Česká pošta

Zpráva pro uživatele TSA

Verze 2.1

Obsah dokumentu

Evidence revizí a změn

Verze	Účinnost od	Důvod a popis změny	Autor	Schválil
0.1	21. 1. 2009	Draft	Daniel Joščák	
0.2	22. 2. 2009	Připomínkování dokumentu	Martin Šlancar	
0.3	24. 2. 2009	Zapracování připomínek	Ondřej Steiner	
1.0	26. 2. 2009	„Milestone“ verze schválená manažerem TSA	Martin Šlancar	Manažer QCA
1.1	22. 5. 2009	„Milestone“ verze schválená manažerem TSA, zapracování připomínek Ministerstva vnitra	Martin Šlancar	Manažer QCA
1.2	1. 8. 2012	Aktualizace dokumentu	H. Radová Švecová	Manažer CA
1.3	21. 1. 2013	Aktualizace seznamu auditů	Miroslav Trávníček	Manažer CA
1.4	12. 4. 2013	Aktualizace seznamu auditů	Miroslav Trávníček	Manažer CA
1.5	21. 7. 2014	Aktualizace seznamu auditů	Miroslav Trávníček	Manažer CA
1.6	20. 2. 2015	Aktualizace seznamu auditů, oprava názvu VOP	Miroslav Trávníček	Manažer CA
1.7	1. 6. 2015	Aktualizace seznamu auditů	Miroslav Trávníček	Manažer CA
1.8	21. 1. 2016	Aktualizace seznamu auditů	Miroslav Trávníček	Manažer CA
2.0	1. 7. 2016	Změny dle eIDAS	Vosková/Trávníček	Manažer CA
2.1	8. 9. 2017	Změny v souvislosti s akreditací	Miroslav Trávníček	Manažer CA

1. Úvod

1.1. Účel dokumentu

Tento dokument poskytuje základní informace o autoritě časových razítek PostSignum TSA, právech a povinnostech uživatelů kvalifikovaných elektronických časových razítek (dále také jen 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
Duben 2017	Audit potvrzující, že poskytované kvalifikované služby vytvářející důvěru jsou ve shodě s nařízením eIDAS a příslušnými technickými normami, provedený společností Tayllorcox s.r.o.	Je ve shodě
Březen 2017	Recertifikační audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS.	Je v souladu
Únor 2016	Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS.	Je v souladu
Září 2015	Částečné posouzení bezpečnostní shody (interní audit ČP)	Vyhovuje
Březen 2015	Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS.	Je v souladu
Září 2014	Částečné posouzení bezpečnostní shody (interní audit ČP)	Vyhovuje
Březen 2014	Recertifikační audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS.	Je v souladu
Září 2013	Částečné posouzení bezpečnostní shody (interní audit ČP)	Vyhovuje
Únor 2013	Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS.	Je v souladu
Prosinec 2012	Celkové posouzení bezpečnostní shody, provedené firmou Deloitte Advisory.	Vyhovuje
Únor 2012	Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS.	Je v souladu
Srpen 2011	Částečné posouzení bezpečnostní shody (interní audit ČP)	Vyhovuje
Únor 2011	Recertifikační audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS.	Je v souladu
Listopad 2010	Částečné posouzení bezpečnostní shody (interní audit ČP)	Vyhovuje
Únor 2010	Částečné posouzení bezpečnostní shody (Microsoft Root Certificate Program), provedené firmou Deloitte Advisory	Vyhovuje
Leden 2010	Dozorový audit na certifikaci vůči ISO 9001 a	Je v souladu

	ISO 27001, provedený firmou CQS.	
Říjen 2009	Částečné posouzení bezpečnostní shody (interní audit ČP)	Vyhovuje

2. Kontaktní informace

2.1. Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb PostSignum 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. Kontaktní informace jsou k dispozici na webových stránkách PostSignum.

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:

e-mail: helpdesk-ca@cpost.cz
tel.: 840 111 244 (linka je zpoplatněna)

2.4. Zveřejňování informací

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

http://www.postsignum.cz

3. Typy časových razítek a jejich vydávání

3.1. Typy časových razítek

Časovým razítkem, které vydává PostSignum TSA, se rozumí kvalifikované elektronické časové razítko v souladu s nařízením eIDAS.

Jde o datovou zprávu, kterou vydal 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 časových razítek PostSignum TSA“. OID politiky je uvedeno v dokumentu.

Časová razítka vydávaná PostSignum TSA vyhovují standardu RFC 3161.

3.2. Uzavření smlouvy

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

3.2.1. Písemná smlouva

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

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.

3.2.2. Elektronická smlouva (předplacený balíček časových razítek)

Zákazník získá přístup ke službám PostSignum TSA zakoupení předplaceného balíčku časových razítek přes objednávkový systém poskytovatele. Tato smlouva se uzavírá v souladu se Všeobecnými obchodními podmínkami certifikačních služeb.

Zákazník v objednávce (elektronické smlouvě) definuje kontaktní osobu. Kontaktní osoba definuje způsob autentizace při zasílání požadavku na vydání časového razítka.

3.3. Ověřovací procedury a podání žádosti o časové razítko

Žádost o vydání 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,
- ukončení platnosti soukromého klíče TSA.

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 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 pečetě TSA, čímž vznikne časové razítko podle RFC 3161, které je archivováno.

Odpověď včetně časového razítka je odeslána žadateli o časové razítko.

3.5. Ověření časového razítka

Pro ověření 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 pečetě pomocí certifikátu TSA.

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

- použitého certifikátu TSA, kterým je razítko označeno,
- certifikátu certifikační autority PostSignum Qualified CA, která vydala certifikát TSA,
- 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 pečetí a příslušných certifikátů, je časové razítko platné.

Minimální životnost elektronické pečetě na časovém razítku PostSignum TSA je rovna platnosti certifikátu TSA.

4. Omezení použití

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 elektronického časového razítka, vydaného v souladu s obsahem politiky pro vydávání časových razítek.

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

- tam, kde se vyžaduje použití kvalifikovaného elektronického časového razítka podle zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce;
- tam, kde se vyžaduje použití kvalifikovaného elektronického časového razítka podle nařízení eIDAS 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 v souladu s právními předpisy ČR.

5. Povinnosti zákazníků a jejich zástupců

Zákazníkem autority PostSignum TSA je právnická nebo fyzická osoba, která je v příslušném smluvním vztahu s Českou poštou. Zákazník musí zejména

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

Pověřená nebo kontaktní osoba zákazníka musí zejména:

- zajistit důvěrnost autentizačních informací

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 zákazníka 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 pečetě pomocí certifikátu TSA.

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

- použitého certifikátu TSA, kterým je razítko pečetěno,
- certifikátu certifikační autority PostSignum Qualified CA, která vydala certifikát TSA,
- 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 časových razítek PostSignum TSA“.

7. Omezení záruky a odpovědnosti

Česká pošta se zavazuje, že splní veškeré povinnosti uložené politikami vydávání časových razítek, podle kterých vydává 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, nebo platnosti zakoupeného předplaceného balíčku časových razítek.

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 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 certifikačních služeb,
- platná politika pro vydávání časových razítek,
- aktuální ceník.

Vztah mezi spoléhající se stranou a Českou poštou (jakožto poskytovatelem služby vydávání časových razítek) je upraven příslušnými ustanoveními platných politik vydávání časových razítek.

Vztah České pošty a spoléhajících se stran není upraven smlouvou.

Všechny vyjmenované dokumenty jsou dostupné na webových stránkách PostSignum nebo na obchodních místech PostSignum.

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 certifikačních služeb 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.

Bližší informace o reklamačním řízení jsou uvedeny na webových stránkách PostSignum.

11. Právní prostředí

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

- zákonem č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce,
- 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 č.101/2000 Sb. o ochraně osobních údajů ve znění pozdějších předpisů.

12. Akreditace a posouzení 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).

Dne 21. 2. 2011 získal informační systém PostSignum TSA certifikaci shody s ISO 9001:2001 (QMS, systém řízení kvality) a ISO 27001 (ISMS, systém řízení bezpečnosti informací).

Dne 1. 7. 2016 se Česká pošta stala kvalifikovaným poskytovatelem služeb vytvářejících důvěru dle eIDAS.

Dne 30. 8. 2017 byly v důvěryhodném seznamu kvalifikovaných služeb přidána kvalifikovaná služba vydávání kvalifikovaných elektronických časových razítek.

Činnost certifikační autority PostSignum podléhá kontrole. Posouzení shody s platnými právními předpisy a technickými normami provádí externí auditor nezávislý na České poště, s.p. Intervaly konání kontrol jsou uvedeny v certifikačních politikách.