Kvalifikovaná certifikační autorita

Zpráva pro uživatele

(kvalifikovaná časová razítka)

verze 1.1

druh dokumentu:
Provozní dokument

identifikace dokumentu:
QCA D41

Květen 2009

Verze	Datum	Autor	Poznámka
0.1	21.1.2009	Daniel Joščák	draft
0.2	22.2.2009	Martin Šlancar	připomínkování dokumentu
0.3	24.2.2009	Ondřej Steiner	zapracování připomínek
1.0	**26.2.2009**	**Martin Šlancar**	**„milestone“ verze schválená manažerem TSA**
1.1	**22.5.2009**	**Martin Šlancar**	**„milestone“ verze schválená manažerem TSA** zapracování připomínek Ministerstva vnitra

Schváleno:

Verze	Schválil	
1.0	Manažer TSA	plachy.pavel@cpost.cz
1.1	Manažer TSA	plachy.pavel@cpost.cz

Obsah

1 Úvod

1.1 Účel dokumentu

Tento dokument poskytuje základní informace o autoritě časových razítek PostSignum TSA, právech a povinnostech uživatelů kvalifikovaných časových razítek vydaných PostSignum TSA a spoléhajících se stran.

Tento dokument má informační charakter, nenahrazuje politiku pro vydávání časových razítek a není součástí smlouvy o poskytování certifikačních služeb uzavírané mezi zákazníkem a Českou poštou, s.p. (dále i Česká pošta nebo ČP).

1.2 Historie uskutečněných auditů a kontrol systému

Datum	Typ auditu/kontroly	Výrok auditora/kontrolora
	Systém PostSignum TSA dosud neprošel žádným auditem či kontrolou.	

2 Kontaktní informace

2.1 Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb je:

Česká pošta, s.p., IČ 47114983
Politických vězňů 909/4
225 99 Praha 1

2.2 Kontaktní pracoviště

Uzavírání smluv se zákazníky PostSignum zajišťují obchodní a kontaktní místa PostSignum TSA. Kontaktní informace jsou k dispozici na webových stránkách:

http://qca.postsignum.cz

Vydávání časových razítek zajišťuje poskytovatel prostřednictvím aplikace na speciálním serveru, která přijímá požadavky na vydání časových razítek.

2.3 Komunikace s klienty

Dotazy týkající se poskytování služeb PostSignum TSA lze zasílat na kontaktní pracoviště pro poskytování služeb.

Odborné dotazy zodpovídá následující pracoviště:

Česká pošta, s.p.
Oddělení vývoje QCA/VCA
Sazečská 603/9
225 99 Praha 10
email: admca.vakph@cpost.cz

Tazatel obdrží odpověď do tří pracovních dnů.

2.4 Zveřejňování informací

Tuto zprávu pro uživatele, politiky pro vydávání časových razítek a ostatní veřejné informace lze nalézt na webových stránkách:

http://qca.postsignum.cz

3 Typy časových razítek a jejich vydávání

3.1 Typy časových razítek

Časovým razítkem, které vydává PostSignum TSA, se rozumí kvalifikované časové razítko v souladu se zákonem č. 227/2000 Sb. o elektronickém podpisu.
Jde o datovou zprávu, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

PostSignum TSA vydává jeden typ časových razítek popsaný v dokumentu „Politika vydávání kvalifikovaných časových razítek PostSignum TSA“.
Časová razítka vydávaná PostSignum TSA vyhovují standardu RFC 3161.

3.2 Uzavření smlouvy

Zákazníkem PostSignum TSA je právnická osoba, podnikající fyzická osoba (podnikatel), nepodnikající fyzická osoba, státní orgán nebo orgán místní samosprávy.

Zákazník získá přístup ke službám PostSignum TSA uzavřením písemné smlouvy o poskytování certifikačních služeb. Tato smlouva se uzavírá v souladu se Všeobecnými obchodními podmínkami elektronických služeb ČP.

Smlouva je zákazníkem podepsána tak, jak je v obchodním styku obvyklé.
Identita fyzické osoby je ověřována na základě jednoho osobního dokladu (občanský průkaz nebo cestovní pas).

Zákazník ve smlouvě definuje pověřenou osobu, která je oprávněna jednat za zákazníka ve věci poskytování služby vydávání časových razítek. Pověřená osoba definuje způsob autentizace při zasílání požadavku na vydání časového razítka a další parametry služby.

3.3 Ověřovací procedury a podání žádosti o časové razítko

Žádost o vydání kvalifikovaného časového razítka podávají zákazníci ČP na základě uzavřené smlouvy mezi ČP a zákazníkem. Žadatel o časové razítko (osoba nebo aplikace vystupující jménem zákazníka) vytvoří bezpečné autentizované spojení s PostSignum TSA prostřednictvím protokolu HTTPS, v rámci kterého se identifikuje a autentizuje:

- komerčním certifikátem vydaným certifikační autoritou PostSignum VCA, nebo
- jménem a heslem.

Po platné identifikaci a autentizaci vytvoří žadatel otisk (hash) elektronických dat (zprávy, dokumentu, transakce, atd.), který je následně uložen do žádosti o kvalifikované časové razítko (dle RFC 3161). Takto vytvořená datová struktura je prostřednictvím navázaného

spojení předána PostSignum TSA. Následně je žádost zaslána jednomu ze serverů TSU (vydávajících samotná časová razítka, dále jen TSU) pro posouzení správnosti a označení.

K zamítnutí žádosti může dojít zejména v případě:

- neúspěšné identifikace a autentizace
- že žádost o časové razítko nesplňuje náležitosti definované politikou pro vydávání časových razítek.

Povolené algoritmy pro výpočet otisku (hashe), který se ukládá do žádosti o časové razítko, jsou:

- SHA-1, SHA-256, SHA-384, SHA-512

3.4 Vydání kvalifikovaného časového razítka

Po přijetí žádosti o časové razítko provede PostSignum TSA kontrolu formální správnosti žádosti a v případě kladného výsledku kontrol žádosti je k otisku (hash) dat, obsaženém v žádosti, přidán do datové struktury časový údaj z důvěryhodného měřidla času. Takto vytvořená datová struktura je elektronicky označena daty pro vytváření elektronické značky TSA, čímž vznikne časové razítko podle RFC 3161, které je archivováno.

Odpověď včetně časového razítka je odeslána žadateli o kvalifikované časové razítko.

3.5 Ověření časového razítka

Pro ověření kvalifikovaného časového razítka se provádějí následující kroky:

- ověření otisku (hash) ověřovaných dat uvedeného v časovém razítku vůči nově vypočtenému otisku (hash) z elektronických dat dostupných ověřující straně,
- ověření platnosti elektronické značky pomocí certifikátu TSU.

Dále je stažen aktuální příslušný seznam zneplatněných certifikátů (CRL) a ověří se platnost:

- použitého certifikátu TSU, kterým je razítko označeno,
- certifikátu certifikační autority PostSignum Qualified CA, která vydala certifikát TSU,
- certifikátu certifikační autority PostSignum Root QCA, která vydala certifikát autority PostSignum Qualified CA.

V případě, že otisky (hash) dat jsou při shodném algoritmu shodné a byla ověřena platnost všech elektronických značek a kvalifikovaných certifikátů, je časové razítko platné.

Minimální životnost elektronické značky na časovém razítku PostSignum TSA je rovna platnosti certifikátů TSU, avšak předpokládaná reálná životnost této elektronické značky je vyšší.

4 Omezení použití

Kvalifikovaná časová razítka vydávaná autoritou PostSignum TSA nejsou primárně určena pro komunikace nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod. nebo v oblastech souvisejících s bezpečností a obranyschopností státu.
Kromě výše uvedeného nejsou stanovena žádná další omezení pro používání kvalifikovaného časového razítka, vydaného v souladu s obsahem politiky pro vydávání časových razítek.

Kvalifikované časové razítko, vydané PostSignum TSA, je možno použít pro následující účely:

- tam, kde se vyžaduje použití kvalifikovaného časového razítka podle zákona č. 227/2000 Sb. o elektronickém podpisu v platném znění;
- tam, kde se vyžaduje použití kvalifikovaného časového razítka podle zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů v platném znění;
- v ostatních případech, kde existuje potřeba prokázání existence konkrétních dat (dokumentu) před daným časovým okamžikem.

4.1 Přesnost času v časovém razítku

Maximální odchylka časového údaje ve vydaném kvalifikovaném časovém razítku od hodnoty světového UTC času je 1 sekunda.

4.2 Doba uchování auditních záznamů

Auditní záznamy (včetně vydaných časových razítek) jsou uchovávány minimálně po dobu deseti let.

5 Povinnosti zákazníků a jejich zástupců

Zákazník musí zejména:

- poskytovat pravdivé a úplné informace při uzavírání smlouvy o poskytování certifikačních služeb,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které jsou uvedeny ve smlouvě.

Pověřená osoba zákazníka musí zejména:

- poskytovat pravdivé a úplné informace o žadatelích oprávněných žádat o časové razítko,
- zajistit důvěrnost autentizačních informací, se kterými při registraci žadatelů přichází do styku.

Žadatelem o časové razítko je fyzická osoba nebo systém, který z pověření zákazníka žádá o vydání časového razítka. Žadatel musí zejména:

- zajistit důvěrnost autentizačních informací potřebných pro ověření identity žadatele při podávání žádosti o časové razítko,
- seznámit se s politikou, podle které mu bylo časové razítko vydáno.

6 Základní povinnosti spoléhajících se stran a ostatních uživatelů

Spoléhající se strana provádí následující činnosti:

- ověřuje otisk (hash) ověřovaných dat,
- ověřuje platnost elektronické značky pomocí certifikátu TSU.

Spoléhající se strana dále získá aktuální příslušný seznam zneplatněných certifikátů (CRL) a ověří platnost:

- použitého certifikátu TSU, kterým je razítko označeno,
- certifikátu certifikační autority PostSignum Qualified CA, která vydala certifikát TSU,
- certifikátu certifikační autority PostSignum Root QCA, která vydala certifikát autority PostSignum Qualified CA;

Spoléhající se strana zváží, zda časové razítko vydané podle této politiky je vhodné pro účel, ke kterému bylo použito.

Podrobný popis platnosti časového razítka je uveden v dokumentu „Politika vydávání kvalifikovaných časových razítek PostSignum TSA“.

7 Omezení záruky a odpovědnosti

Česká pošta se zavazuje, že splní veškeré povinnosti uložené politikami vydávání kvalifikovaných časových razítek, podle kterých vydává kvalifikovaná časová razítka, a mandatorními ustanoveními příslušných právních předpisů. Česká pošta poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb uzavřené se zákazníkem.

Záruky uvedené výše jsou výlučnými zárukami České pošty a Česká pošta jiné záruky neposkytuje.

Česká pošta neodpovídá za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb uživatelům, zejména za provozování v rozporu s podmínkami uvedenými v politice vydávání kvalifikovaných časových razítek, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.

8 Smlouvy a certifikační politiky

Vztah mezi zákazníkem a Českou poštou, jakožto poskytovatelem služby vydávání časových razítek, je (kromě příslušných ustanovení mandatorních právních předpisů) upraven smlouvou, jejíž součástí jsou mimo jiné

- všeobecné obchodní podmínky elektronických služeb ČP,
- platná politika pro vydávání kvalifikovaných časových razítek,
- aktuální ceník.

Vztah mezi spoléhající se stranou a Českou poštou je upraven příslušnými ustanoveními platných politik pro vydávání časových razítek.

Vztah České pošty a spoléhajících se stran není upraven smlouvou.

Všechny vyjmenované dokumenty jsou dostupné na webových stránkách:
http://qca.postsignum.cz
nebo na kontaktních místech PostSignum TSA.

9 Ochrana osobních dat

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování služby vydávání časových razítek. Zásady ochrany osobních údajů jsou obsaženy v politice pro vydávání časových razítek, všeobecných obchodních podmínkách a v aktuální prováděcí směrnici PostSignum TSA a vycházejí z příslušných ustanovení zákona č. 101/2000 Sb. o ochraně osobních údajů ve znění pozdějších předpisů.

10 Politika náhrady a reklamační řízení

V případě nedodání služeb v definované kvalitě má zákazník nárok na vrácení ceny za příslušnou službu nebo poskytnutí nové služby zdarma.

Zákazník PostSignum TSA podává žádost o reklamaci na kontaktních místech PostSignum TSA nebo na pracovišti Helpdesk. Nejpozději do tří pracovních dnů posoudí oprávněnost reklamace reklamační oddělení PostSignum TSA. Zákazník je informován o výsledku rozhodnutí e-mailem nebo dopisem. Se zákazníkem je dohodnuta případná forma náhrady.

11 Právní prostředí

Činnost PostSignum TSA se řídí příslušnými ustanoveními právního řádu České republiky, zejména

- zákonem č. 227/2000 Sb. o elektronickém podpisu ve znění pozdějších předpisů,
- vyhláškou č. 378/2006 ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb,
- zákonem č.101/2000 Sb. o ochraně osobních údajů ve znění pozdějších předpisů.

12 Akreditace a kontrola bezpečnostní shody

Česká pošta se jako poskytovatel certifikačních služeb PostSignum QCA stala dne 3. 8. 2005 akreditovaným poskytovatelem certifikačních služeb na základě akreditace udělené Ministerstvem informatiky ČR.
Následně dne 1.7.2009 ČP rozšířila poskytované certifikační služby o službu vydávání časového razítka s názvem PostSignum TSA (dále i jenom TSA).

Činnost PostSignum TSA podléhá kontrole. Kontrolu bezpečnostní shody provádějí pracovníci České pošty, nebo externí auditor nezávislý na České poště, s.p. Intervaly konání kontrol jsou uvedeny v politice pro vydávání časových razítek.