

Dodatek č. 3 ke smlouvě o poskytování certifikačních služeb

1. Smluvní strany

Poskytovatel

Česká pošta, s.p.

zastoupený: _____

se sídlem Politických vězňů 909/4, 225 99 Praha 1, IČO 47114983, DIČ CZ47114983

zapsaný v obchodním rejstříku, vedeném u Městského soudu v Praze, sp. zn. A 7565

Zákazník

Název / Obchodní firma /

Jméno, příjmení, titul: ^{2,5} NEWPS.CZ s.r.o.

Sídlo: ^{2,5} Vyskočilova 1422/1a, 140 00 Praha 4 - Michle

IČO: ⁸ 25625632

DIČ: CZ25625632

Zastoupený: ³ _____

Pobočka / Org. jednotka: _____

Adresa pro zasílání faktur: ⁵ DS ID: 3y2qms4

E-mailová adresa pro
zasílání faktur: ^{5,9} _____

2. Změna údajů zákazníka ⁴ ☒

Zákazník tímto dodatkem oznamuje poskytovateli změny v údajích. Aktuální údaje viz bod č. 1 tohoto dodatku.

3. Změna trvání smlouvy ⁴ ☒

Obě smluvní strany se dohodly na změně trvání uzavřené smlouvy, a sice

- ☐ na ukončení smlouvy ke dni _____
- ☐ na změně trvání smlouvy z doby určité na dobu neurčitou
- ☒ na změně trvání smlouvy na dobu určitou do 30. 6. 2024

4. Rozšíření poskytovaných služeb ^{4,7} ☐

Obě smluvní strany se dohodly na rozšíření poskytovaných služeb, a sice

☐ rozšíření ⁴ služby poskytování klientské registrační autority PostSignum

Poskytování této služby je možné pouze v rámci služby vydávání kvalifikovaných a komerčních certifikátů PostSignum. Poskytnutí služby je podmíněno vzájemným odsouhlasením Podmínek poskytování klientské registrační autority ⁶.

☐ rozšíření ⁴ služby poskytování kvalifikovaných časových razítek PostSignum

Poskytnutí služby je podmíněno vzájemným odsouhlasením Podmínek poskytování kvalifikovaných časových razítek ⁶.

5. Změna obecných parametrů poskytovaných služeb ⁴ ☐

Obě smluvní strany se dohodly na změně těchto parametrů certifikačních služeb:

5.1 Zákazník požaduje ☐ zasílat / ☐ nezasílat žadatelům o certifikáty upozornění na končící platnost certifikátů. ⁵

5.2 Zákazník požaduje ☐ povolit / ☐ nepovolit žadatelům o certifikáty možnost vydání víceletého certifikátu. ⁵

6. Změna seznamu pověřených osob zákazníka ⁴ ☐

6.1 Na základě požadavku zákazníka se obě smluvní strany dohodly na změně seznamu pověřených osob

Změny jsou uvedeny v Přílohách č. : _____ tohoto dodatku.

7. Jiné změny ⁴ ☒

Smluvní strany se tímto dodatkem dohodly na těchto změnách shora uvedené smlouvy:

1. Smluvní strany se dohodly na úplném nahrazení přílohy č. 1 – Specifikace předmětu smlouvy novou přílohou č. 1, která je nedílnou součástí tohoto dodatku.

2. Smluvní strany se dohodly na úplném nahrazení přílohy č. 2 – Všeobecné obchodní podmínky novou přílohou č. 2, která je nedílnou součástí tohoto dodatku.

Ostatní ujednání smlouvy se nemění a zůstávají nadále v platnosti.

Dodatek č. 3 je platný dnem jeho podpisu smluvními stranami a účinný od 1. 7. 2021.

8. Podpisy smluvních stran

Podpisem smluvních stran se tento dodatek, včetně příloh, stává nedílnou součástí smlouvy. Ostatní ustanovení smlouvy zůstávají beze změny.

Za poskytovatele

Praha		
Místo	Datum	
		
Jméno a příjmení		Podpis a razítko

Za zákazníka

Praha		
Místo	Datum	
		
Jméno a příjmení ³		Podpis a razítko

Legenda:

- 1 Doplníte číslo platné smlouvy, ke které bude dodatek uzavřen.
- 2 Údaje musí souhlasit s údaji uvedenými ve veřejných rejstřících nebo v živnostenském rejstříku.
- 3 Uvede se statutární zástupce zákazníka, nebo osoba jím zmocněná k podepsání tohoto dodatku smlouvy. Pokud je v dokladu o právní osobnosti zákazníka uveden způsob jednání a podepisování, musí být při podepisování dodatku ke smlouvě nebo při podepsání zmocnění k podepsání dodatku ke smlouvě dodrženo.
- 4 Příslušnou změnu označte křížkem a doplňte požadované změny nebo označte změnu dle předtisku.
- 5 Pro změnu tohoto údaje není bezpodmínečně nutné uzavírat dodatek ke smlouvě. V tomto případě stačí, aby zákazník, popř. pověřená osoba zákazníka, zaslala na obchodní místo certifikační autority, jejichž seznam je uvedený na www.postsignum.cz, oznámení o změně.
- 6 Podmínky poskytování klientské registrační autority a Podmínky poskytování kvalifikovaných časových razítek je oprávněna za zákazníka podepsat pověřená osoba.
- 7 Použije se pouze v případě smluv o poskytování certifikačních služeb, které nezahrnují požadované služby.
- 8 Doplníte IČO dle platné smlouvy. V případě změny IČO zákazníka musí být uzavřena nová smlouva.
- 9 Pokud bude uvedena e-mailová adresa pro zaslání faktur, bude faktura zaslána pouze elektronicky na tuto e-mailovou adresu. Faktura již nebude zaslána v listinné podobě.

Příloha č. 1 – Specifikace předmětu smlouvy

1. Úvodní ustanovení a vymezení pojmů

1. 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.

2. 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.

3. Časová razítka jsou poskytována prostřednictvím internetového připojení nebo prostřednictvím Centrálního místa služeb (dále CMS).

2. Podmínky realizace předmětu smlouvy

1. Poskytovatel se zavazuje poskytovat Objednateli časová razítka po celou dobu platnosti smlouvy a to v rozsahu a za podmínek stanovených smlouvou a jejími přílohami.

2. Poskytovatel bude Objednateli poskytovat kvalifikovaná 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 je potřebné využívat běžně dostupných softwarových knihoven (BouncyCastle, IAIK, Eldos, Adobe...).

3. Žádost o časová razítka

1. 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

2. Žádost nesmí obsahovat rozšíření (extensions).

Povolené algoritmy pro výpočet otisku (hashe) jsou SHA-1, SHA-256, SHA-384, SHA-512.

4. Ověření časového razítka

1. Pro ověření kvalifikovaného časového razítka je nezbytné provést následující kroky:

a) ověření obsahu časového razítka tj.

- hodnoty času uvedená v časovém razítku,
- otisku (hash) ověřovaných dat uvedený v časovém razítku vůči nově vypočtenému otisku (hash) z elektronických dat dostupných ověřující straně,
- platnosti elektronické pečeti pomocí certifikátu TSU,

b) získání a ověření, vůči aktuálnímu příslušnému CRL, platnost:

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

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

3. Minimální životnost elektronické pečeti na časovém razítku PostSignum TSA je pět let, avšak předpokládána reálná životnost této elektronické pečeti je vyšší.

5. Formát časového razítka

1. 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).

2. V případě požadavku na certifikát (certReq=true) bude k podpisu přiložen kvalifikovaný systémový certifikát TSA odpovídající požadavkům standardů a platné legislativy. 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.

6. Výkonnostní kritéria TSA

Výkonnostní kritéria TSA:

- Dostupnost systému 99%

Při běžném provozu:

- Maximální počet souběžně připojených uživatelů: 100
- Maximální počet vydaných razítek za 1 hodinu (RSA 2048): 360 000

Při přepojení do záložní lokality (havárie primárního centra):

- Maximální počet souběžně připojených uživatelů: 100
- Maximální počet vydaných razítek za 1 hodinu (RSA 2048): 360 000

7. Omezení použití

1. Kvalifikovaná časová razítka 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 souvislosti s bezpečností a obranyschopností státu.
2. Kvalifikované časové razítko vydané podle této politiky je možno použít tam, kde se vyžaduje použití kvalifikovaného časového razítka podle zákona o službách vytvářejících důvěru pro elektronické transakce, nebo tam, kde existuje potřeba prokázání existence konkrétních dat (dokumentu) před daným časovým okamžikem.

8. Přesnost času v časovém razítku

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

9. Omezení záruky a odpovědnosti

1. Poskytovatel se zavazuje, že splní veškeré povinnosti uložené politikami vydávání kvalifikovaných časových razítek, podle kterých vydává kvalifikované časové razítka, a mandatorními ustanoveními příslušných právních předpisů. Poskytovatel poskytuje výše uvedené záruky po celou dobu platnosti této smlouvy.
2. Záruky uvedené v předchozím odstavci jsou výlučnými zárukami Poskytovatele a Poskytovatel jiné záruky neposkytuje.
3. Poskytovatel neodpovídá za vady plnění předmětu smlouvy vzniklé z důvodu nesprávného nebo neoprávněného užívání předmětu smlouvy Objednatel, 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.
4. Další podmínky záruk a omezení odpovědnosti jsou stanoveny v Příloze č. 2 této smlouvy.

10. Ochrana osobních dat

1. Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování služeb dle této smlouvy. Zásady ochrany osobních údajů jsou obsaženy v politice časového razítka TSA, všeobecných obchodních podmínkách a v aktuální prováděcí směrnici TSA a vycházejí z příslušných ustanovení zákona č. 110/2019 Sb. o zpracování osobních údajů ve znění pozdějších předpisů.