Autorita pro vydávání kvalifikovaných elektronických časových razítek – Politika a prováděcí směrnice

Verze 1.0

Komerční banka, a.s., Na Příkopě 33, 114 07 Praha 1

Obsah

Historie revizí a změn dokumentu

Verze	Datum změny	Důvod změny	Schválil
1.0	1.6.2023	První verze	Tomáš Prjacha, Manažer PKI  Digitálně podepsal(a) Tomáš Prjacha dne 01.06.2023 16:28:48

1 POJMY A ZKRATKY

Pojem	Definice
CA	Certifikační autorita – entita vystavující certifikáty na základě schválených žádostí a generující seznamy CRL.
Certifikát (v oblasti PKI)	Datová zpráva, která je vydána CA, a která spojuje veřejný klíč (data pro ověřování elektronických podpisů) s podepisující osobou a umožňuje ověřit její identitu.
CP	Certifikační politika.
CPS	Certifikační prováděcí směrnice.
CRL	Seznam zneplatněných certifikátů ve formátu, který je v souladu s RFC 5280.
Elektronické časové razítko	Data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku.
Důvěryhodné úložiště	Systém pro důvěryhodné a bezpečné ukládání a správu dat dle platné legislativy.
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
Expirovaný certifikát	Certifikát po skončení doby platnosti uvedené v tomto certifikátu.
GDPR	Nařízení Evropského Parlamentu a Rady (EU) 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.
Hash	Výstup hashovací funkce (také „otisk“).
Hashovací algoritmus	Jednosměrná funkce, která přiřazuje vstupu libovolné délky výstup konstantní délky.
HSM	Hardware Secure Module – kryptografický prostředek pro ochranu a bezpečné použití kryptografických klíčů.
Manažer bezpečnosti	Osoba zodpovědná za provoz, bezpečnost a ostatní aspekty PKI v Komerční bance, a.s.
OID	Identifikátor objektu.
Párová data	Viz „Párové klíče“.
Párové klíče	Vzájemně svázaná dvojice klíčů pro vytváření digitálních podpisů (soukromý klíč) a pro ověřování digitálních podpisů (veřejný klíč). Veřejné klíče jsou publikovány v certifikátech spolu s dalšími údaji zejména o identitě podepisujícího subjektu.
PDS	PKI Disclosure Statement – Zpráva pro uživatele (dokument obsahující základní přehled o poskytovaných certifikačních službách, právech a povinnostech jednotlivých stran).
Poskytovatel časových razítek	Společnost Komerční banka, a.s., jako společnost, která poskytuje služby vydávání kvalifikovaných časových razítek.
Pozastavený certifikát	Dočasně zneplatněný certifikát z důvodu „Pozastavení certifikátu“ (Certificate Hold).
QSealCD	Kvalifikovaný prostředek pro vytváření elektronické pečeti dle nařízení eIDAS.

RFC	Request for Comments - Označení řady standardů a dalších dokumentů popisujících internetové protokoly, systémy apod.
SIEM	Security Information and Event Management – Informační systém pro sběr a vyhodnocování auditních záznamů a událostí.
Služby vytvářející důvěru	Služby definované v nařízení eIDAS.
Spoléhající se strana	Subjekt spoléhající se při své činnosti na časová razítka vydaná dle této politiky.
TSA	Time Stamping Authority – autorita časových razítek obsahující více TSU.
TSU	Time Stamping Unit – jednotka vydávající časová razítka, která disponuje unikátním soukromým klíčem a vlastním certifikátem.
UTC	Coordinated Universal Time – Koordinovaný světový čas.
Zneplatněný certifikát	Certifikát, který je certifikační autoritou označen jako neplatný, a jehož stav zneplatnění je oznámen službou OCSP nebo uvedením na seznamu CRL.
Žadatel	Fyzická osoba, podnikající fyzická osoba či právnická osoba, která žádá o časové razítko na základě písemné smlouvy se společností Komerční banka, a.s.

2 ZÁKLADNÍ POJETÍ

Společnost Komerční banka, a. s. poskytuje službu vydávání kvalifikovaných elektronických časových razítek (dále jen "časová razítka") dle nařízení (EU) eIDAS. Technicky je tato služba poskytována sadou jednotek pro vydávání časových razítek označovaných jako „Komerční banka TSA TSU*nn*". Vydávaná časová razítka podle této politiky mají krátkou časovou platnost a slouží k účelům razítkování obecných dat.

Politika TSA vychází z požadavků standardů a platné legislativy:

- RFC 3628 - Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- RFC 5816 - ESSCertIDv2 Update for RFC 3161
- ETSI EN 319 421 - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 - Time Stamping Protocol and Electronic Time-Stamp Profiles
- Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce
- 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

Služby dle této politiky jsou poskytovány klientům za stanovených podmínek nediskriminačně, bez ohledu na rasu, etnický původ, národnost, pohlaví, sexuální orientaci, věk, zdravotní postižení, náboženské vyznání, vírů, světový názor klienta a jiné faktory.

Osoby se zdravotním postižením nejsou omezeny.

2.1 SLUŽBY AUTORITY ČASOVÝCH RAZÍTEK (TSA)

Služby autority pro vydávání kvalifikovaných časových razítek provozované společností Komerční banka, a.s. jsou poskytovány v souladu s platnou legislativou, smluvními podmínkami a relevantními technickými standardy.

Tyto služby zahrnují následující oblasti:

- službu autentizace žadatelů o časová razítka
- vydávání časových razítek jednotkami „Komerční banka TSA TSU*nn*"

2.2 AUTORITA ČASOVÝCH RAZÍTEK

TSA vystupuje z pohledu klientů a spoléhajících se stran jako důvěryhodná výpočetní a komunikační infrastruktura vydávající kvalifikovaná časová razítka. Z titulu provozovatele nese celkovou odpovědnost za poskytování služeb v oblasti vydávání kvalifikovaných časových razítek společnost Komerční banka, a.s.

2.3 ŽADATELÉ O ČASOVÉ RAZÍTKO

Žadatelem o časové razítko může být na základě písemné smlouvy se společností Komerční banka, a.s. fyzická osoba, podnikající fyzická osoba či právnická osoba.

2.4 POLITIKA A PROVÁDĚCÍ SMĚRNICE

Tento dokument byl vypracován tak, aby splňoval všechny požadavky kladené na politiku TSA i na prováděcí směrnici TSA. Tato skutečnost se projevuje i v názvu tohoto dokumentu.

2.5 SPOLÉHAJÍCÍ SE STRANA

Spoléhající se stranou je myšlen subjekt spoléhající se při své činnosti na kvalifikovaná časová razítka vydaná dle této politiky.

3 POLITIKA TSA

3.1 ZÁKLADNÍ POPIS

Politika vydávání časových razítek je definovaný seznam pravidel, která popisují vlastnosti a poskytované záruky časových razítek vydávaných společností Komerční banka, a.s.

3.2 IDENTIFIKACE

Název dokumentu	Autorita pro vydávání kvalifikovaných časových razítek – Politika a prováděcí směrnice
Verze dokumentu	1.0
OID této politiky	1.3.154.45317054.1000.3.2.1.1.1
Datum vydání	1.6.2023
Datum platnosti	Do odvolání, resp. do vydání nové verze
Kontakt	info_ca@kb.cz

3.3 POUŽITÍ ČASOVÝCH RAZÍTEK

Časová razítka vydaná podle této politiky smí být používány pouze v souladu s platnými právními předpisy.

Toho politika nezavádí žádná omezení použitelnosti časového razítka vydaného v souladu s jejím obsahem.

3.4 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

Ve společnosti Komerční banka, a.s. jsou v souladu s platnými právními předpisy prováděny pravidelné interní i externí kontroly, které se zabývají mimo jiné kontrolou plnění požadavků, které jsou na kvalifikované poskytovatele služeb vytvářejících důvěru kladeny příslušnou legislativou.

3.4.1 Periodicita hodnocení, okolnosti pro provedení hodnocení

Periodicita hodnocení je alespoň jednou za 12 měsíců. Externí audit je prováděn subjektem posuzování shody alespoň jednou za 24 měsíců (dle článku 20 nařízení eIDAS).

3.4.2 Identita a kvalifikace hodnotitele

Kvalifikace interního auditora je specifikována interními předpisy KB.

Externí audit je v souladu s nařízením eIDAS prováděn orgánem posuzování shody zveřejněným na evropském seznamu „Conformity Assessments Bodies for QTSP/QTS".

3.4.3 Vztah hodnotitele k hodnocenému subjektu

Interní kontrolu provádějí zaměstnanci společnosti Komerční banka, a.s. nebo zaměstnanci smluvního partnera.

Externí audit je v souladu s nařízením eIDAS prováděn pracovníky subjektu posuzování shody, kteří nejsou zaměstnanci Komerční banky a.s. či jejího smluvního partnera.

3.4.4 Hodnocené oblasti

Hodnocení se provádí v souladu se standardy ETSI 319 421, ETSI 319 422 a nařízením eIDAS.

3.4.5 Postup v případě zjištění nedostatků

Výsledky hodnocení shody jsou předány Manažerovi bezpečnosti PKI, který zajistí nápravu zjištěných nedostatků, resp. přijme vhodné opatření.

3.4.6 Sdělování výsledků hodnocení

Výstupem hodnocení shody je písemná zpráva, která je předána Manažerovi bezpečnosti PKI. Ten rozhodne o případné distribuci zprávy na další příjemce či o zveřejnění zprávy.

V případě externího auditu vykonávaného dle článku 20 nařízení eIDAS Manažer bezpečnosti PKI předloží výslednou zprávu o posouzení shody do tří pracovních dnů od jejího obdržení orgánu dohledu.

4 ZÁVAZKY A ODPOVĚDNOSTI

4.1 ZÁVAZKY TSA

4.1.1 Obecné závazky TSA

Společnost Komerční banka, a.s. zaručuje, že při poskytování služby vydávání časových razítek:

- zajišťuje nepřetržitý, s výjimkou plánovaných či neplánovaných časových přerušení spojených s technickými zásahy, přístup ke službám TSA za podmínek uvedených v písemné smlouvě
- postupuje v souladu s platnou legislativou vztahující se k procesu vydávání časových razítek
- dodržuje postupy a pravidla stanovená touto politikou
- používá bezpečné systémy a nástroje, zajišťuje dostatečnou úroveň bezpečnosti používaných postupů, včetně dostatečné úroveň kryptografických nástrojů
- zveřejňuje důležité dokumenty vztahující se k službě vydávání časových razítek na webových stránkách poskytovatele služeb vytvářejících důvěru
- na stránce https://www.kb.cz/pki jsou zveřejněny certifikáty všech TSU
- dodržuje závazky TSA ve vztahu k zákazníkům a k žadatelům o časové razítko a držitelům časových razítek

Společnost Komerční banka, a.s. se zavazuje, že:

- vydávaná časová razítka obsahují věcně správné údaje a splňují všechny náležitosti stanovené platnou legislativou, provozní dokumentací a touto politikou
- použije soukromé klíče pro podepisování časových razítek pouze v procesu tvorby časových razítek
- vydá časové razítko neprodleně po obdržení platného požadavku
- využívá důvěryhodnou synchronizaci času
- data v elektronické podobě, která jsou předmětem žádosti o vydání časového razítka, odpovídají datům obsaženým ve vydaném časovém razítku
- časový údaj vložený do časového razítka odpovídá hodnotě UTC v okamžiku vytváření časového razítka s přesností 500 milisekund a je získán z měřidla času navázaného na světový koordinovaný čas
- nezpracovává dokument, ze kterého byl spočten hash, kterému má být časové razítko přiřazeno (s výjimkou kontroly délky otisku)
- dokument, pro který je vytvářeno elektronické kvalifikované časové razítko, je uložen na prostředcích zákazníka nebo na důvěryhodném úložišti KB
- zveřejní tuto a další relevantní politiky na svých webových stránkách, případně jinými vhodnými způsoby

Vydané časové razítko obsahuje:

- identifikátor časového razítka jednoznačný v rámci daného TSU a TSA
- identifikátor politiky, podle které bylo časové razítko vydáno
- časový údaj odpovídající hodnotě UTC v době vytvoření časového razítka s přesností 500 milisekund
- náhodné číslo nonce, které je do časového razítka zkopírováno z žádosti o časové razítko
- data v elektronické podobě obsažená v žádosti o časové razítko (otisk dokumentu, pro který je vydáváno časové razítko)
- kvalifikovanou elektronickou pečeť TSU

4.2 ZÁVAZKY ŽADATELŮ O ČASOVÉ RAZÍTKO A DRŽITELŮ ČASOVÉHO RAZÍTKA

Žadatel o časové razítko, případně jeho držitel, ručí za informace, které uvedl ve smlouvě o poskytování časových razítek a za to, že postupuje v souladu se zmíněnou smlouvou, s platnou legislativou a touto politikou.

Žadatel o časové razítko je před podáním žádosti o vydání časového razítka povinen zvážit, zda je časové razítko vydané podle této politiky vhodné pro účel, pro který má být použito.

Žadatel o časové razítko, je povinen po obdržení odpovědi na žádost o časové razítko zjistit stav odpovědi. V případě, že v procesu vystavení časového razítka nastala chyba, neobsahuje odpověď přiložené časové razítko, ale chybové hlášení, které je žadatel povinen překontrolovat.

V případě, že odpověď obsahuje časové razítko, je žadatel povinen zejména:

- ověřit platnost kvalifikované elektronické pečeti časového razítka a certifikátů vztahujících se k TSU, která toto časové razítko vytvořila
- ověřit, že hash obsažený v časovém razítku odpovídá požadovanému hash na žádosti
- v případě, že žádost obsahovala položky „nonce“ a „reqPolicy“ ověřit, že je jejich hodnota v odpovědi stejná

4.3 ZÁVAZKY SPOLÉHAJÍCÍCH SE STRAN

Spoléhající strana zaručuje, že bude vždy jednat v souladu s touto politikou. Zavazuje se, že zejména, že:

- ověří platnost kvalifikované elektronické pečeti časového razítka, včetně kontroly odvolání certifikátů
- ověří, že hash uvedený v elektronickém časovém razítku odpovídá hash dat, ze kterých bylo toto elektronické časové razítko spočítáno
- vezme v úvahu případné omezení použitelnosti časových razítek stanové v této politice
- zváží, zda je časové razítko vydané podle této politiky vhodné pro účel, ke kterému bylo použito

4.4 ODPOVĚDNOST

Společnost Komerční banka, a.s. neposkytuje žádné další záruky vyjma těch, které vyplývají z platné legislativy, nebo které byly součástí smluvního ujednání mezi společností Komerční banka, a.s. a zákazníkem. Smlouva musí být sjednána písemně.

Společnost Komerční banka, a.s. se zavazuje, že splní veškeré povinnosti vyplývající z platné legislativy, smluvního ujednání a relevantních politik, a že tyto povinnosti bude plnit po celou dobu platnosti smlouvy.

Společnost Komerční banka, a.s. neodpovídá za vady a škody vzniklé z důvodu nesprávného či neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy, zejména za jejich využití v rozporu s platnou legislativou či relevantní politikou, a dále za škody způsobené z důvodu vyšší moci

5 POŽADAVKY NA POSTUPY TSA

5.1 SPRÁVA POLITIKY

5.1.1 Organizace pověřená správou dokumentu

Za správu této politiky pro vydávání časových razítek odpovídá poskytovatel služeb vytvářejících důvěru – Komerční banka, a.s., IČ 45317054, se sídlem Komerční banka, a.s., nám. Junkových 2772/1, Praha 5 - Stodůlky

5.1.2 Kontaktní osoba

Kontaktní osobou pro účely správy této politiky je Manažer bezpečnosti. Role manažera bezpečnosti je v KB zastoupená Manažerem bezpečnosti PKI. Další informace je možné získat na e-mailové adrese info_ca@kb.cz a na webové adrese poskytovatele služeb vytvářejících důvěru https://www.kb.cz/pki

5.1.3 Osoba odpovědná za soulad politiky s odpovídající prováděcí směrnicí

Tento dokument je současně politikou i prováděcí směrnici a za jeho správnost odpovídá Manažer bezpečnosti PKI.

5.1.4 Postupy při schvalování politiky

Tato politika je spravována v souladu s interními pravidly poskytovatele služeb vytvářejících důvěru. Nové verze tohoto dokumentu vznikají podle potřeby, zejména však při změně konfigurace autority pro vydávání časových razítek, vlastností časových razítek či souvisejících postupů, které ovlivní obsah, nebo pokud jakékoli jiné okolnosti její úpravu vyžadují. Tuto politiku schvaluje Manažer bezpečnosti.

5.2 POŽADAVKY NA ŽIVOTNÍ CYKLUS PÁROVÝCH DAT TSA

5.2.1 Generování a instalace párových dat

5.2.1.1 Generování párových dat

Párová data pro jednotlivá TSU jsou generována v kvalifikovaném prostředku pro vytváření elektronické pečeti dle nařízení eIDAS (QSealCD). O generování je pořízen písemný záznam.

5.2.1.2 Poskytování veřejných klíčů

Veřejné klíče sloužící k ověření platnosti elektronických pečetí vydaných časových razítek jsou obsaženy v certifikátu relevantního TSU. Tento certifikát je možno získat:

- prostřednictvím webových stránek společnosti Komerční banka, a.s.
- prostřednictvím webových stránek DIA jako orgánu dohledu

5.2.1.3 Délka párových dat

K vytváření elektronických pečetí, které jsou použity k pečetění vytvořených časových razítek, je použit algoritmus RSA s délkou klíče 3072 bitů.

5.2.2 Ochrana soukromého klíče (dat pro vytváření elektronických značek/podpisů)

5.2.2.1 Standardy a podmínky používání kryptografických modulů

Párová data pro podepisování kvalifikovaných časových razítek jsou vytvářena v QSealCD.

Zálohování soukromých klíčů

Soukromé klíče TSU jsou zálohovány s využitím QSealCD. Zálohy klíčů jsou uchovávány v zašifrované podobě.

5.2.2.2 Uchovávání soukromých klíčů

Po uplynutí doby platnosti soukromých klíčů sloužících k pečetění vydávaných časových razítek jsou klíče včetně záloh zničeny; o zničení klíčů je vyhotoven záznam.

5.2.2.3 Transfer soukromých klíčů

Operace se soukromým klíčem probíhají výhradně v chráněném prostředí QSealCD. Soukromý klíč v otevřené podobě nikdy neopustí prostředí QSealCD.

5.2.2.4 Uložení soukromých klíčů v kryptografickém modulu

Soukromé klíče TSU jsou uloženy v QSealCD v otevřené podobě. Bezpečnostní certifikace použitého QSealCD garantuje, že soukromé klíče z HSM nelze přečíst ani exportovat v otevřené podobě.

5.2.2.5 Aktivační data

Aktivační data jsou vytvářena v průběhu inicializace QSealCD. Aktivační data nejsou nikdy přenášena či uchovávána v otevřené podobě.

Další aspekty aktivačních dat jsou popsány v interních dokumentacích poskytovatele služeb vytvářejících důvěru.

5.2.2.6 Postup aktivace soukromého klíče

Před započetím použití soukromých klíčů TSU je nutné tyto klíče v QSealCD aktivovat. Aktivaci klíčů mohou provést výhradně pověření pracovníci poskytovatele služeb vytvářejících důvěru. Podrobný popis aktivace soukromých klíčů v QSealCD je popsán v interní provozní dokumentaci.

Po aktivaci jsou soukromé TSU použitelné, dokud se neukončí spojení mezi službou a QSealCD, anebo dokud nedojde k ukončení činnosti QSealCD.

5.2.2.7 Postup deaktivace soukromého klíče

Deaktivace soukromého klíče TSU se provede automaticky, pokud nastane jedna z podmínek:

- je ukončena činnost služby využívající klíče v QSealCD
- je přerušeno spojení mezi službou a QSealCD
- je ukončena či restartována činnost QSealCD

5.2.2.8 Postup ničení soukromého klíče

Soukromé klíče TSU se zničí deaktivací klíče v QSealCD a vymazáním všech záložních kopií klíče. Zničení klíče mohou provádět pouze pověření pracovníci poskytovatele certifikačních služeb. O zničení klíče je proveden písemný záznam.

5.2.2.9 Uchovávání veřejných klíčů

Veřejné klíče (ve formě certifikátů) jsou uchovávány po celou dobu existence společnosti Komerční banka, a.s. jako poskytovatele služby vytvářejícího důvěru.

5.2.3 Profil certifikátu TSU

Jednotlivé jednotky pro vydávání časových razítek (TSU) mají svá párová data a své certifikáty, tj. párová data se nesdílí mezi TSU.

Profily certifikátů TSU jsou specifikovány v Certifikační politice kvalifikovaných certifikátů pro elektronickou pečeť určených pro TSA Servery s následujícími specifiky:

1. Doba platnosti soukromého klíče je 12 měsíců. Avšak rozšíření Doba platnosti soukromého klíče (*privateKeyUsagePeriod*) specifikované standardem ITU-T X.509 není použito.
2. Algoritmus veřejného klíče je RSA-PSS s délkou klíče 3072 bitů
3. Předmět certifikátu obsahuje:
    - C=CZ

- O=Komerční banka, a.s.
- OrganizationIdentifier=NTRCZ-45317054
- SERIALNUMBER=TSUESN--<*HWSN*> (určuje výrobní číslo TSA serveru)
- CN=Komerční banka TSA TSU*nn* (*nn* rozlišuje jednotlivé TSA servery)

4. Obsahuje rozšíření Rozšířené použití *(extKeyUsage*) právě s jednou hodnotou *id-kp-timeStamping {1.3.6.1.5.5.7.3.8}*
5. Obsahuje rozšíření qcStatements s hodnotami:
   {0.4.0.1862.1.1} - kvalifikovaný certifikát
   {0.4.0.1862.1.5} - odkazy na PDS v češtině a angličtině
   {0.4.0.1862.1.6} - s hodnotou {0.4.0.1862.1.6.2} - certifikát pro elektronickou pečeť

5.2.4 Výměna párových dat

Platnost certifikátu TSU systému TSA je uvedena v daném certifikátu. Platnost párových dat pro tvorbu kvalifikované elektronické pečeti, případně pro její ověřování, je omezena dobou platnosti certifikátu TSA. Toto období je rozděleno na dvě části:

- v prvním časovém úseku (v době platnosti soukromého klíče), jsou párová data používána k vydávání časových razítek i k ověřování jejich platnosti (resp. k ověřování platnosti elektronické pečeti). Před uplynutím tohoto časového úseku jsou generována nová párová data TSU.
- ve druhém časovém úseku jsou data používána pouze pro ověřování elektronické pečeti časového razítka.

V nutných případech (například v případě prolomení bezpečnosti užitých kryptografických algoritmů či jejich parametrů) je generování nových párových dat i vydání příslušného certifikátu provedeno neprodleně.

5.2.5 Ukončení životního cyklu párových dat

Doba platnosti certifikátu TSU je uvedena v těle tohoto certifikátu. Zneplatnění a pozastavení platnosti certifikátu

Certifikát TSU může být zneplatněn, pokud:

- nastanou skutečnosti uvedené v platné legislativě
- dojde ke kompromitaci, případně existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče certifikační autority vydávající certifikáty pro TSU systému TSA
- dojde ke kompromitaci, případně existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče konkrétní TSU

Služba pozastavení platnosti certifikátu není poskytována.

Seznam zneplatněných certifikátů

Profil seznamu zneplatněných certifikátů, stejně jako místo a způsob jejich zveřejňování je popsán v certifikační politice vydávající CA.

5.2.6 Správa kryptografického modulu používaného při vytváření časových razítek

Při provozu a správě kryptografického modulu používaného při vytváření časových razítek je postupováno v souladu s interní dokumentací.

5.2.6.1 Hodnocení kryptografického modulu

Kryptografický modul sloužící k pečetění vydávaných časových razítek kvalifikovanou elektronickou pečetí splňuje požadavky kladené na QSealCD.

5.3 VYDÁVÁNÍ ČASOVÝCH RAZÍTEK

5.3.1 Časové razítko

Každé časové razítko vydané podle této politiky:

- obsahuje OID politiky dle které bylo vydáno
- obsahuje jedinečný identifikátor časového razítka v rámci TSU
- obsahuje čas synchronizovaný se zdrojem UTC času
- čas obsažený v časovém razítku s přesností stanovenou touto politikou
- pokud je detekováno, že zdroj UTC nedosahuje požadovanou přesnost, pak časové razítko není vydáno
- obsahuje hash poskytnutý žadatelem
- je podepsáno klíčem výhradně k tomu určeným
- mimo jiné obsahuje identifikaci:
    - země, kde je TSA provozována
    - identifikaci TSA
    - identifikaci TSU

5.3.2 Synchronizace měřidla času s UTC

5.3.2.1 Synchronizace

Synchronizace měřidla času s důvěryhodným zdrojem UTC je kontrolována periodicky.

5.3.2.2 Bezpečnost měřidla času

Zabezpečení měřidla času je popsáno v interní dokumentaci.

5.3.2.3 Detekce odchýlení měřidla času

Aktuální stav synchronizace měřidla času na referenční zdroj je periodicky testován a vyhodnocován.

5.3.2.4 Přestupná sekunda

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

5.3.3 Uzavření smlouvy

Vydávání časových razítek společností Komerční banka, a.s. je službou, která je dostupná pouze pro potřeby KB a jejích dceřiných společností. Není poskytována osobám mimo KB.

5.3.4 Zpracování žádosti a časové razítko

5.3.4.1 Identifikace a autentizace

Identita zákazníka je prokazována při uzavírání smlouvy o poskytování certifikačních služeb.

5.3.4.2 Přijetí nebo zamítnutí žádosti o časové razítko

Žadatel o vydání časového razítka vytvoří spojení s TSA pomocí protokolu HTTPS. Toto spojení funguje pouze v rámci interní sítě KB.

Žadatel vytvoří žádost o časové razítko (viz kapitola Struktura žádosti o časové razítko) a tuto datovou strukturu předá systému TSA. Nesplňuje-li žádost požadavky definované v této politice, je automaticky zamítnuta.

5.3.4.3 Doba zpracování žádosti o časové razítko

V případě, že přijatá žádost o vydání časového razítka není zamítnuta, bude toto razítko vytvořeno bez zbytečného odkladu řádově v jednotkách sekund od přijetí žádosti.

5.3.5 Vydání časového razítka

5.3.5.1 Úkony TSA v průběhu vydávání časového razítka

Po přijetí žádosti o časové razítko provede TSA kontrolu formální správnosti žádosti o časové razítko.

Není-li žádost formálně správná, je vytvořena odpověď s odpovídajícím chybovým statusem.

Je-li žádost formálně správná, obsahuje vytvořená odpověď i vygenerované časové razítko, které je opatřeno kvalifikovanou elektronickou pečetí konkrétní TSU.

Každá odpověď na žádost o časové razítko je archivována.

5.3.5.2 Oznámení o vydání časového razítka držiteli časového razítka

Po ukončení úkonů definovaných v předchozí kapitole je vytvořená odpověď (která případně obsahuje vygenerované časové razítko) odeslána zpět žadateli.

5.3.6 Převzetí časového razítka

5.3.6.1 Žadatel o časové razítko

Po obdržení odpovědi na žádost o časové razítko je žadatel povinen zjistit její stav. Obsahuje-li odpověď časové razítko, je žadatel povinen postupovat v souladu s touto politikou.

5.3.6.2 Spoléhající se strana

Spoléhající se strana je povinna postupovat v souladu s touto politikou.

5.3.7 Ukončení poskytování služeb pro žadatele o časové razítko

Služba vydávání časových razítek může být jednostranně ukončena ze strany poskytovatele.

5.3.8 Struktury žádosti, odpovědi a časového razítka

Časová razítka jsou vydávána na základě žádosti o časové razítko. Následující kapitoly obsahují popis struktur žádosti o časové razítko, odpovědi na žádost o časové razítko i samotného časového razítka.

5.3.8.1 Struktura žádosti o časové razítko

Služba vydávání časových razítek, kterou na základě písemné smlouvy poskytuje společnost Komerční banka, a.s. zpracovává žádosti o časové razítko s následujícím obsahem.

Položka	**Hodnota**
version	v1
hashAlgorithm (messageImprint)	Povolené algoritmy: SHA-384
hashedMessage (messageImprint)	Hash zprávy, délka musí odpovídat zvolenému algoritmu
reqPolicy	Volitelná položka, přípustné jsou pouze OID této politiky
nonce	Volitelná položka, obsahuje náhodné číslo zvolené klientem

certReq	Volitelná položka obsahující požadavek na vložení certifikátu TSU do odpovědi. Nabývá hodnot: ● TRUE – odpověď musí obsahovat certifikát TSU, ● FALSE, nebo pole certReq není uvedeno – odpověď nesmí obsahovat certifikát TSU.
extensions	Nesmí být uvedeno

Poznámka: V kulatých závorkách v názvech položek je uveden název nadřízené struktury

2.1.1.1 Struktura odpovědi na žádost o časové razítko

Položka	**Hodnota**
status (status)	Výsledek zpracování žádosti o časové razítko: 0 - časové razítko vydáno 1 - časové razítko vydáno, ale parametry pozměněny 2 - zamítnutí žádosti 3 - čekání 4 - hrozí zneplatnění certifikátu TSU 5 - certifikát TSU zneplatněn
statusString (status)	Volitelný text popisující chybu
failInfo (status)	Důvod odmítnutí žádosti (jen v případě, že není vráceno časové razítko): (0) - neznámý/nepodporovaný algoritmus (2) - nepovolená/nepodporovaná transakce (5) - chybný formát zaslaných dat (14) - nedostupný zdroj času (15) - požadovaná politika není podporována (16) - nepodporované rozšíření (17) - požadované doplňující informace jsou nedostupné (25) -chyba systému
timeStampToken	Časové razítko – jen v případě, kdy položka status (status) nabývá hodnoty 1 nebo 2

2.1.1.2 Struktura časového razítka – obecně

Časové razítko (timeStampToken) je elektronicky podepsaná datová struktura (ContentInfo) formátu CMS, která v sobě obsahuje obsah časového razítka (TSTInfo).

Časové razítko (elektronicky podepsaná datová struktura formátu CMS) obsahuje právě jeden elektronický podpis (SignerInfo), který byl vytvořený jednotkou TSU.

2.1.1.3 Struktura časového razítka – CMS

Obsah struktury ContentInfo:

Položka	**Hodnota**
contentType	id-signedData {1.2.840.113549.1.7.2 }
content	SignedData
version (SignedData)	v3
digestAlgorithms (SignedData)	Hashovací algoritmus použitý pro vytvoření zaručené elektronické pečeti časového razítka (CMS zprávy) SHA384
eContentType (encaContentInfo)	id-ct-TSTInfo {1.2.840.113549.1.9.16.1.4 }
eContent (encaContentInfo)	TSTInfo (tj. obsah časového razítka)
Certificates	Obsahuje certifikát TSU, a to jen v případě, že v žádosti bylo uvedeno certReq=true
crls	Není použito
signerInfos	Obsahuje právě jeden podpis TSU (SignerInfo)

Obsah struktury SignerInfo:

Položka	**Hodnota**
version	v1
sid	issuerAndSerialNumber certifikátu TSU
digestAlgorithm	Hashovací algoritmus použitý pro elektronickou pečeť SHA-384
id-aa-signingCertificateV2 (SignedAttributes)	Identifikace certifikátu pro verifikaci podpisu (viz RFC 5816)
contentType (SignedAttributes)	id-ctTSTInfo {1.2.840.113549.1.9.16.1.4 }
messageDigest	Hash obsahu časového razítka

(SignedAttributes)	
signingTime (SignedAttributes)	Čas podpisu ve formátu UTCTime
signatureAlgorithm	Asymetrický algoritmus použitý pro podpis **RSA-PSS**
signature	Elektronická pečeť
unsignedAttrs	Nepoužito

2.1.1.4 Struktura časového razítka – obsah časového razítka

Obsah struktury TS:

Položka	**Hodnota**
version	v1
policy	Identifikátor politiky, podle které bylo časové razítko vydáno
hashAlgorithm (messageImprint)	Povolené algoritmy: SHA-384
hashedMessage (messageImprint)	Hash zprávy, délka musí odpovídat zvolenému algoritmu
SerialNumber	Jedinečné číslo přiřazené TSU časovému razítku
genTime	Čas vydání časového razítka formátu YYYYMMDDhhmmss.sssZ
seconds (Accuracy)	Nepoužito
millis (Accuracy)	0-500ms v závislosti na údaji ze zdroje času
micros (Accuracy)	Nepoužito
ordering	Nepoužito
nonce	Pokud bylo nonce obsaženo v žádosti, pak odpověď obsahuje nonce se stejnou hodnotou jako v žádosti

tsa	Předmět z certifikátu TSU
id-pe-qcStatements (Extensions)	id-etsi-tsts-EuQCompliance {0.4.0.19422.1.1} - tj. kvalifikované časové razítko

5.4 SPRÁVA A PROVOZNÍ BEZPEČNOST TSA

5.4.1 Řízení bezpečnosti

Řízení bezpečnosti ve společnosti Komerční banka, a.s. je popsáno v interní dokumentaci.

5.4.2 Hodnocení a řízení rizik

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

5.4.2.1 Hodnocení zranitelnosti

Auditní záznamy TSU jsou pravidelně vyhodnocovány na výskyt nestandardních stavů a událostí, které mohou znamenat pokus o narušení zabezpečení. Na jejich základě dochází k vyhodnocení stavu prostředí a odpovídající reakci.

5.4.2.2 Postup při oznamování události subjektu, který ji způsobil

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

5.4.3 Personální bezpečnost

5.4.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Role zajišťující chod a správu TSA jsou dle existujících procedur obsazovány důvěryhodnými a zkušenými pracovníky. Obdobné procedury platí i pro spolupráci s externími subjekty (dodavateli).

5.4.3.2 Posouzení spolehlivosti osob

Do rolí správy TSA jsou jmenovány osoby, které patří mezi zaměstnance provozovatele služeb vytvářejících důvěru, a které mají dobré pracovní i osobní reference. U externích dodavatelů se uplatňují stejná měřítka.

5.4.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Všichni pracovníci podílející se na chodu a správě TSA jsou vyškoleni. Součástí školení je i školení o bezpečnosti PKI infrastruktury a o chování v havarijních situacích.

5.4.3.4 Požadavky a periodicita školení

Školení obsluhy je organizováno nejméně jednou ročně.

5.4.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Žádná ustanovení.

5.4.3.6 Postihy za neoprávněné činnosti zaměstnanců

Postihy za porušení pracovní kázně se řídí organizačními předpisy poskytovatele služeb vytvářejících důvěru, popř. smlouvami s externími dodavateli.

5.4.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Na smluvní (externí) pracovníky jsou uplatňována obdobná kritéria jako na zaměstnance poskytovatele služeb vytvářejících důvěru.

5.4.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci udržující chod a spravující TSA mají k dispozici následující dokumentaci:

- příručka administrátora

Kromě uvedených dokumentů mají pracovníci k dispozici také interní dokumenty, jako jsou normy, pracovní směrnice, metodické pokyny apod.

5.4.4 Fyzické zabezpečení

5.4.4.1 Umístění a konstrukce

Systémy pro vydávání časových razítek jsou umístěny v prostorách datových center KB. Tato pracoviště jsou proti neoprávněnému vniknutí chráněna mechanickými prostředky a bezpečnostní službou. Je zpracována bezpečnostní dokumentace stanovující požadavky na fyzickou bezpečnost těchto prostor.

Systémy pro vydávání časových razítek jsou duplikovány do dvou geograficky oddělených lokalit. V případě výpadku systémů v jedné lokalitě převezmou provoz systémy v druhé lokalitě.

5.4.4.2 Fyzický přístup

Přístup do datových center, která hostují systémy pro vydávání časových razítek, je řízený a monitorovaný. Přístup do datových center je vyhrazen jen pro definovanou množinu pracovníků. Pro přístup je vyžadována biometrická identifikace **krevním řečištěm**. Přistup je pracovníkům udělen na základě dvoustupňového schvalování. Seznam oprávněných uživatelů je průběžně aktualizován.

5.4.4.3 Elektřina a klimatizace

Datová centra jsou připojena na nepřetržitý zdroj napájení (UPS a dieselové generátory) a jsou vybavena klimatizačními jednotkami pro udržení optimální teploty.

5.4.4.4 Vliv vody

Datová centra jsou umístěna mimo zátopové oblasti.

5.4.4.5 Protipožární opatření a ochrana

Datová centra jsou vybavena elektronickou požární signalizací. Signalizace je vyvedena na pracoviště obsazené nepřetržitě 24x7.

5.4.4.6 Ukládání médií

Záložní média jsou uchovávána v chráněných skříních datových center.

5.4.4.7 Nakládání s odpady

Papírové dokumenty a média jsou v případě nepotřebnosti likvidována bezpečným způsobem.

5.4.4.8 Zálohy mimo budovu

Primárním mechanismem pro zajištění kontinuity provozu v případě výpadku datového centra, je duplikace všech podstatných systémů do druhého datového centra.

Vybraná aktiva jsou zálohována mimo datová centra v souladu s interními pokyny Manažera bezpečnosti PKI.

5.4.5 Procesní bezpečnost

5.4.5.1 Důvěryhodné role

Pro správu a provoz jsou definovány bezpečnostní role. KB má vytvořena pravidla pro obsazování osob do těchto rolí, pro jmenování a odvolávání pracovníků. Oprávnění přístupu jsou založena na těchto bezpečnostních rolích.

5.4.5.2 Počet osob požadovaných pro jednotlivé činnosti

Nominace pracovníků do rolí pro správu a provoz je koncipována tak, aby jeden pracovník neměl (bez kontroly jiným pracovníkem) přístup k bezpečnostně citlivým operacím. Nominace pracovníků do rolí rovněž zohledňuje riziko kumulace oprávnění – je definován seznam navzájem se vylučujících rolí, tzn. rolí, jejichž členství nesmí být přiděleno jednomu pracovníkovi.

Operace pro zajištění správy a provozu mohou pracovníci v definovaných rolích provádět samostatně s výjimkou následujících kroků (v závorce uvedený nutný počet osob potřebných k provedení operace):

- Vydání / obnova certifikátu TSU (2 osoby)
- Aktivace / obnova TSU (2 osoby)

5.4.5.3 Identifikace a ověření pro každou roli

Obsluha každé bezpečnostní role se musí před přístupem k informačním aktivům TSA nejprve ověřit vůči adresářové službě Active Directory. Používá se ověření pomocí jména a hesla a/nebo pomocí certifikátu na čipové kartě.

5.4.5.4 Role vyžadující rozdělení povinností

V interní dokumentaci je popsán seznam rolí, které jsou vzájemně separovány. Separace rolí je navržena tak, aby žádný pracovník nekumuloval pravomoci, které umožňují nekontrolovaný přístup k citlivým datům či úkonům.

5.4.6 Počítačová bezpečnost

5.4.6.1 Specifické technické požadavky na počítačovou bezpečnost

Kvalita počítačové bezpečnosti byla zohledněna ve fázi přípravy TSA a je průběžně vyhodnocována a případně zdokonalována.

Každá součást TSA je zabezpečena v souladu s doporučeními výrobce operačního systému a nadstavbových aplikací.

Technické řešení pro zajištění počítačové bezpečnosti je uvedeno v interní dokumentaci.

5.4.6.2 Hodnocení počítačové bezpečnosti

Počítačová bezpečnost TSA vychází ze standardů pro poskytovatele služby vytvářející důvěru – poskytování kvalifikovaných časových razítek. Jde zejména o pravidla, zakotvená v normách:

- ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 Time stamping protocol and electronic time-tamp profiles.

5.4.7 Bezpečnost životního cyklu

5.4.7.1 Řízení vývoje systému

Systém TSA byl navržen tak, aby splňoval bezpečnostní požadavky kladené na poskytování služby vydávání kvalifikovaných časových razítek. Ve fázi návrhu byly zohledněny bezpečnostní zásady stejně jako mechanismy fyzického i logického zabezpečení. Byla také provedena analýza rizik a navrženy mechanismy ochrany aktiv. Byly navrženy procesy, role a oprávnění.

Na základě schváleného návrhu byl systém TSA implementován. Pro dílčí části systému byly vyvinuty specifické softwarové komponenty. Implementace systému TSA byla provedena v souladu s doporučeními výrobce a dle bezpečnostních zásad poskytovatele služeb vytvářejících důvěru pro oblast změnového řízení.

Implementovaný systém TSA byl otestován jak po funkční, tak po bezpečnostní stránce. Po úspěšném dokončení testů byl systém TSA uveden do rutinního provozu.

5.4.7.2 Kontroly řízení zabezpečení

V rámci implementace systému TSA byly deaktivovány všechny nepotřebné funkčnosti, které by mohly představovat příležitost k ohrožení bezpečnosti. Byly deaktivovány výchozí uživatelské účty. Byly nastaveny politiky bezpečnosti hostitelských operačních systémů. Všechny konfigurační parametry modulů byly zváženy a příslušným způsobem nastaveny.

5.4.7.3 Řízení zabezpečení životního cyklu

Systém TSA je předmětem kontroly a auditu dle standardních postupů KB.

Kvalita a funkčnost provozu TSA je průběžně vyhodnocována. Hodnoceny jsou také zranitelnosti. Na nalezená zjištění je aplikována adekvátní reakce, např. ve formě instalace, odinstalace či upgrade komponent, a/nebo také úpravy konfigurací či politik.

5.4.8 Obnova po havárii a kompromitaci

Pro obsluhu TSA je zpracován dokument obsahující postupy pro zvládání krizových a havarijních situací a pro následnou obnovu provozu. Havarijní plány a plány kontinuity jsou uvedeny v interní dokumentaci TSA.

5.4.8.1 Postup v případě incidentu a kompromitace

V případě incidentu či kompromitace se postupuje v souladu se zpracovanými havarijními plány a plány kontinuity.

5.4.8.2 Poškození výpočetních prostředků, softwaru nebo dat

Všechny podstatné části systému TSA jsou pravidelně zálohovány. Podstatné části jsou provozovány redundantně. Vytvořené zálohy obsahují jednotlivé součásti TSA a umožňují provést obnovu i na jiný hardware.

V případě poškození výpočetních prostředků, softwaru nebo dat se postupuje v souladu s havarijními plány a plány kontinuity. Primární snahou je obnovit provoz na záložních systémech, popř. obnovit provoz na nových hostitelích s využitím záložních dat.

5.4.8.3 Postupy při zjištění odchýlení měřidla času

Postup synchronizace časového údaje měřidla času je součástí této politiky. V případě zjištění odchylky od UTC větší, než 0,5 sekundy, je činnost TSU okamžitě ukončena a do vyřešení odchylky není služba vydávání časových razítek poskytována.

5.4.8.4 Postupy při kompromitaci soukromého klíče

V případě důvodného podezření na kompromitaci soukromého klíče TSU bude:

- mimořádně ukončena činnost TSU
- skutečnost bude neprodleně oznámena orgánu dohledu
- Informováni klienti
- Certifikát zneplatněn
- Informace na web, včetně identifikace vydaných razítek

5.4.8.5 Schopnost obnovení činnosti po havárii

Pokračování procesů TSA po havárii závisí na typu havárie a jejich následcích a je věcí rozhodnutí Manažera bezpečnosti PKI. Při rozhodnutí o neukončení provozu nepřekročí doba výpadku autority pro vydávání časových razítek 14 dnů.

5.4.9 Ukončení činnosti autority pro vydávání časových razítek

Ukončení činnost se řídí interním dokumentem (Plán ukončení činnosti).

Při ukončení činnosti proběhnout zejména tyto kroky:

- Nejméně s tříměsíčním předstihem je o ukončení činnosti informován orgán dohledu.
- S dostatečným předstihem jsou o této skutečnosti informování zákazníci a spoléhající se strany.
- Budou odvolány všechny t.č. platné certifikáty Autority pro vydávání časových razítek
- Komisionálně budou zlikvidovány soukromé klíče Autority pro vydávání časových razítek

5.4.10 Soulad s legislativními požadavky

Kvalifikovaná časová razítka jsou vydávána v souladu s eIDAS.

5.4.11 Auditní záznamy

5.4.11.1 Typy zaznamenávaných událostí

Všechny podstatné a citlivé události vznikající v systému poskytovatele certifikačních služeb jsou zaznamenávány. Součástí interní dokumentace je seznam zaznamenávaných typů událostí, a také doplňková data uváděná k jednotlivým typům událostí.

5.4.11.2 Periodicita zpracování záznamů

Auditní i provozní záznamy jsou průběžně shromažďovány do nezávislého úložiště, mimo systémy, v nichž události vznikly a byly zaznamenány.

Auditní záznamy kontrolují pověření pracovníci v intervalu definovaném interními předpisy.

Významné události jsou vyhodnocovány a eskalovány automaticky systémem SIEM.

5.4.11.3 Doba uchování auditních záznamů

Auditní i provozní záznamy jsou uloženy v systému, v němž vznikly, minimálně do doby, než jsou přeneseny do nezávislého centrálního úložiště.

5.4.11.4 Ochrana auditních záznamů

Auditní záznamy jsou uchovávány tak, aby byly chráněny proti krádeži, neoprávněnému zpřístupnění, modifikaci a zničení (úmyslnému i neúmyslnému).

5.4.11.5 Postupy pro zálohování auditních záznamů

Auditní záznamy jsou ve zdrojových systémech zálohovány spolu s hostitelským systémem.

5.4.11.6 Systém shromažďování auditních záznamů

Auditní záznamy jsou shromažďovány v dedikované centrální databázi. Centrální úložiště je provozováno Komerční bankou v rámci interních systémů.

5.4.11.7 Postup při oznamování událostí subjektu, který ji způsobil

Subjektu, který způsobil událost v auditním logu, není taková skutečnost oznamována.

5.4.11.8 Hodnocení zranitelnosti

Auditní záznamy jsou pravidelně vyhodnocovány na výskyt nestandardních stavů a událostí, které mohou znamenat pokus o narušení zabezpečení. Na jejich základě dochází k vyhodnocení stavu prostředí a odpovídající reakci.

5.5 PERIODICITA ZVEŘEJŇOVÁNÍ INFORMACÍ

5.5.1 Informace jsou zveřejňovány v následujících intervalech:

- certifikáty jednotlivých TSU jsou zveřejňovány po jejich vydání a schválení orgánem dohledu
- politika a prováděcí směrnice pro vydávání kvalifikovaných časových razítek (tento dokument) je zveřejňován bezprostředně po schválení nové verze

5.6 POPLATKY

Poplatky se řídí aktuálním ceníkem služeb KB.

5.7 FINANČNÍ ODPOVĚDNOST

Krytí pojištěním

Komerční banka jako poskytovatel certifikačních služeb kvalifikovaný poskytovatel služeb vytvářejících důvěru má uzavřené pojištění rizik pro případ pokrytí případných finančních škod způsobených službou nebo aplikací KB.

Další aktiva a záruky

Komerční banka, jako poskytovatel certifikačních služeb kvalifikovaný poskytovatel služeb vytvářejících důvěru, má dostatečné finanční zdroje pro pokrytí závazků plynoucích z poskytování certifikačních služeb.

5.8 DŮVĚRNOST OBCHODNÍCH INFORMACÍ

Vydaná časová razítka nenesou žádné důvěrné informace.

5.9 OCHRANA OSOBNÍCH ÚDAJŮ

Vydaná časová razítka nenesou žádné osobní údaje.

5.10 PRÁVA DUŠEVNÍHO VLASTNICTVÍ

Vydaná časová razítka nenesou žádná data, která by mohla být považována za duševní vlastnictví.

5.11 DOBA PLATNOSTI, UKONČENÍ PLATNOSTI

5.11.1 Doba platnosti

Doba platnosti této politiky a prováděcí směrnice je od data vydání do odvolání, resp. vydání nové verze.

5.11.2 Ukončení platnosti

Platnost tohoto dokumentu je ukončena:

- jeho nahrazením novější verzí, nebo
- ukončením poskytování služeb vydávání časových razítek

5.11.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti tohoto dokumentu z důvodu ukončení poskytování služeb zůstávají v platnosti ustanovení týkající se obchodních a právních záležitostí.

5.12 KOMUNIKACE MEZI ZÚČASTNĚNÝMI SUBJEKTY

5.12.1 Komunikace s poskytovatelem služeb vytvářejících důvěru

Poskytovatel služeb vytvářejících důvěru oznamuje podstatné informace na webové stránce https://www.kb.cz/pki, případně je doručuje interními komunikačními kanály Komerční banky.

5.12.2 Jazyk komunikace

Primárním komunikačním jazykem je čeština, sekundárním angličtina.

5.13 ZMĚNY

5.13.1 Postup při změnách

Postupy pro změny probíhají dle kapitoly 7.1.

5.13.2 Postup při oznamování změn

Změny týkající se infrastruktury PKI, politiky či jiných dokumentů jsou oznamovány na webové stránce https://www.kb.cz/pki, případně jsou doručovány jinými interními komunikačními kanály Komerční banky.

5.13.3 Okolnosti, při kterých musí být změněn identifikátor OID

OID je přiřazeno politice, podle níž se vydávají časová razítka.

Změny v politice, které se týkají zásadních skutečností významně ovlivňujících základní bezpečnostní funkce TSA, jako změny kryptografických aspektů (použité algoritmy, velikosti klíčů, hashovací algoritmus) apod., jsou okolnostmi, na základě, kterých je nutné nové verzi politiky přidělit nové OID. V případě ostatních změn v politiky lze ponechat stávající OID.

5.14 ŘEŠENÍ SPORŮ

Řešení sporů probíhá:

- v případě zaměstnanců dle interních předpisů a Zákoníku práce
- v případě externistů na základě smlouvy uzavřené se spřízněnou organizací

5.15 ROZHODNÉ PRÁVO

Rozhodným právem je právo České republiky.

5.16 SHODA S PRÁVNÍMI PŘEDPISY

Činnost poskytovatele služeb vytvářejících důvěru je v souladu s právním řádem České republiky.

5.17 DALŠÍ USTANOVENÍ

5.17.1 Rámcová dohoda

Žádná ustanovení.

5.17.2 Postoupení práv

Není stanoveno.

5.17.3 Oddělitelnost ustanovení

Žádná ustanovení.

5.17.4 Zřeknutí se práv

Žádná ustanovení.

5.17.5 Vyšší moc

Žádná ze stran nenese odpovědnost za porušení svých povinností způsobeným vyšší mocí.

5.18 DALŠÍ OPATŘENÍ

Žádná ustanovení.