SPRÁVA ZÁKLADNÍCH REGISTRŮ

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

Praha 7. prosince 2018

NCA

Zpráva pro uživatele TSA

Verze 1.0

OBSAH

1 ÚVOD

Tento dokument podává základní přehled o službě poskytované organizační složkou státu Správa základních registrů (dále též SZR) vydávání kvalifikovaných elektronických časových razítek, včetně práv a povinnostech žadatelů o kvalifikovaná elektronická časová razítka (dále též časová razítka).

Tento dokument je pouze zjednodušeným výběrem informací uvedených v plném rozsahu v politice služby, v prováděcí směrnici a ve smlouvě o vydávání časových razítek. Slouží pro zjednodušení orientace uživatelů časových razítek.

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 časových razítek

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 VYDÁVÁNÍ ČASOVÝCH RAZÍTEK

3.1 Typy vydávaných časových razítek

SZR vydává časová razítka dle platné legislativy pro služby vytvářející důvěru.

Při vydávání časových razítek se SZR řídí vlastní politikou, která zahrnuje všechny požadavky politiky BTSP (Best practices Time-Stamp Policy) specifikované v ETSI EN 319421 verze 1.1.1.

3.2 Ověřovací procedury

Vydávání časových razítek je v SZR založeno na smlouvě uzavřené mezi SZR a žadatelem o časové razítko, ten může být identifikován a autentizován jménem a heslem.

SZR si vyhrazuje právo na využití jiného způsobu implementace procesu identifikace a autentizace žadatele o časové razítko.

3.3 Žádost o časové razítko

Po případně provedené identifikaci a autentizaci, vytvoří žadatel v souladu s příslušnou politikou žádost o časové razítko (v souladu s RFC 3161). Tato žádost je předána systému TSA, který ji následně předá jednomu ze serverů vydávajících časová razítka. V žádosti o časové razítko jsou podporovány kryptografické algoritmy SHA1, SHA-256 a SHA-512.

3.4 Vydání časového razítka

Systém TSA provádí veškeré kontroly formální správnosti žádosti o časové razítko a na základě jejich výsledku vytvoří konkrétní časový server odpověď, obsahující v případě kladného výsledku kontrol časové razítko (viz RFC 3161). Časový údaj (UTC) vkládaný do časového razítka, jehož maximální odchylka při vytváření časového razítka je 1 sekunda od UTC (uvedeno v položce accuracy časového razítka), je synchronizován se zdrojem důvěryhodného času.

Odpověď je opatřena zaručenou elektronickou pečetí vytvořenou soukromým klíčem časového serveru, který časové razítko vydal.

Každá odpověď na žádost o časové razítko je předána žadateli o časové razítko a taktéž umístěna v příslušném úložišti systému TSA.

Certifikáty serverů vydávajících časová razítka lze získat na webových stránkách SZR, nebo Ministerstva vnitra České republiky, případně v příslušném TSL (Trust Service List).

3.5 Ověření časového razítka

Po obdržení odpovědi na žádost o časové razítko je žadatel povinen zjistit status odpovědi. V případě chyby není časové razítko v odpovědi obsaženo a žadatel je povinen překontrolovat odpovídající chybovou zprávu. V případě časového razítka obsaženého v bezchybné odpovědi je žadatel povinen ověřit zejména:

- zda vrácený otisk (hash) je totožný s odeslaným v žádosti,
- platnost zaručené elektronické pečetě časového razítka,
- platnost celé certifikační cesty certifikátu serveru, který časové razítko vydal, včetně kontroly odvolání,
- v případě, že žádost obsahovala položku „nonce“ nebo „reqPolicy“ ověřit, že její hodnota v odpovědi je totožná.

4 OMEZENÍ POUŽITÍ

Nejsou definována žádná omezení použitelnosti časového razítka vydaného v souladu s politikou vydávání časových razítek. Obecně platí, že časové razítko je datová zpráva, která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

5 POVINNOSTI ŽADATELŮ O ČASOVÉ RAZÍTKO

Žadatelé jsou povinni žádat o časová razítka v souladu s odpovídající politikou. Povinnosti při ověření platnosti vráceného časového razítka jsou uvedeny v kapitole 3.5.

6 POVINNOSTI SPOLÉHAJÍCÍCH SE STRAN

Spoléhající se strana je povinna zejména:

- získat z bezpečného zdroje relevantní certifikáty vztahující se k časovému razítku a ověřit kontrolní součet těchto certifikátů,
- ověřit platnost zaručené elektronické pečetě časového razítka a následně všech certifikátů, vztahujících se k časovému serveru, který tuto zaručenou elektronickou pečeť vytvořil,

- ověřit obsah vydaného časového razítka - konkrétně se jedná o hash ověřovaných dat a zda politika, pod kterou bylo časové razítko vydáno, je akceptovatelná její potřebám, popř. potřebám provozovaných aplikací.

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,
- neodpovídá za vady poskytovaných služeb, které vzniknou jejich používáním v rozporu s příslušnou politikou služby, a dále za vady, které vznikly z důvodu vyšší moci včetně dočasného výpadku telekomunikačního spojení atd.

8 SMLOUVY A CERTIFIKAČNÍ POLITIKA

Vztah mezi žadatelem o časové razítko a SZR je (kromě odpovídajících ustanovení povinných právních předpisů) upraven smlouvou a příslušnými ustanoveními politiky služby.

Vztah mezi spoléhající se stranou a SZR je upraven příslušnými ustanoveními politiky služby.

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

Doplňující detailnější informace ohledně vydávání časových razítek je též možné zjistit z příslušné prováděcí směrnice.

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, předmět 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 časového razítka) 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.

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