Prováděcí směrnice pro úlohu
Autorita časových razítek České pošty, s.p.
PostSignum TSA

Verze 3.0.1

Evidence revizí a změn

Verze	Datum revize	Důvod a popis změny	Autor	Schválil
1.0	1.6.2010	První verze	PCA ČP	PAA ČP
2.0	1.7.2012	Aktualizace dokumentu	PCA ČP	PAA ČP
3.0	2.10.2017	Aktualizace v souvislosti s akreditací dle eIDAS	PCA ČP	PAA ČP
3.0	1.9.2020	Revize dokumentu bez změny verze – drobné změny v odkazech na dokumenty a legislativu	PCA ČP	
3.0	1.9.2021	Revize dokumentu beze změn	PCA ČP	
3.0.1	15. 8. 2022	Revize dokumentu beze změn, změna číslování verzí	PCA ČP	

1 ÚVOD

Tato prováděcí směrnice upravuje postupy činnosti autority časového razítka PostSignum TSA (dále i TSA) související s vydáváním kvalifikovaných elektronických časových razítek podle všech platných politik pro vydávání časových razítek. Pro účely tohoto dokumentu 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
e-mail: info@cpost.cz

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, s. p. 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].
PostSignum TSA vydává kvalifikovaná elektronická 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. Certifikáty PostSignum TSA (tedy jednotlivých TSU) jsou vydány certifikační autoritou PostSignum Qualified CA.

Tato Prováděcí směrnice TSA (dále i jen CPS) doplňuje nebo rozvádí vybraná témata popsaná v jednotlivých politikách pro vydávání časových razítek (dále i politika TSA) a upravuje tak vydávání časových razítek v systému PostSignum TSA. V případě rozporu mezi CPS a politikou TSA, která se na toto CPS odkazuje, platí ustanovení politiky TSA.

Autorita časových razítek PostSignum TSA byla vybudována a je provozována v souladu s obecně uznávanými standardy v oblasti PKI.

Tato CPS poskytuje věcné informace popisující

- postupy užívané při poskytování služby vydávání časových razítek,
- technologie, procesy a provozní podmínky, které poskytování služby vydávání časových razítek umožňují.

Postupy popsané v této CPS spolu s technologiemi a procesy popsanými v dalších dokumentech dokumentují postupy a pravidla vedoucí k zajištění důvěryhodnosti a integrity autority PostSignum TSA při poskytování

služby vydávání časových razítek, jakož i důvěryhodnosti časových razítek, která jsou PostSignum TSA vydávána, a to včetně přesnosti časového údaje uvedeného ve vydaných časových razítcích.

3 SEZNAM POUŽITÝCH POJMŮ A ZKRATEK

Předpokládá se, že osoba seznamující se s touto prováděcí směrnicí TSA má základní znalosti z oblasti PKI a [eIDAS], včetně

- použití digitálních podpisů pro zajištění autentizace, integrity a nepopiratelnosti,
- principů asymetrické kryptografie a certifikátů veřejných klíčů,
- rolí certifikační a registrační autority,
- funkce autority časového razítka.

Proto tento seznam neobsahuje některé obecně používané zkraty a pojmy z uvedené oblasti.

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, dat pro vytváření elektronických značek 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 (označuje) časové 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, značky, 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, dat pro ověřování elektronických značek 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 – standardně Certifikační prováděcí směrnice, zde se však tato zkratka používá pro Prováděcí směrnici TSA

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)

IČ – Identifikační číslo (jednoznačné číslo identifikující právnickou osobu)

ISMS – Information Security Management System (Systém řízení informační bezpečnosti)

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

QMS – Quality Management Systém (Systém managementu jakosti)

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

Autorita časového razítka PostSignum TSA doplňuje hierarchii certifikačních autorit PostSignum o službu vydávání časových razítek.

Autorita časového razítka PostSignum TSA může být řízena a provozována pouze Českou poštou, s. p. Výjimkou jsou situace, kdy dochází ke změně právního statutu České pošty. V takovém případě může být činnost PostSignum TSA zajišťována formou outsourcingu nástupnickou organizací. Česká pošta, s.p. je však nadále zodpovědná za dodržování povinností kladených na poskytovatele certifikačních služeb.

Tato prováděcí směrnice TSA se týká
- všech služeb, které jsou poskytovány autoritou časového razítka PostSignum TSA a
- všech časových razítek, které byly vydány autoritou PostSignum TSA.

Není-li uvedeno jinak, je dále v tomto dokumentu pod pojmem:
- certifikát míněn kvalifikovaný certifikát pro elektronický podpis nebo elektronickou pečeť,
- časové razítko míněno kvalifikované elektronické časové razítko,
- certifikát TSA míněn certifikát konkrétního TSU generujícího kvalifikovaná elektronická časová razítka

4.1 Služby autority časových razítek (TSA)

PostSignum TSA poskytuje služby v rozsahu popsaném v níže uvedených politikách TSA, podle nichž jsou vydávána časová razítka pro koncové zákazníky:

• Politika vydávaní kvalifikovaných časových razítek PostSignum TSA, verze 1.1 vydaná dne 16. 6. 2009 [CPTSA] a novější a navazující
• Politika vydávaní časových razítek PostSignum TSA, verze 1.0 vydaná dne 1 .7. 2016 [CPTSA] a novější.

Služby PostSignum TSA jsou poskytovány za podmínek uvedených v [eIDAS] a v uzavřené smlouvě se zákazníkem.

4.2 Autorita časových razítek

PostSignum TSA je tvořena jednou autoritou časového razítka. Tato autorita je prostřednictvím vydaných certifikátů jednotek TSU napojena na hierarchii PostSignum QCA. PostSignum TSA vydává časová razítka, tedy datové zprávy, které důvěryhodným způsobem spojují data v elektronické podobě s časovým okamžikem, a zaručují, že uvedená data (jejich otisk) v elektronické podobě existovala před daným časovým okamžikem.

Z důvodu zajištění vyššího výkonu a vyšší dostupnosti služby zajišťuje vydávání časových razítek více jednotek TSU. Každá jednotka má vlastní klíč a kvalifikovaný certifikát pro elektronickou pečeť. Certifikáty PostSignum TSA (tedy jednotlivých TSU) jsou vydány certifikační autoritou PostSignum Qualified CA. Jednotlivé TSU jsou navzájem zaměnitelné a poskytují stejný typ služeb. Při žádosti o časové razítko není možné určit, která jednotka TSU časové razítko vydá.

Služby vydávání časových razítek jsou zajišťovány poskytovatelem certifikačních služeb (dále též poskytovatel služby TSA).

PostSignum TSA zajišťuje zejména tyto služby (v souladu s dokumentovanými provozními postupy):
• generování vlastních párů klíčů,
• podání žádosti o certifikát TSA u PostSignum Qualified CA,
• zveřejnění všech politik TSA, podle kterých vydává časová razítka, na webových stránkách poskytovatele a na obchodních místech,
• zveřejnění kvalifikovaných certifikátů svých TSU na webových stránkách poskytovatele a na obchodních místech,
• administrativa spojená s uzavíráním smlouvy a registrací žadatelů o časové razítko,
• vydávání časových razítek.

4.2.1 Jednotky TSU1, TSU2, TSU5, TSU6

Tyto jednotky jsou umístěné v Trust centru České pošty a za normálního provozu poskytují časová razítka všechny jednotky. Přičemž jednotky TSU5 a TSU6 nejsou pro běžné zákazníky dostupné.

4.2.2 Jednotky TSU3, TSU4

Tyto jednotky jsou umístěné v záložní lokalitě a stejně jako jednotky TSU v Trust centru poskytují za normálního provozu časová razítka.

4.3 Zákazníci, pověřené osoby, žadatelé a spoléhající se strany

4.3.1 Zákazníci a pověřené osoby

4.3.1.1 Zákazníci

Zákazníkem PostSignum TSA je fyzická osoba, podnikající fyzická osoba, právnická osoba, státní orgán nebo orgán místní samosprávy. Zákazník uzavírá písemnou smlouvu o poskytování certifikačních služeb s Českou poštou.

4.3.1.2 Pověřené osoby

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.

Česká pošta získá při uzavírání smlouvy podpisový vzor pověřené osoby.

4.3.2 Žadatelé o časové razítko

Žadatelem o vydání časového razítka muže 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 strana je libovolný subjekt spoléhající se při své činnosti na časová razítka vydaná PostSignum TSA. Spoléhající se strany nevstupují do smluvního vztahu s poskytovatelem služby TSA.

4.3.4 Jiné participující subjekty

4.3.4.1 Externí participující subjekty

Na provozu TSA se dále podílí zejména následující subjekty:

ICZ, a.s.
IČ 25145444
Hvězdova 1689/2a
140 00 Praha 4
tel.: 244 100 111
fax: 244 100 222
Uvedený subjekt je hlavním dodavatelem řešení autority PostSignum TSA.

DELL Computer, s.r.o.
IČ 45272808
V Parku 2325/16
148 00 Praha 11 – Chodov
Uvedený subjekt je hlavním dodavatelem obecného hardware autority PostSignum TSA.

4.3.4.2 Interní participující subjekty

Komise pro certifikační politiky ČP (PAA ČP)

Orgán, který ustavuje, sleduje a udržuje politiky, jimiž se řídí činnost certifikačních autorit a autority časového razítka v hierarchii PostSignum. Jedná se jak o politiky pro kořenovou certifikační autoritu (PostSignum Root QCA), tak o politiky pro podřízené certifikační autority (PostSignum Qualified CA) a politiku pro autoritu časových razítek (PostSignum TSA).

- ustavuje Tým pro tvorbu certifikačních politik ČP, řídí a kontroluje jeho činnost,
- schvaluje nové certifikační politiky a politiky TSA a v případě politik Root QCA rozhoduje o jejich zveřejnění,
- udržuje a kontroluje existující politiky,
- zodpovídá za konzistenci a integritu politik,
- schvaluje veškeré změny certifikační prováděcí směrnice a/nebo prováděcí směrnice TSA a
- zodpovídá za konzistenci a integritu certifikační prováděcí směrnice a/nebo prováděcí směrnice TSA.

Komisi pro certifikační politiky ČP je možné kontaktovat na adrese
paa.postsignum@cpost.cz

Tým pro tvorbu certifikačních politik ČP (PCA ČP)

Je zodpovědný za tvorbu politik, které předkládá ke schválení Komisi pro politiky ČP. PCA ČP je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován.

5 PROVÁDĚCÍ SMĚRNICE POSTSIGNUM TSA

5.1 Základní popis

Tato prováděcí směrnice TSA rozpracovává pravidla a postupy uvedené v politikách TSA.

5.2 Identifikace

Tabulka 1: Identifikace prováděcí směrnice PostSignum TSA

Název dokumentu	Prováděcí směrnice PostSignum TSA
Verze dokumentu	3.0.1
Stav	finální
OID PostSignum TSA	2.23.134.1.5
OID tohoto CPS	není přidělováno
Datum vydání	8. 9. 2017
Datum účinnosti	2. 10. 2017
Datum revize	15. 8. 2022
Doba platnosti	Do odvolání nebo do dne ukončení služeb autority PostSignum TSA

5.3 Určení směrnice a její použitelnost

Tato směrnice rozpracovává ustanovení a postupy uvedené v politikách TSA do formy podrobnějších postupů nebo odkazuje na dokumenty obsahující tyto podrobnější postupy.

5.3.1 Přípustné použití časového razítka

Podrobnější popis použití časového razítka je uveden v [CPTSA].

5.3.2 Omezení použití časového razítka

Omezení použití časového razítka je uvedeno v [CPTSA].

5.4 Hodnocení shody a jiná hodnocení

Hodnocení shody a jiná hodnocení je uvedeno v [CPTSA].

Podrobný popis hodnocení shody je uveden v dokumentu Auditní a archivační politika, který je přílohou [SBPTSA].

5.4.1 Periodicita a hodnocení nebo okolnosti pro provedení hodnocení

Viz ustanovení v [CPTSA].

5.4.1.1 Interní kontrola

Nejméně jednou za dvanáct měsíců je pracovníky odboru interního auditu České pošty:

- ověřeno dodržování obecně závazných právních předpisů, vnitřních předpisů, přijatých opatření a stanovených postupů,
- ověřena přiměřenost, funkčnost, účinnost a efektivnost řízení rizik, vnitřních řídicích a kontrolních systémů a mechanismů.

O provedení každé interní kontroly musí být vypracována podepsaná písemná zpráva. Zpráva je archivována stejným způsobem jako ostatní záznamy o provozu PostSignum TSA a je uchovávána nejméně po dobu deseti let.

5.4.1.2 Externí kontrola

Bezpečnost a integrita systémů a procesů PostSignum TSA je ověřena externí kontrolou provedenou auditorem nezávislým na České poště..

O provedení každé kontroly musí být vypracována podepsaná písemná zpráva. Zpráva je archivována stejným způsobem jako ostatní záznamy o provozu PostSignum TSA a uchovávána nejméně po dobu deseti let.

5.4.2 Identita a kvalifikace hodnotitele

Viz ustanovení v [CPTSA].

5.4.3 Vztah mezi hodnotitelem a hodnocenou entitou

Viz ustanovení v [CPTSA].

5.4.4 Hodnocené oblasti

V rámci pravidelné interní kontroly je hodnoceno dodržování obecně závazných právních předpisů, vnitřních předpisů, přijatých opatření a stanovených postupů a přiměřenost, funkčnost, účinnost a efektivnost řízení rizik, vnitřních řídicích a kontrolních systémů a mechanismů.

V rámci externí kontroly se hodnotí zejména skutečnost, zda:

- poskytovatel provozuje důvěryhodné systémy v souladu s platnými právními předpisy a příslušnými standardy,
- poskytovatel provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací poskytovatele, a to s jejími částmi upravujícími řízení změn.

Předmětem kontroly bezpečnostní shody jsou:

- všechny součásti systémů TSA, nebo

- všechny změny, které byly provedeny na TSA od provedení předchozí kontroly bezpečnostní shody a jejich vliv na systémy TSA, nebo

- v případě, že k žádným změnám nedošlo, ověření této skutečnosti.

5.4.5 Postupy v případě zjištěných nedostatků

V případě zjištění nedostatků, které závažně ovlivňují schopnost PostSignum TSA dostát svým závazkům a požadavkům uvedeným v platných právních předpisech, přeruší PostSignum TSA vydávání časových razítek do doby, než budou nedostatky odstraněny.

5.4.6 Sdělování výsledků hodnocení

O provedení každé kontroly je vypracována podepsaná písemná zpráva, která je předána Manažerovi CA. Manažer CA zajistí její distribuci a projednání. Pokud je to nutné, zajistí Manažer CA její předání orgánu dohledu do termínu stanoveného platným právním předpisem.

V případě, kdy je součástí zprávy samostatný výrok auditora, může Manažer CA rozhodnout o jeho zveřejnění.

Zpráva o výsledku kontroly je archivována stejným způsobem jako ostatní záznamy o provozu PostSignum TSA a je uchovávána nejméně po dobu deseti let.

6 ZÁVAZKY A ODPOVĚDNOSTI

6.1 Závazky TSA

6.1.1 Obecné závazky TSA

Provozovatel PostSignum TSA se zavazuje, že při poskytování služby vydávání časových razítek:
- postupuje v souladu s platnou legislativou,
- zajišťuje naplnění všech požadavků kladených na TSA uvedených v kapitole 7 tohoto dokumentu,
- zajišťuje dodržení postupů uvedených v [CPTSA],
- postupuje podle ustanovení tohoto dokumentu a další interní dokumentace.

6.1.2 Závazky TSA ve vztahu k zákazníkům a žadatelům o časové razítko a držitelům časového razítka
Tyto závazky jsou uvedené v [CPTSA], která je dostupná zákazníkům i žadatelům.

6.2 Závazky zákazníků a žadatelů o časové razítko a držitelů časového razítka
Tyto závazky jsou uvedené v [CPTSA], která je dostupná zákazníkům i žadatelům.

6.3 Závazky spoléhajících se stran
Tyto závazky jsou uvedené v [CPTSA], která je dostupná spoléhajícím se stranám.

6.4 Odpovědnosti
Tyto závazky jsou uvedené v [CPTSA], která je dostupná zákazníkům, žadatelům i spoléhajícím se stranám.

7 POŽADAVKY NA POSTUPY A PROCEDURY TSA

7.1 Správa prováděcí směrnice

Za iniciování změn v této prováděcí směrnici nebo inicializaci vytvoření nové prováděcí směrnice je odpovědný Manažer CA. Ten předá požadavek týmu pro tvorbu certifikačních politik (PCA ČP).

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

Nová verze prováděcí směrnice bude zveřejněna formou interní směrnice České pošty. PAA ČP rozhodne, zda je nutné zveřejnit informaci o nové verzi prováděcí směrnice též jinou formou, případně jak.

7.1.1 Organizace spravující prováděcí směrnici TSA
Za správu této prováděcí směrnice je odpovědný poskytovatel certifikačních služeb, tedy Česká pošta zastoupená pro tento účel Manažerem CA.

7.1.2 Kontaktní osoba organizace spravující prováděcí směrnici TSA
Kontaktní osobou ve věci správy této prováděcí směrnice 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 prováděcí směrnice TSA

Tento dokument je vytvářen týmem pro tvorbu certifikačních politik ČP (PCA ČP), který je rovněž zodpovědný za tvorbu politik TSA. 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 TSA nebo prováděcí směrnice TSA vznikají podle potřeby, zejména však:
- při změně vlastností, procesů nebo záruk spojených s vydaným časovým razítkem,
- 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 politice pro vydávání časových razítek nebo v CPS nebo za inicializaci vytvoření nové politiky nebo CPS je odpovědný Manažer CA. Při přípravě změn v politice nebo v CPS rozhodne Manažer CA na základě seznamu identifikovaných změn, jakým způsobem budou plánované změny zveřejněny. Komise pro certifikační politiky podle potřeby ustanoví PCA ČP, kterému Manažer CA následně předá seznam požadovaných změn k zapracování. Vypracované politiky nebo CPS předloží Manažer CA ke schválení Komisi pro certifikační politiky, která potom přidělí číslo verze dokumentu.

7.2 Požadavky na životní cyklus párových dat TSA

7.2.1 Generování a instalace párových dat

Klíčové páry TSU jsou generovány v odpovídajícím hardwarovém kryptografickém modulu (HSM). Klíčové páry obsluhy jsou generovány v čipových kartách.

7.2.1.1 Generování párových dat

Klíčové páry jednotlivých TSU jsou generovány a uloženy v hardwarovém kryptografickém modulu . Generování těchto klíčových párů probíhá v souladu s interní dokumentací podléhající interní i externí kontrole v kontrolovaném prostředí České pošty. Parametry používané při vytváření veřejných klíčů TSU jsou generovány odpovídajícím softwarovým a hardwarovým vybavením (nCipher TimeStamp Server obsahující

PCI kartu nCipher nShield F3). Použité algoritmy a jejich parametry odpovídají požadavkům stanovených v příslušných technických normách..

Kvalita parametrů klíčů jednotlivých komponent nebo systémů generovaných v rámci PostSignum TSA je automaticky testována použitým programovým vybavením.

Klíčové páry jednotlivých komponent nebo systémů PostSignum TSA (klíčové páry pro ustanovení SSL spojení) jsou generovány v kontrolovaném prostředí systémů PostSignum TSA. Tyto klíčové páry jsou uloženy ve specializovaných softwarových úložištích; přístup k těmto úložištím je omezen pouze na oprávněné osoby.

Klíčové páry operátorů PostSignum QCA (včetně operátorů RA; kontrolní klíče) jsou generovány ve vyhrazených hardwarových prostředcích, které svou konstrukcí neumožňují export soukromých klíčů. Pro použití soukromých klíčů je vždy nutné zadat PIN.

7.2.1.2 Vlastnosti kryptografického modulu

Viz ustanovení v [CPTSA].

7.2.1.3 Poskytování veřejných klíčů

Viz ustanovení v [CPTSA].

7.2.1.4 Délky párových dat

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

Mohutnost klíčů (modulů) jednotlivých komponent nebo systémů PostSignum TSA (např. klíče pro navázání SSL spojení) pro algoritmus RSA je minimálně 2048 bitů.

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

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.

Soukromé klíče TSA jsou během provozu uloženy v aktivovaném a konfigurovaném kryptografickém modulu (bezpečném kryptografickém modulu), k jehož zapnutí a vypnutí postačuje jedna osoba.

K aktivování kryptografického modulu (bezpečného kryptografického modulu) a k obnově soukromého klíče po havárii (případně v jiném kryptografickém modulu) je zapotřebí součinnosti několika, minimálně však tří osob.

Při používání a správě kryptografického modulu je postupováno v souladu se zásadami dokumentů [SBPTSA] a interní dokumentací.

7.2.2.2 Zálohování soukromých klíčů (dat pro vytváření elektronických značek)

Soukromé klíče TSA jsou zálohovány v zašifrované podobě, k šifrování je použit symetrický algoritmus AES. Zašifrované klíče jsou uložené na pevném disku zařízení obsahujícího příslušný kryptografický modul. Zálohovat tyto klíče může jedna osoba; obnovit do aktivovaného modulu, ze kterého zálohy pocházejí, také jedna osoba.

Při obnově zálohovaných klíčů do nového nebo inicializovaného modulu je však zapotřebí součinnosti minimálně tří osob.

Podrobný popis zálohování a obnovy klíčů v HSM je popsán v interní dokumentaci.

7.2.2.3 Uchovávání soukromých klíčů (dat pro vytváření elektronických značek)

Soukromé klíče TSA nejsou archivovány. Po ukončení používání daného soukromého klíče TSA je uvedený soukromý klíč protokolárně zničen.

7.2.2.4 Transfer soukromých klíčů (dat pro vytváření elektronických značek) 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. Klíč opouští kryptografický modul pouze v zašifrované podobě na zálohách vytvářených a chráněných v souladu s ustanoveními dokumentů [SBPTSA], interní dokumentací a Auditní a archivační politika (součást [SBPTSA]).

Klíč je do aktivovaného kryptografického modulu vkládán se záloh po autentizaci jednoho pracovníka s přístupem k zálohám klíčů a ke kryptografickému modulu.

Klíč je do nového nebo inicializovaného kryptografického modulu vkládán ze záloh za součinnosti minimálně tří osob.

Podrobný popis zálohování a obnovy klíčů v HSM je popsán v interní dokumentaci.

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

Soukromý klíč TSA je během provozu uložen v nezašifrovaném tvaru v aktivovaném a konfigurovaném kryptografickém modulu (bezpečném kryptografickém modulu), k jehož zapnutí a vypnutí postačuje jedna osoba.

K aktivování kryptografického modulu (bezpečného kryptografického modulu) a k obnově soukromého klíče po havárii (případně v jiném kryptografickém modulu) je zapotřebí součinnosti několika, minimálně však tří osob.

Podrobný popis aktivace HSM a spuštění procesu TSU je popsán v interní dokumentaci.

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], interní dokumentaci a další provozní dokumentaci.

Aktivační data jsou většinou vytvářena nebo zadávána pracovníkem, který je bude dále používat.

Všechna vytvářená aktivační data musí splňovat požadavky kladené na jejich délku a složení. Tyto požadavky jsou specifikovány v [SBPTSA].

7.2.2.7 Postup při aktivaci soukromých klíčů

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

Podrobný popis aktivace HSM a spuštění procesu TSU je popsán v interní dokumentaci.

7.2.2.8 Postup při deaktivaci soukromých klíčů

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

Podrobný popis deaktivace HSM a ukončení procesu TSU je popsán v interní dokumentaci.

7.2.2.9 Postup při zničení dat pro vytváření elektronických značek

Viz ustanovení v [CPTSA].

7.2.3 Distribuce veřejných klíčů TSA

Viz ustanovení v [CPTSA].

7.2.4 Výměna párových dat

Viz ustanovení v [CPTSA].

7.2.5 Ukončení životního cyklu párových dat

Viz ustanovení v [CPTSA].

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] a interní dokumentací.

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.

Podrobný popis sledování stavu útoků na HSM je popsán v interní dokumentaci.

7.2.6.2 Vyřazení kryptografického modulu z provozu

Pokud je kryptografický modul užívaný k úschově soukromých klíčů TSA vyřazen z provozu, musí být z tohoto modulu odstraněna párová data pro označování časových razítek (soukromých a veřejných klíčů). Podrobný postup odstranění párových dat je uveden v interní dokumentaci.

7.3 Vydávání časových razítek

Žádost o vydání časového razítka podle politiky TSA 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

Identifikace a autentizace právnické osoby nebo podnikající fyzické osoby

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

Identifikace a autentizace fyzické osoby

Česká pošta uzavírá se zákazníkem smlouvu o poskytování certifikačních služeb za podmínek definovaných obchodním zákoníkem. Zákazník – fyzická osoba prokazuje svou totožnost jedním osobním dokladem. Kontaktní/obchodní místo zkontroluje:

- zda je doklad platný,
- zda fotografie na dokladech odpovídá fyzické osobě.

7.3.1.2 Uzavření smlouvy s právnickou nebo podnikající fyzickou osobou

Zákazník (právnická osoba nebo podnikající 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.

Podrobný popis uzavření smlouvy a zavedení zákazníka je popsán v interní dokumentaci, provozních příručkách a příručce pro zákazníky.

7.3.1.3 Uzavření smlouvy s nepodnikající fyzickou osobou

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

Podrobný popis uzavření smlouvy a zavedení zákazníka je popsán v interní dokumentaci, provozních příručkách a příručce pro zákazníky.

7.3.1.4 Registrace žadatelů

Viz ustanovení v [CPTSA].

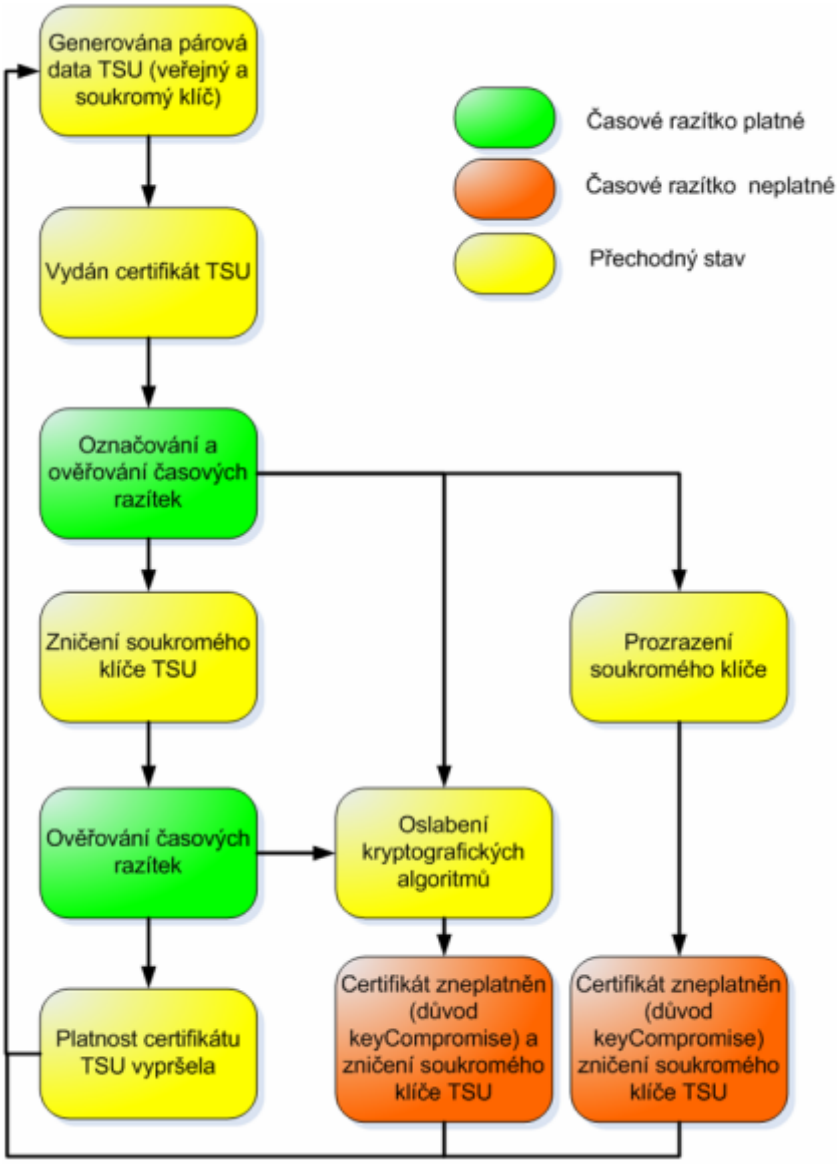
7.3.1.5 Ukončení poskytování služeb pro žadatele o časové razítko

Viz ustanovení v [CPTSA].

7.3.2 Zpracování žádosti o časové razítko

Životní cyklus časových razítek vydávaných PostSignum TSA je úzce propojen s životním cyklem párových dat TSA resp. jednotlivých TSU. Životní cyklus těchto párových dat a časového razítka je následující:

Obrázek 1: Životní cyklus párových dat TSU



Obrázek reprezentuje na nejvyšší úrovni správu párových dat PostSignum TSA. Párová data mohou být v některém z primárních, přechodných nebo sekundárních stavů.

Rozeznáváme tyto primární stavy párových dat:

- označování a ověřování časových razítek (používání soukromého i veřejného klíče) a
- ověřování časových razítek (používání veřejného klíče).

Z těchto primárních stavů se mohou párová data dostat dvou sekundárních stavů:

- zneplatnění certifikátu v důsledku oslabení kryptografických algoritmů a
- zneplatnění certifikátu v důsledku kompromitace soukromého klíče.

Kromě toho existuje řada přechodných stavů, kterými párová data procházejí.

Ve vazbě na životní cyklus párových dat časové razítko prochází následujícími primárními stavy:

- časové razítko vydáváno a

- časové razítko používáno.

Dále se může časové razítko nacházet v jednom sekundárním stavu:

- časové razítko neplatné.

Obrázek 2: Životní cyklus časového razítka

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 PostSignum VCA na webové adrese
  https://tsa.postsignum.cz/TSS/HttpTspServer/ (TSU1 a TSU2)

  https://tsa2.postsignum.cz/TSS/HttpTspServer/ (TSU5 a TSU6)

  https://tsa.postsignum.eu/TSS/HttpTspServer/ (TSU5 a TSU6)

- nebo jménem a heslem na webové adrese
  https://tsa.postsignum.cz:444/TSS/HttpTspServer/ (TSU1 a TSU2)

  https://tsa2.postsignum.cz:444/TSS/HttpTspServer/ (TSU5 a TSU6)

  https://tsa.postsignum.eu:444/TSS/HttpTspServer/ (TSU5 a TSU6)

7.3.2.2 Přijetí nebo zamítnutí žádosti o časové razítko

Viz ustanovení v [CPTSA].

7.3.2.3 Doba zpracování žádosti o časové razítko

Viz ustanovení v [CPTSA].

7.3.3 Vydání časového razítka

7.3.3.1 Úkony TSA v průběhu vydávání časového razítka

Viz ustanovení v [CPTSA].

7.3.3.2 Oznámení o vydání časového razítka držiteli vydávání časového razítka

Vydávaná časová razítka nejsou zveřejňovaná. Platí, že poskytovatel služby vydávání časových razítek neumožňuje veřejný přístup k vydaným časovým razítkům,

Kromě úkonu vlastního vydání časového razítka PostSignum TSA neoznamuje vydání časového razítka žádnému subjektu.

7.3.3.3 Převzetí časového razítka

Viz ustanovení v [CPTSA].

7.3.4 Ověření časového razítka

Seznam zneplatněných certifikátů a informace o stavu certifikátů TSA jsou považovány za veřejně přístupné informace. Seznam zneplatněných certifikátů (CRL) je zveřejňován na těchto místech:

- na webových stránkách poskytovatele,
- u nezávislého poskytovatele webových služeb,
- na distribučních místech CRL (CDP), která jsou uvedena v certifikátu TSA.

Primárním zdrojem aktuálního CRL jsou distribuční místa CRL (CDP).

7.3.4.1 Platnost kvalifikovaného časového razítka

Viz ustanovení v [CPTSA].

7.3.5 Struktura žádosti, odpovědi a časového razítka
Časová razítka vydává konkrétní TSU na základě žádosti o kvalifikované 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

Viz ustanovení v [CPTSA].

7.3.5.2 Struktura odpovědi na žádost o časové razítko

Viz ustanovení v [CPTSA].

7.3.5.3 Struktura časového razítka

Viz ustanovení v [CPTSA].

7.3.6 Synchronizace měřidla času s UTC

7.3.6.1 Synchronizace

V případě, že odchylka přesáhne 250 ms, vytvoří kontrolní NTP server varovný e-mail pro obsluhu TSA.

7.3.6.2 Přesnost času v časovém razítku

Viz ustanovení v [CPTSA].

7.3.6.3 Bezpečnost měřidla času

Viz ustanovení v [CPTSA].

7.3.6.4 Detekce odchýlení měřidla času

V případě, kdy odchylka přesáhne 250 ms, kontrolní server vytvoří varovný e-mail pro obsluhu TSA.
V případě detekce odchýlení měřidla času o více než 1 sekundu, ukončí TSA vydávání časových razítek do doby, než bude sjednána náprava.

Problematika detekce odchýlení měřidla času je podrobněji řešena v interní dokumentaci.

7.3.6.5 Přestupná sekunda

Viz ustanovení v [CPTSA].

7.4 Správa a provozní bezpečnost TSA

Pro PostSignum TSA byly zpracovány dokumenty:

- [SBPTSA], popisující zásady bezpečnosti v oblasti fyzické, procedurální a personální;
- Plán pro zvládání krizových situací a plán obnovy, popisující postupy pro zachování garantované úrovně služeb v případě výskytu mimořádné situace;
- [OZUTSA], která mj. upravuje zejména oblast obsazování rolí PostSignum TSA a
- další interní dokumentace, popisující na logické úrovni postupy dodržované v PostSignum TSA.

Zmíněné dokumenty byly vypracovány na základě výsledků provedené analýzy rizik.

Tyto dokumenty jsou mj. přístupné osobám, které provádějí kontrolu bezpečnostní shody PostSignum TSA. Tato kapitola vychází z výše uvedených dokumentů a poskytuje stručný přehled základních bezpečnostních zásad uplatňovaných v PostSignum TSA.

7.4.1 Řízení bezpečnosti

V roce 2007 bylo vedením ČP rozhodnuto o zavedení systému managementu jakosti (QMS) a systému řízení informační bezpečnosti (ISMS) podle systémové normy [ISO 9001], resp. [27001] pro odbor České pošty, který provozuje služby certifikační autority. v rozsahu:

- úloha Veřejná certifikační autorita (VCA)
- úloha Kvalifikovaná certifikační autorita (QCA)
- úloha Autorita časových razítek (TSA)

7.4.2 Hodnocení a řízení rizik

Viz ustanovení v [CPTSA].

7.4.3 Personální bezpečnost

Podrobný popis požadavků a opatření z oblasti personální bezpečnosti a přidělování rolí je uveden v [OZUTSA], [SBPTSA] a interní dokumentaci.

7.4.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Viz ustanovení v [CPTSA].

7.4.3.2 Posouzení spolehlivosti osob

Viz ustanovení v [CPTSA].

7.4.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Viz ustanovení v [CPTSA].

7.4.3.4 Požadavky na školení a periodicita školení

Viz ustanovení v [CPTSA].

7.4.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Viz ustanovení v [CPTSA].

7.4.3.6 Postihy za neoprávněné činnosti zaměstnanců

Viz ustanovení v [CPTSA].

7.4.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Na smluvní (externí) pracovníky jsou uplatňována obdobná kritéria jako na zaměstnance České pošty, s.p. Tyto požadavky jsou uvedeny ve smlouvě mezi Českou poštou a dodavatelem.

7.4.3.8 Dokumentace poskytovaná zaměstnancům

Personál PostSignum TSA má k dispozici dokumentaci odpovídající jím obsazené roli, zejména [CPTSA], [SBPTSA], tuto prováděcí směrnici a provozní dokumentaci (příručky a pracovní postupy pro obsluhu).

7.4.4 Fyzická bezpečnost a bezpečnost prostředí

Viz ustanovení v [CPTSA].

7.4.5 Řízení provozu

Viz ustanovení v [CPTSA].

7.4.6 Správa řízení přístupu

Viz ustanovení v [CPTSA].

Podrobný popis požadavků a opatření z oblasti personální bezpečnosti je uveden v [SBPTSA].

7.4.7 Vývoj a údržba důvěryhodných systémů

Viz ustanovení v [CPTSA].

7.4.8 Obnova po havárii nebo kompromitaci

Viz ustanovení v [CPTSA].

7.4.9 Ukončení činnosti TSA

Viz ustanovení v [CPTSA].

7.4.10 Shoda s právními předpisy

Viz ustanovení v [CPTSA].

7.4.11 Záznam informací o provozu TSA

Viz ustanovení v [CPTSA].

7.4.12 Uchovávání informací a dokumentace

Podrobný popis vzniku, uchovávání a ochraně auditních záznamů je uveden v dokumentu Auditní a archivační politika TSA (příloha [SBPTSA]). Další body této kapitoly obsahují výtah uvedených ustanovení dokumentu Auditní a archivační politika.

7.4.12.1 Typy informací a dokumentace, které se uchovávají

Viz ustanovení v [CPTSA].

7.4.12.2 Doba uchování uchovávaných informací a dokumentace

Programové vybavení, data a auditní záznamy se archivují po dobu deseti let.
Po této době jsou média nebo dokumenty skartovány v souladu s [SBPTSA].

7.4.12.3 Ochrana úložiště uchovávaných informací a dokumentace

Viz ustanovení v [CPTSA].

7.4.12.4 Postupy při zálohování a archivaci uchovávaných informací a dokumentace

Auditní záznamy v podobě datových souborů jsou archivovány na nepřepisovatelných médiích. Záznamy, u kterých je integrita zajištěna i při přenosu na nepřepisovatelné médium (např. podpisem záznamů apod.), mohou být na médium přesouvány podle provozních potřeb. Záznamy generované v Trust centru a záložní lokalitě, u kterých není při přenosu na médium zajištěna integrita, se na média musí přesouvat za přítomnosti Auditora CA.

Podrobný popis postupů pro archivaci auditních záznamů je uveden v dokumentu Auditní a archivační politika, který je přílohou [SBPTSA].

7.4.12.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Viz ustanovení v [CPTSA].

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

Viz ustanovení v [CPTSA].

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.

V každé lokalitě, kde je umístěn trezor, musí být veden protokol o uložených archivních médiích, do kterého jsou zaznamenávány veškeré manipulace s uloženými médii.

Přístup k archivům je omezen na osoby v odpovídajících rolích. Ostatním osobám povoluje přístup do trezoru Bezpečnostní administrátor CA. O každém takto povoleném přístupu do trezoru je pořizován písemný záznam.

V pravidelných intervalech je kontrolována čitelnost médií uložených v archivech. V případě nečitelnosti média je z druhé kopie vytvořena další archivní kopie jako náhrada za nečitelnost (pokud tato druhá kopie existuje) a nečitelná kopie je skartována.

Podrobný popis této problematiky je uveden v dokumentu Auditní a archivační politika, který je přílohou [SBPTSA].

7.4.13 Zveřejňování informací a dokumentace

Viz ustanovení v [CPTSA].

7.5 Ostatní obchodní a právní záležitosti

7.5.1 Poplatky

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.2 Finanční odpovědnost

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.3 Důvěrnost obchodních informací

Viz ustanovení v [CPTSA].

7.5.4 Ochrana osobních údajů

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování služby TSA. Zásady ochrany osobních údajů jsou obsaženy v této prováděcí směrnici TSA, v politikách TSA, ve [VOP] a vycházejí z příslušných ustanovení [Z110].

Česká pošta poskytuje informace v rozsahu upraveném politikou TSA zákazníkům nebo spoléhajícím se osobám, jakož i auditorům pro účely vyjádření shody, a dále poskytuje informace v nezbytném rozsahu na

základě mandatorních ustanovení platných právních předpisů (např. orgánům činným v trestním řízení v případech požadovaných v trestněprávních předpisech).

Česká pošta provedla analýzu bezpečnostních rizik a na jejím základě stanovila opatření na ochranu zpracovávaných osobních údajů. Podrobná specifikace přijatých bezpečnostních opatření je obsažena v interních dokumentech ČP. Tyto dokumenty jsou pravidelně předmětem kontroly bezpečnostní shody. V příslušné politice TSA a částečně i v tomto dokumentu jsou popsána základní bezpečnostní opatření. ČP průběžně sleduje bezpečnostní prostředí v obdobných společnostech v Evropě s cílem reagovat na potenciální nová bezpečnostní rizika.

Podrobnější informace Viz ustanovení v [CPTSA].

7.5.5 Práva duševního vlastnictví

Viz ustanovení v [CPTSA].

7.5.6 Zastupování a záruky

Viz ustanovení v [CPTSA].

7.5.7 Zřeknutí se záruk

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.8 Omezení odpovědnosti

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.9 Odpovědnost za škodu, náhrada škody

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.10 Doba platnosti, ukončení platnosti

7.5.10.1 Doba platnosti

Doba platnosti této prováděcí směrnice je od data vydání uvedeného v kapitole 5.2.

Konec platnosti tohoto dokumentu je určen dnem ukončení platnosti.

7.5.10.2 Ukončení platnosti

Platnost dokumentu je ukončena v případě:

- jeho nahrazení novější verzí, nebo
- ukončením poskytování služeb vydávání časových razítek Českou poštou, jakožto poskytovatelem certifikačních služeb v oblasti vydávání časových razítek.

7.5.10.3 Důsledky ukončení a přetrvání závazků

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.11 Komunikace mezi zúčastněnými subjekty

Viz ustanovení v [CPTSA].

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 prováděcí směrnice TSA 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 prováděcí směrnice.

V případě, že nebude hrozit nebezpečí z prodlení, bude toto oznámení provedeno min. 1 měsíc před začátkem platnosti nové verze prováděcí směrnice TSA.

7.5.12.3 Okolnosti, při kterých musí být změněn OID

Česká pošta, s. p. přiřadila dle svých interních pravidel identifikátory objektů (OID) užívané v prostředí PostSignum TSA.

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 certifikační politice nebo politice TSA, podle které jsou vydávány certifikáty nebo časová razítka v rámci PostSignum.

OID nejsou přiřazeny této prováděcí směrnici TSA ani interním dokumentům.

Všechny OID jsou zaznamenány:
- v příslušné certifikační politice nebo politice TSA,
- OID přiřazené PostSignum Root QCA a PostSignum Qualified CA je uvedeno v každé certifikační politice vydané v rámci PostSignum QCA,
- OID certifikační politiky PostSignum QCA je uvedeno v odpovídající certifikační politice a vydaném certifikátu,
- OID politiky pro vydávání časových razítek PostSignum TSA je uvedeno v odpovídající politice a vydaném časovém razítku.

Jakákoliv změna v politice TSA 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

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.15 Shoda s právními předpisy

Viz ustanovení v [CPTSA].

7.5.16 Další ustanovení

7.5.16.1 Rámcová dohoda

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.16.2 Postoupení práv

Viz ustanovení v [CPTSA].

7.5.16.3 Oddělitelnost ustanovení

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.16.4 Zřeknutí se práv

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

7.5.16.5 Vyšší moc

Tato oblast, která se přímo netýká zajištění provozu TSA, je popsána v [CPTSA].

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 prováděcí směrnice 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
[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)
[Z110]	Zákon č. 110/2019 Sb. o zpracování osobních údajů v aktuálním znění
[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
[CPTSA]	Politika vydávání časových razítek PostSignum TSA, aktuální verze

7.5.17.2 Návazné dokumenty

V této politice je odkazováno na následující interní dokumenty:

[OZUTSA]	Předpis ČP „Organizační zajištění úlohy Autorita časových razítek České pošty, s. p.“, aktuální verze
[SBPTSA]	Předpis ČP „Systémová bezpečnostní politika pro úlohu Autorita časových razítek České pošty, s. p.“ aktuální verze