Česká pošta

Technické řešení

„Poskytování časových razítek“

Zpracoval	[redacted]
Útvar	Odbor provoz komerčních úloh
Datum vytvoření	1. 11. 2010
Datum aktualizace	7. 1. 2019
Počet stran	07
Počet příloh	00
Verze	2.3

Obsah dokumentu

Úvod

Časovými razítky, která autorita časových razítek (dále jen PostSignum TSA) vydává se rozumí kvalifikovaná elektronická časová razítka v souladu s nařízením Evropského parlamentu a Rady (EU) č. 910/2014 z 23.7.2014 o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES a v souladu se zákonem č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce. Tato elektronická časová razítka důvěryhodným způsobem spojují data v elektronické podobě s časovým okamžikem, a zaručují, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Při podepsání smlouvy (mezi zadavatelem a uchazečem) se stanoví způsob přihlášení k odběru časových razítek – určí se tzv. přihlašovací účty zákazníka. Správu účtů mohou provádět pouze pověřené osoby zákazníka.

Každý účet obsahuje informace o způsobu přihlašování k serverům uchazeče při odběru časových razítek (volba mezi autentizací *certifikátem* nebo autentizací *jméno+heslo*). Tyto účty jsou v systémech sledovány samostatně, lze tedy vykazovat měsíční statistiky na jednotlivé účty.

Předplacené balíčky časových razítek
Zákazník si zakoupí balíček časových razítek (provede dobití účtu). Časová razítka může Zákazník z účtu **čerpat po neomezenou dobu** až do vyčerpání balíčku. Účet lze kdykoliv dobít zakoupením nového balíčku časových razítek a tím navýšit počet časových razítek.

Česká pošta garantuje u časových razítek (dle RFC 3161) platnost **minimálně 5 let**. Certifikáty, kterými se označují (pečetí) časová razítka, jsou vystavovány na šest let a jsou každý rok obměňovány.

Architektura PostSignum TSA

PostSignum TSA je realizována dvěma jednotkami TSU (timestamping unit) umístěnými v primární lokalitě a dvěma jednotkami umístěnými v záložní lokalitě.

Obě provozní jednotky v každé lokalitě vydávají časová razítka současně. Rozdělování žádostí mezi tyto dvě jednotky zajišťuje load-balancing/failover řešení předáním žádostí na jednu z dvojice přístupových jednotek, která žádost po ověření identity žadatele následně předá na jí přiřazenou provozní jednotku.

Timestamp servery jsou realizovány specializovanými zařízeními nCipher Time Stamp Server, označovanými jako DSE200 (Document Sealing Engine 200). Jedná se o síťová zařízení s integrovaným HSM pro uložení soukromých klíčů TSA; použité HSM mají certifikaci podle FIPS 140-2 na úroveň 3.

Technická specifikace - rozhraní TSA pro žádající aplikace

PostSignum TSA poskytuje časová razítka podle standardu RFC3161 (dále jen standard) pomocí protokolu https. Základní popis datových struktur časového razítka je uveden ve standardu, pro práci s nimi doporučujeme využívat běžně dostupných softwarových knihoven (BouncyCastle, IAIK, Eldos, Adobe…).
Časová razítka jsou poskytována prostřednictvím internetového připojení nebo prostřednictvím Centrálního místa služeb (dále CMS).

Žádost o časové razítko

Žádost o časové razítko musí být ve formátu *Time Stamp Request* podle standardu. V žádosti doporučujeme uvádět tyto údaje:

- Nonce (jednoznačný identifikátor),
- certReq=true (v odpovědi jsou pak přiloženy certifikáty),
- messageImprint vytvořený pomocí SHA-1 nebo SHA-2

Žádost nesmí obsahovat rozšíření (extensions).
Povolené algoritmy pro výpočet otisku (hashe) jsou SHA-1, SHA-256, SHA-384, SHA-512.

Zaslání žádosti, příjem odpovědi

Žádost o razítko musí být zaslána na server TSA protokolem https metodou POST v souladu se standardem. Z důvodu zajištění vysoké dostupnosti serverů TSA budou zaslané žádosti distribuovány na více paralelně pracujících serverů, nebude možné tedy zaručit, že pořadí odpovědí bude přesně odpovídat pořadí žádostí a že všechny elektronické značky/pečetě budou vytvořeny s pomocí jednoho páru klíčů. Servery budou identifikovány svou elektronickou značkou/pečetí, každý ze serverů pak bude vést vlastní řadu sériových čísel razítek.

TSA PostSignum bude požadovat autentizaci volitelně:

- komerčním certifikátem PostSignum VCA, nebo
- jménem/heslem (basic).

Podle způsobu autentizace a smluvního vztahu je žádost zaslána na některou z těchto adres:

1. Paušální odběr

a) Přístup přes internet

Lokalita	**Autentizace:**	**Webová adresa:**
Primární	certifikátem	https://tsa.postsignum.cz/TSS/HttpTspServer/
	jménem a heslem	https://tsa.postsignum.cz:444/TSS/HttpTspServer/
Záložní	certifikátem	https://tsa.postsignum.eu/TSS/HttpTspServer/
	jménem a heslem	https://tsa.postsignum.eu:444/TSS/HttpTspServer/

b) Přístup přes CMS2

Lokalita	**Autentizace:**	**Webová adresa:**
Primární	certifikátem	https://tsa.postsignum.cms2.cz/TSS/HttpTspServer/
	jménem a heslem	https://tsa.postsignum.cms2.cz:444/TSS/HttpTspServer/

2. Předplacené balíčky

a) Přístup přes internet

Lokalita	Autentizace:	Webová adresa:
Primární	certifikátem	https://www3.postsignum.cz/TSS/TSS_crt/ https://www.postsignum.cz/TSS/TSS_crt/
	jménem a heslem	https://www3.postsignum.cz/TSS/TSS_user/ https://www.postsignum.cz/TSS/TSS_user/
Záložní	certifikátem	https://www.postsignum.eu/TSS/TSS_crt/
	jménem a heslem	https://www.postsignum.eu/TSS/TSS_user/

b) Přístup přes CMS2

Lokalita	Autentizace:	Webová adresa:
Primární	certifikátem	https://www.postsignum.cms2.cz/TSS/TSS_crt/
	jménem a heslem	https://www.postsignum.cms2.cz/TSS/TSS_user/

Server TSA odpovídá zasláním odpovědi ve formátu *Time Stamp Response* podle standardu. Pokud nedojde k chybě zpracování žádosti (pkiStatus < 2), obsahuje odpověď též časové razítko ve formátu *Time Stamp Token*.

Formát časového razítka

Časové razítko *Time Stamp Token* obsahuje vložené údaje *TSTInfo* tak, jak jsou specifikovány ve standardu. Razítko nebude obsahovat rozšíření (extensions), bude obsahovat příznak řazení (ordering=false).

V případě požadavku na certifikát (certReq=true) bude k podpisu přiložen certifikát TSA odpovídající požadavkům standardů a platné legislativy. Certifikát a elektronickou značku na TSA doporučujeme ověřit běžným způsobem podle pravidel ověřování elektronického podpisu, navíc pak na přítomnost specifických údajů TSA (*KeyPurposeID* musí mít hodnotu *id-kp-timeStamping*). K ověření značky je třeba použít kořenový certifikát PostSignum Root CA.

Nad rámec standardu bude k podpisu dále přiložen atributový certifikát poskytovatele časového údaje obsahující údaje *Timing Metrics* a *Timing Policy*. Tyto údaje nejsou však pro běžnou práci s časovým razítkem podstatné.

Parametry služby

Poskytovatel garantuje níže uvedené parametry poskytování časových razítek:

Dostupnost služby	
Časová dostupnost služby (v %)	99,9% připojení přes Centrální místo služeb (CMS)* 99,5% připojení přes internet*
Rozsah zaručeného provozu služby	0:00 -23:59 hod. (24×7) s výjimkou plánované výluky/odstávky

Plánované výluky/odstávky	8 hodin max. 6x ročně, tj. 48 hodin/rok - o víkendech a svátcích

Výkonnostní parametry služby	
Garantovaný počet zpracovaných žádostí za 1 sekundu pro zákazníka	5
Maximální počet zpracovaných žádostí za 1 sekundu	300**
Maximální počet vydaných časových razítek za 1 hodinu	1 080 000**

** vzorec pro výpočet průměrné dostupnosti služby v procentech je prováděn z času ohlášení/zjištění a vyřešení incidentu podle tohoto schématu:*

$$D_{TSA} = 100 - \frac{100 \sum_{i=0}^{n}(t_{vi} - t_{zi})}{M} \quad [\%]$$

Kde:

D_{TSA}	*dostupnost TSA v % (vypočítává se na jedno desetinné místo)*
n	*celkový počet incidentů (kromě počtu incidentů v rámci plánované výluky)*
t_{vi}	*časový okamžik vyřešení incidentu, tzn. obnovení provozu odstraněním projevu incidentu či nasazením náhradního řešení,*
t_{zi}	*časový okamžik zjištění/ohlášení incidentu*
$(t_{vi} - t_{zi})$	*doba obnovy (v minutách)*
M	*počet minut v měřeném období (ponížený o dobu plánovaných odstávek)*

*** jedná se o maximální kapacitu systému – není vyhrazena pouze pro jednoho zákazníka.*

Testovací (demo) časové razítko

Pro vyzkoušení služby časového razítka je k dispozici zdarma TSA DEMO PostSignum.

Upozornění
Upozorňujeme, že časová razítka získaná na testovací TSA DEMO PostSignum nelze považovat za důvěryhodná (například pro archivaci dat).
Služba TSA DEMO PostSignum nemusí být stále v provozu.

Přihlášení k testovacímu serveru pomocí jména a hesla:
URL adresa 1: https://www3.postsignum.cz/DEMOTSA/TSS_user/
URL adresa 2: https://www.postsignum.cz/DEMOTSA/TSS_user/

Přihlašovací jméno: **demoTSA**
Heslo: **demoTSA2010**

Přihlášení k testovacímu serveru pomocí komerčního certifikátu:

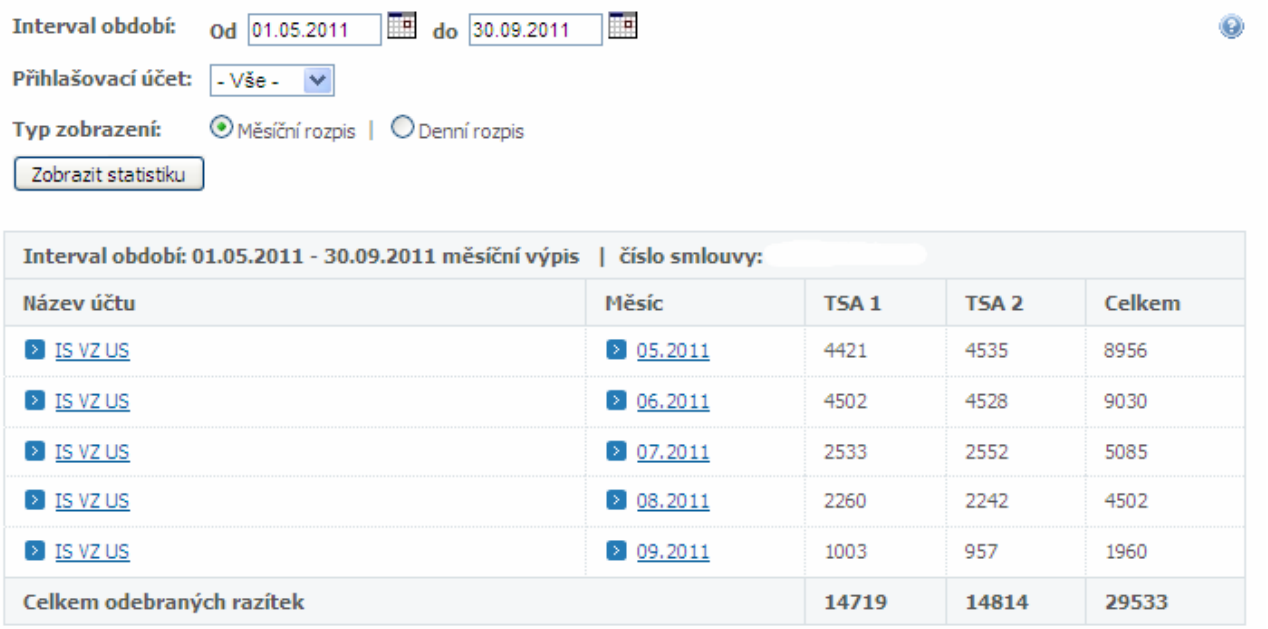
URL adresa 1: https://www3.postsignum.cz/DEMOTSA/TSS_crt/
URL adresa 2: https://www.postsignum.cz/DEMOTSA/TSS_crt/

Pro přihlášení lze využít jakýkoliv komerční certifikát vydaný certifikační autoritou PostSignum (osobní nebo serverový).

Zákaznický portál PostSignum (statistiky, kontrola fakturace)

Pověřené osobě zákazníka bude umožněn zdarma přístup do zákaznického portálu PostSignum, ve kterém bude mít možnost sledovat počet odebraných časových razítek za jednotlivé účty. Portál umožňuje vytváření denních, měsíčních či ročních souhrnů odebraných časových razítek. Aktualizace dat portálu probíhá u časových razítek jedenkrát denně v nočních hodinách.

Statistiky odebraných časových razítek dle smlouvy nebo přihlašovacích účtů (roční, měsíční, denní)



Kontaktní údaje

Hlášení nedostupnosti TSA: incident.postsignum@cpost.cz