Správa základních registrů
Na Vápence 915/14
130 00 Praha 3

Praha 7. prosince 2018

NCA

Zpráva pro uživatele CA

Verze 1.0

OBSAH

1 Úvod 3
1.1 Vývoj dokumentu 3
1.2 Audity a kontroly SZR 3
2 Kontaktní informace 3
2.1 Sídlo společnosti 3
2.2 Zveřejňování informací 3
2.3 Komunikace s veřejností 4
3 Typy certifikátů, ověřovací procedury a použití 4
3.1 Typy certifikátů 4
3.2 Ověřovací procedury 5
4 Užití certifikátů 5
5 Povinnosti žadatelů nebo držitelů certifikátu 5
6 Povinnosti spoléhajících se stran 6
7 Omezení záruky a odpovědnosti 6
8 Smlouvy a certifikační politika 7
9 Ochrana osobních údajů 7
10 Politika náhrad a reklamace 7
11 Právní prostředí 8
12 Kvalifikace, audity a kontroly 8

1 ÚVOD

Tento dokument podává základní přehled o službě poskytované organizační složkou státu Správa základních registrů (dále též SZR) vydávání kvalifikovaných certifikátů, včetně práv a povinnostech žadatelů o tyto certifikáty.

Tento dokument je pouze zjednodušeným výběrem informací uvedených v plném rozsahu v certifikačních politikách, v certifikační prováděcí směrnici a ve smlouvách o vydávání certifikátů. Slouží pro zjednodušení orientace držitelů certifikátů.

1.1 Vývoj dokumentu

Tabulka 1 - Vývoj dokumentu

Verze	Datum vydání	Poznámka
1.0	07.12.2018	První vydání.

1.2 Audity a kontroly SZR

Tabulka 2 – Provedené audity a jiné kontroly

Typ	Výrok kontrolora/auditora
Dosud nebyly provedeny žádné audity ani kontroly.	

2 KONTAKTNÍ INFORMACE

2.1 Sídlo SZR

Adresa sídla je:

Správa základních registrů

Na Vápence 14

130 00 Praha 3

Česká republika.

Telefonické a mailové spojení do sídla SZR je:

tel.: +420 225 514 751

e-mail: epodatelna@szrcr.cz

2.2 Zveřejňování informací

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

2.3 Komunikace pro oblast certifikátů

Komunikace je možná těmito způsoby:

- obecný kontakt: epodatelna@szrcr.cz,
- pracoviště registračních autorit,
- technická podpora:
  - tel.: +420 225 514 758 (PO - PÁ 8:00 - 18:00),
  - e-mail: podpora@szrcr.cz, předmět zprávy musí začínat textem NCA,
- reklamace: podpora@szrcr.cz, předmět zprávy musí začínat textem NCA.

3 TYPY CERTIFIKÁTŮ, OVĚŘOVACÍ PROCEDURY A POUŽITÍ

3.1 Typy certifikátů

SZR vydává certifikáty (určené fyzickým a právnickým osobám), jejichž profil vyhovuje standardu X.509 verze 3.

Kořenová certifikační autorita SZR (délka RSA klíče 3072 bitů, algoritmus SHA256) vydává v souladu s požadavky technických standardů a platné legislativy certifikáty výhradně podřízeným certifikačním autoritám a svému OCSP respondéru.

Podřízená certifikační autorita SZR (délka RSA klíče 3072 bitů, algoritmus SHA256) je určena k vydávání kvalifikovaných certifikátů pro ověřování elektronického podpisu a kvalifikovaných certifikátů pro ověřování elektronické pečetě koncovým uživatelům, svému OCSP respondéru a k vydávání infrastrukturních certifikátů.

Certifikáty koncovým uživatelům jsou vydávány v souladu se 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.

3.2 Ověřovací procedury

V procesu vydávání prvotního certifikátu, kdy je nutná fyzická přítomnost žadatele 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.

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 SZR, 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 a elektronických pečetí 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.

SZR 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 SZR se jedná o osobu (fyzickou, nebo organizaci), která uzavřela se SZR 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 SZR. 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

SZR:

- 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,
- jiné záruky, než výše uvedené, neposkytuje,
- další možné náhrady škody vycházejí z ustanovení příslušných zákonů a o jejich výši může rozhodnout soud.

SZR 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 atd.,
- za škodu vyplývající z použití certifikátu v období po podání žádosti o jeho zneplatnění, pokud SZR dodrží definovanou lhůtu pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL).

8 SMLOUVY A CERTIFIKAČNÍ POLITIKA

Vztah mezi držitelem certifikátu a SZR je (kromě příslušných ustanovení povinných právních předpisů) upraven smlouvou a příslušnými ustanoveními platných certifikačních politik.

Vztah mezi spoléhající se stranou a SZR je upraven příslušnými ustanoveními platných certifikačních politik. Vztah SZR 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 v SZR řešena v souladu s požadavky aktuální legislativy týkající se ochrany osobních údajů, tj. zákona č. 101/2000 Sb., o ochraně 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 podpora@szrcr.cz, předmětu zprávy musí začínat textem NCA,
- doporučenou poštovní zásilkou na adresu sídla SZR,
- zasláním zprávy do datové schránky SZR,
- osobně v sídle SZR.

Reklamující osoba (držitel certifikátu) je povinna uvést:

- co nejvýstižnější popis závad a jejich projevů,
- sériové číslo reklamovaného produktu,
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne SZR 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 v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority,
- v případě, že příslušná certifikační autorita při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát s duplicitním veřejným klíčem.

11 PRÁVNÍ PROSTŘEDÍ

SZR 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 České republiky č. 90/2012 Sb., o obchodních korporacích,
- zákonem České republiky č. 101/2000 Sb., o ochraně 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

SZR je kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Poskytování těchto služeb je pravidelně podrobováno auditům a kontrolám v souladu se zákonnými požadavky vyjmenovanými v kapitole 11.

Za Správu základních registrů

Ing. Michal Pešek