Česká pošta

Technické řešení

„Poskytování časových razítek“

v. 1.0

Obsah dokumentu

Úvod

Časovými razítky, která autorita časových razítek (dále jen PostSignum TSA) vydává se rozumí 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 **neomezeně čerpat po dobu pěti let od zakoupení posledního balíčku**. Účet lze kdykoliv dobít zakoupením nového balíčku časových razítek a tím nejen navýšit počet časových razítek, ale i prodloužit dobu čerpání doposud nevyčerpaných časových razítek z předchozích balíčků.

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..

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.

Poskytovatel si vyhrazuje právo omezit povolené kryptografické algoritmy, pokud si to vyžádá úprava právních předpisů nebo technických norem, které upravují činnost poskytovatelů certifikačních služeb.

Struktura žádosti o časové razítko

Název položky	**Popis**	**Hodnota/příznak použití**
Version	Verze protokolu časového razítka (povinná položka)	1
messageImprint		
HashAlgorithm	OID hash algoritmu (povinná položka)	SHA-1, SHA-256, SHA-384, SHA-512
HashedMessage	Otisk dat (povinná položka)	
reqPolicy	Identifikátor politiky (nepovinná položka)	OID této politiky
nonce	Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka)	
certReq	TRUE – odpověď musí obsahovat certifikát TSA FALSE nebo nevyplněno – odpověď nesmí obsahovat certifikát TSA (nepovinná položka)	TRUE, FALSE
extensions	Žádná rozšíření nejsou povolena	

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 budou vytvořeny s pomocí jednoho páru klíčů. Servery budou identifikovány svou elektronickou značkou, 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/

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/

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*.

Struktura odpovědi na žádost o časové razítko

Název položky	Popis	Hodnota/příznak použití
PKIStatus	Přirozené číslo, označující stav odpovědi (přidělení/nepřidělení časového razítka). Časové razítko bylo přiděleno a je součástí odpovědi, pouze pokud je hodnota tohoto pole 0 nebo 1.	**0** – TST bylo vydáno **1** – TST bylo vydáno (upravené) **2** – odmítnutí žádosti **3** – čekání na odpověď **4** – bezprostřední zneplatnění certifikátu TSA **5** – certifikát byl zneplatněn

PKIFailureInfo	BIT STRING. Uvádí důvod nepřidělení časového razítka. Součástí odpovědi na žádost o časové razítko je pouze v případě, že hodnota pole PKIStatus je jiná než 0 nebo 1 a časové razítko tedy není v odpovědi přítomno.	**BadAlg** – neznámý nebo nepodporovaný algoritmus **BadRequest** – nepovolená nebo nepodporovaná transakce **BadDataFormat** – špatný formát zaslaných dat **TimeNotAvailable** – nedostupný zdroj času TSA **UnacceptedPolicy** – požadovaná politika není podporovaná ze strany TSA **UnacceptedExtension** – požadované rozšíření není podporované ze strany TSA **AddInfoNotAvailable** – požadované doplňující informace nebyly identifikované nebo nejsou dostupné SystemFailure – žádost nemohla být zpracována kvůli chybě systému

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.

Struktura časového razítka

Název položky	**Popis**	**Hodnota/příznak použití**
Version	Verze protokolu časového razítka	1
Policy	Identifikátor politiky	OID této politiky
messageImprint	Shodný se žádostí	
HashAlgorithm	OID hash algoritmu	SHA-1, SHA-256, SHA-384, SHA-512
HashedMessage	Otisk dat	
serialNumber	Přirozené číslo do 160 bitů.	TSU přiděluje každému časovému razítku unikátní číslo
genTime	GeneralizedTime – hodnota UTC	
accurancy	Přesnost	

ordering	Položka definující vztah dvou časových razítek	FALSE
nonce	Náhodné číslo (64 bitů) ze žádosti. Je-li obsaženo v žádosti, pak to samé číslo musí obsahovat i odpověď.	
TSA	Rozlišovací jméno TSU	

Poznámka: Tato struktura je vložena do struktury SignedData podle [RFC 3852] s identifikátorem typu dat id-ct-TSTInfo.

TSA vloží do každého časového razítka údaj, který jednoznačně určuje politiku, podle níž bylo razítko vydáno.

Poskytovatel služby vydávání časových razítek zajistí, aby data v elektronické podobě, která jsou předmětem žádosti o vydání časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném časovém razítku.

TSU vloží do každého nově generovaného časového razítka celé číslo, jehož hodnota je jedinečná – položka serialNumber. Sériové číslo umístěné v časovém razítku je pro každé TSU v rámci TSA jednoznačné. Jednoznačnost v rámci TSA a poskytovatele certifikačních služeb je zajištěna kombinací položek časového razítka serialNumber a TSA.

TSA vloží do každého časového razítka důvěryhodnou hodnotu času, která odpovídá hodnotě UTC v čase přidělení časového razítka. Pole genTime časového razítka uvádí čas, kdy časové razítko bylo vytvořeno autoritou časových razítek.

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).