První certifikační autorita, a.s.

Certifikační politika

vydávání certifikátů pro systém e-Kasa

(algoritmus RSA)

verze 1.02

OBSAH

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	24.02.2019	Ředitel společnosti První certifikační autorita, a.s.	První vydání.
1.01	29.03.2019	Ředitel společnosti První certifikační autorita, a.s.	Formální opravy - zapracování připomínek.
1.02	30.5.2019	Ředitel společnosti První certifikační autorita, a.s.	Formální opravy - zapracování připomínek.

1 ÚVOD

Tento dokument stanoví zásady, které První certifikační autorita, a.s., (dále též I.CA) uplatňuje při vydávání certifikátů pro systém e-Kasa (Certifikát) provozovaný s využitím služeb I.CA, které jsou zprostředkované společností D.Trust Certifikačná Autorita, a.s., (dále též DTCA), ve prospěch rozpočtové organizace Finančné riaditeľstvo SR (dále též FR SR). Vydávání Certifikátů je dále v textu označováno jako Služba. Pro Službu poskytovanou podle této certifikační politiky (dále též CP) je využíván algoritmus RSA.

Certifikáty vydávané podle této CP jsou určené pro:

- ověřování elektronických podpisů / elektronických pečetí vydávaných certifikátů koncových uživatelů, certifikátů OCSP respondéru vydávající certifikační autority, certifikátů pro operátora GUI, certifikátů pro autentizaci modulu PKI e-Kasa a CRL,
- pro ověřování odpovědí s využitím protokolu OCSP na stav certifikátu vydaného I.CA koncovému uživateli.
- autentizace operátorů GUI,
- autentizace modulu PKI e-Kasa a zařízení ICARA,
- ověřování elektronických podpisů / elektronických pečetí vytvářených pokladnami provozovanými daňovými subjekty zapojenými do systému e-Kasa (dále též Subjekt),

Vydávání Certifikátů Subjektům je poskytováno všem Subjektům na základě zákonných povinností vyplývajících ze zákona č. 289/2008 Z. z.[1] ve vztahu s FR SR (dále též Smlouva). I.CA jinak neomezuje potenciální koncové uživatele, poskytování je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

Pozn.: Pokud jsou v dalším textu uváděny odkazy na technické standardy, normy nebo zákony, jedná se vždy buď o uvedený technický standard, normu nebo zákon, resp. o technický standard, normu či zákon, který je nahrazuje. Pokud by byla tato CP v rozporu s technickými standardy, normami nebo zákony, které nahradí dosud platné, bude vydána její nová verze.

1.1 Přehled

Dokument **Certifikační politika vydávání certifikátů pro systém e-Kasa (algoritmus RSA)** vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se k procesům životního cyklu vydávaných Certifikátů a dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC 3647, s přihlédnutím k platným standardům Evropské unie a k právu České republiky a Slovenské republiky v dané oblasti (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k ní irelevantní). Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem, obecně popisuje subjekty participující na poskytování této Služby a definuje přípustné využívání vydávaných Certifikátů.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.

[1] Zákon č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a o zmene a doplnení zákona Slovenskej národnej rady č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení neskorších predpisov.

- Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání Certifikátu, resp. zneplatnění Certifikátu, včetně definování typů a obsahů používaných jmen ve vydávaných Certifikátech.
- Kapitola 4 definuje procesy životního cyklu jí vydávaných Certifikátů, tzn. žádost o vydání a vlastní vydání Certifikátu, žádost o zneplatnění a vlastní zneplatnění Certifikátu, služby související s ověřováním stavu Certifikátu, ukončení poskytování Služby atd.
- 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 typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.
- Kapitola 7 definuje profil vydávaných Certifikátů a seznamů zneplatněných certifikátů.
- Kapitola 8 je zaměřena na problematiku hodnocení poskytované Služby.
- Kapitola 9 zahrnuje problematiku obchodní a právní.

Bližší podrobnosti o naplnění polí a rozšíření Certifikátů vydávaných podle této CP a o jejich správě mohou být uvedeny v odpovídající certifikační prováděcí směrnici (dále CPS).

1.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu:	Certifikační politika vydávání certifikátů pro systém e-Kasa (algoritmus RSA), verze 1.01
OID1 (OID politiky vydávání certifikátů pro OCSP respondér):	1.3.6.1.4.1.23624.10.1.101.1.0
OID2 (OID politiky vydávání certifikátů pro operátory GUI):	1.3.6.1.4.1.23624.10.1.102.1.0
OID3 (OID politiky vydávání certifikátů pro modul PKI e-Kasa):	1.3.6.1.4.1.23624.10.1.103.1.0
OID4 (OID politiky vydávání certifikátů Subjektům):	1.3.6.1.4.1.23624.10.1.110.1.0

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA")

Certifikační autorita systému e-Kasa (dále táž Autorita) vydává (vydala):

- Certifikát Autority, kterým elektronicky podepisuje / opatřuje elektronickou pečetí certifikáty OCSP respondéru, certifikáty pro operátory GUI, certifikáty pro modul PKI e-Kasa, certifikáty koncových uživatelů a CRL,
- Certifikáty pro svůj OCSP respondér s OID1,
- Certifikáty pro operátory GUI s OID2,

- Certifikáty pro modul PKI e-Kasa s OID3.
- Certifikáty Subjektů s OID4.

1.3.2 Registrační autority (dále „RA")

Pro potřeby Certifikátů vlastněných I.CA existuje speciální registrační autorita provádějící ověření právnické a fyzické osoby.

Pro potřeby ostatních vydávaných typů Certifikátů je Služba provozována bez zásahu lidské obsluhy registrační autority. Registrační autorita je jedna a funguje automaticky. Povinnost kontroly identifikačních údajů Subjektů, operátorů GUI a žadatelů o Certifikát modulu PKI e-Kasa je plně v kompetenci FR SR.

1.3.3 Držitelé certifikátů

Držitelem vydávaného Certifikátu:

- v případě Certifikátu Autority je společnost První certifikační autorita, a.s., (dále též I.CA) žadatelem o Certifikát je ředitel I.CA,
- v případě Certifikátu s OID1 je společnost První certifikační autorita, a.s., žadatelem o Certifikát je pracovník pověřený ředitelem I.CA,
- v případě Certifikátu OID2 pracovník pověřený obsluhou systému e-Kasa prostřednictvím GUI,
- v případě certifikátů s OID3 FR SR,
- v případě certifikátu s OID4 Subjekt, který požádal o vydání Certifikátu pro sebe (sebou provozovanou pokladnu) prostřednictvím FR SR a identifikovaný v Certifikátu jako držitel soukromého klíče spojeného s veřejným klíčem uvedeným v tomto Certifikátu.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na Certifikáty vydávané podle této CP.

1.3.5 Jiné participující subjekty

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

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP lze využívat pro:

- ověřování elektronického podpisu / elektronické pečetě dalších typů vydávaných Certifikátů,
- ověřování elektronického podpisu / elektronické pečetě CRL a odpovědí OCSP respondéru,

- autentizaci operátora GUI, modulu PKI e-Kasa a zařízení ICARA,
- ověřování elektronického podpisu / elektronické pečetě vytvořené pokladnou provozovanou Subjektem.

1.4.2 Zakázané použití certifikátu

Certifikáty vydávané podle této CP nesmějí být používány 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 dokument

Tuto CP, resp. jí odpovídající CPS, spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s touto CP, resp. odpovídající CPS, je uvedena ve smluvních dokumentech mezi společnostmi I.CA a DTCA a Finančným riaditeľstvom SR (dále též Kontrakt). Kontaktní osoba na straně FR SR, na kterou se mohou obracet Subjekty, je uvedena na webu www.financnasprava.sk. Subjekty nejsou oprávněny obracet se přímo na společnost I.CA.

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených v CPS s touto CP, je ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování CPS

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

1.6 Přehled použitých pojmů a zkratek

tab. 2 - Pojmy

Pojem	Vysvětlení
bezpečné kryptografické zařízení	zařízení, na kterém je uložen soukromý klíč
bit	z anglického *binary digit* - číslice dvojkové soustavy - základní a současně nejmenší jednotka informace v číslicové technice
časové razítko	elektronické časové razítko, nebo kvalifikované elektronické časové razítko dle eIDAS

dvoufaktorová autentizace	autentizace využívající dvou ze tří faktorů - něco vím (heslo), něco mám (např. čipová karta, hardwarový token) nebo něco jsem (otisky prstů, snímání oční sítnice či duhovky)
elektronický podpis / elektronická pečeť	data připojená k datové zprávě nebo s ní logicky spojená, umožňující ověření identity podepsané osoby nebo pečetící organizace ve vztahu k datové zprávě.
hashovací funkce	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou (hash)
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
párová data	soukromý a jemu odpovídající veřejný klíč
písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
smluvní partner	poskytovatel vybraných certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části
soukromý klíč	jedinečná data využívaná v procesech vytváření elektronického podpisu / elektronické pečetě, autentizace a ~~de~~šifrování
spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát
veřejný klíč	jedinečná data využívaná v procesech ověřování elektronického podpisu / elektronické pečetě, autentizace a šifrování
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, resp. zákon Slovenské republiky č. 2015/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, resp. zákon Slovenské republiky č. 311/2001 Z.z. Zákoník práce

tab. 3 - Zkratky

Zkratka	Vysvětlení
BIH	Bureau International de l'Heure, (anglicky The International Time Bureau), Mezinárodní časová služba
CA	certifikační autorita
CC	Common Criteria for Information Technology Security Evaluation, kritéria hodnocení bezpečnosti IT
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
ČR	Česká republika

ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátu
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
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EZS	elektronická zabezpečovací signalizace
FR SR	Finančné riaditeľstvo Slovenskej republiky
html	Hypertext Markup Language, značkovací jazyk pro vytváření hypertextových dokumentů
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.
ICARA	rozhraní mezi PKI e-Kasa a certifikační autoritou provozovanou I.CA
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IPS	Intrusion Prevention System, systém prevence průniku
ISMS	Information Security Management System, systém řízení bezpečnosti informací
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
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

PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
PUB	Publication, označení standardu FIPS
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu/ kvalifikované elektronické pečetě podle eIDAS
RA	registrační autorita
RFC	Request for Comments, označení řady standardů a dalších dokumentů popisujících internetové protokoly, systémy apod.
RSA	šifra s veřejným klíčem pro podepisování a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)
SHA	typ hashovací funkce
TS	Technical Specification, typ ETSI standardu
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
URI	Uniform Resource Identifier, textový řetězec s definovanou strukturou sloužící k přesné specifikaci zdroje informací
UTC	Coordinated Universal Time, standard přijatý 1.1.1972 pro světový koordinovaný čas - funkci „oficiálního časoměřiče" atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
ZOOÚ	aktuální legislativa České republiky a Slovenské republiky týkající se ochrany osobních údajů

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ZA ÚLOŽIŠTĚ

2.1 Úložiště

Společnost První certifikační autorita, a.s., zřizuje a provozuje úložiště veřejných i neveřejných informací.

2.2 Zveřejňování certifikačních informací

Základní adresy (dále též informační adresy), na nichž lze získat 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.

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

Bližší informace týkající se systému e-Kasa jsou zveřejňovány na webu www.financnasprava.sk.

2.3 Čas nebo četnost zveřejňování

Čas nebo četnost zveřejňování informací na webu www.financnasprava.sk závisí na rozhodnutí FR SR.

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 příslušnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

Zveřejňování informací na webu www.financnasprava.sk je plně v kompetenci FR SR.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Veškerá jména jsou konstruována v souladu s platnými technickými standardy a normami.

3.1.2 Požadavek na významovost jmen

V procesu vydávání Certifikátu je vždy vyžadována významovost všech jmen uvedených v položkách pole Subject, resp. rozšíření SubjectAlternativeName. Podporované položky tohoto pole a rozšíření jsou uvedeny v kapitole 7.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Certifikáty vydávané podle této CP nepodporují anonymitu ani používání pseudonymu.

3.1.4 Pravidla pro interpretaci různých forem jmen

Údaje uváděné v žádosti o Certifikát (formát PKCS#10) se do pole Subject, resp. rozšíření SubjectAlternativeName ve vydávaných Certifikátech přenášejí ve tvaru, ve kterém jsou uvedeny v předkládané žádosti.

3.1.5 Jedinečnost jmen

Autorita zaručuje jedinečnost pole Subject v Certifikátu příslušného držitele soukromého klíče, resp. držitele tohoto Certifikátu.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Není relevantní pro tento dokument, Certifikáty neobsahují obchodní značky.

3.2 Počáteční ověření identity

Ověřování identity Subjektů a operátorů GUI je plně v kompetenci FR SR. Pro ověřování identity fyzické osoby a organizace v případě Certifikátu vlastněného I.CA platí pravidla popsaná v kapitolách 3.2.2 a 3.2.3.

3.2.1 Ověřování vlastnictví soukromého klíče

Vlastnictví soukromého klíče odpovídajícího veřejnému klíči v žádosti o Certifikát se prokazuje předložením žádosti ve formátu PKCS#10. Ta je zmíněným soukromým klíčem elektronicky podepsána / opatřena elektronickou pečetí a držitel soukromého klíče tak prokazuje, že v době tvorby elektronického podpisu / elektronické pečetě soukromý klíč vlastnil.

3.2.2 Ověřování identity organizace

Pro ověření I.CA v případě žádosti o Certifikát Autority nebo certifikát OCSP respondéru musí být předložen:

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

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

Ověřování v případě ostatních Certifikátů je v kompetenci FR SR.

3.2.3 Ověřování identity fyzické osoby

Pro vydávání Certifikátu Autority nebo Certifikátu OCSP respondéru pro osobu zastupující I.CA platí, že je vyžadován osobní doklad obsahující údaje uvedené níže v této kapitole. Osobním dokladem pro občany ČR musí být platný občanský průkaz nebo cestovní pas. Osobním dokladem pro cizince je platný cestovní pas, nebo jím v případě občanů členských států EU může být platný osobní doklad, sloužící k prokazování totožnosti na území příslušného státu.

Z tohoto dokladu jsou ověřovány následující údaje:

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

Pokud osoba zastupující I.CA není osobou ze zákona oprávněnou k zastupování, je dále požadována úředně ověřená plná moc k zastupování I.CA podepsaná statutárním zástupcem I.CA.

Ověřování v případě ostatních Certifikátů je v kompetenci FR SR.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Všechny informace v žádosti o vydání Certifikátu Autority a Certifikátu OCSP respondéru musí být ověřeny. Pro Certifikáty ostatních typů je to v kompetenci FR SR.

3.2.5 Ověřování kompetencí

Není relevantní pro tento dokument.

3.2.6 Kritéria pro interoperabilitu

Není relevantní pro tento dokument.

3.3 Identifikace a autentizace při požadavku na výměnu klíče

Není relevantní pro tento dokument, služba výměny veřejného klíče v Certifikátu není poskytována. Je nutné vydat nový Certifikát s novým veřejným klíčem.

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Viz kapitola 3.3.

3.3.2 Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu

Viz kapitola 3.3.

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Subjekty oprávněné podat žádost o zneplatnění jednotlivých typů Certifikátů jsou vyjmenovány v kapitole 4.9.2.

Žádost o zneplatnění Certifikátu vlastněného I.CA musí být podepsaná ředitelem I.CA, nebo jím písemně pověřenou osobou, identita musí být řádně ověřena osobním dokladem (viz kapitola 3.2.3).

Žádost o zneplatnění ostatních typů Certifikátů musí být elektronicky podepsána / opatřena elektronickou pečetí modulem PKI e-Kasa.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

O vydání Certifikátu může požádat:

- I.CA prostřednictvím osoby, která ji zastupuje v případě Certifikátů vlastněných I.CA, pro kontrolu identity platí požadavky kapitol 3.2.2 a 3.2.3,
- FR SR v případě ostatních typů Certifikátů, a to výhradně elektronicky prostřednictvím spojení mezi modulem PKI e-KASA a zařízením ICARA, žádost ve formátu PKCS#10 musí být dále elektronicky podepsána / opatřena elektronickou pečetí modulem PKI e-KASA.

4.1.2 Registrační proces a odpovědnosti

Registrační proces v případě Certifikátů vlastněných I.CA provádí speciální registrační autorita, které jsou předkládány příslušné doklady.

Registrační proces v případě ostatních typů Certifikátů je plně v kompetenci FR SR.

Poskytovatel Služby je povinen zejména:

- předat organizaci FR SR Certifikát Autority,
- činnosti spojené se Službou poskytovat v souladu s Kontraktem, touto CP, příslušnou CPS, Systémovou bezpečnostní politikou CA a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Provádění identifikace a autentizace

Při vydávání Certifikátu vlastněného I.CA jsou identifikace a autentizace prováděny podle kapitol 3.2.2 a 3.2.3.

Pro ostatní typy Certifikátů není relevantní.

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

V procesu rozhodování o přijetí nebo zamítnutí žádosti o vydání Certifikátu vlastněného I.CA je prováděna identifikace a autentizace dle kapitol 3.2.2 a 3.2.3. Pokud některá z kontrol skončí negativně, proces vydání Certifikátu je ukončen.

V procesu rozhodování o přijetí nebo zamítnutí žádosti o vydání ostatních typů Certifikátů jsou prováděny pouze formální kontroly (délky položek, syntaxe položky organizationIdentifier, vlastnictví soukromého klíče). Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen, v opačném případě je postupováno v souladu s ustanoveními kapitoly 4.3.

4.2.3 Doba zpracování žádosti o certifikát

Pro Certifikáty vlastněné I.CA není doba zpracování explicitně uvedena, obvykle platí, že nepřesáhne tři pracovní dny. Pro Certifikát OCSP serveru je doba vydání do 15 minut a jen ve výjimečných případech může být tato doba delší,

Vydání ostatních typů Certifikátů probíhá automatizovaně a maximální doba vydání je uvedena v Kontraktu.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

Ověřování vlastnictví soukromého klíče, podporované hashovací funkce v žádosti o Certifikát (minimálně sha-256) a kontroly formální správnosti údajů jsou prováděny programovým vybavením jádra systému CA. Pokud některá z kontrol skončí negativně, proces vydání Certifikátu je ukončen.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

Pro Certifikáty vlastněné I.CA není relevantní, zástupce držitele je vydání přítomen.

Koncovému uživateli, tj. Subjektu, je Certifikát předán způsobem definovaným v Kontraktu.

Operátorovi GUI zasílá vydaný Certifikát Autorita e-mailem.

V případě Certifikátu modulu PKI e-Kasa je z vydaného Certifikátu vytvořena struktura ve formátu PKCS#12 a tato je bezpečným způsobem předána organizaci FR SR.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pro vlastněné I.CA není relevantní, I.CA je poskytovatelem služeb a nepřevzetí Certifikátu nepřichází v úvahu.

Pro ostatní typy Certifikátů není relevantní, certifikáty jsou zaslány systému e-Kasa.

4.4.2 Zveřejňování certifikátů certifikační autoritou

Certifikáty nejsou zveřejňovány, seznam vydaných je k dispozici pouze v rámci systému e-Kasa.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Není relevantní pro tento dokument, vydání Certifikátů není jiným subjektům oznamováno.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností všech držitelů Certifikátů je zejména:

- užívat soukromý klíč a odpovídající Certifikát vydaný podle této CP pouze pro účely stanovené v této CP,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v Certifikátu vydaném podle této CP, takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- neprodleně požádat o zneplatnění Certifikátu, pokud vniklo podezření, že soukromý klíč byl zneužit, požádat a ukončit používání příslušného soukromého klíče.

Povinností FR SR je zprostředkovat tato pravidla Subjektům a operátorům GUI.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje Certifikát Autority související s dalšími typy Certifikátů vydanými podle této CP, ověřit hodnoty jejich otisků a jejich platnost,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že Certifikát je platný,
- dodržovat veškerá ustanovení této CP.

4.6 Obnovení certifikátu

Není relevantní pro tento dokument, služba obnovení Certifikátu není poskytována. Je nutné vydat nový Certifikát s novým veřejným klíčem.

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Kdo může žádat o obnovení

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

Viz kapitola 4.6.

4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.6.

4.7 Výměna veřejného klíče v certifikátu

Není relevantní pro tento dokument, služba výměny veřejného klíče v Certifikátu není poskytována. Je nutné vydat nový Certifikát s novým veřejným klíčem.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.2 Kdo může žádat o výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Viz kapitola 4.7.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Viz kapitola 4.7.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.7.

4.8 Změna údajů v certifikátu

Není relevantní pro tento dokument, služba změny údajů v Certifikátu není poskytována. Je nutné vydat nový Certifikát s novým veřejným klíčem.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádost o zneplatnění Certifikátů vlastněných I.CA podává ředitel I.CA prostřednictvím speciální registrační autority.

Žádost o zneplatnění ostatních typů Certifikátů je možné podat pouze elektronickou cestou, a to z modulu PKI e-Kasa do zařízení ICARA. Žádost o zneplatnění musí být elektronicky podepsána / opatřena elektronickou pečetí vytvořenými soukromým klíčem odpovídajícím klíči veřejnému v Certifikátu modulu PKI e-Kasa.

Službu pozastavení platnosti Certifikátu I.CA neposkytuje.

4.9.1 Podmínky pro zneplatnění

Certifikát musí být zneplatněn mj. na základě následujících okolností:

- dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci soukromého klíče odpovídajícího veřejnému klíči tohoto Certifikátu,
- je porušeno ustanovení Smlouvy nebo Kontraktu o poskytování Služby podle této CP ze strany držitele Certifikátu,
- pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném Certifikátu.

I.CA si vyhrazuje právo akceptování i jiných postupů na zneplatnění Certifikátu, které však nesmí být v rozporu se Kontraktem.

4.9.2 Kdo může požádat o zneplatnění

Žádost o zneplatnění Certifikátu mohou podat:

- poskytovatel této Služby (oprávněným žadatelem o zneplatnění Certifikátu vydaného I.CA je v tomto případě ředitel I.CA):
  - pokud prokazatelně zjistí, že soukromý klíč, patřící k veřejnému klíči uvedenému v Certifikátu, byl kompromitován,
  - dozví-li se prokazatelně, že Certifikát byl použit v rozporu s omezením definovaným v kapitole 1.4.2,
  - pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném certifikátu,
- FR SR v případě Certifikátů Subjektů, operátorů GUI a modulu PKI e-Kasa výhradně elektronickou cestou.

4.9.3 Postup při žádosti o zneplatnění

Žádost o zneplatnění Certifikátu podávaná ředitelem I.CA musí být písemná. Musí obsahovat jednak sériové číslo zneplatňovaného Certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“) a dále důvod zneplatnění, možné důvody jsou uvedeny v kapitole 4.9.2.

Žádost o zneplatnění Certifikátu podaná organizací FR SR může být podána pouze elektronickou cestou a musí být elektronicky podepsána / opatřena elektronickou pečetí vytvořenými soukromým klíčem modulu PKI e-Kasa. Žádost musí obsahovat sériové číslo zneplatňovaného Certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“), případně důvod zneplatnění. Datum a čas zneplatnění Certifikátu jsou dány zpracováním této žádosti informačním systémem CA, informace o výsledku zpracování žádosti je systémem ICARA zaslána zpět modulu PKI e-Kasa.

4.9.4 Prodleva při požadavku na zneplatnění certifikátu

Požadavek na zneplatnění Certifikátu musí být podán bezodkladně.

4.9.5 Doba zpracování žádosti o zneplatnění

Maximální doba mezi přijetím žádosti o zneplatnění Certifikátu podané písemně ředitelem I.CA a jeho zneplatněním je 24 hodin.

Maximální doba mezi přijetím žádosti o zneplatnění Certifikátu podané organizací FR SR a jeho zneplatněním je 24 hodin. Prakticky, protože se jedná o automatizovaný proces, je

zneplatnění provedeno okamžitě po přijetí žádosti, o zneplatnění je vrácena odpověď na příslušnou žádost.

4.9.6 Povinnosti třetích stran při kontrole zneplatnění

Spoléhající se strany jsou povinny provádět veškeré úkony uvedené v kapitole 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je vydáván neprodleně po kladném zpracování žádosti o zneplatnění Certifikátu. Nedojde-li ke zneplatnění Certifikátu, je nový CRL vydáván zpravidla dvakrát denně, nejvýše však 24 hodin od vydání předchozího CRL.

Činnosti operátorů CA v procesu vytváření a vydávání CRL jsou popsány v interní dokumentaci.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL je vždy vydán nejvýše 24 hodin od vydání předchozího CRL.

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Služba ověřováni stavu Certifikátu s využitím protokolu OCSP je dostupná.

OCSP odpovědi vyhovují normám RFC 2560 a RFC 5019. Certifikát OCSP respondéru obsahuje rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 2560.

4.9.10 Požadavky při ověřování stavu certifikátu on-line

Viz kapitola 4.9.9.

4.9.11 Jiné možné způsoby oznamování zneplatnění

Není relevantní pro tento dokument.

4.9.12 Zvláštní postupy při kompromitaci klíče

Postup pro zneplatnění Certifikátu v případě kompromitace soukromého klíče není odlišný od výše popsaného postupu pro zneplatnění Certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Není relevantní pro tento dokument, služba pozastavení platnosti Certifikátu není poskytována.

4.9.14 Kdo může požádat o pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti Certifikátu není poskytována.

4.9.15 Postup při žádosti o pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti Certifikátu není poskytována.

4.9.16 Omezení doby pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti Certifikátu není poskytována.

4.10 Služby ověřování stavu certifikátu

4.10.1 Funkční charakteristiky

Distribuční místa CRL jsou uvedena ve vydávaných Certifikátech, stejně jako odkaz na službu OCSP poskytující informace o stavu Certifikátu on-line.

4.10.2 Dostupnost služeb

Autorita garantuje zajištění nepřetržité dostupnosti (7 dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných Certifikátů a seznamu zneplatněných certifikátů (platné CRL), a dále dostupnost služby OCSP.

4.10.3 Další charakteristiky služeb stavu certifikátu

Není relevantní pro tento dokument, další charakteristiky služeb stavu certifikátu nejsou poskytovány.

4.11 Konec smlouvy o vydávání certifikátů

Po ukončení platnosti Kontraktu přetrvávají z něho vyplývající závazky I.CA, a to po dobu platnosti posledního Certifikátu.

4.12 Úschova a obnova klíčů

Není relevantní pro tento dokument, služba úschovy soukromého klíče není poskytována.

4.12.1 Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Viz kapitola 4.12.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Postupy správy, řízení a provozu jsou zaměřeny především na:

- systémy poskytovaných určené k podpoře Služby,
- veškeré procesy podporující poskytování Služby.

Postupy správy, řízení a provozu jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, Systémová bezpečnostní politika CA a TSA - důvěryhodné systémy pro vydávání certifikátů a časových razítek, Certifikační prováděcí směrnice, Plán pro zvládání krizových situací a plán obnovy, tak v upřesňující interní dokumentaci. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

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

Důvěryhodné systémy určené k podpoře Služby jsou umístěny 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. 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, kde jsou umístěny důvěryhodné systémy určené k podpoře 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

Důvěryhodné systémy určené k podpoře Služby 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 umístěny důvěryhodné systémy k podpoře 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.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu

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

5.2 Procedurální postupy

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, který by mohl ohrozit nestrannost operací I.CA.

5.2.2 Počet osob požadovaných pro zajištění jednotlivých činností

Pro procesy související s párovými daty certifikační autority a OCSP respondéru jsou definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

- inicializaci kryptografického modulu,
- generování párových dat Autority a jejího OCSP respondéru,
- ničení soukromého klíče Autority a jejího OCSP respondéru,
- zálohování soukromého klíče certifikační autority,
- obnovu soukromého klíče Autority a jejího OCSP respondéru,
- aktivaci a deaktivaci soukromého klíče Autority.

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 v I.CA jsou přiděleny prostředky pro řádnou identifikaci (jméno, certifikát) a autentizaci (heslo, soukromý klíč) 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 postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

Zaměstnanci I.CA v důvěryhodných rolích jsou vybíráni a přijímáni na základě dále popsaných personálních kritérií:

- občanská bezúhonnost - prokazováno výpisem z rejstříku trestů, nebo čestným prohlášením,
- 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 odpovídající poskytované Službě,
- 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.

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.

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

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem popsaným v interní dokumentaci 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 upraveny bilaterálními obchodními smlouvami. Jedná se o např. dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími certifikačními politikami, relevantními částmi interní dokumentace, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci I.CA mají k dispozici kromě certifikační politiky, certifikační prováděcí směrnice, bezpečnostní a provozní dokumentace 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 technickými standardy a normami, mj. o životním cyklu Certifikátů.

Speciálním případem zaznamenávání událostí je generování párových dat Autority, přičemž minimálně platí, že:

- je prováděno podle připraveného scénáře ve fyzicky zabezpečeném prostředí,
- je prováděno za účasti ředitele I.CA, nebo jím pověřené osoby,
- o průběhu generování ve vytvořen protokol, který podepisují jako svědkové ředitel I.CA, nebo jím pověřená osoba a další osoba jmenovaná do důvěryhodné role.

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 auditních 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

Auditní záznamy jsou uchovávány po dobu určenou FR SR, tedy deseti let.

5.4.4 Ochrana auditních záznamů

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

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

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

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

5.4.5 Postupy pro zálohování auditních záznamů

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

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů CA 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 určenými k podpoře Služby je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

Uchovávání záznamů, tj. informací a dokumentace, je ve společnosti První certifikační autorita, a.s., 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:

- záznamy související s životním cyklem vydaných Certifikátů, včetně těchto Certifikátů,
- další záznamy potřebné pro vydávání, resp. zneplatňování Certifikátů,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentaci.

5.5.2 Doba uchování záznamů

Záznamy vztahující se k Certifikátům Autority a OCSP respondérů, s výjimkou příslušných soukromých klíčů, jsou uchovávány po celou dobu existence I.CA. Ostatní záznamy a dokumentace jsou uchovávány v souladu s ustanoveními kapitoly 5.4.3.

Postupy při uchovávání záznamů jsou upraveny v interní dokumentaci.

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 záznamů jsou upraveny v interní dokumentaci.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny v interní dokumentaci.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

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

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

Záznamy jsou ukládány na místo určené ředitelem I.CA.

Samotná problematika přípravy a způsobu ukládání záznamů v elektronické i písemné podobě je upravena v interní dokumentaci. Shromažďování uchovávaných záznamů je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací

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

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

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

V případě standardních situací (uplynutí platnosti Certifikátu certifikační autority) je výměna prováděna s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto Certifikátu). V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu vydávání certifikátů, tzn. změny kryptografických algoritmů, délky klíčů atd.) je vydání nového Certifikátu certifikační autority prováděno v adekvátním, co nejkratším časovém období.

Jak v případě standardních, tak nestandardních situací je výměna veřejného klíče v Certifikátu certifikační autority s předstihem, je-li to možné, oznámena způsobem definovaným v Kontraktu.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 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.

5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče

V případě vzniku důvodné obavy z kompromitace soukromého klíče Autority postupuje I.CA tak, že:

- ukončí jeho používání,
- okamžitě a trvale zneplatní příslušný Certifikát a zničí jemu odpovídající soukromý klíč,

- zneplatní všechny platné Certifikáty ostatních typů,
- bezodkladně o této skutečnosti, včetně důvodu, způsobem definovaným v Kontraktu informuje FR SR.

Obdobný postup bude uplatněn i v případě, že dojde k takovému vývoji kryptoanalytických metod (např. změny kryptografických algoritmů, délky klíčů atd.), že by mohla být bezprostředně ohrožena bezpečnost Služby.

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interní dokumentací.

5.8 Ukončení činnosti CA nebo RA

V případě ukončení činnosti poskytování Služby bude postupováno v souladu s Kontraktem.

V případě ukončování činnosti certifikační autority se jedná o řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení. Po dobu platnosti i jen jediného Certifikátu musí být zajištěna služby zneplatňování Certifikátů, vydávání CRL a poskytování služby OCSP. Následně certifikační autorita prokazatelně zničí soukromý klíč svůj i soukromý klíč OCSP respondéru a o zničení provede záznam, který bude uchováván podle pravidel této CP.

Pro ukončení činnosti RA není relevantní.

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat Autority je prováděno v zabezpečených vyhrazených prostorách provozního pracoviště, podle předem připraveného scénáře, v souladu s požadavky kapitol 5.2 a 5.4.1. O jeho průběhu je vyhotoven písemný protokol.

Generování párových dat OCSP respondéru Autority je rovněž prováděno v zabezpečených vyhrazených prostorách provozního pracoviště. O jeho průběhu je vyhotoven písemný protokol.

Generování párových dat pro certifikáty operátorů GUI, certifikát modulu PKI e-Kasa a certifikáty Subjektů je v plně kompetenci FR SR.

Generování párových dat pracovníků podílejících se na činnosti systémů poskytujících Službu na straně I.CA je prováděno na čipových kartách, splňujících požadavky na QSCD. Soukromé klíče těchto párových dat jsou na čipové kartě uloženy v neexportovatelném tvaru a k jejich použití je nutné zadat PIN.

6.1.2 Předávání soukromého klíče jeho držiteli

Pro soukromý klíč Autority není relevantní, klíč je generován v kryptografickém modulu, který je pod výhradní kontrolou I.CA.

Pro soukromý klíč OCSP respondéru Autority rovněž není relevantní - soukromý klíč je generován přímo v OCSP respondéru a v zašifrovaném tvar je v něm uložen.

Služba generování párových dat Subjektům, operátorům GUI a modulu PKI e-Kasa není poskytována.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Veřejné klíče Subjektů, operátorů GUI, modulu PKI e-Kasa a OCSP respondéru Autority jsou Autoritě doručeny v žádosti (formát PKCS#10) o vydání Certifikátu.

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Veřejný klíč Autority je obsažen v jejím Certifikátu, který je organizaci FR SR předán způsobem definovaným v Kontraktu.

6.1.5 Délky klíčů

Pro Službu poskytovanou podle této CP je výhradně využíván asymetrický algoritmus RSA. Mohutnost klíče (resp. parametrů daného algoritmu) Certifikátu Autority je 4096 bitů, mohutnost klíčů (resp. parametrů daného algoritmu) v ostatních typech vydávaných Certifikátů je 2048 bitů.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejného klíče Autority a jejího OCSP respondéru splňují požadavky uvedené v technických standardech nebo normách.

Parametry algoritmů použitých při generování veřejných klíčů ostatních typů Certifikátů musí tyto požadavky rovněž splňovat.

I.CA kontroluje povolenou délku klíčů a možný dvojí výskyt veřejného klíče ve vydávaných Certifikátech. V případě duplicitního výskytu je příslušný Certifikát neprodleně zneplatněn, FR SR o tomto neprodleně a vhodným způsobem informována a vyzvána ke generování nových párových dat.

6.1.7 Účely použití klíče (dle rozšíření key usage X.509 v3)

Možnosti použití klíče jsou uvedeny v rozšíření Certifikátu.

6.2 Ochrana soukromého klíče a technologie kryptografických modulů

6.2.1 Řízení a standardy kryptografických modulů

Generování párových dat soukromého klíče Autority je prováděno v kryptografickém modulu podle scénáře popsaného v interní dokumentaci. Následně je soukromý klíč uložen v bezpečném světu (Security World) tohoto kryptografického modulu.

6.2.2 Soukromý klíč pod kontrolou více osob (n z m)

Pokud je pro činnosti spojené s kryptografickým modulem nezbytná přítomnost dvou členů vedení I.CA, potom každý z nich zná část pouze kódu k provedení těchto činností.

6.2.3 Úschova soukromého klíče

Není relevantní pro tento dokument, služba úschovy soukromého klíče není poskytována.

6.2.4 Zálohování soukromého klíče

Kryptografický modul použitý pro správu párových dat Autority ukládá soukromé klíče v tzv. bezpečném světu, což je bezpečně zašifrovaná adresářová struktura. Zálohování soukromého klíče představuje běžnými prostředky prováděnou zálohu této adresářové struktury. O provedeném zálohování je vždy pořízen záznam.

Pro obnovu soukromého klíče z takto vytvořené zálohy jsou zapotřebí čipové karty kryptografického modulu, na kterých jsou rozděleně uloženy šifrovací klíče záloh. O provedené obnově je vždy pořízen záznam.

6.2.5 Uchovávání soukromého klíče

Po uplynutí doby platnosti soukromého klíče Autority je tento včetně záloh zničen.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Transfer soukromého klíče do nebo z kryptografického modulu probíhá pouze v rámci běžné činnosti bezpečného světa a je řízen kryptografickým modulem.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromý klíč Autority je uložen v kryptografickém modulu, resp. v jeho bezpečném světu - viz kapitola 6.2.11.

6.2.8 Postup aktivace soukromého klíče

Aktivace soukromého klíče Autority i soukromého klíče OCSP respondéru je prováděna postupem popsaným v interní dokumentaci. O provedené aktivaci je pořízen písemný záznam.

6.2.9 Postup deaktivace soukromého klíče

Deaktivace soukromého klíče Autority i OCSP respondéru je provedena aktivací klíče nového. O provedené deaktivaci je pořízen písemný záznam.

6.2.10 Postup ničení soukromého klíče

Ničení soukromého klíče Autority je prováděno vždy na všech počítačích bezpečného světa. Externí média, na kterých jsou uloženy zálohy tohoto soukromého klíče jsou rovněž zničena. Ničení spočívá ve fyzické destrukci nosičů a probíhá za přímé osobní účasti nejméně dvou členů vedení I.CA podle přesně určeného postupu, který je upraven v interní dokumentaci. O provedeném ničení je pořízen písemný záznam.

6.2.11 Hodnocení kryptografických modulů

Kryptografický modul, sloužící ke generování párových dat a uložení soukromého klíče Autority v bezpečném světu tohoto modulu je certifikován dle CC s mírou záruky EAL4+.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

Veřejné klíče Autority a jejího OCSP respondéru jsou uchovávány po celou dobu existence I.CA.

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

Maximální doba platnosti každého vydaného Certifikátu je uvedena v těle tohoto Certifikátu, pro Certifikáty Subjektů jsou to obvykle dva roky.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivačními daty soukromého klíče Autority je šifrovací klíč bezpečného světa generovaný během vytváření bezpečné světa s využitím administrátorských čipových karet.

Aktivačními daty soukromého klíče OCSP respondéru je heslo vytvořené při generování tohoto klíče.

6.4.2 Ochrana aktivačních dat

Aktivační data soukromého klíče Autority jsou uložena v kryptografickém modulu.

Aktivační data soukromého klíče OCSP respondéru Autority jsou uložena přímo v kódu OCSP respondéru.

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data Autority jsou určena výhradně pro činnost bezpečného světa použitého kryptografického modulu.

Aktivační data OCSP respondéru Autority jsou určena výhradně pro poskytování OCSP odpovědí na stav vydaného Certifikátu a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent důvěryhodných systémů určených k podpoře Služby je definována v technických standardech a normách.

6.5.2 Hodnocení počítačové bezpečnosti

Systém e-Kasa je z hlediska nařízení eIDAS uzavřeným systémem a požadavky zmíněného nařízení a navazujících technických standardů a norem pro něj nejsou závazné. Každopádně tyto požadavky byly v maximální míře, s omezeními danými požadavky FR SR na systém, dodrženy. Popsány jsou zejména v následujících dokumentech, podle kterých je počítačová bezpečnost v I.CA hodnocena:

- 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 na poskytovatele důvěryhodných služeb podporující elektronické podpisy.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 403 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatelů důvěryhodných služeb - Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb.

- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ČSN ETSI EN 319 411-1 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 1: Obecné požadavky.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- EN 301 549 Accessibility requirements for ICT products and services.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.
- 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.

Činnost Autority se dále řídí požadavky technických standardů a norem:

- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation.
- ISO 3166-1 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.
- ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.
- RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
- RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- ČSN ETSI EN 319 412-1 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 1: Přehled a společné datové struktury.
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ČSN ETSI EN 319 412-2 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám.

- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ČSN ETSI EN 319 412-3 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 3: Profil certifikátu pro certifikáty vydávané právnickým osobám.
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to legal persons.

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.6.2 Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu se standardy, je prováděna 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.

6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je v I.CA 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.

6.7 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 s modulem PKI e-Kasa je vedena šifrovaně.

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

tab. 4 - Certifikát ~~A~~utority

Pole	Obsah
Version	v3 (0x2)
serialNumber	jedinečné sériové číslo certifikátu
SignatureAlgorithm	sha512withRSAEncryption
Issuer	
commonName	e-Kasa SK CA/RSA *MM/RRRR**
organizationName	První certifikační autorita, a.s.
Country	CZ
organizationIdentifier	NTRCZ-26439395
Validity	
notBefore	počátek platnosti Certifikátu (UTC)
notAfter	počátek platnosti Certifikátu + 10 let (UTC)
Subject	viz Issuer
SubjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	4096 bitů
Extensions	viz tab. 9
Signature	elektronický podpis / elektronická pečeť vydavatele (self-signed certifikát)

* *MM/RRRR* - měsíc a rok vydání certifikátu

tab. 5 - Certifikátu OCSP respondéru

Pole	Obsah	Poznámka
Version	v3 (0x2)	
serialNumber	jedinečné sériové číslo vydávaného certifikátu	
SignatureAlgorithm	sha256withRSAEncryption	
Issuer	viz tab. 4	
Validity	110 dnů	

Subject		
commonName	OCSP responder – *<Subject.CN vydávající CA>*	
organizationName	První certifikační autorita, a.s.	
countryName	CZ	
organizationIdentifier	NTRCZ-26439395	
SubjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	2048	
Extensions	viz tab. 10	
Signature	elektronický podpis / elektronická pečeť vydavatele (Autority)	

tab. 6 - Certifikát operátora GUI

Všechny položky pole Subject[2] jsou převzaty ze žádosti o certifikát s výjimkou položek vytvořených Autoritou. Povinné položky musí být v žádosti obsaženy.

Položka	**Obsah položky**	**Poznámka**
Version	v3 (0x2)	
serialNumber	jedinečné sériové číslo vydávaného certifikátu	
SignatureAlgorithm	sha256withRSAEncryption	
Issuer	viz tab. 4	
Validity	365 dní	
Subject		
commonName	povinná, jediný výskyt: jméno a příjmení fyzické osoby v roli operátora GUI	případně doplněno tituly před/za jménem
givenName	povinná, jediný výskyt: jméno fyzické osoby v roli operátora GUI	
surName	povinná, jediný výskyt: příjmení fyzické osoby v roli operátora GUI	
organizationName	název organizace	
countryName	SK	

[2] I.CA si vyhrazuje právo upravit množinu položek a obsah pole Subject, vyžadovanou např. aktualizacemi standardů ETSI.

SubjectPublicKeyInfo		
Algorithm	rsaEncryption	
subjectPublicKey	2048	
Extensions	viz tab. 11	
Signature	elektronický podpis / elektronická pečeť vydavatele (Autority)	

tab. 7 – Certifikát modulu PKI e-Kasa

Všechny položky pole Subject[3] jsou převzaty ze žádosti o certifikát s výjimkou položek vytvořených Autoritou. Povinné položky musí být v žádosti obsaženy.

Položka	Obsah položky	Poznámka
Version	v3 (0x2)	
serialNumber	jedinečné sériové číslo vydávaného certifikátu	
SignatureAlgorithm	sha256withRSAEncryption	
Issuer	viz tab. 4	
Validity	365 dní	
Subject		
commonName	PKI e-Kasa	
countryName	SK	
SubjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	2048	
Extensions	viz tab. 12	
Signature	elektronický podpis / elektronická pečeť vydavatele (Autority)	

tab. 8 - Certifikát daňového subjektu

Všechny položky pole Subject[2] jsou převzaty ze žádosti o certifikát s výjimkou položek vytvořených Autoritou. Povinné položky musí být v žádosti obsaženy.

Pole	Obsah položky	Poznámka
Version	v3 (0x2)	
serialNumber	jedinečné sériové číslo vydávaného certifikátu	

[3] I.CA si vyhrazuje právo upravit množinu položek a obsah pole Subject, vyžadovanou např. aktualizacemi standardů ETSI.

SignatureAlgorithm	sha256WithRSA	
Issuer	viz tab. 4	
Validity	2 roky	
Subject		
commonName	VATSK-*YYYYYYYY* POKLADNICA *XXXXXXXX*	povinná, jediný výskyt kde *YYYYYYYY* je identifikační číslo organizace, *XXXXXXXX* CashRegisterCode
countryName	SK	povinná, jediný výskyt
organizationalUnitName	*XXXXXXXX*	povinná, jediný výskyt kde *XXXXXXXX* je CashRegisterCode povolené hodnoty: 0-9 rozsah {16,17}
organizationIdentifier	VATSK-*YYYYYYYY*	povinná, jediný výskyt, kde *YYYYYYYY* je identifikační číslo organizace
SubjectPublicKeyInfo		
algorithm	rsaEncryption	
subjectPublicKey	2048	
Extensions	viz tab. 13	
Signature	elektronický podpis / elektronická pečeť vydavatele (Autority)	

7.1.1 Číslo verze

Vydávané certifikáty jsou v souladu se standardem X.509 ve verzi 3.

7.1.2 Rozšíření certifikátu

tab. 9 – Rozšíření certifikátu Autority

Pole	Obsah	Poznámka
CertificatePolicies		nekritické, vytváří CA
PolicyInformation		
policyIdentifier	2.5.29.32.0 (anyPolicy)	
BasicConstraints		kritická
cA	True	

KeyUsage	keyCertSign, crlSign	kritická
SubjectKeyIdentifier KeyIdentifier	hash veřejného klíče vydavatele (Autorita)	nekritické

tab. 10 - Rozšíření certifikátu OCSP respondéru

Položka	Obsah	Poznámka
CertificatePolicies.		generuje CA nekritická, povinná
PolicyInformation(1)		
policyIdentifier	viz kapitola 1.2	
authorityInformationAccess		nekritická, povinná
id-ad-caIssuers	http://ekasa.ica.cz/ekasa*RR**_rsa.cer	URI (http) souboru, který obsahuje pouze certifikát příslušné CA
BasicConstraints		nekritická, povinná
cA	False	
KeyUsage	digitalSignature	kritická, povinná
ExtendedKeyUsage	id-kp-OCSPSigning	kritická, povinná
id-pkix-ocsp-nocheck	NULL	
SubjectKeyIdentifier	hash veřejného klíče ve vydávaném certifikátu	nekritická, povinná
AuthorityKeyIdentifier KeyIdentifier	hash veřejného klíče vydavatele (Autorita)	nekritická

* *RR* - rok vydání certifikátu CA

tab. 11 - Rozšíření certifikátu operátora GUI

Položka	Obsah/Kritičnost	Poznámka
CertificatePolicies		nekritická, povinná
PolicyInformation		
policyIdentifier	viz kapitola 1.2	
BasicConstraints		nekritická, povinná
cA	False	
KeyUsage	digitalSignature, nonRepudiation, keyEncipherment	kritická, povinná
SubjectKeyIdentifier	hash veřejného klíče ve	nekritická, povinná

	vydávaném certifikátu	
AuthorityKeyIdentifier KeyIdentifier	hash veřejného klíče vydavatele (Autorita)	nekritická, povinná
SubjectAlternativeName		nekritická, povinná
rfc822Name	e-mail adresa fyzické osoby v roli operátora GUI	nekritická, povinná
CRLDistributionPoints	http://ecrldp1.ica.cz/ekasa*RR**_rsa.crl http://ecrldp2.ica.cz/ekasa*RR**_rsa.crl	generuje CA nekritická, povinná
authorityInformationAccess		generuje CA nekritická, povinná
id-ad-ocsp	http://eocsp.ica.cz/ekasaRR*_rsa	
id-ad-caIssuers	http://ekasa.ica.cz/ekasaRR*_rsa.cer	

* *RR* - rok vydání certifikátu CA

tab. 12 - Rozšíření certifikátu modulu PKI e-Kasa

Položka	**Obsah/Kritičnost**	**Poznámka**
CertificatePolicies		nekritická, povinná
PolicyInformation(1)		
policyIdentifier	viz kapitola 1.2	
BasicConstraints		nekritická, povinná
cA	False	
KeyUsage	digitalSignature, nonRepudiation, keyEncipherment	kritická, povinná
SubjectKeyIdentifier	hash veřejného klíče ve vydávaném certifikátu	nekritická, povinná
AuthorityKeyIdentifier KeyIdentifier	hash veřejného klíče vydavatele (Autorita)	nekritická, povinná
CRLDistributionPoints	http://ecrldp1.ica.cz/ekasa*RR**_rsa.crl http://ecrldp2.ica.cz/ekasa*RR**_rsa.crl	generuje CA nekritická, povinná
authorityInformationAccess		generuje CA nekritická, povinná

id-ad-ocsp	http://eocsp.ica.cz/ekasa*RR**_rsa	
id-ad-caIssuers	http://ekasa.ica.cz/ekasa*RR**_rsa.cer	

* RR - rok vydání certifikátu CA

tab. 13 - Rozšíření certifikátu daňového subjektu

Položka	**Obsah/Kritičnost**	**Poznámka**
CertificatePolicies		generuje CA nekritická, povinná
PolicyInformation(1)		
policyIdentifier	viz kapitola 1.2	
CRLDistributionPoints	http://ecrldp1.ica.cz/ekasa*RR**_rsa.crl http://ecrldp2.ica.cz/ekasa*RR**_rsa.crl	generuje CA nekritická, povinná
authorityInformationAccess		generuje CA nekritická, povinná
id-ad-ocsp	http://eocsp.ica.cz/ekasa*RR**_rsa	
id-ad-caIssuers	http://ekasa.ica.cz/ekasa*RR**_rsa.cer	
BasicConstraints		generuje CA nekritická, povinná
cA	False	
KeyUsage	na základě obsahu žádosti o certifikát jedna z možností (v případě absence tohoto rozšíření v žádosti bude doplněna třetí možnost): ▪ nonRepudiation, ▪ digitalSignature, nonRepudiation, ▪ digitalSignature, nonRepudiation a keyEncipherment,	generuje CA kritická, povinná v případě, že žádost bude obsahovat nepodporované použití, bude odebráno
ExtendedKeyUsage	id-kp-clientAuth	bude získáno z žádosti zadává klient volitelná, nekritická, nepodporované použití bude odebráno

		(konzistence s KU)
SubjectKeyIdentifier	hash veřejného klíče ve vydávaném certifikátu	generuje CA nekritická, povinná
AuthorityKeyIdentifier KeyIdentifier	hash veřejného klíče vydavatele (Autorita)	nekritická, povinná

* RR - rok vydání certifikátu CA

7.1.3 Objektové identifikátory algoritmů

V procesu poskytování Služby jsou využívány algoritmy v souladu s příslušnými technickými standardy a normami.

7.1.4 Tvary jmen

Autorita vydává Certifikáty s tvary jmen, vyhovujícími standardu RFC 5280. Dále platí ustanovení kapitoly 3.1.

7.1.5 Omezení jmen

Není relevantní pro Certifikáty vydávané dle této CP.

7.1.6 Objektový identifikátor certifikační politiky

Společnost První certifikační autorita, a.s., vkládá do certifikátu Autority speciální označení politiky anyPolicy a do Certifikátů vydávaných Autoritou pak objektový identifikátor certifikačních politiky, podle které je certifikát vydán (viz kapitola 1.2).

7.1.7 Použití rozšíření Policy Constrainsts

Není relevantní pro Certifikáty vydávané dle této CP.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz rozšíření Certifikátu v kapitole 7.1.2 výše.

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Není relevantní pro tento dokument - není označeno jako kritické.

7.2 Profil seznamu zneplatněných certifikátů

tab. 14 - Profil CRL[4]

Pole	Obsah
Version	v2(0x1)
SignatureAlgorithm	sha256withRSAEncryption
Issuer	vydavatele CRL (Autorita)
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu - viz tab. 15
crlExtensions	rozšíření CRL - viz tab. 15
Signature	zaručená elektronická pečeť vydavatele

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X.509 verze 2.

7.2.2 Rozšíření CRL a záznamů v CRL

tab. 15 - Rozšíření CRL[4]

Rozšíření	Obsah	Poznámka
crlEntryExtensions		
CRLReason	důvod zneplatnění Certifikátu důvod certificateHold je nepřípustný, I.CA nepoužívá	nepovinné, nekritické
crlExtensions		
AuthorityKeyIdentifier		
KeyIdentifier	hash veřejného klíče vydavatele CRL (Autorita)	povinné, nekritické
CRLNumber	jedinečné číslo vydávaného CRL	povinné, nekritické

7.3 Profil OCSP

Profily OCSP žádosti i odpovědi jsou v souladu s RFC 6960 a RFC 5019.

[4] I.CA si vyhrazuje právo upravit množinu a obsah polí CRL, vyžadovanou např. aktualizacemi standardů ETSI.

OCSP odpovědi jsou typu BasicOCSPResponse a obsahují všechna povinná pole. V případě odvolaného certifikátu je uvedeno volitelné pole revocationReason. Pro certifikáty nevydané příslušnou CA je vrácena odpověď unAuthorized. Jako přenosový protokol je používáno pouze http.

Bližší podrobnosti jsou uvedeny v kapitole 7.3 CPS.

7.3.1 Číslo verze

V žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP je uvedena verze 1.

7.3.2 Rozšíření OCSP

Konkrétní rozšíření uváděná v žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP jsou uvedena v kapitole 7.3.2 CPS.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita nebo okolnosti hodnocení

Periodicita hodnocení Služby je dána technickými standardy a normami, dle kterých je hodnocení prováděno.

8.2 Identita a kvalifikace hodnotitele

Kvalifikace hodnotitele Služby je dána příslušnými technickými standardy a normami.

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.

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

8.4 Hodnocené oblasti

Hodnocené oblasti Služby jsou konkretizovány technickými standardy a normami, podle kterých je hodnocení prováděno.

8.5 Postup v případě zjištění nedostatků

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

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení Služby 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.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za vydání Certifikátu jsou řešeny Kontraktem. Služby obnovení Certifikátu, výměny veřejného klíče v Certifikátu nebo změny údajů v Certifikátu nejsou poskytovány.

9.1.2 Poplatky za přístup k certifikátu

Není relevantní pro tento dokument, Certifikáty vydané podle této CP jsou k dispozici pouze v rámci systému e-Kasa.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Není relevantní pro tento dokument, informace o zneplatněných Certifikátech (CRL) a o stavech certifikátů vydaných Autoritou jsou k dispozici pouze v rámci systému e-Kasa.

9.1.4 Poplatky za další služby

Není relevantní pro tento dokument.

9.1.5 Postup při refundování

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

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.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

9.3 Důvěrnost obchodních informací

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

9.3.2 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.

9.3.3 Odpovědnost za ochranu důvěrných informací

Žádný zaměstnanec I.CA, který přijde do styku s 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, tedy ZOOÚ.

9.4.2 Informace považované za osobní údaje

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

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

9.4.3 Informace nepovažované za osobní údaje

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

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

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

9.4.6 Poskytování osobních údajů pro soudní či správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz důvěryhodných systémů určených k podpoře vydávání a správy Certifikátů, 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 CA

I.CA zaručuje, že:

- použije soukromý klíč Autority pouze pro vydávání Certifikátů a vydávání seznamů zneplatněných certifikátů,
- použije soukromé klíče OCSP respondéru Autority pouze pro poskytování odpovědí na stav Certifikátu,
- vydávané Certifikáty splňují v maximální možné míře náležitosti požadované relevantními technickými standardy a požadavky zadání organizace FR SR,
- zneplatní vydané Certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným Kontraktem.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud:

- držitel Certifikátu neporušil povinnosti plynoucí mu ze Smlouvy nebo Kontraktu a z této CP,
- spoléhající se strana neporušila povinnosti této CP.

Držitel Certifikátu vydaného podle této CP uplatňuje záruku způsobem definovaným Smlouvou nebo Kontraktem.

I.CA vyjadřuje a poskytuje držitelům Certifikátů a spoléhajícím se stranám záruky, že při vydávání Certifikátů a v průběhu doby jejich platnosti bude při jejich správě vyhovovat své CP a CPS.

Záruky zahrnují:

- že v režimu 24x7 je udržováno úložiště informací o stavu Certifikátu,
- že Certifikát může být zneplatněn z důvodů uvedených v této CP.

9.6.2 Zastupování a záruky RA

Pro vydávání Certifikátů Subjektů, operátorů GUI a modulu PKI e-Kasa je využívána jedna automatická RA, která zaručuje včasnost oběma směry prováděných přenosů, tedy žádostí o Certifikáty a jejich zneplatnění směrem od FR SR do I.CA a vydaných certifikátů směrem obráceným.

9.6.3 Zastupování a záruky držitele certifikátu

Ve Kontraktu je uvedeno, že držitelé Certifikátů jsou povinni řídit se ustanoveními této CP. Povinností FR SR je zprostředkovat tuto skutečnost Subjektům.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle této CP.

9.6.5 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 a dále záruky sjednané Kontraktem.

9.8 Omezení odpovědnosti

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

9.9 Záruky a odškodnění

Pro poskytování Služby platí relevantní ustanovení platné legislativy týkající se vztahů mezi poskytovatelem a spotřebitelem a dále takové záruky, které byly sjednány Kontraktem.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované Kontraktem i touto CP,
- poskytuje výše uvedené záruky po celou dobu platnosti Kontraktu,
- 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 Kontraktu, zejména za využívání v rozporu s podmínkami uvedenými v této CP, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení,
- za škodu vyplývající z použití Certifikátu v období po podání žádosti o jeho zneplatnění, pokud dodrží definovanou lhůtu pro zveřejnění zneplatněného Certifikátu na seznamu zneplatněných certifikátů (CRL nebo OCSP).

Reklamaci může podat organizace FR SR způsobem definovaným Kontraktem. Uvedeny musí být:

- co nejvýstižnější popis závady,
- sériové číslo reklamovaného produktu,
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne I.CA nejpozději do tří pracovních dnů od doručení reklamace. Vyrozumí o tom FR SR způsobem definovaným Kontraktem, pokud se strany nedohodnou jinak.

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do 30 dnů ode dne uplatnění reklamace, pokud se strany nedohodnou na jiném způsobu.

Nový Certifikát bude příslušnému držiteli Certifikátu poskytnut zdarma v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority,
- na základě rozhodnutí členů vedení I.CA s přihlédnutím ke konkrétním okolnostem,
- v případě, že Autorita při příjmu žádosti o vydání Certifikátu zjistí, že existuje jiný Certifikát s duplicitním veřejným klíčem.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato CP nabývá platnosti dnem uvedeným v kapitole 10 a platí minimálně po dobu platnosti posledního podle ní vydaného Certifikátu.

9.10.2 Ukončení platnosti

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

9.10.3 Důsledky ukončení a přetrvání závazků

Postup při ukončení a přetrvání závazků se řídí ustanoveními Kontraktu.

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

Veškeré upozorňování a komunikace se zúčastněnými Subjekty probíhá prostřednictvím FR SR a řídí se ustanoveními Kontraktu.

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interní dokumentaci.

9.12.2 Postup a periodicita oznamování

Oznámení o vydání nové verze CP je v kompetenci FR SR.

9.12.3 Okolnosti, při kterých musí být změněn OID

OID politiky musí být změněn v případě významných změn ve způsobu poskytování této Služby.

V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

9.13 Ustanovení o řešení sporů

Případné spory jsou řešeny v souladu s ustanoveními Kontraktu.

9.14 Rozhodné právo

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

9.15 Shoda s platnými právními předpisy

Systém poskytování Služby je provozován ve shodě s legislativními požadavky České republiky a Slovenské republiky a dále s relevantními mezinárodními standardy.

9.16 Různá 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 CP, 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 ustanovení

Není relevantní pro tento dokument.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato certifikační politika vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem uvedeným v tab. 1 - Vývoj dokumentu.