



EISLX01E5VVO

Objednávka č. DO202502595

OBJEDNATEL

Statutární město Liberec
Náměstí Dr. E. Beneše 1/1
460 59 Liberec

IČO: 00262978

DIČ: CZ00262978

Bankovní spojení: 4096302/0800

Vyřizuje: Mgr. Ivana Morávková

Telefon: 485 243 116

E-mail: moravkova.ivana@magistrat.liberec.cz**DODAVATEL**

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

IČO: 47114983

DIČ: CZ47114983

Termín dodání:	31. 8. 2025
Způsob úhrady:	bankovní převod
Splatnost faktury:	min. 14 dní

Na základě Vaší cenové nabídky u Vás objednáváme:

Kvalifikovaná časová razítka - předplacený balíček 500 000 kusů, cena za 1 kus 0,20 Kč bez DPH. Čerpání je časově neomezené. Dobití balíčku od objednávky trvá cca 1–2 pracovní dny od provedení platby zákazníkem. Nedílnou součástí objednávky je nabídka "Kvalifikovaná časová razítka" a technické řešení "Poskytování časových razítek".

Cena bez DPH	100 000 Kč
DPH 21 %	21 000 Kč
Celková cena včetně DPH	121 000 Kč

Na faktuře prosím uveďte **číslo naší objednávky**: DO202502595

Faktury zasílejte do datové schránky **7c6by6u** nebo na e-mail posta@magistrat.liberec.cz

Za objednatele schválil
Ing. Zbyněk Vavřina
vedoucí odboru vnitřních věcí

Datum a podpis oprávněné osoby za dodavatele

Objednávku tímto akceptujeme

Nabídka

“Kvalifikovaná časová razítka”

Zpracoval	Miroslav Trávníček
Útvar	útvar CAT
Datum vytvoření	1. 8. 2025
Aktualizace	
Počet stran	4
Počet příloh	1
Poskytovatel	Česká pošta, s. p., IČO 47114983 Politických vězňů 909/4, 225 99 Praha 1

Obsah dokumentu

1. Profil poskytovatele certifikačních služeb	3
2. Předmět nabídky	4
3. Cena	4
4. Popis řešení	4

1. Profil poskytovatele certifikačních služeb

Česká pošta, s.p. (ČP) je největším českým poskytovatelem poštovních služeb s dlouholetou tradicí a silnou pozicí na trhu. Mezi její klíčové služby patří zejména doručování listovních, balíkových a peněžních zásilek, dále pak zprostředkování platebních operací a emituje poštovní známky.

Stále významněji se však ČP prosazuje i na trhu elektronických služeb. Mezi elektronické služby patří i služby certifikační autority PostSignum, díky kterým může zákazník za velmi příznivou cenu získat především kvalifikované či komerční certifikáty nebo časová razítka. Elektronická komunikace je každodenním standardem. Je levná, rychlá a díky moderním službám České pošty, s.p. je také důvěryhodná a bezpečná.

Na základě dlouhodobé strategie poskytování elektronických služeb zákazníkům zprovoznila ČP v roce 2003 Veřejnou certifikační autoritu pro poskytování komerčních certifikátů. Zkušenosti z realizace a provozu této certifikační autority pak byly využity při budování Kvalifikované certifikační autority. V roce 2005 proběhlo akreditační řízení, po kterém Ministerstvo informatiky udělilo ČP akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb s účinností od 3.8.2005.

Dalším významným milníkem pro certifikační autoritu PostSignum byl rok 2009, kdy bylo zahájeno poskytování kvalifikovaných časových razítek. Časové razítko spojuje dokument v elektronické podobě s časovým okamžikem jeho vzniku a zaručuje, že konkrétní data v elektronické podobě v daný časový okamžik existovala, a je proto vhodným doplňkem elektronického podpisu. Služba kvalifikovaného časového razítka je významná pro spisové služby a především pro archivaci dokumentů v elektronické podobě.

Tyto hlavní služby jsou poskytovány prostřednictvím rozsáhlé sítě kontaktních míst ČP (cca 1000 míst s označením Czech POINT), dále pak prostřednictvím mobilních registračních autorit ČP (MRA), které realizují služby přímo u zákazníka. Na počátku roku 2012 byla distribuční síť rozšířena o tzv. Klientské registrační autority (KRA), kdy si část poskytované služby zajišťuje zákazník sám s tím, že jsou proškoleni jím určení zaměstnanci, kteří poskytují certifikační služby dalším zaměstnancům zákazníka. Od poloviny roku 2012 budou poskytovány rovněž služby Externí registrační autority (ERA), tj. zastupování ČP v poskytování certifikačních služeb externí firmou nejen pro vlastní zaměstnance, ale i pro třetí strany.

Všechny důležité informace o poskytování certifikačních služeb jsou publikovány na webových stránkách www.postsignum.cz.

Správu certifikátů, statistiky a konfiguraci služeb si mohou zákazníci provádět nebo sledovat prostřednictvím Zákaznického portálu. Tento portál je pro naše zákazníky zdarma.

Vedle základních certifikačních služeb si mohou zákazníci využít i doplňkové služby a produkty, prostřednictvím elektronického objednávkového systému na webových stránkách. Jedná se například o produkty pro bezpečné uložení soukromých klíčů, o SW produkty pro elektronické podepisování dokumentů a jejich archivaci, a spoustu dalších drobných převážně SW aplikací.

Certifikační autorita PostSignum v současné době poskytuje měsíčně přes 20 tis. kvalifikovaných certifikátů (celkem více jak 2 mil. kvalifikovaných certifikátů) a měsíčně vydává přes 40 mil. časových razítek (celkem více jak 2 mld. časových razítek), což ji řadí na první místo mezi akreditovanými poskytovateli certifikačních služeb v ČR.

Kvalitu a bezpečnost svých služeb může Certifikační autorita PostSignum jako jediná z akreditovaných poskytovatelů certifikačních služeb prokázat certifikací shody s ČSN EN ISO 9001:2016 (QMS, systém řízení kvality) a s ČSN ISO/IEC 27001:2014 (ISMS, systém řízení bezpečnosti informací).

Od roku 2010 je certifikační autorita PostSignum zařazena mezi důvěryhodné certifikační autority ve všech operačních systémech společnosti Microsoft. Na konci roku 2016 se certifikační autorita PostSignum stala důvěryhodnou autoritou rovněž v produktech společnosti Adobe.

V roce 2017 byl certifikační autoritě PostSignum na základě výsledku auditu udělen správním orgánem (Ministerstvem vnitra ČR) statut kvalifikovaného poskytovatele služeb vytvářejících důvěru v souladu s nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „nařízení eIDAS“).

Statut kvalifikovaného poskytovatele služeb vytvářejících důvěru byl udělen pro tyto služby:

- Vydávání kvalifikovaných certifikátů pro elektronické podpisy
- Vydávání kvalifikovaných certifikátů pro elektronické pečete
- Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek
- Vydávání kvalifikovaných elektronických časových razítek

2. Předmět nabídky

Předmětem nabídky je předplacený balíček časových razítek.

3. Cena

Balíček časových razítek	Cena za 1 ks razítka bez DPH	Celková cena balíčku bez DPH
100 000 ks	0,37 Kč	37 000,- Kč
300 000 ks	0,25 Kč	75 000,- Kč
500 000 ks	0,20 Kč	100 000,- Kč
750 000 ks	0,18 Kč	135 000,- Kč
1 000 000 ks	0,15 Kč	150 000,- Kč

4. Popis řešení

Zákazník si zakoupí balíček časových razítek (provede dobítí účtu). Tato razítka postupně z účtu čerpá. Účet lze kdykoliv dobít zakoupením nového balíčku časových razítek. Čerpání je časově neomezené.

Dobítí balíčku od objednávky trvá cca 1-2 pracovní dny od provedení platby zákazníkem. V případě nutnosti lze zařídit i okamžité dobítí s následnou platbou.

Stav účtu časových razítek lze monitorovat v Zákaznickém portále, případně automatizovaně zavoláním webové služby, která vrátí počet zbývajících časových razítek.

Technické řešení je popsáno v příloze.

Nabídka je platná do 1. 2. 2026.

Technické řešení

„Poskytování časových razítek“

Zpracoval	
Útvar	Specializovaný útvar CAT
Datum vytvoření	1. 11. 2010
Datum aktualizace	25. 1. 2022
Počet stran	07
Počet příloh	00
Verze	2.5

Obsah dokumentu

Úvod	3
Architektura PostSignum TSA	3
Technická specifikace - rozhraní TSA pro žádající aplikace	3
Žádost o časové razítko	4
Zaslání žádosti, příjem odpovědi.....	4
Formát časového razítka.....	5
Parametry služby	5
Testovací (demo) časové razítko	6
Zákaznický portál PostSignum (statistiky, kontrola fakturace).....	6
Kontaktní údaje	7

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 dobítí účtu). Časová razítka může Zákazník z účtu **čerpát 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 pečeti 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 v režimu 50/50, která žádost po ověření identity žadatele následně předá na jí přiřazenou provozní jednotku. Při výpadku jakéhokoliv serveru je stále zajištěna maximální kapacita systému.

Timestamp servery jsou realizovány specializovanými zařízeními. Jedná se o síťová zařízení s integrovaným HSM pro uložení soukromých klíčů TSA; použité HSM mají certifikaci podle FIPS 140-2 na úroveň 3 i certifikaci dle CC na EAL 4.

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 pečete budou vytvořeny s pomocí jednoho páru klíčů. Servery budou identifikovány svou elektronickou pečeti, 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 CMS

Lokalita	Autentizace:	Webová adresa:
Primární	certifikátem	https://tsa.postsignum.cms2.cz/TSS/HttpTspServer/
	jménem a heslem	https://tsa.postsignum.cms2.cz:444/TSS/HttpTspServer/
Záložní	certifikátem	https://tsa2.postsignum.cms2.cz/TSS/HttpTspServer/
	jménem a heslem	https://tsa2.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 CMS

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 a také certifikát vydávající autority daného pečetiho certifikátu. Elektronická pečeť časového razítka bude mít vždy hashovací algoritmus SHA-256 bez ohledu na to, jakým hashovacím algoritmem byl vytvořen otisk dat uvedený v žádosti o časové razítko. Certifikát a elektronickou pečeť 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 pečeti je třeba použít kořenový certifikát PostSignum Root CA.

Parametry služby

Poskytovatel garantuje níže uvedené parametry poskytování časových razítek:

Dostupnost služby	
Časová dostupnost služby (v %)	99,9% připojení přes 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 - mimo pracovní dobu 22- 06 hod - o víkendech a svátcích

Výkonnostní parametry služby	
Garantovaný počet zpracovaných žádostí za 1 sekundu pro zákazníka	5
Maximální počet zpracovaných žádostí jedné lokality TSA za 1 sekundu	700 **
Maximální počet vydaných časových razítek jedné lokality TSA za 1 hodinu	2 520 000 **

* 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: <https://demo.postsignum.cz:444/DEMO-TSS/HttpTspServer/>

Přihlašovací jméno: **demoTSA**

Heslo: **demoTSA2010**

Přihlášení k testovacímu serveru pomocí komerčního certifikátu:

URL adresa: <https://demo.postsignum.cz/DEMO-TSS/HttpTspServer/>

Pro přihlášení lze využít jakýkoliv komerční certifikát vydaný certifikační autoritou PostSignum nebo DEMO CA PostSignum VCA 4+5 (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)

Interval období: Od do

Přihlašovací účet:

Typ zobrazení: ☒ Měsíční rozpis | ☐ Denní rozpis

[Zobrazit statistiku](#)

Interval období: 01.05.2011 - 30.09.2011 měsíční výpis číslo smlouvy:				
Název účtu	Měsíc	TSA 1	TSA 2	Celkem
IS VZ US	05.2011	4421	4535	8956
IS VZ US	06.2011	4502	4528	9030
IS VZ US	07.2011	2533	2552	5085
IS VZ US	08.2011	2260	2242	4502
IS VZ US	09.2011	1003	957	1960
Celkem odebraných razítek		14719	14814	29533

Kontaktní údaje

Hlášení nedostupnosti TSA: helpdesk-ca@cpost.cz