

Aplikační programové vybavení služby se skládá z klientské komponenty a serverové části.

1.1 Přehled

Dokument **Prováděcí směrnice kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí** (dále též „Směrnice“) 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 deseti kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument, obecně popisuje subjekty, které participují na poskytování služby QVerify a definuje přípustné využití služby.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace ke službě QVerify.
- Kapitola 4 definuje základní funkční charakteristiky služby QVerify.
- Kapitola 5 definuje procesy životního cyklu služby QVerify až po ukončení poskytování služby.
- Kapitola 6 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání těchto záznamů a reakce po haváriích nebo kompromitaci.

- Kapitola 7 je zaměřena na technickou bezpečnost včetně počítačové a síťové ochrany.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytované služby QVerify.
- Kapitola 9 zahrnuje problematiku obchodní a právní, včetně ochrany osobních údajů.
- Kapitola 10 obsahuje závěrečná ustanovení.

1.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu:	Prováděcí směrnice kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí, verze 1.12.
OID dokumentu:	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 Spoléhající se strany

Spoléhající se stranou je fyzická osoba, právnická osoba nebo organizační složka státu, obecně jakýkoli subjekt, který uzavřel s První certifikační autoritou, a.s., smluvní vztah na využívání služby QVerify.

1.3.3 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 QVerify

1.4.1 Přípustné použití služby

Službu QVerify provozovanou podle této Směrnice lze využívat v procesech ověřování platnosti elektronického podpisu v souladu s platnou legislativou.

1.4.2 Omezení použití služby

Služba QVerify 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 Směrnice

1.5.1 Organizace spravující Směrnici

Tuto Směrnici, spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba organizace spravující Směrnici

Kontaktní osoba společnosti První certifikační autorita, a.s. je uvedena na internetové adrese (viz kapitola 2.2).

1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů služeb vytvářejících důvěru

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., s postupy jiných poskytovatelů služeb vytvářejících důvěru, je ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování souladu podle bodu 1.5.3

V případě, že je potřebné provést změny v této Směrnici s ohledem na soulad podle kapitoly 1.5.3 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. Dále platí požadavky kapitoly 9.12.

1.6 Přehled použitých pojmů a zkratek

tab. 2 - 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	v tomto dokumentu elektronický podpis, resp. zaručený elektronický podpis, resp. uznávaný elektronický podpis, resp. kvalifikovaný elektronický podpis dle platné legislativy
kvalifikovaná elektronická pečeť	v tomto dokumentu zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť dle platné legislativy
legislativa	aktuálně platná legislativa ČR a nařízení eIDAS
orgán dohledu	orgán dohledu nad dodržováním legislativy spojené s poskytováním služeb vytvářejících důvěru
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 pečetě
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
Zákon o službách vytvářejících důvěru pro elektronické transakce	zákon č. 297/2016 Sb.

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
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
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	zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů), ve znění pozdějších předpisů

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 informace o službě QVerify.

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:

- Směrnice služby QVerify - 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.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace (viz kapitoly 2.2 a 2.3) zpřístupňuje I.CA bezplatně bez omezení.

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

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

3 IDENTIFIKACE A AUTENTIZACE KE SLUŽBĚ QVERIFY

3.1 Počáteční ověření identity

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

3.1.1 Pověřené osoby

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.

3.2 Autentizace ke službě QVerify

- Autentizace ke službě QVerify je možná pouze prostřednictvím autentizačního certifikátu.

4 ZÁKLADNÍ FUNKČNÍ CHARAKTERISTIKA SLUŽBY QVERIFY

Kvalifikovaná služba QVerify, provozovaná společností První certifikační autorita, a.s., zajišťující ověřování elektronických podpisů a pečetí, je definována ve formě klientské komponenty a serverové části.

Služba QVerify ověřuje elektronické podpisy a pečetě ve formátech:

- PAdES-B-B, PAdES-B-T,
- CAdES-B-B, CAdES-B-T,
- XAdES-B-B. XAdES-B-T,

Služba QVerify je poskytována všem Klientům na základě uzavřeného smluvního vztahu.

4.1 Klientská komponenta

Poskytování služby QVerify se realizuje prostřednictvím klientské komponenty instalované v prostředí Klienta. Tato komponenta zajišťuje:

1. Autentizaci uživatele ke službě (komerční technologický/komerční serverový 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.

4.2 Serverová část

Služba QVerify – 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.

5 POŽADAVKY NA ŽIVOTNÍ CYKLUS SLUŽBY QVERIFY

5.1 Žádost o uzavření smlouvy

5.1.1 Subjekty oprávněné uzavřít smlouvu

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

5.1.2 Proces uzavření smlouvy a odpovědnosti

Klient hodlající využívat službu QVerify je povinen zejména:

- seznámit se s touto 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 pověřené osoby druhé smluvní strany 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 QVerify poskytovat v souladu s platnou legislativou, touto Směrnicí, Systémovou bezpečnostní politikou a provozní dokumentací.

5.2 Definování technických parametrů implementace služby QVerify

Technické parametry konkrétní implementace služby QVerify jsou uvedeny ve Smlouvě.

5.3 Testovací prostředí

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

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

5.4 Produkční prostředí

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

5.5 Provoz služby QVerify

Po úspěšné instalaci služby QVerify 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 QVerify podle této Směrnice pouze pro účely stanovené v této Směrnici a platnou legislativou,
- neprodleně uvědomit poskytovatele služeb vytvářejících důvěru o skutečnostech, které mohou ohrozit řádné využívání předmětné služby.

5.6 Změny při provozování a využívání služby QVerify

Jakékoli změny v procesu provozování a využívání služby QVerify musí nastat změnou smluvních podmínek, a to vzestupně číslovanými dodatky Smlouvy podepsanými k tomu oprávněnými osobami.

Technické parametry klientské komponenty, tj. přepis do jiného programovacího jazyka, jiné parametry atd., po definování smluvních podmínek Smlouvou (např. ceny a doby úprav) mohou být nově definovány v technickém popisu služby QVerify.

5.7 Ukončení poskytování služby QVerify

Viz kapitola 9.10.3.

5.8 Úschova dat pro ověřování platnosti elektronických podpisů a pečetí

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

6 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Management bezpečnosti je zaměřen především na:

- systém poskytované služby QVerify,
- veškeré procesy podporující poskytování služby QVerify.

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

6.1 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.

6.1.1 Umístění a konstrukce

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

6.1.2 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.

6.1.3 Elektřina a klimatizace

V prostorách určených k výkonu služby QVerify 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.

6.1.4 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.

6.1.5 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 QVerify, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

6.1.6 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.

6.1.7 Nakládání s odpady

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

6.1.8 Zálohy mimo budovu

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

6.2 Procesní bezpečnost

6.2.1 Důvěryhodné role

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“,
- „Příručka administrátora“.

6.2.2 Počet osob požadovaných na zajištění jednotlivých činností

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

- „Příručka administrátora“.

6.2.3 Identifikace a autentizace pro každou roli

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“.

6.2.4 Role vyžadující rozdělení povinností

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

- „Příručka administrátora“.

6.3 Personální bezpečnost

6.3.1 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 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.

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

6.3.2 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.

6.3.3 Požadavky na přípravu pro výkon role, vstupní školení, popis rolí

Zaměstnanci I.CA jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samopřípravy 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 12 měsíců jsou zaměstnancům poskytovány aktuální informace o vývoji v předmětných oblastech.

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

6.3.4 Administrativní a řídící postupy zaměstnanců a vedoucích zaměstnanců

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

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

6.3.5 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.

6.3.6 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“.

6.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

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 vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

6.3.8 Dokumentace poskytovaná zaměstnancům

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

6.4 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“.

6.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované platnou legislativou.

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.

6.4.2 Periodicita zpracování záznamů

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

- „Příručka administrátora“,

v případě bezpečnostního incidentu okamžitě.

6.4.3 Doba uchování auditních záznamů

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

6.4.4 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.

6.4.5 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.

6.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

6.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

6.4.8 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 službou QVerify je popsáno v interní dokumentaci.

6.5 Uchovávání informací a dokumentace

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“.

6.5.1 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 QVerify,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentace.

6.5.2 Doba uchování uchovávaných informací a dokumentace

Informace vztahující se k poskytované službě QVerify jsou uchovávány po celou dobu existence I.CA.

- Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací - viz kapitola 6.5.

6.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Prostory, ve kterých se uchovávané 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 6.5.

6.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny interní dokumentací - viz kapitola 6.5.

6.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

6.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)

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

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

6.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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 kontrolním subjektům, orgánům činným v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

6.6 Obnova po havárii nebo kompromitaci

6.6.1 Postup v případě incidentu a kompromitace

V případě výskytu uvedených 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“.

6.6.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz kapitola 6.6.1.

6.6.3 Schopnost obnovit činnost po havárii

Viz kapitola 6.6.1.

6.7 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 QVerify.
- 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 pokračováno 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 QVerify,
- 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.

7 TECHNICKÁ BEZPEČNOST

7.1 Počítačová bezpečnost

7.1.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro službu QVerify je definována platnou legislativou, resp. v ní odkazovaných technických standardech nebo 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“.

7.1.2 Hodnocení počítačové bezpečnosti

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

- CEN/TS 419 261:2015 Security requirements for trustworthy systems managing certificates and time-stamps.
- ETSI EN 319 403 V.2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI TS 119 312 V1.2.1 (2017-05) 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.
- ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- 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.
- ISO/IEC 17021-1:2015 Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements.
- ISO/IEC 17065:2012 Conformity assessment -- Requirements for bodies certifying products, processes and services.

7.2 Bezpečnost životního cyklu

7.2.1 Řízení vývoje služby QVerify

Při vývoji systému je postupováno v souladu s interní dokumentací:

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

7.2.2 Kontroly řízení 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.

7.2.3 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.

7.3 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. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

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

7.4 Ochrana proti padělání a odcizení dat

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

7.5 Klientská komponenta

7.5.1 Podporované platformy

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

7.5.2 Funkce klientské komponenty

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 = 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

7.6 Serverová komponenta

7.6.1 Funkce serverové komponenty

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 QVerify.

Data nutná pro ověření jsou uložena pro případné kontrolní účely.

7.7 Bezpečnostní požadavky

7.7.1 Důvěrnost

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 dočasného) nebo databáze. Po procesu ověření jsou data z paměti vymazána.

Celý proces ověření je logován.

7.7.2 Integrita

Ověřovaná data nejsou v systému ukládána. Integrita vstupních dat při přenosu je řešena na úrovni datové struktury webové služby (vstupem je hash ověřovaných dat a hash z podpisu nebo pečetě) a jejich kontrolou na serveru.

7.7.3 Dostupnost

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

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 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.

8.2 Identita a kvalifikace hodnotitele

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

8.3 Vztah hodnotitele k hodnocenému subjektu

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

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

8.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného eIDAS jsou hodnocené oblasti konkretizovány touto legislativou, v ostatních případech jsou hodnocené oblasti dány standardy, podle kterých je hodnocení prováděno.

8.5 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 QVerify, přeruší I.CA tuto službu do doby, než budou tyto nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

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.

Sdělování výsledků hodnocení podléhá požadavkům legislativy.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za využívání služby QVerify

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

9.1.2 Poplatky za další služby

Není relevantní pro tento dokument.

9.1.3 Jiná ustanovení týkající se poplatků (vč. refundací)

Není relevantní pro tento dokument.

9.2 Finanční odpovědnost

9.2.1 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.

9.2.2 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 I.CA.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

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

- veškeré soukromé klíče, sloužící v procesu poskytování služby QVerify,

- obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

9.3.2 Informace mimo rámec citlivých informací

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

9.3.3 Odpovědnost za ochranu citlivých informací

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

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

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

9.4.2 Osobní údaje

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

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.

9.4.3 Údaje, které nejsou považovány za citlivé

Za citlivé údaje nejsou považovány údaje, které nejsou citlivými osobními údaji podle ZOOÚ.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

9.4.5 Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací

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

9.4.6 Poskytnutí citlivých informací pro soudní či správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky 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 QVerify vždy právně a technicky aktuální 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 QVerify neporušil povinnosti plynoucí mu ze Smlouvy a této Směrnice.

9.6.2 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., poskytuje pouze záruky, uvedené v kapitole 9.6.

9.8 Omezení odpovědnosti

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

9.9 Odpovědnost za škodu, náhrada škody

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 QVerify. 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 QVerify,
- 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 QVerify Klientem, zejména za využívání v rozporu s podmínkami uvedenými v této 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 (pověřená osoba ve Smlouvě) 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, 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 jednoho měsíce ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato Směrnice nabývá platnosti dnem uvedeným v kapitole 10 a platí minimálně po dobu poskytování služby QVerify, nebo jejího nahrazení novou verzí.

9.10.2 Ukončení platnosti

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

9.10.3 Opatření pro případ ukončení poskytování služby QVerify

V případě, že dojde k ukončení poskytování služby QVerify, bez ohledu na to, zda k tomu došlo na popud I.CA či Klienta, budou data získaná klientskou komponentou uchovávána 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.

9.11 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.

9.12 Změny

9.12.1 Postup při změnách

Postup je realizován řízeným procesem popsaným v interním dokumentu.

9.12.2 Postup při oznamování změn

Vydání nové verze Směrnice je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněn OID

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

9.13 Řešení sporů

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

- 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.

9.14 Rozhodné právo

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

9.15 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.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost ustanovení

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

9.16.4 Zřeknutí se práv

Není relevantní pro tento dokument.

9.16.5 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.

9.17 Další opatření

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato Směrnice služby QVerify vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 30.1.2018.