První certifikační autorita, a.s.

Politika

systému elektronické identifikace

Verze 1.04

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	30.9.2019	Generální ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.01	30.09.2021	Generální ředitel společnosti První certifikační autorita, a.s.	Textové úpravy, vyznačena klasifikace dokumentu, oprava terminologie v souladu s doporučením právníka.
1.02	20.04.2023	Generální ředitel společnosti První certifikační autorita, a.s.	Zohledněny organizační změny v souvislosti se vznikem Digitální a informační agentury. Revize textu.

1.03	26.08.2024	Generální ředitel společnosti První certifikační autorita, a.s.	Aktualizace seznamu odkazovaných standardů, zohlednění požadavků ETSI TS 119 411-6. Revize textu.
1.04	15.01.2025	Generální ředitel společnosti První certifikační autorita, a.s.	Doplněny způsoby ověření identity fyzické osoby o využití aplikace eDoklady a o ověřování listinného dokladu v ROB.

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 umožňování přístupu prostřednictvím systému elektronické identifikace (dále též Služba). Služba poskytuje nejvyšší úroveň záruky (VYSOKÁ) podle prováděcího nařízení komise (EU) 2015/1502.

Právní požadavky na Službu jsou definovány:

- nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění,
- zákonem České republiky č. 250/2017 Sb., o elektronické identifikaci,
- zákonem České republiky č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů,
- právní úpravou týkající se ochrany osobních údajů, v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

Služba společnosti První certifikační autorita, a.s., zajišťující přístup do systému elektronické identifikace je poskytována fyzickým osobám (dále též Klient) na základě smluvního vztahu uzavřeného buď přímo s Klientem, nebo s jinou právnickou osobou nebo organizační složkou státu (dále též Organizace) uzavřeného ve prospěch Klienta. I.CA dále nijak neomezuje potenciální Klienty, poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

Pozn.: Pokud jsou v dalším textu uváděny odkazy na technické standardy, normy nebo právní předpisy, jedná se vždy buď o uvedený technický standard, normu nebo právní předpis, resp. o technický standard, normu či právní předpis, který je nahrazuje. Pokud by byl tento dokument v rozporu s technickými standardy, normami nebo právními předpisy, které nahradí dosud platné, bude vydána jeho nová verze.

1.1 Přehled

Dokument **Politika systému elektronické identifikace** (dále též Politika) 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: Politika systému elektronické identifikace, verze 1.04

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 (RA), kde je na základě smlouvy o poskytování Služby mezi I.CA a Klientem, nebo mezi I.CA a Organizací ve prospěch Klienta, vydán komerční certifikát pro systém elektronické identifikace na kartě Starcos 3.5 a vyšší a provedeny všechny potřebné akce ve vztahu k Národní identitní autoritě (dále též NIA) provozované Digitální a informační agenturou (dále též DIA).

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 elektronickou identifikaci prostřednictvím komerčního certifikátu pro elektronickou identifikaci vydaného na čipové kartě Starcos 3.5 a vyšší, provedenou První certifikační autoritou, a.s. v roli důvěryhodného poskytovatele identit dle zákona č. 250/2017 Sb.

1.3.4 Jiné participující subjekty

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

1.4 Použití služby

1.4.1 Přípustné použití služby

Službu provozovanou podle této Politiky lze využívat v procesech elektronické identifikace v souladu s platnou právní úpravou.

1.4.2 Omezení použití služby

Služba provozovaná podle této Politiky 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 Politiku spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici

Kontaktní osobou společnosti První certifikační autorita, a.s., v souvislosti s touto Politikou je výkonný ředitel I.CA. Platí kontaktní údaje uvedené v kapitole 2.2.

Mailová adresa certproblem@ica.cz je sledována nepřetržitě v režimu 24x7 a slouží pro hlášení problémů s Certifikátem, tedy např. podezření na kompromitaci klíče nebo na zneužití Certifikátu.

1.5.3 Postupy při schvalování Politiky

Pokud je potřebné provést změny v této Politice a vytvořit její novou verzi, určuje generální ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze Politiky předchází její schválení generálním ředitelem společnosti První certifikační autorita, a.s.

1.6 Přehled použitých pojmů a zkratek

tab. 2 - Pojmy

Pojem	Vysvětlení
elektronická identifikace	implementace principu Single Sign On pro přihlašování k nejrůznějším agendám, v první řadě veřejné správy
Národní bod	informační systém veřejné správy, jehož správcem je DIA, nástroj pro bezpečné a zaručené ověření totožnosti uživatele online služeb poskytovaných zejména veřejnou správou
orgán dohledu	orgán dohledu nad dodržováním právní úpravy týkající se Služby v ČR

právní úprava pro služby vytvářející důvěru	nařízení eIDAS a aktuálně platná relevantní právní úprava Evropské unie
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
DIA	Digitální a informační agentura, ústřední orgán státní správy, jednotné expertní centrum pro řízení a plánování digitalizace státní správy
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění
EN	European Standard, typ ETSI standardu
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
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu nebo pečetě
ROB	Registr obyvatel
TS	Technical Specification, typ ETSI standardu
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
ZOOÚ	právní úprava týkající se ochrany osobních údajů, v souladu s GDPR

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, ID datové schránky I.CA je a69fvfb.

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.

V případě zneplatnění certifikátů sloužících v procesech souvisejících se Službou (dále též infrastrukturní certifikáty) z důvodu podezření na kompromitaci, případně samotné kompromitace příslušného soukromého klíče oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes.

2.3 Čas nebo četnost zveřejňování

I.CA zveřejňuje informace s následující periodicitou:

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

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 právní úpravou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

3 IDENTIFIKACE A AUTENTIZACE KE SLUŽBĚ

3.1.1 Počáteční ověření identity

Službu mohou využívat Klienti, kteří mají s I.CA uzavřenou platnou smlouvu o využívání této Služby, nebo Klienti, v jejichž prospěch uzavřela smlouvu s I.CA Organizace.

3.1.2 Ověřování identity organizace

Identifikace Organizace uzavírající smlouvu s I.CA ve prospěch Klienta je prováděna standardně jako při uzavírání jakékoliv jiné hospodářské smlouvy. Součástí této smlouvy je také definování způsobu, jak bude I.CA informována o tom, kdo Klientem na základě této smlouvy je.

Pro ověření jiné právnické osoby nebo organizační složky státu musí být předložen:

- originál nebo úředně ověřená kopie výpisu z obchodního nebo jiného právním předpisem 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).

3.1.3 Ověřování identity fyzické osoby

Ověřování identity fyzické osoby je možné následujícími způsoby:

- předložením dvou osobních dokladů v listinné podobě,
- předložením elektronického osobního dokladu, a to občanského průkazu, v aplikaci eDoklady [1],
- předložením jednoho osobního dokladu v listinné podobě a jeho ověřením v Registru obyvatel (ROB) [2].

3.1.3.1 Dva doklady v listinné podobě

Je požadováno předložení dvou osobních dokladů v listinné podobě – primárního a sekundárního. 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. 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,

[1] Viz kapitola 9.

[2] Viz kapitola 9.

- fotografii obličeje.

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

Operátor RA porovnává fotografii žadatele na primárním dokladu se skutečnou podobou žadatele, v případě pochybností má právo požádat o předložení dalšího dokladu v listinné podobě, nebo případně ověřování ukončit. Další doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s osobním dokladem primárním.

Pokud kontrola fotografie skončí s kladným výsledkem, jsou z předloženého primárního osobního dokladu ověřovány následující údaje:

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

Výše uvedené údaje jsou v rámci tzv. počátečního ztotožnění kontrolovány vůči registru obyvatel prostřednictvím DIA. Pokud kontrola neproběhne správně, je operátor RA vyzván k nápravě, bez kladného výsledku kontroly není možné Certifikát vydat.

Potvrzení o zaměstnaneckém poměru lze předložit i v elektronické podobě v případě, že je ve formátu .PDF a podepsané zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu pro elektronický podpis osoby oprávněné jednat za Organizaci.

V případě, že držitele Certifikátu zastupuje na RA zmocněnec, je vyžadováno úředně ověřené zplnomocnění k jednání v zastoupení.

Pokud je fyzická osoba žádající o vydání Certifikátu pro sebe samu fyzickou osobou podnikající a tato skutečnost má být v Certifikátu uvedena, platí dále relevantní požadavky kapitoly 3.2.2.

3.1.3.2 Elektronický doklad v aplikaci eDoklady

Tato možnost je relevantní pouze pro občany ČR s aktivní mobilní aplikací pro prokazování totožnosti eDoklady. Požadováno je předložit digitální stejnopis průkazu (občanského průkazu). Žadatel nejprve pomocí aplikace eDoklady naskenuje QR kód pobočky RA, který je mu je operátorem předložen. Po naskenování kódu je žadateli v aplikaci zobrazena informace o požadavku na předání konkrétních dat do I.CA a žadatel musí jejich předání odsouhlasit.

Operátor RA porovnává fotografii žadatele na digitálním stejnopisu průkazu s jeho skutečnou podobou, v případě pochybností má právo požádat o předložení dalšího dokladu v listinné podobě, nebo případně ověřování ukončit. Další doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s digitálním stejnopisem průkazu.

Pokud kontrola fotografie skončí s kladným výsledkem, jsou převzaty potřebné údaje, tedy:

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

Výše uvedené údaje jsou v rámci tzv. počátečního ztotožnění kontrolovány vůči registru obyvatel prostřednictvím DIA. Pokud kontrola neproběhne správně, je operátor RA vyzván k nápravě, bez kladného výsledku kontroly není možné Certifikát vydat.

Potvrzení o zaměstnaneckém poměru lze předložit i v elektronické podobě v případě, že je ve formátu .PDF a podepsané zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu pro elektronický podpis osoby oprávněné jednat za Organizaci.

V případě, že držitele Certifikátu zastupuje na RA zmocněnec, je vyžadováno úředně ověřené zplnomocnění k jednání v zastoupení.

Pokud je fyzická osoba žádající o vydání Certifikátu pro sebe samu fyzickou osobou podnikající a tato skutečnost má být v Certifikátu uvedena, platí dále relevantní požadavky kapitoly 3.2.2.

3.1.3.3 Jeden doklad v listinné podobě s jeho kontrolou v ROB

Tato možnost je relevantní pouze pro občany ČR. Požadováno je předložit jeden osobní doklad v listinné podobě, kterým může být platný občanský průkaz nebo cestovní pas.

Operátor RA porovnává fotografii žadatele na dokladu s jeho skutečnou podobou, v případě pochybností má právo požádat o předložení dalšího dokladu v listinné podobě, nebo případně ověřování ukončit. Další doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s původně předloženým osobním dokladem.

Pokud kontrola fotografie skončí s kladným výsledkem, operátor RA z předloženého dokladu přetypuje jméno, příjmení, číslo dokladu a typ dokladu a tyto údaje jsou odeslány do ROB za účelem kontroly. Zpět se vrátí potvrzení, že daný doklad existuje, patří svéprávnému a žijícímu člověku, případně další údaje. Údaje z ROB jsou převzaty bez možnosti jakékoliv dalších úprav, jsou to:

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

Výše uvedené údaje jsou v rámci tzv. počátečního ztotožnění kontrolovány vůči registru obyvatel prostřednictvím DIA. Pokud kontrola neproběhne správně, je operátor RA vyzván k nápravě, bez kladného výsledku kontroly není možné Certifikát vydat.

Potvrzení o zaměstnaneckém poměru lze předložit i v elektronické podobě v případě, že je ve formátu .PDF a podepsané zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu pro elektronický podpis osoby oprávněné jednat za Organizaci.

V případě, že držitele Certifikátu zastupuje na RA zmocněnec, je vyžadováno úředně ověřené zplnomocnění k jednání v zastoupení.

Pokud je fyzická osoba žádající o vydání Certifikátu pro sebe samu fyzickou osobou podnikající a tato skutečnost má být v Certifikátu uvedena, platí dále relevantní požadavky kapitoly 3.2.2.

3.2 Ověření identity při prodloužení služby

Prodloužení Služby probíhá automatizovaně po vydání následného certifikátu – viz kapitola 4.5.

3.3 Ověření identity při žádosti o zneplatnění certifikátu

V případě **osobního předání žádosti o zneplatnění certifikátu na RA** musí být žádost o zneplatnění certifikátu písemná a podepsaná osobou, jejíž identita musí být řádně ověřena primárním osobním dokladem (viz kapitola 3.1.3).

V případě **předání žádosti o zneplatnění certifikátu elektronickou cestou** jsou přípustné tyto způsoby identifikace a autentizace:

- prostřednictvím formuláře na webových stránkách společnosti (s využitím hesla pro zneplatnění certifikátu),
- prostřednictvím nepodepsané elektronické zprávy obsahující heslo pro zneplatnění certifikátu odeslané na adresu revoke@ica.cz,
- prostřednictvím elektronicky podepsané elektronické zprávy (elektronický podpis musí být realizován soukromým klíčem příslušným k certifikátu, který má být zneplatněn), odeslané na adresu revoke@ica.cz,
- prostřednictvím datové schránky I.CA (s využitím hesla pro zneplatnění certifikátu),
- prostřednictvím definované osoby pověřené za Organizaci vystupovat ve smluvním vztahu s I.CA,
- způsobem definovaným pravidly provozování Národního bodu (v případě zneplatnění na žádost NIA).

V případě použití **listovní zásilky pro předání žádosti o zneplatnění certifikátu** s využitím hesla pro zneplatnění certifikátu musí být tato zaslána doporučeně na adresu sídla společnosti I.CA.

Údaje, které musí žádost o zneplatnění certifikátu obsahovat, jsou uvedeny v kapitole 4.6.1.

3.4 Změna údajů

Změna údajů je možná pouze na žádost NIA, viz kapitola 4.4.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS SLUŽBY

V následujících podkapitolách je popsán životní cyklus služby.

4.1 Uzavření smlouvy

Smlouva o zřízení a využívání Služby je uzavírána buď mezi I.CA a Klientem, nebo mezi I.CA a Organizací ve prospěch Klienta.

4.2 Zřízení Služby

Zřízení Služby probíhá na kontaktních místech, kterými jsou registrační autority I.CA. Klient je navštíví, je provedeno ověření jeho identity viz kapitola 3.1.3 a potom vydán komerční certifikát pro elektronickou identifikaci uložený spolu s příslušným soukromým klíčem na kartě Starcos 3.5 a vyšší.

4.2.1 Registrační proces a odpovědnosti

Registrační proces prováděný pouze v případě zřízení Služby, a tedy vydávání prvotního komerčního certifikátu zahajuje Klient (držitel soukromého klíče) dostavením se s potřebnými dokumenty a případně s žádostí o certifikát na kontaktní místo, kde probíhá zanesení údajů obsažených v předkládaných dokladech do informačního systému Autority a zpracování žádosti o certifikát.

Držitel soukromého klíče, resp. držitel certifikátu je povinen zejména:

- seznámit se s touto Politikou a smluvně se zavázat jednat podle ní (je doporučeno seznámit se také s Certifikační politikou vydávání komerčních certifikátů pro elektronickou identifikaci),
- seznámit se se smlouvou o zřízení a využívání Služby, zvlášť v případě, že je Služba zřizována Klientovi na základě smlouvy mezi I.CA a Organizací,
- dodržovat veškerá ustanovení Smlouvy,
- používat Službu v souladu s ustanoveními kapitoly 1.4,
- nakládat s údaji pro identifikaci a autentizaci ke Službě tak, aby nemohlo dojít k jejímu zneužití,
- neprodleně vyrozumět poskytovatele Služby o podezření, že údaje pro identifikaci a autentizaci ke Službě byly zneužity a požádat o zneplatnění certifikátu pro elektronickou identifikaci.
- poskytovat pravdivé a úplné informace pro zřízení Služby, resp. pro vydání certifikátu,
- překontrolovat, zda údaje získané z předložených dokumentů jsou správné a odpovídají požadovaným údajům,
- zvolit vhodné heslo pro zneplatnění certifikátu (minimální/maximální délka hesla 4/32 znaků, povolené znaky 0..9, A..Z, a..z).

Poskytovatel Služby je povinen zejména:

- před uzavřením Smlouvy informovat Klienta o smluvních podmínkách,

- uzavírat s Klientem nebo Organizací smlouvu obsahující náležitosti požadované platnou právní úpravou a technickými standardy,
- v procesu zřizování Služby ověřit všechny ověřitelné údaje podle předložených dokladů,
- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou poskytovateli Služby k dispozici v době vydávání tohoto certifikátu,
- zveřejnit certifikáty vydávající certifikační autority a kořenové CA,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- činnosti spojené se Službou poskytovat v souladu s platnou právní úpravou, touto Politikou, odpovídající certifikační politikou, certifikační prováděcí směrnicí, Celkovou bezpečnostní politikou a s provozní dokumentací.

Povinností Organizace je v případě požadavku na ukončení Služby pro určitého Klienta informovat o této skutečnosti neprodleně I.CA, a to způsobem dohodnutým ve smlouvě mezi Organizací a I.CA.

4.2.2 Úkony spojené s převzetím prostředku pro elektronickou identifikaci

Pokud byly splněny veškeré podmínky pro vydání, je povinností Klienta prostředek pro elektronickou identifikaci převzít. Jediným způsobem, jak odmítnout převzetí, je zažádat v souladu s touto Politikou o zneplatnění komerčního certifikátu pro elektronickou identifikaci.

4.3 Aktivace Služby

Aktivace Služby proběhne do jedné hodiny po vydání certifikátu pro elektronickou identifikaci na kartě Starcos 3.5 a vyšší. Je provedeno ztotožnění vůči NIA, pokud proběhne bez chyby, je prostředek pro elektronickou identifikaci převeden do stavu „aktivní" a může být následně v rámci systému elektronické identifikace používán. Pokud ztotožnění není bezchybné (vzhledem k předběžnému ztotožnění před vydáním certifikátu se jedná o minimální počet případů), je prostředek pro elektronickou identifikaci převeden do stavu „ukončený" a pro identifikaci v rámci systému elektronické identifikace použitelný není. Komerční certifikát ale zůstává v platnosti a může být nadále používán jako jiný komerční certifikát.

4.4 Změna údajů

Změna údajů není možná na žádost klienta. Může být provedena výhradně na základě důvěryhodným způsobem získaných informací od NIA a v úvahu přicházejí následující možnosti:

- NIA oznámí změnu čísla primárního identifikačního dokladu Klienta – I.CA si v důsledku toho opraví svoji interní databázi.
- NIA oznámí změnu jména nebo příjmení Klienta – certifikát pro elektronickou identifikaci je zneplatněn, prostředek pro elektronickou identifikaci je uveden do stavu „ukončený" a NIA je o této skutečnosti dohodnutým způsobem informována. Pokud má Klient s I.CA individuální smlouvu, je její platnost ukončena, pokud ve prospěch Klienta uzavřela smlouvu Organizace, zůstává tato v platnosti. V obou případech musí být vydán nový certifikát pro elektronickou identifikaci na kartě Starcos 3.5 a vyšší.
- NIA oznámí změnu bydliště Klienta – pokud je tento údaj uveden v certifikátu, následuje postup popsaný v předchozím bodu, tj. certifikát pro elektronickou identifikaci je

zneplatněn, prostředek pro elektronickou identifikaci je uveden do stavu „ukončený" a NIA je o této skutečnosti dohodnutým způsobem informována. Pokud má Klient s I.CA individuální smlouvu, je její platnost ukončena, pokud ve prospěch Klienta uzavřela smlouvu Organizace, zůstává tato v platnosti. V obou případech musí být vydán nový certifikát pro elektronickou identifikaci na kartě Starcos 3.5 a vyšší. Pokud bydliště v certifikátu uvedeno není, opraví si I.CA údaj v interní databázi

- NIA oznámí změnu data narození Klienta – I.CA si v důsledku toho opraví svoji interní databázi (tato možnost není příliš pravděpodobná).

4.5 Prodloužení Služby

Služba je automaticky prodloužena tak, že Klient požádá o vydání následného certifikátu pro elektronickou identifikaci – viz kapitola 4.5.1. Uživateli jsou standardně, tedy měsíc a potom týden před vypršením platnosti certifikátu, zaslány upozorňovací e-maily. Pokud Klient o vydání následného certifikátu pro elektronickou identifikaci nepožádá, certifikát expiruje, prostředek pro elektronickou identifikaci je uveden do stavu „ukončený" a NIA je o této skutečnosti dohodnutým způsobem informována. Pokud má Klient s I.CA individuální smlouvu, je její platnost ukončena, pokud ve prospěch Klienta uzavřela smlouvu Organizace, zůstává tato v platnosti. V obou případech musí být vydán nový certifikát pro elektronickou identifikaci na kartě Starcos 3.5 a vyšší.

4.5.1 Postup při žádosti o vydání následného certifikátu

Proces vydání následného certifikátu s vyměněným veřejným klíčem probíhá výhradně elektronicky. Standardním způsobem, tedy jeden měsíc a jeden týden před vypršením platnosti je Klient o vypršení platnosti e-mailem od I.CA informován, žádost musí splňovat níže uvedené podmínky:

- položky pole subject a rozšíření subjectAlternativeName musí být totožné jako v certifikátu, který je předmětem výměny,
- veřejný klíč musí být jiný než v certifikátu, který je předmětem výměny,
- ostatní položky žádosti zůstávají shodné s původními údaji v dokumentech předložených v procesu počátečního ověřování identity fyzické osoby,
- proces ověření elektronické žádosti o vydání následného certifikátu je proveden v souladu s kapitolou 3.2.

4.6 Ukončení Služby

Ukončení Služby je možné dvěma způsoby:

- Klient požádá o zneplatnění certifikátu pro elektronickou identifikaci – viz kapitola 4.6.1. V takovém případě jsou zneplatněny všechny certifikáty na příslušné kartě Starcos 3.5 a vyšší a prostředek pro elektronickou identifikaci je uveden do stavu „neplatný". Pokud má Klient s I.CA individuální smlouvu, je její platnost ukončena, pokud ve prospěch Klienta uzavřela smlouvu Organizace, zůstává tato v platnosti. V obou případech musí být vydán nový certifikát pro elektronickou identifikaci na kartě Starcos 3.5 a vyšší.
- Organizace způsobem dohodnutým ve smlouvě mezi Organizací a I.CA informuje, že poskytování Služby pro určitého Klienta má být ukončeno. V takovém případě je prostředek pro elektronickou identifikaci uveden do stavu „neplatný".

4.6.1 Postup při žádosti o zneplatnění certifikátu

Pro žádost o zneplatnění certifikátu podávanou jeho držitelem platí:

- V případě osobního předání žádosti o zneplatnění certifikátu na kontaktním místě (RA) musí žádost obsahovat sériové číslo certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“), jméno, popř. jména a příjmení fyzické osoby oprávněné žádat zneplatnění certifikátu a heslo pro zneplatnění certifikátu. Pokud fyzická osoba oprávněná žádat zneplatnění certifikátu heslo pro zneplatnění nezná, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla osobního dokladu předloženého při žádosti o vydání certifikátu, nebo čísla nového primárního osobního dokladu, pokud byl původní nahrazen novým. Tímto osobním dokladem se musí pracovníkovi RA prokázat. V případě, že je žádost oprávněná, pracovník RA certifikát zneplatní – datum a čas zneplatnění certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. V případě, že žádost o zneplatnění certifikátu nelze akceptovat (nesprávné heslo pro zneplatnění, neprokazatelná identita fyzické osoby oprávněné žádat zneplatnění certifikátu), pokusí se pracovník RA v součinnosti s touto fyzickou osobou tyto skutečnosti napravit a pokud to z libovolného důvodu nebude možné, žádost o zneplatnění certifikátu bude zamítnuta. Žadatel o zneplatnění certifikátu je vždy o výsledku informován prostřednictvím pracovníka RA.
- V případě předání žádosti o zneplatnění certifikátu elektronickou cestou jsou přípustné následující možnosti:
  - Prostřednictvím formuláře na internetové informační adrese. Datum a čas zneplatnění certifikátu jsou dány zpracováním platné žádosti o zneplatnění certifikátu informačním systémem CA. O kladném vyřízení je žadatel informován.
  - Elektronicky podepsaná elektronická zpráva – tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

    Zadam o zneplatneni certifikatu cislo = xxxxxxx,

    kde „*xxxxxxx*“ je sériové číslo certifikátu a musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

    Zpráva musí být elektronicky podepsána soukromým klíčem odpovídajícím veřejnému klíči ve zneplatňovaném certifikátu.
  - Elektronicky nepodepsaná elektronická zpráva – tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

    Zadam o zneplatneni certifikatu cislo = xxxxxxx

    Heslo pro zneplatneni = yyyyyy,

    kde „*xxxxxxx*“ je sériové číslo certifikátu a „*yyyyyy*“ je heslo pro zneplatnění. Sériové číslo musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).
  - Elektronicky podepsaná či ve zvláštních případech elektronicky nepodepsaná elektronická zpráva odeslaná definovanou osobou pověřenou za Organizaci vystupovat ve smluvním vztahu s I.CA:

    Zadam o zneplatneni certifikatu cislo = xxxxxxx

    kde „*xxxxxxx*“ je sériové číslo certifikátu. Sériové číslo musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

Pozn.: Pokud žádost splňuje požadavky tří výše uvedených možností, odpovědný pracovník certifikát v systému CA neprodleně zneplatní – datum a čas zneplatnění certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. O kladném vyřízení je žadatel informován.

- V případě použití doporučené listovní zásilky pro podání žádosti o zneplatnění certifikátu musí být žádost v následujícím tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

  Zadam o zneplatneni certifikatu cislo = xxxxxxx

  Heslo pro zneplatneni = yyyyyy,

  kde „*xxxxxxx*“ je sériové číslo certifikátu a „*yyyyyy*“ je heslo pro zneplatnění. Sériové číslo je buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“). V případě, že žádost uvedené požadavky splňuje, odpovědný pracovník I.CA certifikát v informačním systému CA zneplatní – datum a čas zneplatnění certifikátu jsou dány zpracováním tohoto požadavku v informačním systémem CA. V případě, že žádost nelze akceptovat (nesprávné heslo pro zneplatnění) bude žádost o zneplatnění certifikátu zamítnuta. O vyřízení žádosti je žadatel informován doporučeným dopisem na poštovní adresu uvedenou jako adresa odesilatele.

Žádost o zneplatnění certifikátu podávaná NIA musí být podána způsobem definovaným v pravidlech provozování Národního bodu. Žádost o zneplatnění certifikátu podávaná Organizací musí být podána způsobem definovaným ve smlouvě mezi I.CA a Organizací.

Oznámení o podezření na kompromitaci soukromého klíče vztahujícího se k veřejnému klíči v Certifikátu, zneužití Certifikátu nebo jiné typy podvodu, kompromitace, zneužití, nevhodného chování spojené s vydaným Certifikátem je možné zaslat na e-mailovou adresu uvedenou v kapitole 1.5.2, případně doporučenou listovní zásilkou na adresu sídla společnosti, nebo podat prostřednictvím datové schránky – viz kapitola 2.2.

4.7 Zablokování a odblokování prostředku pro elektronickou identifikaci

Prostředek pro elektronickou identifikaci může být, např. v případech ztráty nebo odcizení, zablokován, v případě jeho nalezení potom odblokován.

4.7.1 Zablokování prostředku pro elektronickou identifikaci

Zablokování prostředku pro elektronickou identifikaci znamená, že prostředek pro elektronickou identifikaci je převeden do stavu „blokovaný" a nadále není možné tento prostředek používat pro elektronickou identifikaci. Certifikát pro elektronickou identifikaci zůstává nadále v platnosti (je možné ho nadále používat jako běžný komerční certifikát se vším, co z toho vyplývá). Možnosti zablokování prostředku pro elektronickou identifikaci jsou:

- Telefonicky na číslo +420 284 081 930, +420 284 081 931, +420 284 081 933. Pracovník technické podpory zjišťuje jméno, příjmení a akademický titul Klienta, identifikační číslo primárního dokladu, bydliště Klienta a dále se může zeptat na jakýkoliv další údaj neuvedený v certifikátu, ale zadaný při žádosti a zřízení Služby. Pracovník technické podpory může při jakýchkoliv nejasnostech v odpovědích Klienta odkázat na jiný způsob zablokování prostředku pro elektronickou identifikaci.
- E-mailem na adresu podpora@ica.cz, e-mail musí být odeslán z e-mailové adresy zadané při zřizování služby. E-mail musí obsahovat tyto údaje:

- Klient *akademický titul, jméno (jména) a příjmení*, datum narození *dd.mm.rrrr*, číslo primárního identifikačního dokladu *abcdefghij*, bydliště *ulice, čp., psč, město* žádá o zablokování prostředku pro elektronickou identifikaci.

V případě jakýchkoliv nejasností může být zablokování odmítnuto, o výsledku je Klient odpovědí na jeho e-mail vždy informován.

- Osobně na kontaktním místě, kdy musí být ke kontrole předloženy primární a sekundární doklad (sekundární nemusí být stejný jako při počátečním ověření identity dle kapitoly 3.1.2, ale musí obsahovat alespoň jeden z údajů dle kapitoly 3.1.2).

4.7.2 Odblokování prostředku pro elektronickou identifikaci

Jediným způsobem odblokování prostředku pro elektronickou identifikaci je osobní návštěva kontaktního místa a předložení primárního i sekundárního dokladu (viz předchozí bod).

4.8 Používání prostředku pro elektronickou identifikaci

Účelem systému elektronické identifikace je umožnit zjednodušené přihlašování uživatele k poskytovatelům služeb, v první řadě z oblasti veřejné správy. Uživatel nemusí mít pro každého poskytovatele služeb unikátní přihlašovací údaje, ale pro přihlašování k těmto poskytovatelům je realizován princip jednotného přihlašování (Single Sign On – SSO).

Postup je následující:

- uživatel přistoupí na webové stránky poskytovatele služeb, protože zde chce vyřídit nějakou agendu,
- uživatel je přesměrován na webové stránky NIA,
- NIA nabídne uživateli seznam poskytovatelů (Identity Provider – IdP), kteří jsou mu schopni ztotožnění s úrovní záruky požadovanou poskytovatelem služby (I.CA poskytuje nejvyšší záruku) provést, jedním z IdP je První certifikační autorita, a.s.,
- uživatel si z nabízeného seznamu vybere IdP a je přesměrován na jeho webové stránky.

Pokud je jako IdP vybrána I.CA, je uživatel přesměrován na její webové stránky. Následně je požádán o identifikaci (čipová karta) a autentizaci (PIN), I.CA provede kontrolu ve své databázi, provede ztotožnění vůči NIA a pokud vše proběhne úspěšně, je uživatel jako řádně identifikovaný a autentizovaný vrácen na stránky poskytovatele služeb a může zde požadovanou agendu vyřídit.

V paměti webového prohlížeče zůstávají po určitou údaje o úspěšné identifikaci, autentizaci a ztotožnění, pokud se bude uživatel v době platnosti hlásit k jinému poskytovateli služeb, budou tyto údaje použity.

4.9 Účtování za Službu

Účtování za službu se liší podle toho, zda se jedná o individuálního Klienta uzavírajícího Smlouvu přímo s I.CA, nebo o Klienta, v jehož prospěch uzavřela Smlouvu Organizace.

- individuální Klient platí za vydání komerčního certifikátu pro elektronickou identifikaci a za čipovou kartu Starcos 3.5 a vyšší, neplatí za jednotlivé operace přihlášení,
- klient, v jehož prospěch uzavřela smlouvu Organizace neplatí za vydání komerčního certifikátu pro elektronickou identifikaci, platí za čipovou kartu Starcos 3.5 a vyšší

a jednotlivé operace přihlášení jsou zpoplatněny Organizaci formou pásem počtů přihlášení.

Konkrétní výše poplatků jsou uvedeny v aktuálním ceníku vystaveném na webu společnosti (viz kapitola 2.2).

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, tato Politika 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

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 míst a registračních autorit.

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, na kterém záznamy vznikly.

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

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 výkonným 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.

Všichni zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, které by mohly ohrozit nestrannost operací I.CA. Postupy jmenování zaměstnanců do důvěryhodných rolí a specifikace těchto rolí jsou uvedeny v interní dokumentaci.

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.

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.

5.2.4 Role vyžadující rozdělení povinností

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

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 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 a registračních autorit 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 dokumentacích společnosti a řídícím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

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 a relevantními částmi interní dokumentace I.CA, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou uplatňovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

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

5.4 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované relevantní platnou právní úpravou 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 interní dokumentaci, v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

Nestanoví-li relevantní právní úprava 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, odcizením a zničením (ať již úmyslným nebo neúmyslným).

Elektronické auditní záznamy jsou ukládány ve dvou kopiích. 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 s důvěryhodnými systémy je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

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

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, resp. s Organizacemi a jejich případné dodatky související se Službou,
- záznamy o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- provozní a bezpečnostní dokumentaci.

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 výkonným 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 dohledovým a kontrolním subjektům a orgánům činným v trestním řízení, pokud je to právními předpisy vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

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.

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 Služby

Ukončení činnosti kvalifikovaného poskytovatele Služby se řídí dokumentem Plán ukončení činnosti kvalifikovaného správce kvalifikovaného systému elektronické identifikace.

Pro ukončování činnosti kvalifikovaného poskytovatele Služby platí následující pravidla:

- ukončení činnosti poskytovatele Služby musí být písemně oznámeno orgánu dohledu a všem subjektům, které mají uzavřenou Smlouvu na využívání Služby.
- ukončení činnosti poskytovatele Služby 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 právní úpravou.

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

- 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 generální ředitel I.CA na základě rozhodnutí orgánu dohledu.

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 právní úpravou, resp. v ní odkazovanými technickými standardy a normami.

6.1.2 Hodnocení počítačové bezpečnosti

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

- CEN/TS 419261 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 319 403-1 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatele důvěryhodné služby – Část 1: Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodné služby.
- ETSI EN 319 403-1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- 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.
- ČSN EN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

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.

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 právní úpravy a dále formou interních a externích auditů systému řízení bezpečnosti informací (ISMS).

Bezpečnost informací se v I.CA řídí těmito normami:

- ČSN EN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.
- ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky.
- ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti.

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 Služby 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.

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 právní úpravou 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 právní úpravy je dána touto právní úpravou 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 personálně svázán.

7.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného platnou právní úpravou jsou hodnocené oblasti konkretizovány touto právní úpravou, 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 platné právní úpravy a příslušných technických standardů a norem.

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

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

8 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 Poplatky

8.1.1 Poplatky za využívání Služby

Viz kapitola 4.9.

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 platně uzavřené pojištění podnikatelských rizik takovým způsobem, aby byly pokryty případné finanční škody.

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

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 Služby s ohledem na riziko vzniku odpovědnosti za škodu.

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

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 generálního ředitele I.CA poskytnout třetí straně.

8.4 Ochrana osobních údajů

8.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných právních předpisů, tedy zejména ZOOÚ a GDPR. Informace o zásadách ochrany osobních údajů klientů je uvedena v dokumentu „Zásady nakládání s osobními údaji klientů“ vystaveném na webu společnosti – viz kapitola 2.2.

8.4.2 Informace považované za osobní údaje

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

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

8.4.3 Informace nepovažované za osobní údaje

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

8.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný generální 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 právních předpisů.

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 právních předpisů.

8.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

8.5 Práva duševního vlastnictví

Tato Politika, 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 Politiky.

8.6.2 Zastupování a záruky kontaktních míst

Určené kontaktní místo (RA):

- přejímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost, pokud se nepodařilo ověřit některou z položek žádosti s výjimkou položek neověřovaných, nebo neproběhlo správně prvotní ztotožnění vůči NIA, nebo držitel certifikátu odmítá potřebné údaje sdělit, nebo není oprávněn k podání žádosti o certifikát,

- v případě osobního podání žádosti o zneplatnění certifikátu odpovídá za včasné předání této žádostí k vyřízení na kontaktní místo (RA),
- odpovídá za vyřizování připomínek a stížností.

8.6.3 Zastupování a záruky Klienta

Ve smlouvě mezi I.CA a Klientem, resp. mezi I.CA a Organizací ve prospěch Klienta je uvedeno, že Klienti jsou povinni řídit se ustanoveními této Politiky.

8.6.4 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 v případě této Služby za škody způsobené v případech nesplnění povinností požadovaných touto Politikou. Dále neodpovídá za škody vzniklé v důsledku porušení povinností I.CA z důvodu vyšší moci.

8.9 Záruky a odškodnění

Pro poskytování Služby platí relevantní ustanovení platné právní úpravy a dále takové záruky, které byly sjednány Smlouvou mezi společností První certifikační autorita, a.s., a Klientem, resp. Organizací. Smlouva nesmí být v rozporu s platnou právní úpravou a musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak platnou právní úpravou, 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 právní úpravy 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 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 Politika nabývá platnosti dnem uvedeným v kapitole 9 a platí minimálně po dobu poskytování Služby, nebo do nahrazení Politiky novou verzí.

8.10.2 Ukončení platnosti

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

8.10.3 Důsledky ukončení a přetrvání závazků

Po ukončení platnosti této Politiky přetrvávají z ní vyplývající závazky I.CA, a to po dobu platnosti posledního certifikátu pro elektronickou identifikaci tvořícího spolu s kartou Starcos 3.5 a vyšší prostředek pro elektronickou identifikaci.

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.

Způsob komunikace s NIA je dán pravidly provozování Národního bodu.

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 interní dokumentaci.

8.12.2 Postup a periodicita oznamování

Vydání nové verze Politiky je vždy oznámeno formou zveřejňování informací.

8.12.3 Okolnosti, při kterých musí být změněn OID

OID není Politice 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),
- generální 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

Služba je provozována ve shodě s právními 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 Politikou, stanoví, že provádění některého povinného požadavku je protiprávní, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a v souladu s platnou právní úpravou.

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 vyplývajících ze smluvních vztahů s Klientem vzniklých na základě zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu, popř. výpadku komunikačního spojení.

8.17 Další opatření

Není relevantní pro tento dokument.

9 ZÁVĚREČNÁ USTANOVENÍ

Tato Politika vydaná společností První certifikační autorita, a.s., nabývá platnosti dnem uvedeným v tab. 1 a účinnosti zveřejněním udělení akreditace na internetových stránkách Ministerstva vnitra dle § 19 zákona č. 250/2017 Sb. Využití nově zaváděných postupů ověřování identity fyzické osoby popisovaných v kapitolách 3.1.3.2 a 3.1.3.3 je vázáno na jejich schválení orgánem dohledu.