První certifikační autorita, a.s.

Zpráva pro uživatele CA

Verze 1.6

OBSAH

1 ÚVOD

Tento dokument poskytuje základní přehled o dvouúrovňové topologii certifikačních autorit, provozovaných společností První certifikační autorita, a.s. (I.CA), povinnostech a právech držitelů certifikátů a spoléhajících se stran.

1.1 Vývoj dokumentu

Tabulka 1 - Vývoj dokumentu

Verze	Datum vydání	Poznámka
1.0	02.09.2015	První vydání.
1.1	07.04.2016	Rozšíření o další vydávající CA.
1.2	18.04.2017	Aktualizace údajů o kontrolách a auditech. Aktualizace vyplývající z legislativy pro služby vytvářející důvěru.
1.3	16.11.2017	Aktualizace typů certifikačních autorit a údajů o provedených auditech.
1.4	08.08.2018	Aktualizace údajů o provedených auditech.
1.5	27.06.2019	Aktualizace údajů o provedených auditech.
1.6	27.01.2020	Podpora kryptografie eliptických křivek (ECC, kryptografie EC). Aktualizace údajů o provedených auditech.

1.2 Audity a kontroly I.CA

Tabulka 2 – Provedené kontroly bezpečnostní shody, audity, jiné kontroly

Typ	Výrok kontrolora/auditora
Kontrola bezpečnostní shody – zpráva ze dne 26.06.2006	VYHOVUJE
Audit bezpečnosti poskytovania certifikačných činností – zpráva ze dne 09.08.2006	VYHOVUJE
Audit systému řízení bezpečnosti informací (ISMS) - zpráva ze dne 30.04.2007	VYHOVUJE
Kontrola bezpečnostní shody – zpráva ze dne 28.06.2007	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - March 3rd, 2008	VYHOVUJE
Kontrola bezpečnostní shody – zpráva ze dne 18.6.2008	VYHOVUJE
Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s.	VYHOVUJE

(akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 30.04.2009	
Audit stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 30.04.2009	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - April 3rd, 2009	VYHOVUJE
Kontrola bezpečnostní shody – zpráva ze dne 18.6.2009	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - April 28th, 2010	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 30.04.2010	VYHOVUJE
Kontrola bezpečnostní shody – zpráva ze dne 30.06.2010	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - May 2nd, 2011	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 2.5.2011	VYHOVUJE
Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s. (akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 2.5.2011	VYHOVUJE
Kontrola bezpečnostní shody – zpráva ze dne 1.9.2011	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - Final Report, May 2012	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Záverečná správa, máj 2012	VYHOVUJE
Kontrola bezpečnostní shody (celková) - zpráva ze dne 31.8.2012	VYHOVUJE
Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s. (akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 14.5.2013	VYHOVUJE

Audit stavu bezpečnosti poskytovania certifikačných činností – Závěrečná zpráva ze dne 14.5.2013	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - Final Report, May 2013	VYHOVUJE
Kontrola bezpečnostní shody (částečná) - zpráva ze dne 28.8.2013	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Záverečná správa, máj 2014 (ze dne 20.5.2014)	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - Final Report, May 2014 (ze dne 20.5.2014)	VYHOVUJE
Kontrola bezpečnostní shody (částečná) - zpráva ze dne 27.8.2014	VYHOVUJE
Kontrola I.CA jako akreditovaného poskytovatele certifikačních služeb pracovníky odboru eGovernmentu MV ČR – předmětem kontroly je dodržování ustanovení § 6 odst. 1 písm. d) a odst. 5 a 6	Kontrolou bylo ověřeno, že akreditovaný poskytovatel certifikačních služeb I.CA dodržuje uvedená ustanovení (viz. http://www.mvcr.cz/clanek/vysledky-probehle-kontroly-akreditovaneho-poskytovatele-certifikacnich-sluzeb-i-ca.aspx)
Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s. (akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 14.5.2015	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Záverečná správa, máj 2015 (ze dne 20.5.2015)	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 101 456 - Final Report, May 2015	VYHOVUJE
Audit of the company První certifikační autorita, a.s. for compliance with policy requirements for certification authorities issuing certificates in accordance with ETSI TS 102 042 (policies DVCP, OVCP, NCP) - Audit Statement Report, August 2015	VYHOVUJE
Kontrola bezpečnostní shody (celková) - zpráva ze dne 27.8.2015	VYHOVUJE

AUDIT STATEMENT REPORT- Root CA/RSA: ETSI TS 101 456 V1.4.3 (2007-05): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates", policies QCP public + SSCD, QCP public and ETSI TS 102 042V2.4.1 (2013-02): "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates", policies NCP, NCP+, DVCP, OVCP Audit Statement Report, ze dne 18.5. 2016.	VYHOVUJE
Audit stavu bezpečnosti poskytovania certifikačných činností – Záverečná správa, máj 2016 (ze dne 20.5.2016)	VYHOVUJE
Kontrola bezpečnostní shody (částečná) - zpráva ze dne 27.8.2016	VYHOVUJE
Audit požadovaný Microsoft Trusted Root Certificate Program – AUDIT STATEMENT REPORT – I.CA Root CA/RSA, 18.5.2017 **ETSI EN 319 411-2 V2.1.1 (2016-02)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, policies: a) QCP-n Policy for EU qualified certificate issued to a natural person b) QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD c) QCP-l Policy for EU qualified certificate issued to a legal person d) QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD **ETSI EN 319 411-1 V1.1.1 (2016-02)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, policies: a) NCP: Normalized Certificate Policy b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device c) DVCP: Domain Validation Certificate Policy d) OVCP: Organizational Validation Certificate Policy	VYHOVUJE

Audit požadovaný eIDAS/ČR pro služby: a) Vydávání kvalifikovaných certifikátů pro elektronické podpisy, 26.05.2017 b) Vydávání kvalifikovaných certifikátů pro elektronické pečetě, 26.05.2017	SHODA
Audit požadovaný eIDAS/SR pro služby: a) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, 13.06.2017 b) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať, 13.06.2017	SHODA
Audit požadovaný Microsoft Trusted Root Certificate Program – AUDIT STATEMENT REPORT – I.CA Root CA/RSA **ETSI EN 319 411-2 V2.1.1 (2016-02)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, policies: a) QCP-w: Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person **ETSI EN 319 411-1 V1.1.1 (2016-02)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, policies: a) EVCP: Extended Validation Certificate Policy	VYHOVUJE
Audit požadovaný eIDAS/ČR pro službu: a) Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek, 11.12. 2017	SHODA
Audit požadovaný Microsoft Trusted Root Certificate Program – AUDIT STATEMENT REPORT – I.CA Root CA/RSA, 18.5.2018 **ETSI EN 319 411-2 V2.1.1 (2016-02)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, policies: a) QCP-n Policy for EU qualified certificate issued to a natural person b) QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD c) QCP-l Policy for EU qualified certificate issued to a legal person	VYHOVUJE

d) QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD e) QCP-w: Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person **ETSI EN 319 411-1 V1.1.1 (2016-02)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, policies: a) NCP: Normalized Certificate Policy b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device c) DVCP: Domain Validation Certificate Policy d) OVCP: Organizational Validation Certificate Policy e) EVCP: Extended Validation Certificate Policy	
Kontrola společnosti První certifikační autorita, a.s., pracovníky odboru eGovernmentu MV ČR – předmětem kontroly bylo dodržování ustanovení § 2, § 3 odst. 1 a 2, §19 odst. 7 zákona č. 297/2016 Sb., a rovněž čl. 24 odst. 2 písm. b) nařízení EU č. 910/2014. Kontrola probíhala 25.4. – 31.5.2018	Kontrolou bylo ověřeno, že poskytovatel První certifikační autorita, a.s. dodržuje uvedená ustanovení (https://www.mvcr.cz/clanek/obecne-vysledky-kontroly-poskytovatelu-sluzeb-vytvarejicich-duveru.aspx).
Audit požadovaný eIDAS/ČR pro služby: a) Vydávání kvalifikovaných certifikátů pro elektronické podpisy, 29.06.2018 b) Vydávání kvalifikovaných certifikátů pro elektronické pečetě, 29.06.2018 c) Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek, 29.06.2018	SHODA
Audit požadovaný eIDAS/SR pro služby: a) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, 29.06.2018 b) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať, 29.06.2018	SHODA
Audit požadovaný Microsoft Trusted Root Certificate Program - AUDIT STATEMENT REPORT – I.CA Root CA/RSA: **ETSI EN 319 411-2 V2.2.2 (2018-04)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates: a) QCP-n Policy for EU qualified certificate issued to a natural person (for electronic signatures) b) QCP-n-qscd Policy for EU qualified certificate	VYHOVUJE

issued to a natural person where the private key and the related certificate reside on a QSCD (for qualified electronic signatures) c) QCP-l Policy for EU qualified certificate issued to a legal person (for electronic seals) d) QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (for qualified electronic seals) e) QCP-w: Policy for EU qualified certificates for website authentication **ETSI EN 319 411-1 V1.2.2 (2018-04)** Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements: a) NCP: Normalized Certificate Policy b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device c) DVCP: Domain Validation Certificate Policy for TLS/SSL certificates d) OVCP: Organizational Validation Certificate Policy for TLS/SSL certificates e) EVCP: Extended Validation Certificate Policy for TLS/SSL certificates Auditní závěrečná zpráva z 17.května 2019	
Audit požadovaný eIDAS/ČR pro služby: a) Vydávání kvalifikovaných certifikátů pro elektronické podpisy b) Vydávání kvalifikovaných certifikátů pro elektronické pečetě c) Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek Auditní závěrečná zpráva z 24.května 2019	SHODA
Audit požadovaný eIDAS/SR pro služby: a) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis b) Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať Auditní závěrečná zpráva z 13.června 2019	SHODA

Audit kvalifikovaného systému elektronické identifikace a vydávání prostředku pro elektronickou identifikaci s příslušnými požadavky Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 Auditní závěrečná zpráva z 13.listopadu 2019	SHODA
Audit systému řízení bezpečnosti informací společnosti První certifikační autorita, a.s. - Provoz důvěryhodných systémů podporujících požadavky eIDAS Auditní závěrečná zpráva z 25.listopadu 2019	VYHOVUJE

2 KONTAKTNÍ INFORMACE

2.1 Sídlo společnosti

Adresa sídla společnosti je:

První certifikační autorita, a.s.

Podvinný mlýn 2178/6

190 00 Praha 9

Česká republika.

Telefonické a mailové spojení do sídla společnosti je:

tel.: +420 284 081 940

fax.: +420 284 081 965

e-mail: info@ica.cz

2.2 Zveřejňování informací

Veškeré veřejné informace lze nalézt na internetové adrese: http://www.ica.cz.

2.3 Komunikace s veřejností

Komunikace s veřejností je možná těmito způsoby:

- obecný kontakt: info@ica.cz,
- pracoviště registračních autorit: http://www.ica.cz,
- technická podpora:
  - tel.: +420 284 081 930 – 33,
  - e-mail: support@ica.cz,

- reklamace: reklamace@ica.cz,
- obchodní oddělení: sales@ica.cz.

3 TYPY CERTIFIKÁTŮ, OVĚŘOVACÍ PROCEDURY A POUŽITÍ

3.1 Soulad se standardy

Společnost První certifikační autorita, a.s. vydává certifikáty (určené fyzickým a právnickým osobám), jejichž profil vyhovuje standardu X.509 verze 3 v souladu s normami a standardy:

- 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.
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 2: Požadavky na poskytovatele důvěryhodných služeb vydávající kvalifikované certifikáty EU.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- CA/Browser Forum – Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.
- CA/Browser Forum – Guidelines for the Issuance and Management of Extended Validation Certificates.
- ETSI TS 119 495 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

3.2 Typy certifikátů – algoritmus RSA

Kořenová certifikační autorita **I.CA Root CA/RSA** (klíč RSA 4096 bitů, algoritmus podpisu sha512WithRSAEncryption) společnosti První certifikační autorita, a.s., vydává v souladu s požadavky technických standardů a platné legislativy certifikáty výhradně podřízeným certifikačním autoritám a svému OCSP respondéru (s klíčem RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption). Tyto podřízené certifikační autority vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

Certifikační autorita **I.CA Qualified CA/RSA 07/2015** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro

elektronický podpis a elektronickou pečeť (Slovenská republika) a svému OCSP respondéru (s klíči RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

Certifikační autorita **I.CA Qualified 2 CA/RSA 02/2016** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro elektronický podpis a elektronickou pečeť (volitelně s rozšířením vyžadovaným směrnicí Evropské unie o platebních službách č. 2015/2366) a systémových certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

Certifikační autorita **I.CA TSACA/RSA 04/2017** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání kvalifikovaných certifikátů pro elektronickou pečeť pro systém TSA2 a svému OCSP respondéru (s klíči RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

Certifikační autorita **I.CA Public CA/RSA 07/2015** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je určena k vydávání komerčních certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

Certifikační autorita **I.CA SSL CA/RSA 07/2015** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je vyhrazena pouze pro vydávání certifikátů pro přístup k webovým službám chráněným protokoly TLS/SSL (SSL certifikáty, „domain validation“ a „organization validation“) a svému OCSP respondéru (s klíči RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

Certifikační autorita **I.CA SSL EV CA/RSA 10/2017** (klíč RSA 4096 bitů, algoritmus podpisu sha256WithRSAEncryption) je vyhrazena pouze pro vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek („extended validation“ SSL certifikáty) v souladu s eIDAS (volitelně s rozšířením vyžadovaným směrnicí Evropské unie o platebních službách č. 2015/2366) a svému OCSP respondéru (s klíči RSA 2048 bitů, algoritmus podpisu sha256WithRSAEncryption).

3.3 Typy certifikátů – ECC

Kořenová certifikační autorita **I.CA Root CA/EC 12/2016** (klíč EC P-521 bitů, algoritmus podpisu ecdsa-with-SHA512) společnosti První certifikační autorita, a.s., vydává v souladu s požadavky technických standardů a platné legislativy certifikáty výhradně podřízeným certifikačním autoritám a svému OCSP respondéru (s klíčem EC P-256 bitů, algoritmus podpisu ecdsa-with-SHA256). Tyto podřízené certifikační autority vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

Certifikační autorita **I.CA Qualified 2 CA/ECC 06/2019** (klíč EC P-521 bitů, algoritmus podpisu ecdsa-with-SHA512) je určena k vydávání kvalifikovaných certifikátů pro elektronický podpis a elektronickou pečeť a svému OCSP respondéru (s klíči EC P-256 bitů, algoritmus podpisu ecdsa-with-SHA256).

Certifikační autorita **I.CA Public CA/ECC 12/2016** (klíč EC P-521 bitů, algoritmus podpisu ecdsa-with-SHA512) je určena k vydávání komerčních certifikátů koncovým uživatelům a svému OCSP respondéru (s klíči EC P-256 bitů, algoritmus podpisu ecdsa-with-SHA256).

3.4 Ověřovací procedury

V procesu vydávání prvotního certifikátu, kdy je nutná fyzická přítomnost žadatele nebo jeho zástupce na pracovišti registrační autority (s výjimkou, uvedenou v následujícím odstavci), je

vždy ověřována totožnost této fyzické osoby na základě jejích osobních dokladů. V případě certifikátu pro organizaci je ověřována i vazba žadatele o certifikát na tuto organizaci.

Povinnost přítomnosti fyzické osoby v případě vydávání SSL, resp. EV SSL certifikátů není na pracovišti registrační autority vyžadována a proces ověření probíhá, je-li to možné, s využitím veřejně dostupných registrů.

Pokud příslušná certifikační politika umožňuje vydání tzv. následného certifikátu (jedná se o certifikát, který bude v souladu se smlouvou o poskytování příslušné služby, uzavřenou mezi žadatelem a I.CA, vydán žadateli na základě nové žádosti o certifikát v období platnosti certifikátu, ke kterému je tento následný certifikát vydáván), není fyzická přítomnost žadatele o certifikát na pracovišti registrační autority vyžadována. Podrobný popis registračních postupů je uveden v příslušných certifikačních politikách.

4 UŽITÍ CERTIFIKÁTŮ

Kvalifikované certifikáty lze použít k ověřování elektronických podpisů, elektronických pečetí a autentizaci internetových stránek v souladu s 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.

Ostatní typy certifikátů lze obecně použít k ověřování elektronických podpisů, identifikaci, autentizaci a k zabezpečené komunikaci.

Při využívání certifikátů je vždy nutno postupovat v souladu s příslušnou certifikační politikou.

Nestanoví-li relevantní legislativní norma jinak, jsou auditní záznamy a záznamy vzniklé v průběhu registračního procesu uchovávány po dobu nejméně 10 let od jejich vzniku.

Společnost První certifikační autorita, a.s., uchovává vydané certifikáty a seznamy zneplatněných certifikátů po celou dobu své existence.

5 POVINNOSTI ŽADATELŮ NEBO DRŽITELŮ CERTIFIKÁTU

Držitelem certifikátů je žadatel o certifikát, kterému byl tento certifikát vydán. Z pohledu společnosti První certifikační autorita, a.s., se jedná o osobu (fyzickou, nebo organizaci), která uzavřela se společností První certifikační autorita, a.s., smlouvu o vydání certifikátu. Mezi základní povinnosti žadatele o certifikát a následně držitele tohoto certifikátu patří zejména:

- poskytovat pravdivé a úplné informace při registraci žádosti o vydání certifikátu,
- neprodleně uvědomit poskytovatele certifikačních služeb o změně údajů, uvedených ve vydaném certifikátu, popř. ve smlouvě,
- seznámit se s certifikační politikou, podle které bude certifikát vydán,
- překontrolovat, zda údaje uvedené v žádosti o certifikát a certifikátu jsou správné a odpovídají požadovaným údajům,

- nakládat s prostředkem a se soukromým klíčem, který odpovídá veřejnému klíči ve vydaném certifikátu takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- užívat soukromý klíč a odpovídající certifikát vydaný podle příslušné certifikační politiky pouze pro účely stanovené touto certifikační politikou,
- neprodleně požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče zejména v případech kompromitace soukromého klíče, případně podezření, že soukromý klíč byl zneužit.

6 POVINNOSTI SPOLÉHAJÍCÍCH SE STRAN

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na certifikát vydaný společností První certifikační autorita, a.s. Mezi základní povinnosti těchto subjektů patří zejména:

- získat z bezpečného zdroje relevantní certifikáty certifikačních autorit uvedených v kapitole 3.2 a ověřit kontrolní součet těchto certifikátů,
- před použitím certifikátu koncového uživatele ověřit platnost certifikátů certifikačních autorit souvisejících s certifikátem tohoto koncového uživatele,
- ujistit se, zda certifikát koncového uživatele je vhodný pro jeho využití,
- dodržovat veškerá relevantní ustanovení certifikační politiky, dle které byl certifikát koncového uživatele vydán.

7 OMEZENÍ ZÁRUKY A ODPOVĚDNOSTI

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak příslušnými právními předpisy, tak příslušnými certifikačními politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování služeb, resp. služeb vytvářejících důvěru; pokud bylo zjištěno porušení povinností držitele certifikátu nebo spoléhající se strany, mající souvislost s uváděnou škodou, záruční plnění se neposkytne – tato skutečnost musí být držiteli certifikátu nebo spoléhající se straně oznámena a zaprotokolována,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, kteří mají platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo potenciální odpovědnost s výjimkou případů, kde poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele,
- jiné záruky než výše uvedené, neposkytuje,
- další možné náhrady škody vycházejí z ustanovení příslušných zákonů 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, zejména za provozování v rozporu s podmínkami uvedenými

v certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.,

- za škodu vyplývající z použití certifikátu v období po podání žádosti o jeho zneplatnění, pokud společnost První certifikační autorita, a.s., dodrží definovanou lhůtu pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL).

8 SMLOUVY A CERTIFIKAČNÍ POLITIKA

Vztah mezi držitelem certifikátu a poskytovatelem služeb, resp. služeb vytvářejících důvěru – společností První certifikační autorita, a.s., je (kromě příslušných ustanovení povinných právních předpisů) upraven smlouvou a příslušnými ustanoveními platných certifikačních politik.

Vztah mezi spoléhající se stranou a poskytovatelem služeb, resp. služeb vytvářejících důvěru – společností První certifikační autorita, a.s., je upraven příslušnými ustanoveními platných certifikačních politik. Vztah společnosti První certifikační autorita, a.s., a spoléhajících se stran smlouvou upraven není.

Veškeré veřejné informace je možné získat na kontaktních adresách, uvedených v kapitole 2 tohoto dokumentu.

9 OCHRANA OSOBNÍCH ÚDAJŮ

Ochrana osobních údajů je ve společnosti První certifikační autorita, a.s., řešena v souladu s požadavky aktuální legislativy týkající se ochrany osobních údajů, tj. zákona České republiky č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů, resp. nařízení 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 (obecné nařízení o ochraně osobních údajů).

10 POLITIKA NÁHRAD A REKLAMACE

Reklamaci je možné podat těmito způsoby:

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

Reklamující osoba (držitel certifikátu) je povinna uvést:

- co nejvýstižnější popis závad a jejich projevů,
- sériové číslo reklamovaného produktu.

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 30 dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

Nový certifikát bude držiteli 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 příslušná certifikační autorita při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát s duplicitním veřejným klíčem.

11 PRÁVNÍ PROSTŘEDÍ

Společnost První certifikační autorita, a.s. se při své činnosti řídí zákonnými požadavky, zejména:

- nařízením Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS),
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
- zákonem Slovenské republiky č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),
- zákonem České republiky č. 90/2012 Sb., o obchodních korporacích,
- zákonem České republiky č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů,
- 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 (obecné nařízení o ochraně osobních údajů).

12 KVALIFIKACE, AUDITY A KONTROLY

Společnost První certifikační autorita, a.s., je kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Poskytování těchto služeb je pravidelně podrobováno auditům a kontrolám v souladu se zákonnými požadavky vyjmenovanými v kapitole 11.

Společnost První certifikační autorita, a.s., je členem programu Microsoft Trusted Root Certificate Program (zařazení kořenového certifikátu I.CA do důvěryhodných kořenových certifikačních autorit společnosti Microsoft), proto jsou poskytované služby podrobovány také pravidelným auditům vyžadovaných touto společností.

Za společnost První certifikační autorita, a.s.

Ing. Petr Budiš, Ph.D., MBA v.r.