První certifikační autorita, a.s.

Zpráva pro uživatele CA

hierarchická topologie kvalifikované a komerční certifikační služby

Verze 1.1

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	Pozn.
1.0	02.09.2015	První vydání
1.1	07.04.2016	Rozšíření o další vydávající CA

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. (akreditovaný poskytovatel kvalifikovaných certifikačních služeb) – Závěrečná zpráva ze dne 30.04.2009	VYHOVUJE
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

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 Typy certifikátů

Společnost První certifikační autorita, a.s. vydává kvalifikované certifikáty (určené fyzickým osobám), kvalifikované systémové certifikáty (určené fyzickým osobám, organizacím a zařízením), komerční certifikáty (určené fyzickým osobám), komerční serverové certifikáty (určené fyzickým osobám, organizacím a zařízením) a komerční certifikáty pro přístup k chráněným webovým službám (určené organizacím), jejichž profil vyhovuje standardu X.509 verze 3.

Kořenová kvalifikovaná certifikační autorita (I.CA Root CA/RSA, délka RSA klíče 4096 bitů, algoritmus 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. Tyto podřízené certifikační autority vydávají certifikáty koncovým uživatelům a svým OCSP respondérům.

Kvalifikovaná certifikační autorita I.CA Qualified CA/RSA 07/2015 (délka RSA klíče 4096 bitů, algoritmus SHA256) je určena k vydávání kvalifikovaných systémových certifikátů pro systém TSA, kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů koncovým uživatelům (Slovenská republika) a svému OCSP respondéru (délka RSA klíče 2048 bitů, algoritmus SHA256).

Kvalifikovaná certifikační autorita I.CA Qualified 2 CA/RSA 02/2016 (délka RSA klíče 4096 bitů, algoritmus SHA256) je určena k vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů koncovým uživatelům a svému OCSP respondéru (délka RSA klíče 2048 bitů, algoritmus SHA256).

Komerční certifikační autorita I.CA Public CA/RSA 07/2015 (délka RSA klíče 4096 bitů, algoritmus SHA256) je určena k vydávání komerčních certifikátů koncovým uživatelům a svému OCSP respondéru (délka RSA klíče 2048 bitů, algoritmus SHA256).

Výše uvedené certifikační autority vydávají certifikáty koncovým uživatelů v souladu se standardy ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates a normami řady ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.

Komerční SSL certifikační autorita I.CA SSL CA/RSA 07/2015 (délka RSA klíče 4096 bitů, algoritmus SHA256) je vyhrazena pouze pro vydávání certifikátů pro přístup k webovým službám chráněným protokoly TLS/SSL (SSL certifikáty), konkrétně tzv. „domain validation“ a „organization validation“ certifikáty, v souladu se standardem ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates a CA/Browser Forum - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Baseline Requirements) a svému OCSP respondéru (délka RSA klíče 2048 bitů, algoritmus SHA256.

3.2 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 certifikátu 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 certifikační 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 a kvalifikované systémové certifikáty lze použít výhradně k ověřování elektronického podpisu, resp. elektronické značky/pečetě.

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 a 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 3.1 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 certifikačních služeb; 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 certifikačních služeb - 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 certifikačních služeb - 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 zákona č. 101/2000 Sb. o ochraně osobních údajů ve znění pozdějších předpisů.

Žadatel o certifikát dává souhlas se zpracováním osobních údajů v rozsahu nezbytném pro vydání a zneplatnění tohoto certifikátu. V případě kvalifikovaného certifikátu, resp. kvalifikovaného systémového certifikátu dává společnosti První certifikační autorita, a.s., písemný souhlas se zpracováním a uchováváním osobních údajů v rozsahu požadavků platné legislativy, vztahující se k problematice elektronickém podpisu.

10 POLITIKA NÁHRAD A REKLAMACE

Oprávněnou 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 jednoho měsíce 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 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 v oblasti kvalifikovaných certifikačních služeb řídí příslušnými aktuálními ustanoveními právního řádu České republiky, zejména:

- zákonem České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn

provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb., a zákonem č. 440/2004 Sb.,

- vyhláškou České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb)
- zákonem České republiky č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

S ohledem na poskytování kvalifikovaných certifikačních služeb na území Slovenské republiky se společnost První certifikační autorita, a.s. se při své činnosti řídí příslušnými aktuálními ustanoveními právního řádu Slovenské republiky, zejména zákonem Slovenské republiky č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení a s ním spojených vykonávacích vyhlášok

Společnost První certifikační autorita, a.s., se při své činnosti v oblasti komerčních certifikačních služeb, tedy služeb neregulovaných národními zákony pro oblast elektronického podpisu, příslušnými aktuálními ustanoveními právního řádu České republiky, zejména zákony České republiky č. 90/2012 Sb., o obchodních korporacích a č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

12 AKREDITACE, AUDITY A KONTROLY

Společnost První certifikační autorita, a.s., je akreditovaným poskytovatelem certifikačních služeb v České republice a Slovenské republice. Poskytování kvalifikovaných certifikačních služeb společností První certifikační autorita, a.s., je pravidelně podrobováno auditům a kontrolám, požadovaných legislativami těchto států.

S ohledem na zařazení kořenových certifikátů do důvěryhodných kořenových certifikačních autorit společnosti Microsoft, je poskytování certifikačních služeb podrobováno pravidelným auditům vyžadovaných touto společností.

Za společnost První certifikační autorita, a.s.

Ing. Petr Budiš, Ph.D., MBA v.r.