# Politika vydávání časových razítek PostSignum TSA

Verze 2.0

**OBSAH**

# Evidence revizí a změn

| Verze | Účinnost od | Důvod a popis změny | Autor | Schválil |
|---|---|---|---|---|
| 1.0 | 1. 7. 2016 | První verze | PCA ČP | PAA ČP |
| 1.1 | 2. 10. 2017 | Změny v souvislosti s akreditací dle eIDAS | PCA ČP | PAA ČP |
| 2.0 | 1. 4. 2019 | Změny v souvislosti s novým řešením TimeStamp serveru | PCA ČP | PAA ČP |

# 1 ÚVOD

Tento dokument, Politika vydávání časových razítek PostSignum TSA, stanovuje pravidla a postupy pro vydávání kvalifikovaných elektronických časových razítek dle [eIDAS]. Pro účely této politiky bude používán souhrnný pojem časová razítka.

Identifikační a kontaktní údaje poskytovatele certifikačních služeb jsou:

Česká pošta, s.p.

IČ 47114983, DIČ CZ47114983

Politických vězňů 909/4

225 99 Praha 1

tel. 954 301 111

email: info@cpost.cz

- Tento dokument je v souladu s platnými právními předpisy a s normami [ETSI EN 319 421], [ETSI EN 319 422] a [RFC 3647].

# 2 PŘEHLED

Česká pošta, s.p. (dále i Česká pošta či ČP) ustavila dvouúrovňovou hierarchii certifikačních autorit s názvem PostSignum QCA. Kořenem této hierarchie je PostSignum Root QCA, která vydala certifikát pro certifikační autoritu PostSignum Qualified CA. PostSignum Qualified CA vydává kvalifikované certifikáty koncových uživatelů.

Česká pošta se stala akreditovaným poskytovatelem certifikačních služeb vydávání kvalifikovaných certifikátů dne 3. 8. 2005 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).

Česká pošta se dne 1. 7. 2016 stala kvalifikovaným poskytovatelem služeb vytvářejících důvěru v souladu s [eIDAS].

Dne 30. 8. 2017 byla do důvěryhodného seznamu kvalifikovaných služeb EU přidána k certifikační autoritě PostSignum služba vydávání kvalifikovaných elektronických časových razítek v souladu s [eIDAS].

PostSignum TSA vydává časová razítka, tedy datové zprávy, které důvěryhodným způsobem spojují data v elektronické podobě s časovým okamžikem a které zaručují, že uvedená data (jejich otisk) v elektronické podobě existovala před daným časovým okamžikem. Poskytování služby vydávání časových razítek zajišťuje více jednotek (TSU). Každá jednotka má vlastní klíč a kvalifikovaný certifikát pro elektronickou pečeť (dále bude tento certifikát označován také jako certifikát TSA). Certifikáty PostSignum TSA (tedy jednotlivých TSU) jsou vydány certifikační autoritou PostSignum Qualified CA.

Časová razítka vydaná podle této certifikační politiky jsou vydávána zákazníkům České pošty, kteří s Českou poštou uzavřeli smlouvu o poskytování certifikačních služeb.

Plnění zásad této politiky rozpracovává a zajišťuje Prováděcí směrnice PostSignum TSA [CPSTSA] v aktuální verzi, která je zveřejněna na webových stránkách poskytovatele. Další dokumenty [OZUTSA] a [SBPTSA], na které je v této politice odkazováno, jsou z důvodu zajištění bezpečnosti provozu neveřejnými interními dokumenty; podléhají však pravidelné interní a externí kontrole.

Vydávání a správa kvalifikovaných certifikátů pro elektronickou pečeť pro TSU se řídí dokumentem Certifikační politika PostSignum Qualified CA pro certifikáty TSA [CPQCATSA] a Certifikační prováděcí směrnicí PostSignum QCA [CPSQCA].

# 3 SEZNAM POUŽITÝCH POJMŮ A ZKRATEK

## 3.1 Rejstřík pojmů

**Akreditace –** Pod pojmem akreditace je myšleno získání statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru dle [eIDAS].

**Autentizace** – proces, při kterém prokazuje jedna strana druhé svoji identitu

**Bezpečnostní administrátor CA** – osoba zodpovědná za dodržování a kontrolu bezpečnostních zásad a odstranění zjištěných bezpečnostních nedostatků v PostSignum TSA

**Bit string** – jedna z datových struktur normy ASN.1, definující způsob uložení dat

**Certifikační politika** – dokument obsahující účel použití, seznam omezení, podmínky používání a další ustanovení týkající se certifikátů, které jsou podle tohoto dokumentu vydávány

**Certifikační prováděcí směrnice** – dokument upřesňující ustanovení v certifikačních politikách

**Certifikát pro elektronickou pečeť –** certifikát ve smyslu [eIDAS].

**Coordinated Universal Time (UTC)** – Světový koordinovaný čas, časový standard založený na Mezinárodním atomovém čase (TAI) s přestupnými sekundami.

**CRL (Certificate Revocation List)** – seznam zneplatněných certifikátů. Obsahuje certifikáty, které nadále nelze pokládat za platné například z důvodu prozrazení odpovídajícího soukromého klíče subjektu. CRL je digitálně podepsán vystavitelem certifikátů – certifikační autoritou.

**Firewall** – specializované síťové zařízení, které propustí jen explicitně povolenou datovou komunikaci; používá se pro bezpečné oddělení vnitřní datové sítě od vnější nedůvěryhodné sítě (obvykle Internetu)

**Fyzická osoba** – zákazník bez přiděleného IČ, fakticky se jedná o běžného občana, který používá nasmlouvané služby pro své soukromé potřeby

**Hardwarový kryptografický modul** – specializované zařízení pro bezpečné uložení klíčů a certifikátů, práce s tímto zařízením vyžaduje obvykle součinnost více osob

**Hash** – unikátní datový řetězec o neměnné délce, který je vypočítán z libovolných vstupních dat; jednoznačně reprezentuje vstupní data, tj. neexistuje stejný hash pro dvě různé zprávy

**Identifikace** – proces, při kterém sděluje jedna strana druhé svoji identitu

**Komise pro certifikační politiky ČP (Policy Approval Authority, PAA)** – orgán, v jehož pravomoci je schvalovat, sledovat a udržovat politiky a certifikační prováděcí směrnici, jimiž se řídí činnost certifikační autority.

**Kontaktní místo ČP** – pracoviště České pošty, na němž dochází k nabídce či poskytnutí vybraných služeb klientům.

**Kvalifikovaný certifikát pro elektronický podpis** – kvalifikovaný certifikát ve smyslu [eIDAS].

**Kvalifikovaný systémový certifikát** – kvalifikovaný systémový certifikát ve smyslu [ZoEP].

**Kvalifikované elektronické časové razítko** – kvalifikované časové razítko ve smyslu [eIDAS].

**Manažer CA** – osoba v řídící roli zodpovědná za provoz PostSignum TSA

**Modulus** – jedna z částí RSA klíče (modulus, public exponent, secret exponent), velikost modulu (v bitech) se označuje jako velikost celého klíče.

**Obchodní místo** – centrální regionální pracoviště certifikační autority odpovědné za uzavírání a evidenci smluv.

**Orgán dohledu –** Dohledový orgán nad kvalifikovanými poskytovateli služeb vytvářejících důvěru dle [eIDAS], který je stanoven na základě platných právních předpisů.

**Otisk** – český výraz pro anglický termín **hash**.

**Párová data** – jsou základním primitivem asymetrické kryptografie. Tvoří je soukromý a veřejný klíč. Z pohledu citlivosti je potřeba zabezpečit především jejich generování a chránit vytvořený soukromý klíč.

**Pečetící osoba –** osoba definovaná v [eIDAS].

**Platné právní předpisy** – Jsou jimi myšleny právní předpisy upravující oblast elektronického podpisu, zejména potom Zákon o službách vytvářejících důvěru pro elektronické transakce 297/2016 Sb. a NAŘÍZENÍ 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 včetně navazujících právních předpisů.

**Podnikající fyzická osoba** – zákazník s přiděleným IČ, fakticky se jedná o podnikatele, který používá nasmlouvané služby pro zajištění své podnikatelské činnosti

**PostSignum** – hierarchie certifikačních autorit a autority časového razítka tvořená kořenovou certifikační autoritou PostSignum Root QCA, všemi podřízenými certifikačními autoritami, pro něž PostSignum Root QCA vydala certifikát, a autoritami časového razítka, pro které některá z certifikačních autorit PostSignum vydala kvalifikovaný systémový certifikát nebo certifikát pro elektronickou pečeť.

**PostSignum QCA** – hierarchie certifikačních autorit, vydávajících kvalifikované certifikáty ve smyslu [eIDAS].

**PostSignum VCA** – hierarchie certifikačních autorit, vydávajících komerční certifikáty.

**PostSignum Root QCA** – kořenová certifikační autorita, která má samopodepsaný kvalifikovaný systémový certifikát nebo certifikát pro elektronickou pečeť. Vydává systémové certifikáty nebo certifikáty pro elektronickou pečeť pro podřízené certifikační autority a CRL. V hierarchii PostSignum mohou existovat další kořenové certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Root QCA 2.

**PostSignum Qualified CA** – certifikační autorita, která má kvalifikovaný systémový certifikát nebo certifikát pro elektronickou pečeť podepsaný kořenovou certifikační autoritou PostSignum Root QCA.

Vydává kvalifikované certifikáty pro subjekty, které nejsou certifikačními autoritami. V hierarchii PostSignum QCA mohou existovat další podřízené certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Qualified CA 2.

**PostSignum Public CA** – certifikační autorita, která má kvalifikovaný systémový certifikát nebo certifikát pro elektronickou pečeť podepsaný kořenovou certifikační autoritou PostSignum Root QCA. Vydává komerční certifikáty pro subjekty, které nejsou certifikačními autoritami. V hierarchii PostSignum VCA mohou existovat další podřízené certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Public CA 2.

**PostSignum TSA** – autorita vydávající kvalifikovaná elektronická časová razítka ve smyslu [eIDAS]. Autoritu tvoří více jednotek (TSU). Každá jednotka má vlastní klíč a kvalifikovaný certifikát pro elektronickou pečeť.

**Pověřená osoba** – zástupce zákazníka, který s Českou poštou komunikuje za účelem upřesnění podmínek poskytování certifikačních služeb a za účelem ohlašování změn v poskytování služeb či změn ve smluvním vztahu. Pověřené osoby musí být vyjmenovány ve smlouvě mezi zákazníkem a Českou poštou.

**Právnická osoba** – zákazník s přiděleným IČ, fakticky se jedná o organizaci s více zaměstnanci, která používá nasmlouvané služby pro zajištění své obchodní činnosti.

**Rozlišovací jméno** – posloupnost údajů v certifikátu, která jednoznačně identifikuje podepisující, označující nebo pečetící osobu dle pravidel definovaných příslušnou certifikační politikou.

**Soukromý klíč** – souhrnné označení dat pro vytváření elektronického podpisu a dat pro vytváření elektronických pečetí.

**Spoléhající se strana** – subjekt spoléhající se při své činnosti na kvalifikovaný certifikát, kvalifikovaný systémový certifikát, kvalifikovaný certifikát pro elektronický podpis, certifikát pro elektronickou pečeť nebo časové razítko vydané autoritami v rámci hierarchie PostSignum.

**Time Stamp Unit** – konkrétní serverová jednotka, která vydává (pečetí) časová razítka.

**Time Stamp Token** – souhrnné označení dat tvořících časové razítko.

**Trust centrum** – zabezpečené centrální pracoviště České pošty, v němž jsou umístěny provozní servery PostSignum TSA.

**Tým pro tvorbu certifikačních politik (Policy Creation Authority, PCA)** – tým, který vytváří politiky, jež předkládá ke schválení Komisi pro certifikační politiky. PCA je ustaven Komisí pro certifikační politiky, která řídí a kontroluje jeho činnost.

**Uživatel certifikátu (relying party)** – osoba, která užívá certifikát vydaný certifikačními autoritami v rámci hierarchie PostSignum například pro ověření elektronického podpisu, pečetě, časového razítka nebo pro zajištění jiných bezpečnostních služeb. Jinak též označována jako Spoléhající se strana.

**Veřejný klíč** – souhrnné označení dat pro ověřování elektronického podpisu nebo dat pro ověřování elektronických pečetí.

**Webové stránky poskytovatele** – http://www.postsignum.cz – webové stránky poskytovatele služby PostSignum TCA

**Zákazník** – fyzická či právnická osoba, která uzavírá s Českou poštou smlouvu o poskytování certifikačních služeb.

**Záložní lokalita** – zabezpečené centrální pracoviště České pošty, v němž jsou umístěny záložní provozní servery PostSignum TSA; provoz do záložní lokality přechází v případě, že nelze zajistit provoz v Trust centru.

**Zneplatnění** – proces, při kterém dochází k okamžitému ukončení platnosti certifikátu na žádost žadatele o zneplatnění certifikátu; zneplatněný certifikát je umístěn na CRL.

**Žadatel** – subjekt, který má jakožto zástupce zákazníka právo žádat u PostSignum TSA o časové razítko podle platné politiky. Žadatelem o vydání časového razítka může být konkrétní fyzická osoba nebo systém.

## 3.2 Rejstřík zkratek

**ASN.1** – Abstract Syntax Notation One (standard popisující reprezentaci datových struktur a jejich zakódování a dekódování)

**CA** – Certifikační autorita

**CPS** – Certifikační prováděcí směrnice

**CRL** – Certificate Revocation List (Seznam zneplatněných certifikátů)

**ČP** – Česká pošta, s.p.

**ČR** – Česká republika

**DIČ** – Daňové identifikační číslo (přidělené pro účely daně z přidané hodnoty)

**DMZ** – Demilitarizovaná zóna (datová síť, na kterou je směrována komunikace z nedůvěryhodné sítě)

**EPS** – Elektronická požární signalizace

**HSM** – Hardware Security Module (Hardwarový kryptografický modul)

**HTTPS** - Hypertext Transfer Protocol over SSL (protokol pro přenos webového obsahu se zapnutým bezpečnostním rozšířením SSL)

**IČO** – Identifikační číslo (jednoznačné číslo identifikující právnickou osobu)

**NTP** – Network Time Protocol (protokol pro časovou synchronizaci počítačů)

**OID** – Object identifier (jednoznačný identifikátor objektu nebo algoritmu)

**PAA** – Policy Approval Authority (Komise pro certifikační politiky)

**PCA** – Policy Creation Authority (Tým pro tvorbu certifikačních politik)

**PKI** – Public Key Infrastructure (Infrastruktura veřejného klíče)

**QCA** – zkratka pro kvalifikovanou certifikační autoritu České pošty, PostSignum QCA

**RSA** – asymetrický kryptografický algoritmus (zkratku tvoří jména tvůrců algoritmu: Rivest, Shamir, Adleman)

**SSH** – Secure Shell (komunikační protokol pro bezpečné vzdálené přihlášení k počítači)

**SSL** – Secure Socket Layer (protokol zabezpečující komunikaci šifrováním a autentizací)

**TLS** – Transport Layer Security (protokol zabezpečující komunikaci šifrováním a autentizací)

**TSA** – Time Stamp Authority (Autorita časových razítek)

**TST** – Time Stamp Token (časové razítko)

**TSU** – Time Stamp Unit (server vydávající časová razítka)

**UPS** – Uninterruptible power supply (zdroj záložního napájení)

**UTC** – Coordinated Universal Time

**VCA** – zkratka pro komerční certifikační autoritu České pošty, PostSignum VCA

**X509** – standard, který specifikuje formát certifikátů, CRL atd.

# 4 ZÁKLADNÍ POJETÍ

Není-li uvedeno jinak, je dále v tomto dokumentu pod pojmem:

- **certifikát** míněn kvalifikovaný certifikát pro elektronický podpis nebo kvalifikovaný certifikát pro elektronickou pečeť,
- **časové razítko** míněno kvalifikované elektronické časové razítko dle [eIDAS],
- **certifikát TSA** míněn certifikát konkrétního TSU generujícího časová razítka.

## 4.1 Služby autority časových razítek (TSA)

Česká pošta, jakožto provozovatel PostSignum TSA, zajišťuje pro své zákazníky následující základní služby spojené s vydáváním časových razítek:

- služba vydání časového razítka,
- služba zavedení a správy uživatelských účtů, pod kterými žadatelé o časová razítka přistupují ke službě vydání časového razítka.

Tyto služby jsou poskytovány za podmínek uvedených v platných právních předpisech a v uzavřené smlouvě se zákazníkem.

K zajištění kvality poskytovaných služeb a požadavků [ZoEP] provozovatel PostSignum TSA zajišťuje provoz, monitorování a řízení dalších podpůrných služeb (např. synchronizace času, správa soukromých klíčů TSU) definovaných v interní dokumentaci.

## 4.2 Autorita časových razítek

Autorita časového razítka PostSignum TSA vystupuje (z pohledu zákazníků a spoléhajících se stran) v roli důvěryhodné třetí strany vydávající časová razítka, která obsahují důvěryhodný časový údaj.

Z titulu provozovatele nese celkovou zodpovědnost za poskytování certifikačních služeb v oblasti vydávání časových razítek Česká pošta.

Poskytování služeb vydávání časových razítek zajišťuje více jednotek TSU. Každá jednotka má vlastní klíč a kvalifikovaný certifikát pro elektronickou pečeť.

Podrobnější informace jsou v [CPSTSA].

4.3 Zákazníci, pověřené osoby, žadatelé a spoléhající se strany

4.3.1 Zákazník a pověřená osoba

Zákazníkem oprávněným žádat prostřednictvím žadatelů o vydání časového razítka může být fyzická osoba, podnikající fyzická osoba, právnická osoba, státní orgán nebo orgán místní samosprávy. Zákazník musí mít s ČP uzavřenou smlouvu o poskytování certifikačních služeb zahrnující poskytování služby vydání časových razítek.

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.

V případě zákazníka – fyzické osoby představuje pověřenou osobu přímo samotný zákazník.

4.3.2 Žadatelé o časové razítko

Žadatelem o vydání časového razítka může být na základě písemné smlouvy mezi zákazníkem a ČP konkrétní fyzická osoba nebo systém. Žadatel se vůči TSA identifikuje a autentizuje za účelem pozdějšího vyúčtování poskytnuté služby.

4.3.3 Spoléhající se strana

Spoléhající se stranou je subjekt, spoléhající se při své činnosti na vydaná časová razítka. Subjekt v této roli nevstupuje do smluvního vztahu s Českou poštou.

4.3.4 Jiné participující subjekty

Viz [CPSTSA]

# 5 POLITIKA TSA

5.1 Základní popis

Politika vydávání časových razítek je definovaný seznam pravidel, která popisují životní cyklus časového razítka vydaného PostSignum TSA, jeho vlastnosti a poskytované záruky.

Pravidla a postupy uvedené v této politice jsou detailněji rozpracována v [CPSTSA] a dalších interních dokumentech a pracovních směrnicích.

5.2 Identifikace

Identifikace politiky

PostSignum TSA používá vlastní identifikátor politiky pro vydávání časového razítka.

| | |
|---|---|
| Název dokumentu | Politika vydávání časových razítek PostSignum TSA |
| Verze dokumentu | 2.0 |
| Stav | finální |

| | |
|---|---|
| OID poskytovatele certifikačních služeb | 2.23.134 |
| OID PostSignum TSA | 2.23.134.1.5 |
| OID této politiky | 2.23.134.1.5.1.11.200 |
| Datum vydání | 1. 4. 2019 |
| Doba platnosti | Do odvolání nebo do dne ukončení služeb autority PostSignum TSA. |

5.3 Určení politiky a její použitelnost

5.3.1 Přípustné použití časového razítka

Časové razítko vydané podle této politiky je možno použít v případech, kde se vyžaduje použití časového razítka podle platných právních předpisů, nebo kde existuje potřeba prokázání existence konkrétních dat (dokumentu) před daným časovým okamžikem.

Časová razítka není možné používat pro:

- prokázání vzniku dat v daném časovém okamžiku a
- zajištění ověření původu a nepopiratelnosti dat (nenahrazuje elektronický podpis).

5.3.2 Omezení použití časového razítka

Časová razítka vydávaná podle této politiky 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. Česká pošta je připravena diskutovat se zákazníkem zvláštní podmínky poskytování certifikačních služeb ve výše uvedených sektorech.

Časová razítka vydávaná podle této politiky je možné využívat pouze v souvislosti s řádnými a legálními účely a v souladu s platnými právními předpisy.

Kromě výše uvedeného politika vydávání časových razítek nedefinuje žádná omezení pro používání časového razítka, vydaného v souladu s jejím obsahem.

5.4 Hodnocení shody a jiná hodnocení

V prostředí PostSignum TSA jsou v souladu s platnými právními předpisy prováděny pravidelné kontroly bezpečnostní shody, které se mimo jiné zaměřují na splnění požadavků kladených legislativou na kvalifikované poskytovatele certifikačních služeb.

5.4.1 Periodicita a hodnocení nebo okolnosti pro provedení hodnocení

V prostředí PostSignum TSA jsou pravidelně prováděny interní kontroly (jednou za 12 měsíců). Kromě těchto interních kontrol jsou prováděny externí kontroly dle platných právních předpisů. Tyto pravidelné kontroly mohou být podle potřeby doplněny další kontrolou, mimo jiné na základě rozhodnutí Manažera CA, managementu České pošty nebo odboru interního auditu České pošty.

5.4.2 Identita a kvalifikace hodnotitele

Interní kontrolu provádějí pracovníci znalí problematiky PKI a proškolení pro daný úkol. Pracovníci provádějící kontrolu jsou v dokumentaci TSA označováni jako Auditoři CA.

Externím auditorem smí být pouze osoba nebo společnost znalá problematiky implementace PKI s dostatečnou zkušeností v této oblasti.

5.4.3 Vztah mezi hodnotitelem a hodnocenou entitou

Interní kontrolu provádí zaměstnanci České pošty.

Externí kontrolu smí provádět pouze osoba nebo společnost nezávislá na České poště.

5.4.4 Hodnocené oblasti

V rámci kontrol je ověřována bezpečnost a integrita systémů a dodržování obecně závazných a interních předpisů.
Oblasti hodnocené v rámci pravidelných kontrol jsou specifikovány v [CPSTSA] a v příloze [SBPTSA] - Auditní a archivační politice.

5.4.5 Postupy v případě zjištěných nedostatků

Výsledky kontrol jsou předávány Manažerovi CA, který zajistí nápravu zjištěných nedostatků.

Podrobnější informace viz [CPSTSA].

5.4.6 Sdělování výsledků hodnocení

O provedení každé kontroly je vypracována podepsaná písemná zpráva, která je předána Manažerovi CA.

Podrobnější informace viz [CPSTSA].

# 6 ZÁVAZKY A ODPOVĚDNOSTI

## 6.1 Závazky TSA

### 6.1.1 Obecné závazky TSA

Česká pošta se zavazuje, že při poskytování služby vydávání časových razítek:

- postupuje v souladu s platnými právními předpisy,
- zajišťuje naplnění všech požadavků kladených na TSA uvedených v kapitole 7 tohoto dokumentu,
- zajišťuje dodržení postupů uvedených v této politice,
- postupuje podle ustanovení [CPSTSA] a další interní dokumentace.

### 6.1.2 Závazky TSA ve vztahu k zákazníkům a žadatelům o časové razítko a držitelům časového razítka

Česká pošta se zavazuje, že vydávaná časová razítka obsahují věcně správné údaje a splňují všechny požadavky stanovené platnými právními předpisy; zejména že

- časový údaj vložený do časového razítka odpovídá hodnotě UTC v okamžiku vytváření časového razítka s přesností 1 sekunda; časový údaj je získán z měřidla času navázaného na světový koordinovaný čas,
- data v elektronické podobě, která jsou předmětem žádosti o vydání časového razítka, jednoznačně odpovídají datům v elektronické podobě obsaženým ve vydaném časovém razítku,

- vydá časové razítko neprodleně po obdržení platného požadavku,
- využívá důvěryhodnou synchronizaci času a odchylka času uvedeného ve vydávaných časových razítkách od UTC nepřesáhne 1 sekundu,

Česká pošta zveřejňuje politiku časových razítek, podle které vydává časová razítka, na webových stránkách poskytovatele, na kontaktních místech ČP, případně jinými vhodnými způsoby.

Česká pošta věnuje náležitou péči všem činnostem spojeným s poskytováním služby vydávání časového razítka. Náležitá péče zahrnuje provoz v souladu

- s platnými právními předpisy,
- s touto politikou,
- s [CPSTSA],
- s [SBPTSA],
- s provozní dokumentací.

Vydané časové razítko obsahuje:

- číslo časového razítka,
- identifikátor politiky, podle které bylo časové razítko vydáno,
- obchodní firmu a stát, ve kterém je kvalifikovaný poskytovatel služeb vytvářejících důvěru usazen,
- hodnotu času v UTC, která odpovídá koordinovanému světovému času při vytváření časového razítka,
- data v elektronické podobě – otisk (hash), pro která bylo časové razítko vydáno,
- zaručenou elektronickou pečeť založenou na kvalifikovaném certifikátu pro elektronickou pečeť vydaném kvalifikovaným poskytovatelem služeb vytvářejících důvěru, který časové razítko vydal (dále jen elektronická pečeť).

6.2 Závazky zákazníků a žadatelů o časové razítko a držitelů časového razítka

Žadatelé zkontrolují po obdržení odpovědi na žádost o časové razítko informaci o stavu zpracování žádosti uvedenou v odpovědi na žádost o časové razítko.

Pokud je součástí odpovědi časové razítko, žadatel provede tyto činnosti:

- ověří platnost elektronické pečetě na časovém razítku pomocí certifikátu TSA,
- bezpečným způsobem získá aktuální příslušné CRL a ověří platnost:
    - použitého certifikátu TSA, kterým je razítko opečetěno,
    - certifikátu certifikační autority PostSignum Qualified CA, která vydala certifikát TSA,
    - certifikátu certifikační autority PostSignum Root QCA, která vydala certifikát autority PostSignum Qualified CA (viz. kapitola 7.4.13),

- ověří, zda OID politiky pro vydávání časových razítek, které je uvedeno v certifikátu TSA, odpovídá OID uvedenému v této politice,

- v případě, že žádost obsahovala položku „nonce“, ověří, že její hodnota v odpovědi je shodná,

- v případě, že žádost obsahovala položku „reqPolicy“, ověří, že její hodnota v odpovědi je shodná.

Zákazník ručí za naplnění všech povinností uvedených v této certifikační politice a povinností uvedených v platných právních předpisech.

6.3 Závazky spoléhajících se stran

Spoléhající se strana ověřuje obsah časového razítka, tj.:

- otisk (hash) ověřovaných dat,

- platnost elektronické pečetě pomocí certifikátu TSA.

Spoléhající se strana získá bezpečným způsobem aktuální příslušné CRL a ověří platnost:

- použitého certifikátu TSA, kterým je razítko opečetěno,

- certifikátu certifikační autority PostSignum Qualified CA, která vydala certifikát TSA,

- certifikátu certifikační autority PostSignum Root QCA, která vydala certifikát autority PostSignum Qualified CA (viz. kapitola 7.4.13).

Spoléhající se strana zváží, zda časové razítko vydané podle této politiky je vhodné pro účel, ke kterému bylo použito.

Spoléhající se strana ověří, zda jsou kryptografické funkce použité v časovém razítku stále platné a bezpečné. Tyto informace jsou poskytnuty na elektronické informační adrese (kapitola 7.4.13.2) a konkrétně se jedná o:

- kryptografickou funkci pro tvorbu otisku (hashe),

- kryptografický algoritmus použitý při pečetění razítka,

- délku klíče u kryptografického algoritmu použitého pro opečetění razítka.

6.4 Odpovědnosti

Česká pošta neodpovídá za vady poskytnutých služeb a škody vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb zákazníkem, zejména za jejich využití v rozporu s podmínkami uvedenými v této politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.

Česká pošta neodpovídá za škodu vyplývající z použití časového razítka, pokud došlo ze strany zákazníka, žadatele nebo spoléhající se osoby k nedodržení omezení pro jeho použití, uvedených v této politice a zveřejněných na webové stránce poskytovatele nebo k nedodržení podmínek pro využití této služby uvedených v této politice.

Česká pošta bude průběžně s rostoucími provozními zkušenostmi s poskytováním certifikačních služeb ověřovat, zda podmínky omezení odpovědnosti České pošty uvedené v tomto ustanovení odpovídají obvyklým podmínkám na trhu a přiměřenému obchodnímu riziku České pošty.

Ustanovení tohoto článku zůstávají v platnosti i po ukončení platnosti této politiky.

Pokud nevyplývá z mandatorních ustanovení platných právních předpisů jinak, odpovídá Česká pošta výhradně za škodu způsobenou porušením povinností České pošty v souvislosti s plněním smlouvy o poskytování certifikačních služeb.

# 7 POŽADAVKY NA POSTUPY A PROCEDURY TSA

## 7.1 Správa politiky

Za iniciování změn v této politice nebo inicializaci vytvoření nové politiky pro vydávání časových razítek je odpovědný Manažer CA. Ten předá požadavek týmu pro tvorbu certifikačních politik (PCA ČP).

Veškeré změny v této politice podléhají schválení Komise pro certifikační politiky ČP (PAA ČP). PAA ČP přidělí nové číslo verze, které umožňuje danou verzi politiky identifikovat.

Nová verze politiky vydávání časových razítek bude zveřejněna na webových stránkách poskytovatele. PAA ČP rozhodne, zda je nutné zveřejnit informaci o nové verzi certifikační politiky též jinou formou, případně jak.

### 7.1.1 Organizace spravující politiku vydání časových razítek

Za správu této politiky je odpovědný poskytovatel služby TSA, tedy Česká pošta, konkrétně Manažer CA.

### 7.1.2 Kontaktní osoba organizace spravující politiku TSA

Kontaktní osobou ve věci správy této politiky je Manažer CA. Další informace je možné získat na e-mailové adrese

manager.postsignum@cpost.cz

nebo na webových stránkách poskytovatele

### 7.1.3 Postupy při změnách politiky

Tento dokument je vytvářen Týmem pro tvorbu certifikačních politik ČP (PCA ČP). PCA ČP je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován. PCA ČP předává dokument ke schválení Komisi pro certifikační politiky.

Nové verze politik vznikají podle potřeby, zejména však:

- při takové změně PostSignum TSA (např. změně postupů), která ovlivní obsah těchto dokumentů,
- pokud při pravidelné kontrole okolního prostředí PostSignum TSA byly identifikovány požadavky na změny těchto dokumentů.

Za iniciování změn v této politice nebo za inicializaci vytvoření nové politiky vydávání časových razítek je odpovědný Manažer CA. Při přípravě změn v této politice rozhodne Manažer CA na základě přehledu změn, jakým způsobem budou plánované změny zveřejněny. Manažer CA pak předá požadavek Týmu pro tvorbu certifikačních politik (PCA ČP) a vypracované politiky předloží ke schválení Komisi pro certifikační politiky, která přiřadí nové OID a číslo verze dokumentu.

7.2 Požadavky na životní cyklus párových dat TSA

7.2.1 Generování a instalace párových dat

7.2.1.1 Generování párových dat

Generování párových dat probíhá v Trust centru ČP v souladu s dokumenty [SBPTSA] a [CPSTSA]. Klíčové páry jednotlivých TSU jsou generovány a uloženy v hardwarovém kryptografickém modulu splňujícím požadavky technických norem, které upravují činnost poskytovatelů certifikačních služeb. Generování těchto klíčových párů probíhá v souladu s interní dokumentací podléhající interní i externí kontrole v kontrolovaném prostředí České pošty.

7.2.1.2 Vlastnosti kryptografického modulu

Kryptografický modul použitý pro generování a úschovu soukromých klíčů TSA (bezpečný kryptografický modul) splňuje požadavky standardu FIPS 140–2 Level 3.

7.2.1.3 Poskytování veřejných klíčů

Data pro ověření platnosti elektronických pečetí TSU jsou poskytována ve formě certifikátů veřejných klíčů TSU odpovídajících standardu X509. Certifikáty TSA je možno získat na webových stránkách poskytovatele.

7.2.1.4 Délky párových dat

TSA používá pro vytváření elektronických pečetí asymetrický kryptografický algoritmus RSA. Mohutnost klíčů (modulů) použitých pro pečetění vydávaných časových razítek je minimálně 2048 bitů.

7.2.2 Ochrana soukromého klíče TSA (dat pro vytváření elektronických pečetí)

7.2.2.1 Standardy a podmínky používání kryptografického modulu

Kryptografický modul použitý pro generování a úschovu soukromých klíčů TSA (bezpečný kryptografický modul) splňuje požadavky standardu FIPS 140–2 Level 3.

7.2.2.2 Zálohování soukromých klíčů (dat pro vytváření elektronických pečetí)

Soukromé klíče TSA jsou zálohovány v zašifrované podobě.

7.2.2.3 Uchovávání soukromých klíčů (dat pro vytváření elektronických pečetí)

Soukromé klíče TSA nejsou archivovány.

7.2.2.4 Transfer soukromých klíčů (dat pro vytváření elektronických pečetí) do kryptografického modulu nebo z kryptografického modulu

Soukromý klíč TSA je generován v kryptografickém modulu (bezpečném kryptografickém modulu) a veškeré operace s nezašifrovaným klíčem se provádějí pouze v tomto modulu. Stejný soukromý klíč nesmí být importován současně do jiného kryptografického modulu.

7.2.2.5 Uložení soukromých klíčů (dat pro vytváření elektronických pečetí) v kryptografickém modulu

Soukromý klíč TSA je během provozu uložen v aktivovaném a konfigurovaném kryptografickém modulu (bezpečném kryptografickém modulu) v nezašifrovaném tvaru. V jednu chvíli v jednom kryptografickém modulu existuje pouze jeden aktivní soukromý klíč TSA.

7.2.2.6 Aktivační data

V systémech PostSignum TSA jsou používána aktivační data různého charakteru, například přístupová hesla, PIN a jiné. Všechny aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v [SBPTSA], [CPSTSA] a další provozní dokumentaci.

7.2.2.7 Postup při aktivaci soukromých klíčů

Soukromé klíče TSA jsou aktivovány autorizovanou obsluhou v souladu s ustanoveními dokumentů [SBPTSA] a [CPSTSA].

7.2.2.8 Postup při deaktivaci soukromých klíčů

Soukromé klíče TSA jsou deaktivovány autorizovanou obsluhou v souladu s ustanoveními dokumentů [SBPTSA] a [CPSTSA].

7.2.2.9 Postup při zničení dat pro vytváření elektronických pečetí

Soukromé klíče TSA uložené v hardwarovém kryptografickém modulu jsou zničeny prostředky poskytovanými kryptografickým modulem v případě, že kryptografický modul má být dočasně použit k jiným účelům, v případě ukončení činnosti kryptografického modulu, v případě ukončení činnosti jednotky TSU, jehož klíče jsou v kryptografickém modulu uloženy, nebo v případě ukončení používání konkrétního soukromého klíče. Toto zničení soukromého klíče provádí autorizovaná obsluha v souladu s ustanoveními dokumentů [SBPTSA] na základě požadavku Manažera CA.

Zničení soukromého klíče zahrnuje i smazání všech zálohovaných kopií klíčů.

7.2.3 Distribuce veřejných klíčů TSA

Veřejné klíče ve formě certifikátů TSA, které jsou nutné pro ověřování platnosti časových razítek, je možné získat prostřednictvím webových stránek poskytovatele.

7.2.3.1 Žádost o certifikáty TSA

Žádost o certifikát každé jednotky TSU vzniká při generování párových dat (viz kapitola 7.2.1) a je ve formátu PKCS#10 předávána zástupci certifikační autority PostSignum Qualified CA. Příslušné činnosti se řídí ustanoveními dokumentů [CPQCATSA] a podléhají interní a externí kontrole.

7.2.3.2 Certifikáty TSA

Certifikáty PostSignum TSA (jednotlivých TSU) jsou vydány certifikační autoritou PostSignum Qualified CA podle politiky [CPQCATSA].

Základní profil kvalifikovaného certifikátu pro elektronickou pečeť PostSignum TSA je uveden v následující tabulce (podrobný profil certifikátu včetně rozšíření je uveden v dokumentu [CPQCATSA]):

Základní profil certifikátu TSA

| **Název položky** | **Hodnota/příznak použití** |
|---|---|
| **Version** | 3 (0x2) |
| **Serial Number** | *jednoznačné číslo certifikátu přidělené PostSignum Qualified CA* |
| **SignatureAlgorithm** | sha256WithRSAEncryption |
| **Issuer** | |
| C | CZ |

| | |
|---|---|
| countryName | |
| O<br>organisationName | Česká pošta, s.p. |
| CN<br>commonName | PostSignum Qualified CA X<br>*(X je číslo označující konkrétní podřízenou certifikační autoritu)* |
| **Validity** | |
| Not Before | Počátek platnosti vydaného certifikátu (UTCTime) |
| Not After | Konec platnosti vydaného certifikátu (UTCTime) |
| **Subject** | |
| C<br>countryName | CZ |
| OID 2.5.4.97<br>organizationIdentifier | NTRCZ-47114983 |
| O<br>organisationName | Česká pošta, s.p. |
| OU<br>organizationUnitName | Time Stamping Authority |
| CN<br>commonName | PostSignum TSA - TSU X<br>*(X je číslo označující konkrétní jednotku TSU)* |
| **Subject Public Key Info** | |
| Algorithm | rsaEncryption |
| SubjectPublicKey | *veřejný klíč TSU*<br>*algoritmus RSA, velikost klíče je minimálně 2048 bitů* |
| **Extensions** | *rozšíření certifikátu* |
| **Signature** | *elektronická pečeť poskytovatele certifikačních služeb* |

7.2.4 Výměna párových dat

Platnost párových dat pro pečetění časových razítek (soukromých a veřejných klíčů) jednotek TSU je omezena na dobu platnosti certifikátu TSA. Toto období je rozděleno do dvou časových úseků:

- prvního časového úseku, který trvá zpravidla 1 rok, kdy jsou párová data používána jak k vydávání časových razítek (používán soukromý klíč), tak i ověřování elektronické pečetě (používán veřejný klíč) a

- navazujícího časového úseku, kdy jsou data používána výhradně pro ověřování elektronické pečetě (pouze používán veřejný klíč).

Po ukončení prvního časového úseku jsou generována nová párová data pro každou TSU a jsou vydány nové certifikáty TSA. Následně je soukromý klíč z původních párových dat automaticky zničen a zničeny jsou také všechny zálohy soukromého klíče.

Procesy výměny párových dat pro jednotky TSU jsou popsány v interní dokumentaci a respektují ustanovení dokumentu [SBPTSA]. Při výměně párových dat jsou hodnoceny pokroky v oblasti kryptografie a následně upravován seznam použitých algoritmů a jejich parametrů.

Plánovaná výměna párových dat TSA bude zákazníkům oznámena na webových stránkách poskytovatele před provedením výměny a následně budou na webových stránkách poskytovatele také zveřejněny příslušné nově vydané certifikáty TSA.

7.2.5 Ukončení životního cyklu párových dat

Platnost párových dat pro pečetění časových razítek (soukromých a veřejných klíčů) jednotek TSU je omezena na dobu platnosti certifikátu TSA. Toto období je rozděleno do dvou časových úseků podle používání soukromého klíče (viz. kapitola 7.2.4).

První časový úsek je ukončen

- vygenerováním nové dvojice párových dat,
- vydáním certifikátu TSA, obsahujícího veřejný klíč z této nové dvojice párových dat, a
- protokolárním zničením soukromého klíče z původních párových dat a jeho záloh.

Po tomto okamžiku je možné původní párová data používat pouze k ověřování elektronické pečetě na vydaných časových razítkách.

Celková platnost párových dat je ukončena v okamžiku uvedeném v certifikátu obsahujícím veřejný klíč z párových dat nebo zneplatněním certifikátu s důvodem zneplatnění keyCompromise (1), caCompromise (2) nebo bez uvedeného důvodu pro zneplatnění.

Ihned po ukončení používání soukromého klíče je tento zničen včetně všech svých záloh.

V případě, že bude nutné provést výměnu dat z důvodu nedostatečnosti záruk poskytovaných použitým algoritmem nebo jeho parametry (např. velikostí modulu) mimo plánovaný termín, bude příslušný certifikát TSA zneplatněn s důvodem zneplatnění keyCompromise (1) a dojde k výměně párových dat (viz kapitola 7.2.4).

7.2.5.1 Zneplatnění a pozastavení platnosti certifikátu

Platnost vydaných časových razítek je úzce spojena s platností příslušného kvalifikovaného systémového certifikátu nebo certifikátu pro elektronickou pečeť TSA používaného pro ověření elektronické pečetě na vydaném časovém razítku.

Platnost certifikátu je ukončena v okamžiku jeho zneplatnění s důvodem zneplatnění keyCompromise (1), caCompromise (2) nebo bez uvedeného důvodu pro zneplatnění a zveřejnění na seznamu zneplatněných certifikátů.

Pokud není certifikát po dobu jeho platnosti nutné zneplatnit nebo je zneplatněn s důvodem zneplatnění unspecified (0), affiliationChanged (3), superseded (4) nebo cessationOfOperation (5), skončí jeho platnost v časovém okamžiku uvedeném v certifikátu.

U certifikátů TSA nebude používáno pozastavení platnosti certifikátu.

7.2.5.2 Seznam zneplatněných certifikátů

Profil seznamu zneplatněných certifikátů vydaných autoritou PostSignum Qualified CA, včetně místa a způsobu jeho zveřejňování, je uveden v certifikační politice [CPQCATSA], kterou je možné nalézt na webových stránkách poskytovatele:

7.2.6 Správa kryptografického modulu používaného při vytváření časových razítek

Při provozu a správě kryptografického modulu používaného při vytváření časových razítek je postupováno v souladu s ustanoveními [SBPTSA].

7.2.6.1 Hodnocení kryptografického modulu

Vzhledem ke skutečnosti, že kryptografický modul užívaný k úschově soukromých klíčů TSA úspěšně prošel hodnocením podle standardu FIPS 140–2 na úroveň 3, nepředpokládá se, že by obsahoval závažné chyby na úrovni konstrukce zařízení. Přesto se průběžně sleduje, zda nebyl objeven útok na toto zařízení, aby bylo možné včas na takové ohrožení reagovat.

7.3 Vydávání časových razítek

Žádost o vydání časového razítka podle této politiky pro vydání časového razítka podávají zákazníci ČP zastoupení žadateli (viz kapitola 4.3.2) na základě uzavřené smlouvy mezi ČP a zákazníkem (viz kapitola 7.3.1).

7.3.1 Uzavření smlouvy a registrační proces

7.3.1.1 Identifikace a autentizace

Identita zákazníka se prokazuje při uzavírání smlouvy o poskytování certifikačních služeb způsobem obvyklým v obchodním styku.

7.3.1.2 Uzavření smlouvy s právnickou nebo podnikající fyzickou osobou, státním orgánem nebo orgánem místní samosprávy

Zákazník (právnická osoba, podnikající fyzická osoba, státní orgán nebo orgán místní samosprávy) získá přístup ke službě vydávání časových razítek uzavřením písemné smlouvy o poskytování certifikačních služeb. Tato smlouva se uzavírá v souladu s [VOP] tak, jak je v obchodním styku obvyklé.

7.3.1.3 Uzavření smlouvy s nepodnikající fyzickou osobou

Zákazník (nepodnikající fyzická osoba) získá přístup ke službě vydávání časových razítek uzavřením písemné smlouvy o poskytování certifikačních služeb. Tato smlouva se uzavírá v souladu s [VOP] tak, jak je v obchodním styku obvyklé.

7.3.1.4 Registrace žadatelů

Pro zahájení vydávání časových razítek je nutné zajistit bezpečné předání autentizačních dat pro přístup ke službám TSA mezi ČP a zákazníkem. Generování resp. nastavování autentizačních údajů za zákazníka zajišťuje pověřená osoba.

Budou používány dva druhy autentizace (a tedy i autentizačních údajů):

- autentizace soukromým klíčem a certifikátem vydaným certifikační autoritou PostSignum VCA, nebo
- autentizace jménem a heslem.

V případě použití autentizace soukromým klíčem a certifikátem vydaným PostSignum VCA předává pověřená osoba České poště údaje o certifikátu, který bude používán pro přístup ke službě vydávání časových razítek. Pověřená osoba odpovídá za správnost poskytnutých údajů.

V případě použití autentizace jménem a heslem je pověřená osoba jedinou osobou oprávněnou k určení hesla resp. k žádosti o vygenerování hesla (nové generování) a jedinou osobou, které může být toto heslo předáno (vytištěné na papíře).

Dále může pověřená osoba požádat o zrušení konkrétního přístupového účtu.

Tyto změny probíhají po ověření identity pověřené osoby vůči záznamům v databázi TSA.

V době platnosti smlouvy pro zákazníka (právnické osoby, podnikající fyzické osoby) může dojít ke změně ve jmenování pověřených osob. Změna musí být zachycena v dodatku smlouvy, kde bude uvedena nová pověřená osoba a její podpisový vzor.

7.3.1.5 Ukončení poskytování služeb pro žadatele o časové razítko

Poskytování služeb pro žadatele o časová razítka končí ukončením platnosti smlouvy mezi zákazníkem a poskytovatelem služby vydávání časových razítek.

Ukončení smlouvy o poskytování certifikačních služeb nebo odstoupení od této smlouvy se řídí [VOP].

7.3.2 Zpracování žádosti o časové razítko

7.3.2.1 Identifikace a autentizace

Před zpracováním žádosti musí být žadatel o časové razítko identifikován a musí být provedena jeho autentizace.

Žadatel o časové razítko vytvoří bezpečné autentizované spojení s TSA prostřednictvím protokolu HTTPS, v rámci kterého se identifikuje a autentizuje

- komerčním certifikátem vydaným certifikační autoritou PostSignum VCA,
- nebo jménem a heslem.

webové adresy jsou uvedeny v [CPSTSA] a ve smlouvě o poskytování certifikačních služeb.

7.3.2.2 Přijetí nebo zamítnutí žádosti o časové razítko

Přijetí žádosti probíhá následujícím způsobem:

- po platné identifikaci a autentizaci vytvoří klientská aplikace otisk (hash) elektronických dat (zprávy, dokumentu, transakce, atd.),
- otisk je následně uložen v žádosti o časové razítko (dle [RFC 3161]),
- takto vytvořená datová struktura je prostřednictvím protokolu HTTPS předána TSA,
- následně je žádost zaslána jedné z jednotek TSU pro posouzení správnosti a opečetění.

K zamítnutí žádosti může dojít zejména v případě:

- neúspěšné identifikace a autentizace,
- že žádost o časové razítko nesplňuje náležitosti definované touto politikou,
- ukončení platnosti soukromého klíče TSA.

PostSignum TSA žádným způsobem neověřuje otisk dat uvedený v žádosti a následně i ve vydaném časovém razítku.

7.3.2.3 Doba zpracování žádosti o časové razítko

PostSignum TSA vytvoří časové razítko neprodleně po přijetí platné žádosti o časové razítko. Do celkové doby zpracování z pohledu žadatele je však nutné započítat další čas, zejména čas potřebný pro vytvoření otisku (hash) dat a čas potřebný pro přenos dat přes síť Internet.

Výše uvedené platí v případě podání žádosti prostřednictvím on–line protokolu SSL/TLS.

7.3.3 Vydání časového razítka

7.3.3.1 Úkony TSA v průběhu vydávání časového razítka

Po přijetí žádosti o časové razítko provede TSA:

- kontrolu formální správnosti žádosti; v případě negativního výsledku kontrol je vytvořena odpověď podle standardu [RFC 3161] obsahující odpovídající chybový status,
- v případě kladného výsledku kontrol žádosti je k otisku dat, obsaženém v žádosti, přidán do datové struktury časový údaj odpovídající hodnotě UTC v okamžiku vytváření časového razítka s přesností 1 sekunda; tato hodnota je získaná z měřidla času navázaného na světový koordinovaný čas,
- takto vytvořená datová struktura je elektronicky opečetěna daty pro vytváření elektronické pečetě relevantního TSU, čímž vznikne časové razítko,
- časové razítko je archivováno,
- časové razítko je přidáno do odpovědi podle [RFC 3161],
- odpověď včetně časového razítka je odeslána žadateli o časové razítko.

7.3.3.2 Oznámení o vydání časového razítka žadateli o vydání časového razítka

Po ukončení všech úkonů uvedených v kapitole 7.3.3.1 je výsledná datová zpráva odeslána žadateli jako odpověď na žádost o časové razítko. Následně platí, že:

- o vydání konkrétního časového razítka je informován pouze žadatel,
- o celkovém počtu vydaných razítek je v pravidelných intervalech informován zákazník prostřednictvím vyúčtování služeb.

7.3.3.3 Převzetí časového razítka

Po obdržení odpovědi na žádost o časové razítko je klient povinen zjistit status odpovědi (položka PKIStatus, viz kapitola 7.3.5.2). V případě chyby není časové razítko v odpovědi obsaženo a klient ve stavové informaci odpovědi může zjistit bližší informace o příčině chyby.

Při převzetí časového razítka je žadatel povinen ověřit přijaté časové razítko postupem popsaným v kapitole 7.3.4.

7.3.4 Ověření časového razítka

Ověřování časového razítka probíhá následovně:

1. ověření obsahu časového razítka, tj.:

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

2. získání aktuálního příslušného CRL a ověření platnosti:

- použitého certifikátu TSA, kterým je razítko opečetěno,
- certifikátu certifikační autority PostSignum Qualified CA, která vydala certifikát TSA
- certifikátu certifikační autority PostSignum Root QCA, která vydala certifikát autority PostSignum Qualified CA (viz. kapitola 7.4.13).

V případě, že otisky dat jsou při shodném algoritmu shodné, byla ověřena platnost všech elektronických pečetí a platnost příslušných kořenových certifikátů PostSignum a certifikátu TSA (viz podrobněji kapitola 7.3.4.1), je časové razítko platné.

7.3.4.1 Platnost časového razítka

Stav časového razítka je úzce spojen se stavem certifikátu TSA, který je používán pro ověření elektronické pečetě na časovém razítku.

Pravidla pro určení platnosti časového razítka ve vazbě na stav certifikátu TSA jsou následující:

Pokud je certifikát TSA **platný** vzhledem k uvedené době platnosti v certifikátu a **nebyl zneplatněn**, je časové razítko, pro jehož ověření je uvedený certifikát používán, **platné**.

Pokud je certifikát TSA **platný** vzhledem k uvedené době platnosti v certifikátu a byl **zneplatněn s následujícími důvody zneplatnění**:

- unspecified (0),
- affiliationChanged (3),
- superseded (4), nebo
- cessationOfOperation (5),

je časové razítko, pro jehož ověření je uvedený certifikát používán a které bylo vydáno **před časem** zneplatnění certifikátu, **platné**.

Pokud je certifikát TSA **platný** vzhledem k uvedené době platnosti v certifikátu a **byl zneplatněn s následujícími důvody zneplatnění**:

- unspecified (0),
- affiliationChanged (3),
- superseded (4), nebo
- cessationOfOperation (5),

je časové razítko, pro jehož ověření je uvedený certifikát používán a které bylo vydáno **po čase** zneplatnění certifikátu, **neplatné**.

Pokud byl certifikát TSA **zneplatněn s následujícími důvody zneplatnění**:

- keyCompromise (1),
- caCompromise (2),
- nebo bez uvedeného důvodu pro zneplatnění,

je časové razítko, pro jehož ověření je uvedený certifikát používán, **neplatné** (a to i zpětně).

Pokud je certifikát TSA **neplatný** vzhledem k uvedené době platnosti v certifikátu (skončila mu platnost), není standardními kontrolami možné ověřit platnost časového razítka. V daném případě je podle potřeb spoléhající se strany nezbytné použít **dodatečná opatření**. Mezi tato opatření může patřit například:

- „přeorazítkování“ v době platnosti certifikátu TSA,
- kontrola, že certifikát TSA nebyl zneplatněn a že nedošlo k oslabení použitých kryptografických algoritmů,
- protokolární uložení dat na nepřepisovatelné médium,
- protokolární převod dat do papírové formy,
- použití nadstandardních kontrol uvedených v [ETSI EN 319421], příloze D.

### 7.3.5 Struktura žádosti, odpovědi a časového razítka

Časová razítka vydává konkrétní TSU na základě žádosti o časové razítko. V následujících tabulkách je postupně popsána struktura žádosti o časové razítko, struktura odpovědi PostSignum TSA a struktura samotného časového razítka.

#### 7.3.5.1 Struktura žádosti o časové razítko

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<br>(povinná položka) | |
| reqPolicy | Identifikátor politiky<br>(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<br>FALSE nebo nevyplněno – odpověď nesmí | TRUE, FALSE |

| | | |
|---|---|---|
| | obsahovat certifikát TSA (nepovinná položka) | |
| extensions | Žádná rozšíření nejsou povolena | |

Povolenými kryptografickými algoritmy, které mohou být použity při vytváření otisku dat, je:

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.

7.3.5.2 Struktura odpovědi na žádost o časové razítko

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<br>**1** – TST bylo vydáno (upravené)<br>**2** – odmítnutí žádosti<br>**3** – čekání na odpověď<br>**4** – bezprostřední zneplatnění certifikátu TSA<br>**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<br>**BadRequest** – nepovolená nebo nepodporovaná transakce<br>**BadDataFormat** – špatný formát zaslaných dat<br>**TimeNotAvailable** – nedostupný zdroj času TSA<br>**UnacceptedPolicy** – požadovaná politika není podporovaná ze strany TSA<br>**UnacceptedExtension** – požadované rozšíření není podporované ze strany TSA<br>**AddInfoNotAvailable** – požadované doplňující informace nebyly identifikované nebo nejsou dostupné<br>SystemFailure – žádost nemohla být zpracována kvůli chybě systému |

7.3.5.3 Struktura časového razítka

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 | |

Rozšíření časového razítka

| **QCStatement** | | |
|---|---|---|
| OID | 0.4.0.19422.1.1<br>*esi4-qtstStatement-1* | Položka id-etsi-tsts-EuQCompliance značí, že časové razítko bylo vydáno kvalifikovaným poskytovatelem služeb vytvářejících důvěru a je v souladu s eIDAS. |

Poznámka: Tato struktura je vložena do struktury SignedData podle [RFC 3852] s identifikátorem typu dat id-ct-TSTInfo. Podpisový algoritmus časového razítka je neměnný a je vždy sha256WithRSAEncryption.

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.

### 7.3.6 Synchronizace měřidla času s UTC

#### 7.3.6.1 Synchronizace

V systémech TSA jsou využívána tři nezávislá měřidla času, která jsou navázána na světový koordinovaný čas. V pravidelných intervalech jsou synchronizována se zdrojem UTC času, konkrétně UTC(USNO), pomocí technologie GPS. Návaznost času poskytovaného měřidlem času na UTC je prokázána úředním

kalibračním měřením. Písemný záznam o kalibračním měření je uložen u Manažera CA. V systémech TSA se musí používat pouze měřidla času, která mají platnou kalibraci.

Čas získaný z těchto měřidel je dále uvnitř systémů TSA distribuován (probíhá synchronizace času) pomocí protokolu NTP v3. Problematika synchronizace je podrobně řešena interní dokumentací TSA.

Jako kontrolní zdroj času je použit NTP server, který je přímo navázán na zdroj UTC(TP), kterým je státní etalon času. Tento server v pravidelných intervalech kontroluje stav měřidel času a jejich časovou odchylku (viz kapitola 7.3.6.4).

7.3.6.2 Přesnost času v časovém razítku

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

7.3.6.3 Bezpečnost měřidla času

Měřidlo času je umístěno v zabezpečených prostorách Trust centra. Problematika bezpečnosti měřidla času je podrobněji řešena v dokumentu [SBPTSA].

7.3.6.4 Detekce odchýlení měřidla času

Za účelem kontroly odchýlení měřidla času je v systémech TSA provozován NTP server, který je přímo navázán na zdroj UTC(TP), kterým je státní etalon času. Na tomto serveru dále běží aplikace, která kontroluje odchylku času poskytovaného tímto NTP serverem a času poskytovaného měřidly času. V případě detekce odchýlení měřidla času o více než 1 sekundu, ukončí TSA vydávání časových razítek do doby, než bude sjednána náprava.

7.3.6.5 Přestupná sekunda

Použitá měřidla času jsou synchronizována s UTC včetně výskytu přestupné sekundy.

Problematika výskytu přestupné sekundy je dále řešena v interní dokumentaci TSA.

7.4 Správa a provozní bezpečnost TSA

7.4.1 Řízení bezpečnosti

Odboru České pošty, který zajišťuje poskytování certifikačních služeb, byl vydán certifikát pro systém managementu bezpečnosti informací v souladu s [ISO 27001] a certifikát pro systém managementu kvality v souladu s [ISO 9001].

7.4.2 Hodnocení a řízení rizik

Procesy a pravidla pro identifikaci a ohodnocení aktiv, hrozeb a zranitelností, stanovení rizik a pravidla pro jejich řízení jsou součástí interní dokumentace systému managementu bezpečnosti informací.

7.4.3 Personální bezpečnost

7.4.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Role, zajišťující provoz, správu, údržbu a rozvoj systémů PostSignum TSA jsou obsazovány na základě procedur (např. vyžadování referencí, zkušební období apod.), které zajišťují, aby tyto funkce byly

obsazovány důvěryhodnými a kvalifikovanými pracovníky. Obdobné procedury platí pro uzavírání smluv s externími spolupracovníky nebo smluvními partnery.

V případě, že daná osoba není zaměstnancem České pošty, ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

7.4.3.2 Posouzení spolehlivosti osob

Do rolí obsluhy centrálních systémů PostSignum TSA jsou jmenovány výhradně osoby, které jsou delší dobu zaměstnány v České poště a mají dobré pracovní a osobní reference. Ostatní role mohou zastávat rovněž pracovníci smluvních partnerů České pošty.

V případě, že daná osoba není zaměstnancem České pošty, ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

7.4.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Všichni pracovníci, podílející se na provozu, správě, údržbě a rozvoji systémů PostSignum TSA, jsou vyškoleni. Součástí školení je i školení o bezpečnosti systému a o chování v havarijních situacích.

U rolí určených Manažerem CA může být školení nahrazeno prokazatelným seznámením pracovníka se všemi dokumenty upravujícími provoz TSA se vztahem k příslušné roli.

V případě, že daná osoba není zaměstnancem České pošty, ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

7.4.3.4 Požadavky na školení a periodicita školení

V PostSignum TSA existuje program vytváření, udržování a prohlubování bezpečnostního vědomí, diferencovaný podle rolí.

Manažer CA v pravidelných intervalech (zejména při změnách v postupech PostSignum TSA,) organizuje školení obsluhy.

7.4.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Požadavky na rotaci pracovníků a její frekvenci nejsou definovány.

7.4.3.6 Postihy za neoprávněné činnosti zaměstnanců

Postihy za porušení pracovní kázně se řídí organizačními předpisy České pošty nebo ustanoveními smlouvy mezi Českou poštou a smluvním partnerem.

7.4.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Na smluvní (externí) pracovníky jsou uplatňována obdobná kritéria jako na zaměstnance České pošty.

7.4.3.8 Dokumentace poskytovaná zaměstnancům

Dokumentace je vyjmenovaná v [CPSTSA].

7.4.4 Fyzická bezpečnost a bezpečnost prostředí

Fyzická bezpečnost a bezpečnost prostředí se řídí dokumenty uvedenými v [CPSTSA].

7.4.4.1 Umístění a konstrukce

V PostSignum TSA existují následující typy stabilních pracovišť umístěné v prostorách České pošty nebo jejích smluvních partnerů:

- centrální pracoviště (hlavní a záložní lokalita),
- operátorská pracoviště centra (zejména pro správu podpůrného informačního systému),
- obchodní a kontaktní místa.

Struktura pracovišť vyplývá z bezpečnostních požadavků uvedených v [SBPTSA]. Obecně platí, že všechny výše uvedené typy pracovišť mají jasně definovaný perimetr a jsou proti neoprávněnému vniknutí chráněny mechanickými prostředky.

7.4.4.2 Fyzický přístup

Pro každý typ pracoviště je v jeho provozním řádu definováno, kteří pracovníci mají na pracoviště fyzický přístup. Prostory jsou chráněny proti neoprávněnému vniknutí mechanickými prostředky (bezpečnostní zámky a mříže), na centrálním pracovišti též samostatnou smyčkou elektronického zabezpečovacího zařízení.

7.4.4.3 Elektřina a klimatizace

Centrální pracoviště jsou připojena na nepřerušitelný zdroj napájení (UPS) a mají nainstalovánu klimatizaci, která udržuje teplotu a vlhkost optimální pro provozovaná zařízení.

7.4.4.4 Vliv vody

Centrální pracoviště jsou umístěna mimo zátopové oblasti.

Prostory centrálních pracovišť jsou vybaveny signalizací zatopení vodou. Tato signalizace je vyvedena na pracoviště obsazené nepřetržitě 24 hodin denně, 7 dní v týdnu.

7.4.4.5 Protipožární opatření a ochrana

Prostory centrálních pracovišť jsou vybaveny elektronickou požární signalizací (EPS). Tato signalizace je vyvedena na pracoviště obsazené nepřetržitě 24 hodin denně, 7 dní v týdnu.

7.4.4.6 Ukládání médií

Pro účely uskladnění dat PostSignum TSA jsou k dispozici trezory

7.4.4.7 Nakládání s odpady

Papírové dokumenty a média, která jsou používána v PostSignum TSA, jsou poté, co nejsou zapotřebí, likvidována bezpečným způsobem:

- média jsou fyzicky zlikvidována ve skartovacím zařízení nebo je použit vhodný program zajišťující úplné smazání média,
- papírové dokumenty jsou zlikvidovány ve skartovacím zařízení.

7.4.4.8 Zálohy mimo budovu

Pro PostSignum TSA byla vybudována záložní lokalita, kam provoz přechází v mimořádných situacích, kdy není možné zabezpečit řádný provoz TSA v hlavní lokalitě, a kam jsou také pravidelně zasílány zálohy systémů PostSignum TSA.

7.4.5 Řízení provozu

7.4.5.1 Specifické technické požadavky na počítačovou bezpečnost

Bezpečnost provozu PostSignum TSA je zajištěna množinou bezpečnostních opatření na fyzické, technické, personální nebo organizační úrovni. Jednotlivá bezpečnostní opatření vycházejí z provedené analýzy rizik nebo z konkrétních požadavků platných právních předpisů a technických norem, které upravují činnost poskytovatelů certifikačních služeb, a to zejména ze standardů [ETSI EN 319401], [ETSI EN 319421] a, [ETSI EN 319422].

7.4.5.2 Organizace řízení provozu

Bezpečnost provozu PostSignum TSA je zajištěna množinou bezpečnostních opatření na fyzické, technické, personální nebo organizační úrovni.

Jednotlivá bezpečnostní opatření jsou uvedena v interní dokumentaci, zejména v dokumentu [SBPTSA].

7.4.5.3 Síťová bezpečnost

Lokální sítě centrálních pracovišť (hlavní a záložní lokalita) obsahující centrální systémy PostSignum TSA jsou od interní sítě ČP a od externích sítí odděleny firewallem. Tento firewall neumožňuje žádnou komunikaci směrem z interní sítě ČP resp. externích sítí přímo do lokální sítě obsahující systémy PostSignum TSA. Veškerá komunikace směrem do lokální sítě centrálního pracoviště je ukončena na vyhrazené DMZ síti.

Interní síť ČP je mimo to od všech externích sítí oddělena vlastním firewallem.

Veškerá komunikace mimo vyhrazené lokální sítě centrálních pracovišť je šifrovaná.

7.4.5.4 Hodnocení počítačové bezpečnosti

Systém PostSignum TSA prochází v pravidelných intervalech kontrolou bezpečnostní shody zaměřenou na splnění požadavků kladených legislativou na kvalifikovaného poskytovatele služeb vytvářejících důvěru, a to zejména požadavků uvedených v [eIDAS].

7.4.6 Správa řízení přístupu

7.4.6.1 Důvěryhodné role

V PostSignum TSA byly definovány role, které zastává obsluha PostSignum TSA. Jsou stanovena pravidla, podle kterých jsou role obsazovány, tedy kdo pracovníka v dané roli jmenuje a odvolává, které role nesmí zastávat současně jedna osoba. Veškerá přístupová práva (na úrovni fyzického přístupu, na úrovni přístupu k operačnímu systému, na úrovni přístupu k aplikaci) jsou vázána na tyto role.

Zvláštní pozornost je zejména věnována při obsazování rolí s možností přístupu k centrálním systémům PostSignum TSA.

7.4.6.2 Počet osob požadovaných na zajištění jednotlivých činností

V PostSignum TSA jsou definovány činnosti vyžadující přítomnost více než jedné osoby. Jedná se zejména o činnosti, při kterých se manipuluje se soukromými klíči TSA a s kryptografickým modulem použitým pro generování a úschovu soukromých klíčů TSA (bezpečným kryptografickým modulem).

7.4.6.3 Identifikace a autentizace pro každou roli

Představitel každé role se musí při přístupu k prostředkům PostSignum TSA identifikovat a autentizovat. Každý uživatel má přidělenou jednoznačnou identifikaci ve všech systémech, ke kterým má přístup. V systémech PostSignum TSA je používaná identifikace jménem resp. komerčním certifikátem a autentizace heslem resp. soukromým klíčem.

7.4.6.4 Role vyžadující rozdělení povinností

V PostSignum TSA jsou stanovena pravidla, podle kterých jsou obsazovány jednotlivé role, a rovněž byla stanovena pravidla pro separaci rolí. Tato pravidla jsou uvedena v [OZUTSA].

7.4.7 Vývoj a údržba důvěryhodných systémů

7.4.7.1 Řízení vývoje systému

Implementace systému probíhala podle zásad metodologie KeyStep, která byla vytvořena speciálně pro návrh a implementaci rozsáhlých PKI projektů. Vývoj dílčích aplikací probíhal v souladu s interní metodikou vývoje České pošty.

Následné změny jsou realizovány v souladu s definovaným změnovým řízením. Součástí změnového řízení je i hodnocení dopadu změn na bezpečnost řešení. V případě velkých změn nebo po sérii menších změn je provedena rozdílová nebo opakovaná analýza rizik.

7.4.7.2 Kontroly řízení bezpečnosti

Bezpečnost systémů PostSignum TSA je ověřována provozními kontrolami prováděnými v rámci zavedeného systému řízení informační bezpečnosti podle [ISO 27001], kontrolami bezpečnostní shody prováděnými pracovníky odboru interního auditu ČP a externími audity, které provádí externí subjekt.

7.4.8 Obnova po havárii nebo kompromitaci

Plán zvládání krizových situací a plán obnovy PostSignum TSA popisuje dokument Plán pro zvládání krizových situací a plán obnovy.

Tato dokumentace je mj. přístupná pro osoby provádějící kontrolu PostSignum TSA.

Personál PostSignum TSA je řádně vyškolen jak postupovat v případě havárie. Test havarijního plánu se provádí minimálně jedenkrát ročně.

7.4.8.1 Postup v případě incidentu a kompromitace

Zabezpečení prostředků TSA po živelné katastrofě nebo jiné mimořádné události je rozpracováno v dokumentu Plán pro zvládání krizových situací a plán obnovy.

7.4.8.2 Poškození výpočetních prostředků, softwaru nebo dat

Zabezpečení prostředků TSA po živelné katastrofě nebo jiné mimořádné události je rozpracováno v dokumentu Plán pro zvládání krizových situací a plán obnovy.

7.4.8.3 Postup při zjištění odchýlení měřidla času

Postup synchronizace časového údaje měřidla času je uveden v kapitole 7.3.6. Pokud je zjištěná odchylka od UTC větší než 1 sekunda, je činnost jednotky TSU okamžitě ukončena a do provedení nové inicializace jednotky TSU není služba vydávání časových razítek poskytována.

Následně PostSignum TSA zveřejní na svých webových stránkách bližší popis události a identifikaci časových razítek, jejichž důvěryhodnost byla touto událostí ovlivněna, a událost oznamuje orgánu dohledu.

7.4.8.4 Kompromitace soukromého klíče TSA

V případě podezření na kompromitaci soukromého klíče TSA (přesněji jedné z jednotek TSU), musí PostSignum TSA:

- písemně nebo elektronicky informovat všechny zákazníky s platnými smlouvami,
- písemně nebo elektronicky informovat orgán dohledu o mimořádném ukončení činnosti této TSU,
- oznámení o kompromitaci zveřejnit na webových stránkách poskytovatele,
- certifikát zneplatnit s důvodem keyCompromise (1),
- po zneplatnění kompromitovaného certifikátu odstranit důvody kompromitace a následně vygenerovat nový klíčový pár a nechat si vydat nový certifikát podle kapitoly 7.2,
- zveřejní na svých webových stránkách bližší popis události a identifikaci časových razítek, jejichž důvěryhodnost byla touto událostí ovlivněna.

PostSignum Qualified CA okamžitě zneplatní certifikát dotčené TSU; zneplatněný certifikát bude nejpozději do 24 hodin zveřejněný na příslušném CRL.

Po zveřejnění informace o zneplatnění certifikátu TSA z důvodu kompromitace klíče končí platnost všech časových razítek opečetěných soukromým klíčem z daného klíčového páru.

Česká pošta prokazatelně zničí data pro vytváření elektronických pečetí dotčené TSU, která sloužila pro pečetění časových razítek, u nichž existuje podezření na kompromitaci, a o tomto zničení provede záznam.

Tento postup bude také použit u všech jednotek TSU v případě, že dojde k náhlému oslabení algoritmu použitého pro vytváření elektronických pečetí, které nepopiratelně zpochybní důvěryhodnost vydávaných časových razítek.

7.4.8.5 Kompromitace soukromého klíče nadřízené certifikační autority

V případě kompromitace nebo podezření na kompromitaci soukromého klíče PostSignum Root QCA či PostSignum Qualified CA je dotčena také platnost certifikátů TSA.

Jako technické opatření provede poskytovatel certifikačních služeb zneplatnění certifikátu příslušné certifikační autority a všech jimi vydaných platných certifikátů – důvod ukončení platnosti certifikátu caCompromise (2). Zneplatněné certifikáty budou nejpozději do 24 hodin zveřejněny na příslušném CRL.

Tím se certifikáty TSA stávají neplatnými stejně jako vydaná časová razítka, jejichž pečeť bylo možné těmito certifikáty ověřit.

Poznámka: Vlastní důvěryhodnost časového razítka v takovém případě není ohrožena; ohrožena je pouze důvěryhodnost řetězu certifikátů. V případě získání certifikátů TSA resp. jednotlivých TSU z důvěryhodného zdroje (např. ze stránek PostSignum TSA), a ověření jejich původu, je možné platnost časového razítka ověřit.

7.4.8.6 Schopnost obnovit činnost po havárii

Pokračování procesů časové autority po havárii závisí na typu havárie a jejích následcích.

V případě havárie malého a středního rozsahu přechází provoz PostSignum TSA do záložní lokality. Postup přesunu provozu je uveden v dokumentu Plán pro zvládání krizových situací a plán obnovy.

V případě havárie velkého rozsahu (přírodní pohroma, válečný stav), je obnova činnosti PostSignum TSA věcí rozhodnutí managementu České pošty. O rozhodnutí managementu musí být s minimální prodlevou informováni všichni zákazníci PostSignum TSA.

Pokud management České pošty nerozhodne o ukončení provozu PostSignum TSA, nepřekročí doba výpadku služeb PostSignum TSA 20 pracovních dní.

7.4.9 Ukončení činnosti TSA

7.4.9.1 Ukončení činnosti TSA

Řádně plánované ukončení činnosti PostSignum TSA v oblasti vydávání časových razítek musí být orgánu dohledu písemně nahlášeno nejméně 3 měsíce před plánovaným ukončením činnosti. Součástí oznámení musí být i informace o ukončení platnosti certifikátů TSA včetně příslušného důvodu ukončení.

Na webových stránkách poskytovatele musí být zveřejněny informace o ukončení činnosti i ukončení platnosti pečetících certifikátů TSA včetně příslušného důvodu ukončení a to nejméně 2 měsíce před plánovaným ukončením činnosti.

Činnost poskytovatele certifikačních služeb bude ukončena v souladu s platnými právními předpisy. Pokud po ukončení činnosti poskytovatele certifikačních služeb nebude nadále možné zajistit přístup k údajům, které byly evidovány z důvodu poskytování certifikačních služeb a které by mohly sloužit pro účely poskytnutí důkazů v soudním a správním řízení a pro účely zajištění kontinuity služby, tak tyto údaje předá Manažer CA orgánu dohledu. Tuto informaci zahrne do zprávy, odeslané všem svým klientům, kteří jsou držiteli platných smluv o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek. Smlouvy budou ukončeny ze strany ČP dohodou nebo výpovědí.

Následně ČP prokazatelně zničí data pro vytváření elektronických pečetí PostSignum TSA, která sloužila pro pečetění časových razítek a zneplatní všechny certifikáty TSA s důvodem „cessationOfOperation“

7.4.9.2 Ukončení činnosti poskytovatele certifikačních služeb

Poskytovatel je povinen informovat každého zákazníka v dostatečném předstihu o svém záměru ukončit svou činnost a splnit veškeré závazky vyplývající z platných právních předpisů. Poskytovatel se především zavazuje v případě ukončení poskytování certifikačních služeb:

- informovat všechny dotčené strany,

- vyvinout přiměřené úsilí pro převzetí evidence, vedené dle platné legislativy, jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání časových razítek, pokud se to nepodaří, tak předat evidované údaje v souvislosti s poskytovanou službou orgánu dohledu,
- ukončit poskytování služby vydávání časových razítek,
- prokazatelně zničit párová data PostSignum TSA pro vytváření elektronických pečetí časových razítek.

7.4.9.3 Odnětí akreditace

V případě odnětí akreditace musí být informace o odnětí akreditace písemně nebo elektronicky sdělena všem zákazníkům. Informace o odnětí akreditace bude zveřejněna na webových stránkách poskytovatele, na všech pracovištích PostSignum TSA a dalšími způsoby uvedenými v platných právních předpisech.

O dalším postupu v tomto případě rozhodne management ČP na základě příslušného rozhodnutí orgánu dohledu.

7.4.10 Shoda s právními předpisy

Viz kapitola 7.5.15

7.4.11 Záznam informací o provozu TSA

Pro PostSignum TSA byl zpracován dokument Auditní a archivační politika TSA (příloha [SBPTSA]), který popisuje zásady kontroly, auditu a archivace PostSignum TSA. Tento dokument je zejména přístupný osobám, které provádějí kontrolu bezpečnostní shody PostSignum TSA. Tato kapitola vychází z dokumentu Auditní a archivační politika a poskytuje stručný přehled základních zásad uplatňovaných při kontrole PostSignum TSA.

7.4.11.1 Typy zaznamenávaných událostí

Pro potřeby kontroly a případné analýzy a vyšetření mimořádných událostí (obecně pro zajištění možnosti prokázat sled operací PostSignum TSA a jejich přiřazení osobě, která je vyvolala) jsou vedeny záznamy o událostech při synchronizaci času, nakládání s klíči a certifikáty PostSignum TSA a dalších významných událostech. Seznam zaznamenávaných událostí je uveden v dokumentu Auditní a archivační politika TSA (příloha [SBPTSA]). Auditní záznamy jsou vedeny v elektronické nebo písemné podobě.

Dále jsou v souladu s požadavky platných právních předpisů zaznamenávána (a archivována) všechna vydaná časová razítka.

Auditní záznamy v písemné podobě musí být podepsány, musí uvádět jméno pracovníka, který záznam pořídil, a čas záznamu.

7.4.11.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány osobami v odpovídající roli pověřené tímto úkolem v intervalech definovaných [SBPTSA]. Dále podléhají interní a externí kontrole, viz kapitola 5.4.1.

7.4.11.3 Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány po dobu deseti let, pokud jiný předpis nestanoví dobu delší.

7.4.11.4 Ochrana auditních záznamů

Auditní záznamy jsou uloženy tak, aby byly ochráněny proti krádeži, modifikaci a zničení úmyslnému i neúmyslnému (ohněm, vodou).

Písemné auditní záznamy v podobě deníků musí být uschovány v trezoru nebo uzamykatelné skříni. Auditní záznamy v podobě datových souborů jsou archivovány na nepřepisovatelných médiích.

7.4.11.5 Postupy pro zálohování auditních záznamů

Auditní záznamy (kromě auditních záznamů o činnosti centrálních komponent autority časového razítka v elektronické podobě) nejsou obecně zálohovány; jsou pouze archivovány. Důležité auditní záznamy spojené s vydáním časových razítek, manipulací s klíčovými páry TSA a synchronizací času, jsou uchovávány ve dvou kopiích, které jsou uložené v různých lokalitách.

7.4.11.6 Systém shromažďování auditních záznamů (interní nebo externí)

V prostředí PostSignum TSA není nasazen systém na centrální shromažďování auditních záznamů. Auditní záznamy jsou shromažďovány v rámci jednotlivých systémů PostSignum TSA.

V případě výskytu definovaných bezpečnostně zajímavých událostí je automaticky vytvořeno upozornění o události, které je e-mailem odesláno odpovědné osobě.

7.4.11.7 Postup při oznamování události subjektu, který ji způsobil

Subjektu, který způsobil událost zaznamenanou v auditním logu, není tato skutečnost nijak oznamována.

7.4.11.8 Hodnocení zranitelnosti

Auditní záznamy jsou v pravidelných intervalech procházeny, kontrolovány a analyzovány na výskyt záznamů o nestandardních událostech, které mohou znamenat pokus o narušení bezpečnosti. Jsou definovány postupy, jak v těchto případech dále postupovat.

Zprávy o nestandardních událostech jsou předávány Manažerovi CA, který zajistí vyhodnocení závažnosti a rozhodne o dalším postupu; mimo to jsou zprávy předávány i Auditorovi TSA.

7.4.12 Uchovávání informací a dokumentace

Pro PostSignum TSA byl zpracován dokument Auditní a archivační politika (příloha [SBPTSA]), který popisuje zásady kontroly, auditu a archivace v PostSignum TSA. Tento dokument je mj. přístupný osobám, které provádějí kontrolu PostSignum TSA.

7.4.12.1 Typy informací a dokumentace, které se uchovávají

V PostSignum TSA se archivují tyto záznamy:

- programové vybavení a data,
- vydaná časová razítka,
- písemné smlouvy o poskytování služeb časového razítka,
- zprávy o provedení kontroly,
- auditní záznamy (např. provozní deníky, záznamy automaticky vytvářené komponentami informačního systému PostSignum TSA).

Podrobný výčet archivovaných záznamů je specifikován v Auditní a archivační politice (příloha [SBPTSA]).

7.4.12.2 Doba uchování uchovávaných informací a dokumentace

Programové vybavení, data a auditní záznamy se archivují po dobu deseti let.

7.4.12.3 Ochrana úložiště uchovávaných informací a dokumentace

Archiv je zabezpečen pomocí opatření technické a objektové bezpečnosti. Je rovněž chráněn proti vlivům prostředí, jako jsou teplota, vlhkost atd.

7.4.12.4 Postupy při zálohování uchovávaných informací a dokumentace

Zálohovací procedury archivu jsou upraveny samostatným dokumentem Auditní a archivační politika (příloha [SBPTSA]), který je mj. přístupný osobám provádějícím kontrolu PostSignum TSA.

7.4.12.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V PostSignum TSA jsou časová razítka používána při pečetění souborů s archivy vydaných časových razítek. Kromě tohoto případu nejsou při uchovávání informací a dokumentace časová razítka používána.

7.4.12.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)

V prostředí PostSignum TSA jsou auditní záznamy shromažďovány a přesouvány do archivu CA v souladu s postupy uvedenými v dokumentu Auditní a archivační politika.

7.4.12.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Archivy dat a programového vybavení jsou umístěny v k tomu určených trezorech.

7.4.13 Zveřejňování informací a dokumentace

Informace o používaných certifikátech, o provozu PostSignum TSA a dokumentace PostSignum TSA jsou zveřejňovány v níže uvedeném rozsahu.

7.4.13.1 Zveřejňování certifikátů a CRL

Certifikáty TSA jsou zveřejňovány na webových stránkách poskytovatele a na webových stránkách orgánu dohledu.

CRL pro ověření platnosti certifikátů TSA a certifikátů nadřízených certifikačních autorit jsou zveřejňovány na webových stránkách poskytovatele:

Informace o zneplatněných certifikátech jsou zveřejňovány ve formě seznamu zneplatněných certifikátů (CRL)

- na webových stránkách poskytovatele
- na webových stránkách externího poskytovatele webových služeb
- na distribučních bodech (CRL Distribution Points), které jsou uvedeny v certifikátu

7.4.13.2 Zveřejňování informací o autoritě časového razítka

Politiky autority časového razítka, zprávy pro uživatele a případně i další dokumenty jsou zveřejňovány na:

- webových stránkách poskytovatele.

Další důležité informace (např. odnětí akreditace, zneplatnění certifikátu TSA) nebo informace o mimořádné události jsou zveřejňovány:

- na webových stránkách poskytovatele
- na obchodních místech ve formě vyvěšeného textového oznámení
- v celostátně distribuovaném deníku.

7.4.13.3 Periodicita zveřejňování informací

Informace jsou zveřejňovány v následujících intervalech:

- certifikáty TSA jsou zveřejňovány ihned po ověření orgánem dohledu,
- politiky TSA a zpráva pro uživatele jsou zveřejňovány po schválení a vydání nové verze, vždy však před počátkem platnosti daného dokumentu (a v případě politiky TSA před vydáním prvního časového razítka);
- všechny důležité informace jsou zveřejňovány neprodleně.

7.4.13.4 Řízení přístupu k jednotlivým typům úložišť

Politiky TSA, certifikáty TSA a další důležité informace jsou přístupné pro čtení bez jakéhokoliv omezení.

Poskytovatel služby vydávání časových razítek neumožňuje veřejný přístup k vydaným časovým razítkům.

Modifikace zveřejněných údajů je povolena pouze autorizované obsluze a procesům autority časového razítka.

7.5 Ostatní obchodní a právní záležitosti

7.5.1 Poplatky

7.5.1.1 Poplatky za vydání časového razítka

Cena za poskytnutou službu vydání časového razítka je stanovena ve smlouvě mezi zákazníkem a poskytovatelem služby a běžně se řídí aktuálním platným ceníkem. Cena za vydaná časová razítka může být i zahrnuta v ceně jiné služby poskytované Českou poštou.

7.5.1.2 Poplatky za přístup k certifikátu poskytovatele

Služba přístupu k certifikátu ze seznamu vydaných certifikátů je poskytována bezplatně.

7.5.1.3 Poplatky za informace o stavu certifikátu nebo o zneplatnění certifikátu poskytovatele

Tuto službu poskytuje certifikační autorita PostSignum QCA a případné poplatky jsou uvedené v ceníku této certifikační autority.

7.5.1.4 Poplatky za další služby

Cena za další služby PostSignum TSA je stanovena v ceníku služeb České pošty, který je mj. dostupný na webových stránkách poskytovatele.

7.5.2 Finanční odpovědnost

7.5.2.1 Krytí pojištěním

Česká pošta má sjednané pojištění odpovědnosti za škodu takovým způsobem, aby byly pokryty případné škody.

7.5.2.2 Další aktiva a záruky

Aktiva České pošty jsou uvedena ve Výroční zprávě. Výroční zpráva je uložena v obchodním rejstříku u Městského soudu v Praze pod spisovou značkou A7565.

Výroční zpráva je k nahlédnutí též na webových stránkách České pošty (www.ceskaposta.cz).

7.5.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

PostSignum TSA tuto službu neposkytuje.

7.5.3 Důvěrnost obchodních informací

V maximálním rozsahu podle mandatorních ustanovení platných právních předpisů se každá ze zúčastněných stran zavazuje uchovat v tajnosti veškeré důvěrné informace, okolnosti a údaje, které se dozvěděla v souvislosti s plněním smlouvy o poskytování certifikačních služeb a o kterých nebylo písemně dohodnuto mezi smluvními stranami, že mohou být zveřejněny.

7.5.3.1 Výčet důvěrných informací

Za důvěrné jsou považovány všechny informace s výjimkou informací uvedených v dokumentech určených pro veřejnost.

7.5.3.2 Informace mimo rámec důvěrných informací

Za důvěrné se nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opominutím přijímající strana,
- měla přijímající strana legálně k dispozici před uzavřením smlouvy o poskytování certifikačních služeb, pokud takové informace nebyly předmětem jiné, dříve mezi zúčastněnými stranami uzavřené smlouvy o ochraně informací, nebo pokud takové informace nemají samy o sobě charakter obchodního tajemství,
- jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je schopna to doložit svými záznamy nebo důvěrnými informacemi třetí strany,
- po uzavření smlouvy o poskytování certifikačních služeb poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem, nebo je nezíská nezákonným způsobem, o čemž by přijímající strana věděla nebo vědět musela,
- jsou uvedené v časovém razítku.

7.5.3.3 Odpovědnost za ochranu důvěrných informací

Odpovědnost za zpracování důvěrných informací v PostSignum TSA nese Česká pošta, jakožto poskytovatel certifikačních služeb, všichni její zaměstnanci a smluvní partneři.

7.5.3.4 Poskytnutí citlivých informací pro soudní či správní účely

Veškeré informace zpracovávané v PostSignum QCA jsou zpřístupněny orgánům zmocněným ze zákona v případech, kdy to zákon vyžaduje, a do té míry, do jaké to zákon vyžaduje. Zpřístupnění informací zajistí Manažer CA poté, co orgány zmocněné ze zákona prokáží své zmocnění způsobem obvyklým v těchto případech.

7.5.4 Ochrana osobních údajů

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů jsou obsaženy ve Všeobecných obchodních podmínkách certifikačních služeb a vycházejí z [GDPR].

7.5.4.1 Osobní údaje

Za osobní údaje jsou považovány veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat.

7.5.4.2 Odpovědnost za ochranu osobních údajů

Odpovědnost za ochranu osobních údajů zpracovávaných v systémech PostSignum nese Česká pošta, jakožto poskytovatel certifikačních služeb, všichni její zaměstnanci a smluvní partneři v rozsahu stanoveném [GDPR].

7.5.4.3 Poskytnutí osobních údajů

V této oblasti je postupováno podle příslušných ustavení [GDPR], obecně závazných právních přepisů a interních předpisů České pošty upravujících problematiku ochrany osobních údajů.

7.5.5 Práva duševního vlastnictví

Tato politika pro vydávání časových razítek a veškeré související dokumenty jsou chráněny autorskými právy České pošty a představují významné know-how České pošty. Česká pošta je rovněž nositelem výlučných práv k informačnímu systému pro provoz PostSignum TSA a ke struktuře, organizaci, vzhledům obrazovek a obsahu webových stránek poskytovatele.

7.5.6 Zastupování a záruky

Česká pošta zaručuje, že splní veškeré povinnosti uložené touto politikou a mandatorními ustanoveními příslušných právních předpisů.

Česká pošta poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb.

7.5.6.1 Zastupování a záruky TSA

Viz ustanovení kapitola 7.5.6.

7.5.6.2 Zastupování a záruky třetí strany

V oblasti uzavírání smluv o poskytování certifikačních služeb může být Česká pošta, jakožto poskytovatel služby vydávání časových razítek, zastupována třetím subjektem na základě uzavřeného smluvního vztahu. Uvedená úroveň záruk není tímto dotčena.

Jinak viz ustanovení v kapitole 7.5.6.

7.5.6.3 Zastupování a záruky zákazníka, pověřené osoby nebo žadatele

Zákazník, pověřená osoba nebo žadatel ručí za naplnění všech povinností zákazníků, pověřených osob a žadatelů o časové razítko uvedených v této politice a povinností uvedených v platných právních předpisech.

7.5.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strana se zaručuje, že časové razítko bude používat podle ustanovení v této politice, především v kapitole 6.3.

7.5.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Subjekty, které se přímo podílí na provozu PostSignum TSA na základě smluvního vztahu s poskytovatelem služby vydávání časových razítek, mají povinnost dodržovat ustanovení této politiky, [CPSTSA], [SBPTSA] a dalších interních dokumentů.

Záruky, které v těchto případech poskytuje poskytovatel služby vydávání časových razítek, jsou definovány příslušnými ustanoveními platných právních předpisů.

7.5.7 Zřeknutí se záruk

Záruky uvedené v kapitole 7.5.6 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, zejména za provozování v rozporu s podmínkami uvedenými v této certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.

7.5.8 Omezení odpovědnosti

Česká pošta neodpovídá za škodu vyplývající z použití časového razítka, pokud došlo ze strany zákazníka, žadatele nebo spoléhající se strany k nedodržení omezení pro jeho použití, uvedených v této politice a zveřejněných na webových stránkách poskytovatele.

Česká pošta bude průběžně s rostoucími provozními zkušenostmi s poskytováním certifikačních služeb ověřovat, zda podmínky omezení odpovědnosti České pošty uvedené v tomto ustanovení odpovídají obvyklým podmínkám na trhu a přiměřenému obchodnímu riziku České pošty.

Ustanovení tohoto článku zůstávají v platnosti i po ukončení platnosti této certifikační politiky.

7.5.8.1 Odpovědnost zákazníka

Zákazník je povinen zejména:

- poskytovat pravdivé a úplné informace při uzavírání smlouvy o poskytování certifikačních služeb,
- neprodleně uvědomit poskytovatele služby vydávání časových razítek o změnách údajů, které jsou ve smlouvě uvedeny, zejména o změnách údajů o pověřených osobách.

7.5.8.2 Odpovědnost pověřených osob

Pověřená osoba je povinna zejména:

- poskytovat pravdivé a úplné informace o žadatelích oprávněných žádat o časové razítko podle této politiky,
- zajistit důvěrnost autentizačních informací, se kterými při registraci žadatelů přichází do styku.

7.5.8.3 Odpovědnost žadatele

Žadatel je povinen zejména:

- zajistit důvěrnost autentizačních informací potřebných pro ověření identity žadatele při podávání žádosti o časové razítko,
- seznámit se s politikou, podle které mu bylo časové razítko vydáno (u žadatele – systému se tato povinnost vztahuje na správce systému resp. aplikace).

7.5.8.4 Odpovědnost poskytovatele

Poskytovatel služby vydávání časových razítek je zejména povinen:

- během procesu uzavírání smlouvy o poskytování certifikačních služeb ověřit všechny údaje podle předložených dokladů,
- ověřit autentizační údaje žadatele při podání žádosti o vydání časového razítka,
- vydat časové razítko obsahující věcně správné údaje na základě informací, které jsou TSA k dispozici v době vydávání časového razítka,
- zveřejňovat politiky, podle kterých vydává časová razítka, na webových stránkách poskytovatele,
- zveřejnit certifikát TSA tak, aby se každý mohl ujistit o jeho identitě,
- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje zejména provoz v souladu:
    - s platnými právními předpisy,
    - s touto politikou,
    - s [CPSTSA],
    - s [SBPTSA],
    - s provozní dokumentací.

7.5.9 Odpovědnost za škodu, náhrada škody

Pokud nevyplývá z mandatorních ustanovení platných právních předpisů jinak, odpovídá Česká pošta zákazníkovi za škodu způsobenou porušením povinností České pošty v souvislosti s plněním smlouvy o poskytování certifikačních služeb.

7.5.10 Doba platnosti, ukončení platnosti

7.5.10.1 Doba platnosti

Doba platnosti této politiky pro vydávání časových razítek je od data vydání, uvedeného v kapitole 5.2, do odvolání.

7.5.10.2 Ukončení platnosti

Platnost dokumentu je ukončena v případě

- odvolání, nebo
- ukončení poskytování služeb Českou poštou, jakožto poskytovatelem certifikačních služeb v oblasti vydávání časových razítek.

7.5.10.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti tohoto dokumentu v důsledku ukončení poskytování služeb zůstávají v platnosti omezení a ustanovení uvedená v kapitole 7.5, která se týkají obchodních a právních záležitostí.

7.5.11 Komunikace mezi zúčastněnými subjekty

7.5.11.1 Komunikace s poskytovatelem služby vydávání časových razítek

Veškeré informace, které chce poskytovatel služby vydávání časových razítek sdělit zákazníkům, zveřejní na svých webových stránkách a na vývěskách na pracovištích kontaktních a obchodních míst. Závažné informace, jako například podezření na kompromitaci klíče některé z jednotek TSU, sděluje poskytovatel služby vydávání časových razítek opět na webových stránkách a současně písemným nebo elektronickým upozorněním směrovaným na zákazníky.

Zákazník komunikuje s poskytovatelem služby TSA prostřednictvím pověřené osoby nebo osoby oprávněné k zastupování organizace. Příslušná osoba se obrací na pracoviště obchodního místa.

Komunikace zákazníka s poskytovatelem služby TSA může probíhat rovněž elektronicky. V případě požadavku na právní prokazatelnost elektronické komunikace musí být tato založena na certifikátech vydaných PostSignum QCA nebo jinou autoritou, kterou Česká pošta označí za důvěryhodnou, a o akceptaci jejíhož certifikátu se zákazníkem předem písemně dohodne formou dodatku ke smlouvě.

7.5.11.2 Komunikace v rámci systému PostSignum TSA

Komunikace v systému PostSignum TSA se řídí platnými předpisy České pošty a interními dokumenty úlohy PostSignum TSA.

7.5.11.3 Komunikační jazyk

Veškerá komunikace v systému PostSignum TSA musí probíhat v českém jazyce, pokud se obě strany nedohodnou jinak.

7.5.12 Změny

7.5.12.1 Postup při změnách

Postupy pro zapracování změn jsou uvedeny v kapitole 7.1.3.

7.5.12.2 Postup při oznamování změn

Vydání nové politiky pro vydávání časových razítek se změněným OID (viz následující odstavec) bude oznámeno v aktualitách na webových stránkách poskytovatele.

Zákazníci, pověřené osoby nebo žadatelé se mohou na webových stránkách poskytovatele přihlásit k odebírání e-mailového zpravodaje, kterým bude mj. oznamováno vydání nové verze politiky.

V případě, že nebude hrozit nebezpečí z prodlení, bude toto oznámení provedeno min. 1 měsíc před začátkem platnosti nové verze politiky pro vydávání časových razítek.

7.5.12.3 Okolnosti, při kterých musí být změněn OID

Česká pošta přiřadila dle svých interních pravidel identifikátory objektů (OID) užívané v hierarchii PostSignum.

OID jsou přiřazeny:

- certifikační autoritě PostSignum Root QCA,
- každé certifikační autoritě, které PostSignum Root QCA vydala certifikát, zejména certifikační autoritě PostSignum Qualified CA,
- autoritě časového razítka PostSignum TSA,
- každé politice, podle které jsou vydávány certifikáty nebo časová razítka v rámci hierarchie PostSignum.

OID nejsou přiřazeny prováděcí směrnici TSA ani interním dokumentům.

Jakákoliv změna v této politice vyvolá změnu verze dokumentu i změnu OID.

7.5.13 Řešení sporů

V případě vzniku sporu mezi zákazníkem a PostSignum TSA je možné se obrátit na

- Manažera CA, nebo
- kontaktní místo nebo pracoviště Helpdesk (formou žádosti o reklamaci).

Pokud ani jedna z výše uvedených instancí nesjedná ukončení sporu, bude se spor mezi zákazníkem a PostSignum TSA řešit u místně a věcně příslušného soudu.

7.5.14 Rozhodné právo

Činnost PostSignum TSA se řídí právním řádem České republiky.

7.5.15 Shoda s právními předpisy

Činnost PostSignum TSA je v souladu s právním řádem České republiky.

Vztah mezi Českou poštou a zákazníkem je upraven písemnou smlouvou o poskytování certifikačních služeb.

7.5.16 Další ustanovení

7.5.16.1 Rámcová dohoda

Žádná ustanovení v tomto odstavci.

7.5.16.2 Postoupení práv

Česká pošta může pro zajištění vykonávání svých činností využít služeb jiného právního subjektu, u kterého je zajištěna stejná úroveň bezpečnosti i poskytovaných služeb. Vztahy mezi Českou poštou a tímto subjektem budou upraveny zvláštní smlouvou. Povinnosti a odpovědnost České pošty, jakožto poskytovatele certifikačních služeb, zůstávají tímto nedotčeny.

V případě ukončení činnosti kvalifikovaného poskytovatele služby vydávání časových razítek vyvine Česká pošta v souladu s platnými právními předpisy přiměřené úsilí pro převzetí správy zákazníků a související agendy jiným kvalifikovaným poskytovatelem služby vydávání časových razítek. V tomto případě budou vztahy mezi tímto kvalifikovaným poskytovatelem a Českou poštou rovněž upraveny zvláštní smlouvou.

Převzetí části nebo všech činností poskytovatele služby vydávání časových razítek třetí stranou neomezuje služby ani záruky poskytované Českou poštou vzhledem k zákazníkům a spoléhajícím se stranám.

7.5.16.3 Oddělitelnost ustanovení

Smlouva o poskytování certifikačních služeb uzavřená mezi zákazníkem a Českou poštou zůstává platná i v případě, že jakákoliv její dílčí část pozbude platnost, pokud se obě strany nedohodnou jinak.

7.5.16.4 Zřeknutí se práv

Žádná ustanovení v tomto odstavci.

7.5.16.5 Vyšší moc

Česká pošta nenese odpovědnost za porušení svých povinností způsobené zásahy vyšší moci, jako jsou například přírodní katastrofy velkého rozsahu, stávky, občanské nepokoje nebo válečný stav.

7.5.16.6 Přístupnost pro osoby se zdravotním postižením

Poskytované služby vytvářející důvěru a konečné uživatelské produkty používané při poskytování těchto služeb jsou dostupné osobám se zdravotním postižením.

7.5.17 Další opatření

7.5.17.1 Použitá literatura a řídící dokumenty

Při tvorbě této politiky bylo zejména přihlíženo k následujícím dokumentům:

[eIDAS] NAŘÍZENÍ 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

[ETSI EN 319 401] Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[ETSI EN 319 411] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1 – 3

[ETSI EN 319 412] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5

[ETSI EN 119 312] Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[ETSI EN 319 421] Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[ETSI EN 319 422] Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

[GDPR] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

[ISO 27001] ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

[RFC 6960] Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

[RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[RFC 3161] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

[ZoEP] Zákon č. 227/2000 Sb. o elektronickém podpisu (zrušen zákonem 297/2016 Sb.)

[ZoSVD] Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce v platném znění

[VOP] Všeobecné obchodní podmínky certifikačních služeb

[CPQCATSA] Certifikační politika PostSignum QCA pro certifikáty TSA, aktuální verze

[CPSQCA] „Certifikační prováděcí směrnice pro úlohu Kvalifikovaná certifikační autorita České pošty, s.p.“, aktuální verze

[CPSTSA] „Prováděcí směrnice pro úlohu Autorita časových razítek České pošty, s.p.“, aktuální verze

7.5.17.2 Návazné dokumenty

V této politice je odkazováno rovněž na následující interní dokumenty:

[OZUTSA] „Organizační zajištění úlohy Autorita časových razítek České pošty, s.p.“, aktuální verze

| | |
|---|---|
| [SBPTSA] | „Systémová bezpečnostní politika pro úlohu Autorita časových razítek České pošty, s.p.“ aktuální verze |