CERTIFIKAČNÍ POLITIKA KVALIFIKOVANÝCH CERTIFIKÁTŮ PRO ELEKTRONICKOU PEČEŤ URČENÝCH PRO TSA SERVERY

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	29.5.2023	První verze	Tomáš Prjacha, Manažer PKI  Digitálně podepsal(a) Tomáš Prjacha dne 29.05.2023 10:22:52

1 ÚVOD

Tento dokument představuje certifikační politiku kvalifikovaných certifikátů pro elektronickou pečeť. Certifikáty jsou vydávány pro interní potřebu společnosti Komerční banka, a.s. (dále jen Komerční banka nebo KB), konkrétně pro kvalifikovaného poskytovatele služeb vytvářejících důvěru, provozovaného Komerční bankou.

1.1 PŘEHLED

Tato Certifikační politika (dále CP) popisuje pravidla využívání certifikátů a požadavky, které musejí být splněny při vydávání a práci s certifikáty pro elektronickou pečeť.

Certifikáty vydávané podle této CP jsou určeny pro technické prostředky, vytvářející kvalifikovaná elektronická časová razítka, provozované v Komerční bance. Technické prostředky, jimž jsou vydávány certifikáty podle této CP, jsou v tomto dokumentu označovány jako TSA servery (Time Stamping Authority, autority pro vydávání časových razítek).

Soukromé klíče odpovídající veřejnému klíči v certifikátu TSA serverů jsou používány k vytváření kvalifikovaných elektronických pečetí časových razítek.

Formálně je držitelem certifikátů organizace provozující TSA servery, pro které se certifikát vydává, tzn. Komerční banka. TSA servery pak za KB vytvářejí kvalifikovaná elektronická časová razítka. Vydané certifikáty s krátkou dobou platnosti slouží k ověření integrity a původu elektronických časových razítek, vzniklých v KB za účelem zafixování času podpisu obecných dat nebo zafixování času obecných dat, ve kterých prokazatelně existoval.

1.2 NÁZEV DOKUMENTU A IDENTIFIKACE

Název dokumentu	Certifikační politika kvalifikovaných certifikátů pro elektronickou pečeť určených pro TSA servery
Verze dokumentu	1.0
OID této certifikační politiky	1.3.154.45317054.1000.1.2.1.6.1
Datum vydání	29.5.2023
Datum platnosti	Do odvolání, resp. do vydání nové verze

Struktura dokumentu odpovídá standardu RFC 3647.

1.3 PARTICIPUJÍCÍ SUBJEKTY

Kvalifikovaným poskytovatelem služeb vytvářejících důvěru je Komerční banka, a.s. která k tomuto účelu provozuje PKI, tj. infrastrukturu veřejných klíčů (v dalším textu PKI Komerční banky nebo PKI KB).

V rámci PKI je provozována kořenová certifikační autorita KB Root 3 CA a podřízené certifikační autority poskytující certifikační služby. Tato kapitola popisuje relevantní účastníky (subjekty) PKI v KB.

Kontaktní a identifikační údaje kvalifikovaného poskytovatele služeb vytvářejících důvěru:

Komerční banka, a.s.

IČO 45317054, DIČ CZ699001182

Na Příkopě 33, 114 07 Praha 1

Tel: 800 521 521

e-mail: info_ca@kb.cz

1.3.1 Certifikační autority

PKI Komerční banky je tvořeno třívrstvou hierarchií PKI.

KB Root 3 CA je kořenovou certifikační autoritou v hierarchii PKI systému KB. Úkolem *KB Root 3 CA* je vydávat a spravovat certifikáty podřízených certifikačních autorit provozovaných v rámci PKI KB. Kořenová CA tak vytváří důvěryhodnou kotvu PKI KB.

Komerční banka provozuje několik podřízených certifikačních autorit určených pro vydávání koncových certifikátů. Certifikáty těchto vydávajících CA jsou vydány z *KB Root 3 CA*.

- Některé z vydávajících CA jsou určeny pro interní použití Komerční banky: vydávají certifikáty pro zaměstnance a infrastrukturu KB.
- Jiné vydávající CA jsou určeny pro vydávání certifikátů klientům Komerční banky a také certifikátů, které mají být akceptovány veřejnými spoléhajícími se stranami. Jednou z certifikačních autorit, které vydávají certifikáty pro akceptaci veřejností, je *Komerční banka Qualified CA/RSA*.

Komerční banka Qualified CA/RSA vydává kvalifikované certifikáty podle této certifikační politiky. (Vydává i další typy kvalifikovaných certifikátů, podle jiných certifikačních politik.)

1.3.1.1 Soulad se standardy

Certifikační autorita *Komerční banka Qualified CA/RSA* je vybudována a provozována způsobem, který zohledňuje relevantní legislativu, normy a průmyslové standardy, zejména:

- [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
- [297/2016] Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce
- [ETSI EN 319 401] Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- [ETSI EN 319 411-1] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- [ETSI EN 319 411-2] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- [ETSI TS 119 312] Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- [ETSI EN 319 412-2] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- [ETSI EN 319 412-5] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
- [GDPR] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- [ISO 27001] ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky
- [RFC 6960] Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- [PKCS10] RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- [FIPS PUB 140-2] Requirements for Cryptographic Modules.
- [ISO/IEC 15408] Information technology — Security techniques — Evaluation criteria for IT security

- [ISO 3166-1] ISO 3166-1 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.
- [X.501] ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- [X.509] ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- [X.520] ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.

1.3.2 Registrační autority

Registrační autorita je provozována v kancelářských prostorách Komerční banky. Registrační autorita není přístupná pro veřejnost, přístup k registrační autoritě mají pouze pracovníci KB, pracovníci dceřiných společností KB, popř. smluvní spolupracovníci KB. Registrační proces zajišťují pracovníci Komerční banky.

Registrační autorita:

- jedná za Komerční banku, a.s. při poskytování certifikačních služeb,
- podepisuje za KB dokumenty a protokoly, které jsou podmínkou pro podání žádosti a převzetí certifikátu.
- ověřuje totožnost žadatelů,
- prověřuje existenci a legální status organizace, pro kterou se žádá o certifikát,
- prověřuje, zda je žadatel oprávněn žádat o certifikát za danou organizaci,
- prověřuje, zda byl klíčový pár žádosti vygenerován v kvalifikovaném prostředku pro vytváření elektronických pečetí,
- přijímá žádosti o certifikáty a zajišťuje předání vydaného certifikátu.

1.3.3 Žadatelé o certifikát

O certifikáty podle této CP mohou požádat osoby, které splňují všechny následující podmínky:

- Jsou pracovníky Komerční banky nebo smluvními spolupracovníky KB.
- Jsou zmocněni k podání žádosti o certifikát pro KB, resp. pro kvalifikovaného poskytovatele služeb vytvářejících důvěru, jímž je KB.
- Před podáním žádosti byla ověřena jejich osobní identita.

1.3.4 Držitelé certifikátů

Držitelem certifikátu je Komerční banka, jako kvalifikovaný poskytovatel služeb vytvářejících důvěru. Identifikační údaje držitele (Komerční banky) jsou uvedeny v certifikátu. Držitel certifikátu má v držení soukromý klíč, jehož veřejný klíč je součástí vydaného certifikátu.

1.3.5 Spoléhající se strany

Spoléhající se stranou je entita spoléhající se při ověřování elektronické pečetě kvalifikovaných elektronických časových razítek na certifikát vydaný podle této CP.

1.3.6 Další zúčastněné subjekty

Dalšími participujícími subjekty jsou orgány dohledu nad kvalifikovanými poskytovateli služeb vytvářejících důvěru, popř. další subjekty, které jsou zainteresovány podle právní úpravy pro služby vytvářející důvěru.

1.4 POUŽITÍ CERTIFIKÁTŮ

1.4.1 Přípustné použití certifikátu

Kvalifikované certifikáty vydané podle této certifikační politiky mohou být použity pouze k ověřování kvalifikované elektronické pečetě kvalifikovaných elektronických časových razítek právnické osoby, v souladu s platnými právními předpisy pro služby vytvářející důvěru.

1.4.2 Omezení použití certifikátu

Certifikáty vydávané podle této certifikační politiky nelze používat k jiným účelům, než je stanoveno v kapitole 1.4.1.

Certifikáty vydávané podle této certifikační politiky jsou kvalifikovanými certifikáty ve smyslu [EIDAS].

Certifikáty nelze používat v rozporu s platnými právními předpisy.

1.5 SPRÁVA POLITIKY

1.5.1 Organizace pověřená správou dokumentu

Za správu této certifikační politiky odpovídá kvalifikovaný poskytovatel služeb vytvářejících důvěru: Komerční banka, a.s., IČO 45317054, se sídlem Na Příkopě 33, 114 07 Praha 1.

1.5.2 Kontaktní osoba

Kontaktní osobou pro účely správy této certifikační politiky je Manažer PKI. Další informace je možné získat na e-mailové adrese info_ca@kb.cz a na webové adrese kvalifikovaného poskytovatele služeb vytvářejících důvěru https://www.kb.cz/pki

1.5.3 Osoba odpovědná za soulad CP s odpovídající CPS

Za soulad této certifikační politiky s příslušnou certifikační prováděcí směrnicí odpovídá Manažer PKI.

1.5.4 Postupy při schvalování CP

Tato certifikační politika je spravována v souladu s interními pravidly kvalifikovaného poskytovatele služeb vytvářejících důvěru. Nové verze certifikační politiky vznikají podle potřeby, zejména však při změně konfigurace CA, vlastností certifikátů či souvisejících postupů, které ovlivní její obsah, nebo pokud jakékoli jiné okolnosti její úpravu vyžadují. Certifikační politiku schvaluje Manažer PKI.

Nová verze CP je vždy zveřejněna před tím, než se podle této verze začnou vydávat certifikáty.

Nejméně jednou za rok je tato CP revidována s cílem posoudit její aktuálnost a nutnost případných změn.

1.6 DEFINICE A ZKRATKY

Následující tabulka obsahuje definice použitých názvů a zkratek.

Zkratka / pojem	Definice
AIA	Authority Information Access. Rozšíření certifikátu, v němž lze získat informaci o certifikátu vydávající (nadřízené) CA. Popř. lze v tomto rozšíření získat také URL pro ověření stavu certifikátu protokolem OCSP.
Aktivace klíče	Uvedení kryptografického klíče do stavu, kdy lze klíč použít pro aktivní operace. Viz také RFC 3647
Aktivační data	Data, potřebná k aktivaci kryptografického klíče, tzn. uvedení klíče do stavu, kdy lze s klíčem provádět aktivní operace. Viz také RFC 3647.

CA	Certifikační autorita – entita, která vydává certifikáty na základě schválených žádostí, a zveřejňuje seznamy CRL
CDP	CRL Distribution Point. URL adresa, z níž lze stáhnout aktuální seznam zneplatněných certifikátů.
Certifikát (v oblasti PKI)	Je datová struktura, která je vydána CA, spojuje veřejný klíč (=data pro ověřování elektronických podpisů) s podepisující osobou a umožňuje ověřit její identitu.
Common Criteria	Mezinárodní standard ISO/IEC 15408 pro hodnocení IT systémů a komponent.
CP	Certifikační politika, viz RFC3647
CPS	Certifikační prováděcí směrnice, viz RFC3647
CRL	Seznam zneplatněných certifikátů, v souladu s RFC 5280
DNS	Domain Name System. Systém doménových jmen, přidělovaným jednotlivým prvkům síťové komunikace. Jeho hlavním úkolem jsou vzájemné převody doménových jmen a IP adres uzlů sítě.
Držitel certifikátu	Viz kapitolu 1.3.4
EAL	Evaluation Assurance Level. Bezpečnostní hodnocení IT systému nebo komponenty podle mezinárodního standardu Common Criteria security evaluation. Čím vyšší ohodnocení, tím vyšší úroveň jistoty, že jsou bezpečnostní funkce hodnocené komponenty či systému správně implementovány.
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
Elektronická pečeť	Data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu.
Expirovaný certifikát	Certifikát po skončení doby platnosti uvedené v daném 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
HSM	Hardware Secure Module, kryptografický prostředek pro ochranu a bezpečné použití kryptografických klíčů.
KB klíč	Mobilní aplikace Komerční banky. Aplikace umožňuje vzdálenou identifikaci, přihlašování a odesílání plateb v internetovém bankovnictví KB.
Klíčový pár (též párové klíče, párová data)	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.
Kořenový certifikát	Nadřízený certifikát, který je podepsán privátním klíčem příslušným veřejnému klíči uvedenému v tomto certifikátu (angl. self-signed). Je na vrcholu hierarchie důvěry.
Kvalifikovaná elektronická pečeť	Zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.

Kvalifikované elektronické časové razítko	Elektronické časové razítko, které splňuje požadavky stanovené v článku 42 [EIDAS]
Kvalifikovaný certifikát	Certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky přílohy 1 [EIDAS]
Kvalifikovaný certifikát pro elektronickou pečeť	Certifikát pro elektronickou pečeť, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky v příloze III. [EIDAS]
Kvalifikovaný poskytovatel služeb vytvářejících důvěru	Obecně (podle [EIDAS]): poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele V tomto dokumentu: společnost Komerční banka, a.s., jako kvalifikovaný poskytovatel služeb vytvářejících důvěru, který provozuje certifikační autoritu a vydává kvalifikované certifikáty.
Kvalifikovaný prostředek pro vytváření elektronických pečetí	Prostředek pro vytváření elektronických pečetí, který přiměřeně splňuje požadavky stanovené v článcích 19 a 30 [EIDAS] a v příloze II [EIDAS]
Manažer bezpečnosti PKI	Osoba zodpovědná za administraci kvalifikovaného poskytovatele a implementaci bezpečnostních pravidel kvalifikovaného poskytovatele certifikačních služeb. Osoba je zodpovědná za schvalování změn, které mají dopad na úroveň bezpečnosti kvalifikovaného poskytovatele certifikačních služeb.
Manažer PKI	Osoba zodpovědná za akreditaci kvalifikovaného poskytovatele, interní audit, certifikaci a provoz certifikačních autorit i autorit pro vydávávání časových razítek. Osoba schvaluje dokumenty kvalifikovaného poskytovatele (certifikační politiky, havarijní plány atd.)
Nadřízený certifikát	Certifikát, jehož párové klíče slouží k podepisování a ověřování vydávaných certifikátů. Certifikát certifikační autority, která vydala (podřízený) certifikát.
Obnovení pozastaveného certifikátu	Obnovení platnosti pozastaveného certifikátu; uvedení dočasně zneplatněného certifikátu zpět do platného stavu.
OCSP	Online Certificate Status Protocol. Protokol pro zjišťování stavu zneplatnění certifikátu. Protokol je definován v RFC 6960, popř. v RFC 2560.
Operátor registračního místa	Pracovník kvalifikovaného poskytovatele služeb vytvářejících důvěru, zodpovědný za ověření identity žadatele o certifikát i identity právnické osoby, pro kterou se žádá o certifikát.
Orgán dohledu	Subjekt dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru, podle [EIDAS] a § 13 zákona č. 297/2016 Sb.
Párové klíče, též párová data	Soukromý a veřejný klíč. Viz také Klíčový pár.
Pečetící osoba	Právnická osoba, která vytváří elektronickou pečeť.
Pozastavený certifikát	Dočasně zneplatněný certifikát z důvodu „Pozastavení certifikátu“ (Certificate Hold)
Prodloužení platnosti certifikátu	Vydání nového nebo následného certifikátu, který využívá stejná párová data jako jeho „předchůdce“, tzn. starší certifikát stejného typu, vydaný pro tentýž subjekt.
Prostředek pro vytváření elektronických pečetí	Konfigurované programové nebo technické zařízení, které se používá k vytvoření elektronických pečetí. Držitelé certifikátů,

	vydaných podle této CP, provozují prostředek v rámci svých informačních systémů. Prostředek má typicky formu hardwarového zařízení pro ochranu a použití kryptografických klíčů (viz HSM).
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.
Správce CA	Osoba zodpovědná za technologii a provoz certifikačních autorit KB, které vydávají certifikáty podle této politiky.
Správce certifikátů	Osoba, která řídí životní cyklus certifikátů. Má oprávnění zjišťovat informace o vydaných certifikátech a zneplatňovat certifikáty.
Statut certifikátu	Stav, ve kterém se certifikát nachází, tj. platný, zneplatněn pozastavený, expirovaný.
Subjekt	Entita, pro kterou byl certifikát vydán nebo je vydáván. Subjekt je žadatelem a držitelem certifikátu. Viz také kapitolu 1.3.3.
TSA	Time Stamping Authority. Autorita pro vydávání časových razítek. Tato instituce pro výkon své role provozuje jeden nebo více TSA serverů. Formálně jsou certifikáty podle této CP vydávány pro TSA. Technicky jsou soukromé klíče certifikátů, vydávaných podle této CP, chráněny a používány v TSU, tzn. TSA serverech.
TSA server	Synonymum pro TSU
TSU, nebo též TSA server	Time Stamping Unit. Technický prostředek pro vydávání elektronických časových razítek, podle IETF RFC 3161. V rámci jedné TSA může být provozováno několik TSU, typicky pro zajištění vysoké dostupnosti.
URL	Uniform Resource Locator. Textový řetězec, který slouží ke specifikaci umístění zdrojů informací v internetu. Adresa webové stránky, webové služby apod…
UTC	Coordinated Universal Time. Mezinárodní systém měření času, časový standard založený na Mezinárodním atomovém čase (TAI).
Zaručená elektronická pečeť	Elektronická pečeť, která splňuje požadavky článku 36 [EIDAS]
Zneplatněný certifikát	Certifikát, jenž je certifikační autoritou označen jako neplatný a jehož stav zneplatnění je oznámen službou OCSP anebo uvedením na seznamu CRL.
Žadatel	Viz kapitolu 1.3.3.

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

Komerční banka, a.s. provozuje úložiště veřejných a neveřejných informací spojených s provozem a správou certifikátů vydávaných podle této certifikační politiky.

Za zabezpečení a dostupnost úložiště informací a dokumentace odpovídá společnost Komerční banka, a.s., jako kvalifikovaný poskytovatel služeb vytvářejících důvěru.

2.2 ZVEŘEJŇOVÁNÍ INFORMACÍ A DOKUMENTACE

Vydané certifikáty jsou uloženy v databázi certifikační autority. Informace o vydaných certifikátech, o provozu certifikačních autorit a dokumentace CA jsou zveřejňovány v dále uvedeném rozsahu.

Údaje, které nejsou v následujících podkapitolách uvedeny, jsou neveřejné.

2.2.1 Zveřejňování informací o certifikátech

Certifikáty vydávající certifikační autority *Komerční banka Qualified CA/RSA* jsou zveřejňovány prostřednictvím distribučních adres uvedených ve vydaných certifikátech (v rozšíření AIA). Certifikát CA je dostupný protokolem HTTP.

Seznamy zneplatněných certifikátů (CRL) jsou zveřejňovány prostřednictvím distribučních adres, uvedených ve vydaných certifikátech (v rozšíření CDP). CRL je dostupné protokolem HTTP.

Publikační úložiště certifikátu CA i CRL je hostováno na webovém serveru spravovaném Komerční bankou. Toto úložiště je veřejně přístupné z prostředí internetu (na adresách uvedených v certifikátech).

K ověření stavu zneplatnění certifikátů vydaných podle této certifikační politiky lze využít také OCSP protokol. URL OCSP serveru je uvedena ve vydávaných certifikátech, v rozšíření AIA. Ověření stavu zneplatnění pomocí OCSP je veřejně dostupné z internetu.

Certifikáty vydané podle této CP jsou volně dostupné pro spoléhající se strany na webové stránce https://www.kb.cz/pki a také na důvěryhodném seznamu dle nařízení eIDAS.

2.2.2 Zveřejňování informací o certifikačních autoritách

Certifikační politiky, případně další dokumenty týkající se provozu PKI Komerční banky, jsou zveřejňovány na webové stránce: https://www.kb.cz/pki

2.3 ČAS NEBO ČETNOST ZVEŘEJŇOVÁNÍ INFORMACÍ

Informace jsou zveřejňovány v následujících intervalech:

- Certifikát vydávající certifikační autority *Komerční banka Qualified CA/RSA* je zveřejňován po jeho vydání a po schválení orgánem dohledu. Certifikát CA je publikován před započetím používání příslušného soukromého klíče CA k podepisování vydávaných certifikátů či CRL.
- Seznam CRL je zveřejňován bezodkladně po jeho vygenerování, nejpozději 24 hodin od vydání předchozího CRL.
- Certifikační politika je zveřejňována po schválení a vydání nové verze, vždy před započetím vydávání certifikátů podle dané CP.
- Certifikační prováděcí směrnice (CPS) je zveřejňována po schválení a vydání nové verze.

2.4 ŘÍZENÍ PŘÍSTUPŮ K JEDNOTLIVÝM TYPŮM ÚLOŽIŠŤ

Certifikační politika, certifikační prováděcí směrnice, certifikáty CA, certifikáty vydané dle této CP, seznamy zneplatněných certifikátů (CRL) a informace o stavu certifikátů poskytované protokolem OCSP jsou pro čtení veřejně a bezplatně přístupné bez omezení.

Tyto veřejné informace jsou k dispozici 24 hodin denně 7 dní v týdnu s výjimkou případů plánovaných odstávek zveřejněných na webu.

Interní dokumentace PKI systému je přístupná pouze pracovníkům kvalifikovaného poskytovatele služeb vytvářejících důvěru, popř. subjektům definovaným interními pravidly KB anebo příslušnou právní úpravou.

1 Identifikace a ověření

2.5 POJMENOVÁNÍ

2.5.1 Typy jmen

Název subjektu v certifikátu je vytvořen podle standardu [X.501], resp. [X.520].

E-mailová adresa v certifikátu odpovídá standardu RFC 5322.

2.5.2 Požadavky na významovost jmen

Jména slouží k rozlišení subjektů, pro něž jsou certifikáty vydávány. Obsahují proto identifikační údaje držitele certifikátu.

V certifikátech vydávaných podle této CP se uvádí:

- Identifikátor TSA serveru, pro který byl certifikát vydán
- Identifikátor kvalifikovaného prostředku pro vytváření elektronických pečetí, který hostuje soukromý klíč certifikátu
- Identifikátor právnické osoby, pro kterou byl certifikát vydán
- Název právnické osoby, pro kterou byl certifikát vydán
- E-mailová adresa držitele certifikátu (nepovinný údaj)

Identifikační údaje držitele se uvádějí v položce předmět certifikátu a v alternativních názvech.

2.5.3 Anonymita a používání pseudonymu

Certifikáty vydávané podle této CP neobsahují anonymní údaje ani pseudonymy.

2.5.4 Pravidla pro interpretaci různých forem názvů

Identifikační údaje držitele uvedené v žádosti o certifikát musí odpovídat informacím, které o držiteli eviduje kvalifikovaný poskytovatel služeb vytvářejících důvěru.

Položky předmětu a alternativních názvů jsou ze žádosti přeneseny do vydaného certifikátu.

2.5.5 Jedinečnost jmen

CA zaručuje jedinečnost jmen v předmětu vydávaných certifikátů. Kromě ostatních údajů slouží k odlišení jmen především identifikátor TSA serveru a identifikátor prostředku pro vytváření elektronických pečetí.

Danému držiteli může být podle této CP vydáno více certifikátů pro jednotlivé TSA servery. V takovém případě bude každý certifikát obsahovat jednoznačné označení konkrétního TSA serveru v položkách commonName a serialNumber; viz také kapitolu 6.1.

2.5.6 Obchodní značky

Certifikáty vydávané podle této CP obsahují identifikátory právnické osoby, pro kterou se certifikát vydává. Identifikace právnické osoby je ověřována v rámci procesu zpracování žádosti o certifikát.

Kromě identifikátorů právnické osoby neobsahují certifikáty vydané podle této CP žádné obchodní značky nebo registrované ochranné známky.

2.6 POČÁTEČNÍ OVĚŘENÍ IDENTITY

Počáteční ověření identity se provádí před vydáním každého certifikátu.

2.6.1 Ověřování vlastnictví soukromého klíče

Žadatel o certifikát prokazuje vlastnictví příslušného soukromého klíče k certifikovanému veřejnému klíči tím, že předkládá žádost podepsanou tímto soukromým klíčem (ve formátu PKCS#10). Ověřením elektronického podpisu žádosti je prokázáno, že právnická osoba, kterou žadatel zastupuje, měla v době vytváření žádosti pod kontrolou soukromý klíč odpovídající veřejnému klíči v žádosti.

2.6.2 Ověřování identity organizace

Identitu právnické osoby, pro kterou se žádá o certifikát, ověřuje operátor registrační autority před přijetím žádosti. Kvalifikovaný poskytovatel služeb vytvářejících důvěru vydává podle této CP certifikáty pouze pro sebe, formálně tedy pro svou mateřskou organizaci, jíž je Komerční banka. Operátor registrační autority ověřuje identitu organizace náhledem do Obchodního rejstříku.

2.6.3 Ověření identity žadatele o certifikát

Identitu žadatele ověřuje operátor registrační autority na základě osobního dokladu, obsahujícího fotografii.

Při ověření totožnosti jsou ověřovány údaje osoby:

- Jméno a příjmení
- Adresa bydliště
- Datum narození
- Číslo a typ identifikačního dokladu

2.6.4 Neověřované informace

V kapitolách 2.6.3 a 2.6.5 je uvedeno, které údaje o žadateli jsou ověřovány. Ostatní údaje nejsou ověřovány.

Ověřovány nejsou ani následující údaje zapisované do certifikátu:

- název TSA serveru, pro který se vydává certifikát,
- e-mailová adresa, uváděná v certifikátu.

V případě těchto údajů se kvalifikovaný poskytovatel služeb vytvářejících důvěru spoléhá na údaje v dokumentu zmocňujícím žadatele požádat o certifikát. Viz také kapitolu 2.6.5.

2.6.5 Ověřování oprávnění

Žadatel musí před podáním žádosti doložit, že je zmocněn zastupovat Komerční banku při podání žádosti o certifikát. Zmocnění lze doložit:

- buď papírovou formou plné moci, podepsané statutárním zástupcem Komerční banky
- anebo elektronickým požadavkem evidovaným v interním systému KB a prokazatelně schváleným nadřízeným pracovníkem žadatele.

Kromě identifikace žadatele a právnické osoby musí zmocnění obsahovat identifikační údaje a typ certifikátu, o který je žadatel oprávněn žádat.

Žadatel musí doložit, že klíčový pár, jehož veřejný klíč je obsažen v žádosti, vzniknul v kvalifikovaném prostředku pro vytváření elektronických pečetí. Žadatel tuto skutečnost doloží prostřednictvím protokolu o vytvoření klíčového páru v kvalifikovaném prostředku pro elektronickou pečeť. Protokol musí být přiložen k žádosti o certifikát a musí být podepsán žadatelem a pověřeným zástupcem kvalifikovaného poskytovatele služeb vytvářejících důvěru. Součástí protokolu musí být také identifikátor technického prostředku, v němž byl vytvořen klíčový pár žádosti. Viz také kapitolu 3.1.2.1.

2.6.6 Kritéria pro interoperabilitu (spolupráci)

Certifikační autorita *Komerční banka Qualified CA/RSA* nespolupracuje při vydávání certifikátů podle této CP s jinými poskytovateli služeb vytvářejících důvěru. Provoz jiných certifikačních autorit v rámci KB není pokládán za formu spolupráce.

2.7 IDENTIFIKACE A AUTENTIZACE PŘI POŽADAVKU NA VÝMĚNU KLÍČE

Žádost o certifikát s novým veřejným klíčem může podat pouze žadatel, specifikovaný v kapitole 1.3.3.

2.7.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Identifikace při běžném požadavku na výměnu klíče se provádí stejně jako při počátečním ověření identity. Viz kapitolu 2.6.

2.7.2 Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu

Identifikace při požadavku na výměnu klíče po zneplatnění certifikátu se provádí stejně jako při počátečním ověření identity. Viz kapitolu 2.6.

2.8 IDENTIFIKACE A AUTENTIZACE PŘI POŽADAVKU NA ZNEPLATNĚNÍ CERTIFIKÁTU

Ke zneplatnění certifikátu může dojít:

- Z vůle držitele certifikátu (lze požádat o zneplatnění pouze certifikátu daného držitele).
- Z rozhodnutí pověřených pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru.
- Z rozhodnutí orgánu dohledu, podle § 13 odst. 2 zákona č. 297/2016 Sb.
- Držitel certifikátu, který žádá o zneplatnění certifikátu, tak může učinit jedním z následujících postupů:
- Osobně na pracovišti registrační autority, prostřednictvím zmocněného žadatele. Žadatel musí předložit plnou moc, podepsanou statutárním zástupcem právnické osoby, která je držitelem certifikátu. Plná moc musí obsahovat identifikační údaje žadatele, statutárního zástupce, organizace i certifikátu, který má být zneplatněn. Operátor registračního místa ověří identitu žadatele na základě osobního dokladu, který obsahuje fotografii.
- Elektronicky pomocí schváleného požadavku v evidenčním systému KB. Požadavek musí být vznesen zástupcem právnické osoby a schválen nadřízením pracovníkem daného zástupce.

3 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

3.1 ŽÁDOST O VYDÁNÍ CERTIFIKÁTU

3.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu může podle této certifikační politiky podat zmocněný zástupce právnické osoby (žadatel). Právnickou osobou, pro kterou se žádá o certifikát, musí být Komerční banka, a.s. jako kvalifikovaný poskytovatel služeb vytvářejících důvěru. Pro více informací viz kapitoly 1.3.3 a 1.3.4.

3.1.2 Podání žádosti a odpovědnosti poskytovatele a žadatele

3.1.2.1 Příprava žádosti

Žadatel musí podat žádost v souboru; formát souboru musí odpovídat standardu PKCS#10.

Procesu generování klíčů a žádosti musí být osobně přítomen zástupce kvalifikovaného poskytovatele služeb vytvářejících důvěru: interní auditor anebo Manažer PKI anebo Manažer bezpečnosti PKI. Generování klíčového páru a žádosti musí proběhnout takovým způsobem, který zástupci kvalifikovaného poskytovatele služeb vytvářejících důvěru umožní ověřit, že klíčový pár byl vygenerován v identifikovaném kvalifikovaném prostředku pro vytváření elektronických pečetí. Zástupce kvalifikovaného poskytovatele služeb vytvářejících důvěru o vygenerování žádosti vystaví protokol, který obsahuje mimo jiné:

- Identifikátor kvalifikovaného prostředku pro vytváření elektronických pečetí, použitého pro generování klíčového páru
- Identifikační údaje, uvedené v žádosti
- Identifikátor veřejného klíče, který vzniknul při dané operaci a který je součástí žádosti; uvádí se otisk (hash) veřejného klíče
- Identifikační údaje osoby, která generovala žádost
- Identifikační údaje zástupce kvalifikovaného poskytovatele služeb vytvářejících důvěru, který byl svědkem generování žádosti
- Datum a čas vytvoření žádosti

3.1.2.2 Podání žádosti

Žádost o certifikát se podává vždy na registračním místě KB, za osobní účasti žadatele. Žadatel předkládá podklady operátorovi registračního místa, a ten podklady ověřuje:

- Žadatel se musí identifikovat pomocí svého osobního dokladu, viz také kapitolu 2.6.3.
- Žadatel musí doložit, že je oprávněn žádat o daný certifikát pro společnost Komerční banka, a.s. (Kvalifikovaný poskytovatel služeb vytvářejících důvěru vydává certifikát sám pro sebe.)
- Žadatel musí předložit soubor s žádostí o certifikát.
- Žadatel musí podat písemnou žádost o certifikát. Žádost musí obsahovat identifikační údaje žadatele a také údaje odpovídající podané (elektronické) žádosti.
- Žadatel musí předložit protokol prokazující vytvoření klíčového páru v identifikovaném kvalifikovaném prostředku pro vytváření elektronických pečetí; viz také kapitolu 3.1.2.1

Operátor registračního místa načte obsah žádosti do aplikačního vybavení registrační autority. Porovná, zda obsah žádosti odpovídá podkladům, které předložil žadatel.

Operátor registračního místa také – proti internímu seznamu – prověří, zda lze daný typ certifikátu vydat dané právnické osobě, a zda údaje v žádosti odpovídají identifikačním údajům dané právnické osoby.

Pokud žadatel nedodá některý z podkladů anebo pokud kontrola obsahu žádosti neodpovídá podkladům, je žádost operátorem registračního místa odmítnuta.

3.1.2.3 Odpovědnosti poskytovatele služeb vytvářejících důvěru

Kvalifikovaný poskytovatel služeb vytvářejících důvěru je zejména povinen:

- Informovat žadatele o podmínkách poskytování certifikátů.
- Zveřejňovat důležité dokumenty vztahující se k životnímu cyklu vydávaných certifikátů (např. tuto certifikační politiku) na webových stránkách kvalifikovaného poskytovatele služeb vytvářejících důvěru.
- Ověřit totožnost žadatele o certifikát, fyzicky na základě předložených osobních dokladů.
- Ověřit, že je žadatel zmocněn požádat o daný typ certifikátu pro Komerční banku, a.s. (pro kvalifikovaného poskytovatele služeb vytvářejících důvěru).
- Evidovat identifikační údaje žadatele a další informace spojené se správou certifikátů žadatele.
- Evidovat identifikační údaje právnické osoby, pro kterou se certifikát vydává.
- Ověřit, že klíčový pár žádosti vznikl v kvalifikovaném prostředku pro vytváření elektronických pečetí.
- Ověřovat platnost identifikačních údajů právnické osoby, které jsou uvedeny v žádosti a mají být zapsány do certifikátu.
- Ověřovat, zda právnická osoba, pro kterou se žádá o certifikát, je Komerční banka, a.s., jako kvalifikovaný poskytovatel služeb vytvářejících důvěru.
- Vydat certifikát obsahující věcně správné údaje.
- Zveřejnit certifikáty kořenové certifikační autority KB Root 3 CA a certifikační autority *Komerční banka Qualified CA/RSA*, aby bylo možné ověřit elektronickou identitu kvalifikovaného poskytovatele služeb vytvářejících důvěru.
- Poskytovat certifikační služby v souladu s platnými právními předpisy včetně [EIDAS] a v souladu s dokumentací PKI (certifikační politika, certifikační prováděcí směrnice, systémová bezpečnostní politika a ostatní provozní dokumentace).

3.1.2.4 Odpovědnosti žadatele

Žadatel je povinen zejména:

- Dodat platné podklady pro podání žádosti – viz kapitolu 3.1.2.2
- Před podáním žádosti zkontrolovat platnost identifikačních údajů uváděných do žádosti. Požádat o certifikát jen v případě, že jsou identifikační údaje platné.
- Zkontrolovat, zda jsou údaje uvedené ve vydaném certifikátu správné.
- Seznámit se s certifikační politikou a další dokumentací týkající se používání certifikační služby.

3.1.2.5 Odpovědnost držitele certifikátu

Držitel (Komerční banka) je povinen zejména:

- Příslušným způsobem zmocnit žadatele k podání žádosti o certifikát pro společnost Komerční banka, a.s. (kvalifikovaný poskytovatel služeb vytvářejících důvěru).
- Zkontrolovat, zda jsou údaje uvedené ve vydaném certifikátu správné.
- Zajistit, aby prostředek, v němž je uložen klíčový pár certifikátu, byl pod výhradní kontrolou Komerční banky, kvalifikovaného poskytovatele služeb vytvářejících důvěru.
- Nakládat se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu tak, aby nemohlo dojít k jeho neoprávněnému užití nebo zneužití.
- Zajistit, aby užívání klíčového páru a odpovídajícího certifikátu odpovídalo účelům stanoveným v této certifikační politice.

- V případě podezření na zneužití soukromého klíče neprodleně požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče.
- Seznámit se s certifikační politikou a další dokumentací týkající se používání certifikační služby.
- Sdělit kvalifikovanému poskytovateli služeb vytvářejících důvěru změny v údajích, uvedených ve vydaném certifikátu.

3.2 ZPRACOVÁNÍ ŽÁDOSTI O CERTIFIKÁT

3.2.1 Identifikace a ověření

Identifikace žadatele i právnické osoby pro kterou se žádá o certifikát se provádí v rámci procesu podání žádosti. Žadatel i právnická osoba jsou identifikovány a ověřeny operátorem registračního místa. Žadatel se musí na registrační místo dostavit osobně, je identifikován pomocí osobního dokladu. Podrobněji je proces identifikace popsán v kapitolách 2.6.2 a 2.6.3.

V rámci podání žádosti musí žadatel předložit podklady, uvedené v kapitole 3.1.2.2. Podklady jsou ověřovány operátorem registračního místa.

3.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Při podání žádosti musí žadatel operátorovi registračního místa předložit žádost a podklady. Mezi požadované podklady patří:

- Osobní doklad, pro ověření identity žadatele.
- Potvrzení, že je žadatel oprávněn žádat o daný certifikát pro společnost Komerční banka, a.s., viz také kapitolu 2.6.5.
- Písemná žádost o certifikát.
- Protokol prokazující vytvoření klíčového páru v daném kvalifikovaném prostředku pro vytváření elektronických pečetí; viz také kapitolu 3.1.2.1

Operátor registračního místa načte obsah žádosti do aplikačního vybavení registrační autority. Porovná, zda obsah žádosti odpovídá podkladům, které předložil žadatel.

Operátor registračního místa také prověří, zda se žádá o certifikát po společnost Komerční banka, a.s., a zda údaje v žádosti odpovídají identifikačním údajům této právnické osoby.

Pokud žadatel nedodá některý z požadovaných podkladů anebo údaje v žádosti neodpovídají dodaným podkladům, že žádost o certifikát odmítnuta.

Pokud jsou všechny podklady dodány, obsahují platné údaje a odpovídají údajům v žádosti, že žádost přijata do zpracování. Operátor registračního místa zavede žádost do systému certifikační autority, zároveň k žádosti doplní informace:

- Identifikační údaje žadatele
- Požadovaný typ certifikátu

Po kontrole všech zadaných údajů odešle operátor registračního místa žádost ke zpracování systémem certifikační autority. Žádost je při odeslání autorizována elektronickým podpisem, který prokazuje, že žádost korektně prošla procesem registrace a údaje žádosti byly ověřeny.

Žádost o certifikát je zpracovávána systémem certifikační autority. CA při zpracování využívá informace, uvedené operátorem registračního místa.

CA při zpracování žádosti prověřuje především:

- Zda byl žadatel identifikován, resp. zda byla ověřena totožnost žadatele.
- Zda identifikovaný žadatel splnil všechny podmínky a je oprávněn požádat o daný typ certifikátu.
- Integritu žádosti o certifikát, včetně elektronického podpisu žádosti. K ověření podpisu se využije veřejný klíč, uvedený v žádosti. (Tímto krokem se ověřuje, zda měl žadatel v době vzniku žádosti k dispozici soukromý klíč.)

- Autorizační podpis žádosti, který prokazuje, že žádost byla korektně prověřena na registračním místě.
- Zda identifikační údaje v žádosti odpovídají údajům, které zkontroloval a ověřil operátor registračního místa.

Pokud proběhnou všechny kroky ověření žádosti úspěšně, je žádost přijata certifikační autoritou – na základě žádosti pak CA automaticky vydá certifikát.

Pokud některý z kroků ověření skončí neúspěšně, je žádost automaticky zamítnuta a certifikát není vydán.

3.2.3 Doba zpracování žádosti o certifikát

Žádosti o certifikáty jsou zpracovány bezodkladně po doručení do certifikační autority.

3.3 VYDÁNÍ CERTIFIKÁTU

3.3.1 Úkony CA při vydávání certifikátu

Pokud žádost projde úspěšně procesem zpracování (viz kapitolu 3.2), vydá certifikační autorita na základě žádosti obratem certifikát.

Certifikační autorita zapíše do vydaného certifikátu identifikační údaje držitele, TSA serveru a kvalifikovaného prostředku pro vytváření elektronických pečetí – tak, jak byly dodány v žádosti.

Kromě identifikačních údajů zavede CA do vydaného certifikátu i další údaje (aplikační politiky, účel použití certifikátu, atd…), viz kapitolu 6.1.

Certifikát je elektronicky podepsán soukromým klíčem CA.

3.3.2 Oznámení žadateli o vydání certifikátu

Žadatel je o vydání certifikátu či zamítnutí žádosti informován pracovníkem registračního místa, bezprostředně po zpracování podané žádosti.

3.4 PŘEVZETÍ VYDANÉHO CERTIFIKÁTU

3.4.1 Úkony spojené s převzetím certifikátu

Převzetí certifikátu bezprostředně navazuje na proces podání a zpracování žádosti.

Operátor registračního místa připraví Smlouvu o vydání a používání kvalifikovaného certifikátu pro elektronickou pečeť, jejíž součástí je i protokol o převzetí certifikátu. Smlouva uvádí mimo jiné i tyto informace:

- Identifikační údaje žadatele
- Identifikační údaje právnické osoby, která je držitelem certifikátu
- Identifikační údaje TSA serveru, pro který byl certifikát vydán
- Podstatné údaje o vydaném certifikátu: sérové číslo, identifikační údaje, datum platnosti, otisk veřejného klíče, identifikátor certifikační politiky apod…
- Identifikační údaje operátora registračního místa
- Informační klauzule, povinnosti žadatele
- Prohlášení o převzetí certifikátu žadatelem

Žadatel svým podpisem potvrdí převzetí vydaného certifikátu; na základě toho obdrží od operátora registračního místa soubor s certifikátem.

Pokud žadatel odmítne převzít certifikát, pak operátor registračního místa požádá o zneplatnění vydaného certifikátu.

3.4.2 Zveřejnění certifikátu certifikační autoritou

Certifikáty vydané podle této CP jsou volně dostupné pro spoléhající se strany na webové stránce https://www.kb.cz/pki a také na důvěryhodném seznamu dle nařízení eIDAS.

3.4.3 Oznámení o vydání certifikátu jiným subjektům

Informace o vydání certifikátu není oznamována jiným subjektům.

3.5 POUŽITÍ KLÍČOVÉHO PÁRU A CERTIFIKÁTU

3.5.1 Soukromý klíč držitele a přípustné použití certifikátu

Klíčový pár certifikátu, vydaného podle této certifikační politiky, musí být vytvořen a uložen v kvalifikovaném prostředku pro vytváření elektronických pečetí. Generování klíčového páru musí být přítomen zástupce kvalifikovaného poskytovatele služeb vytvářejících důvěru, viz kapitolu 3.1.2.1. O vygenerování klíčového páru musí být vyhotoven protokol, který je pak jedním z podkladů pro podání žádosti.

Držitel certifikátu se zavazuje:

- Dodržovat veškerá relevantní ustanovení této certifikační politiky a dalších souvisejících ujednání KB, jako je Smlouva o vydání a používání kvalifikovaného certifikátu pro elektronickou pečeť, obchodní podmínky apod…
- Používat soukromý klíč s certifikátem, vydaným podle této CP, pouze pro účely stanovené v této CP – viz kapitolu 1.4.1.
- Nakládat se soukromým klíčem v souladu s touto certifikační politikou tak, aby nemohlo dojít k jeho odcizení či zneužití.
- V případě ztráty, odcizení nebo podezření na zneužití soukromého klíče bezodkladně požádat o zneplatnění certifikátu a ukončit používání takového soukromého klíče.
- V případě změny platnosti údajů, uvedených v certifikátu, oznámit tyto změny kvalifikovanému poskytovateli služeb vytvářejících důvěru.

Držitel se navíc zavazuje přiměřeným způsobem splnit požadavky přílohy II [EIDAS].

3.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strana je před použitím certifikátu, vydaného podle této certifikační politiky povinna:

- Získat nadřízené certifikáty PKI systému KB, které jsou v hierarchii certifikátu, z důvěryhodného zdroje (např. webové stránky kvalifikovaného poskytovatele služeb vytvářejících důvěru).
- Před použitím certifikátu ověřit jeho platnost, stejně jako platnost certifikátů certifikačních autorit, vůči aktuálnímu seznamu zneplatněných certifikátů (CRL) nebo službou OCSP.
- Zvážit vhodnost použití certifikátu k zamýšlenému účelu.
- Dodržovat ustanovení této certifikační politiky, která se vztahují k používání certifikátu.

3.6 OBNOVENÍ CERTIFIKÁTU

Obnovením certifikátu se rozumí vydání dalšího certifikátu k témuž klíčovému páru. Tato funkčnost není podporována. Nelze vydat certifikát s veřejným klíčem, který již byl obsažen v jiném certifikátu.

3.6.1 Podmínky pro obnovení certifikátu

Služba obnovení certifikátu není poskytována.

3.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Služba obnovení certifikátu není poskytována.

3.6.3 Zpracování požadavku na obnovení certifikátu

Služba obnovení certifikátu není poskytována.

3.6.4 Oznámení o obnovení certifikátu držiteli certifikátu

Služba obnovení certifikátu není poskytována.

3.6.5 Úkony spojené s převzetím obnoveného certifikátu

Služba obnovení certifikátu není poskytována.

3.6.6 Zveřejňování obnovených certifikátů

Služba obnovení certifikátu není poskytována.

3.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

Služba obnovení certifikátu není poskytována.

3.7 VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU

Vydáním následného certifikátu se rozumí vydání nového certifikátu s jiným klíčovým párem, přičemž nový certifikát obsahuje totožné identifikační údaje v položkách předmět a alternativní název.

Při vydání následného certifikátu se nevyužívá jiný certifikát držitele. Žádost o nový certifikát není autorizována podpisem, vytvořeným pomocí soukromého klíče stávajícího certifikátu držitele. Žadatel o následný certifikát nemusí mít v držení platný certifikát. Z uvedených důvodů platí pro vydání následného certifikátu stejné podmínky, jako pro vydání prvního certifikátu.

3.7.1 Podmínky pro vydání následného certifikátu

Podmínky pro vydání následného certifikátu jsou popsány v kapitole 2.7.

3.7.2 Subjekty oprávněné požadovat následný certifikát

Žádost o následný certifikát může podat žadatel, který splňuje podmínky uvedené v kapitole 3.1.1.

3.7.3 Zpracování požadavku o následný certifikát

Postup zpracování požadavku o následný certifikát je shodný s postupem zpracování prvního certifikátu – viz kapitoly 3.2 a 3.3.1.

3.7.4 Oznámení žadateli o vydání následného certifikátu

Platí stejné ustanovení, jako pro vydání prvního certifikátu – viz kapitolu 3.3.2.

3.7.5 Úkony spojené s převzetím následného certifikátu

Platí stejné ustanovení, jako pro převzetí prvního certifikátu – viz kapitolu 3.4.1.

3.7.6 Zveřejnění následného certifikátu certifikační autoritou

Stejně jako první vydané certifikáty nejsou zveřejňovány ani následné certifikáty – viz také kapitolu 3.4.2.

3.7.7 Oznámení o vydání certifikátu jiným subjektům

Platí stejné ustanovení, jako pro první vydaný certifikát – viz kapitolu 3.4.3.

3.8 ZMĚNA ÚDAJŮ V CERTIFIKÁTU

Změnou údajů v certifikátu se rozumí vydání dalšího certifikátu pro stejného držitele, přičemž nově vydaný certifikát obsahuje jiné identifikační údaje anebo jiné atributy certifikátu (např. účel použití certifikátu apod…).

3.8.1 Podmínky pro změnu údajů v certifikátu

Vydání každého certifikátu podle této certifikační politiky je zpracováváno stejně jako vydání prvotního certifikátu. Při vydání certifikátů není žádným způsobem zohledňována vazba na jiné certifikáty, které mohly být dříve vydány stejnému držiteli. Z uvedených důvodů jsou podmínky pro vydání certifikátu se změněnými údaji stejné, jako podmínky pro vydání prvního certifikátu. Žadatel musí příslušným způsobem doložit platnost údajů v žádosti o certifikát.

3.8.2 Subjekty oprávněné žádat změnu údajů

O změnu údajů v certifikátů žádá držitel prostřednictvím zmocněného žadatele. Žadatel musí splnit podmínky pro podání žádosti o certifikát podle této CP, mimo jiné musí být zmocněn příslušnou právnickou osobou k podání žádosti o certifikát – viz také kapitolu 2.6.5.

3.8.3 Zpracování požadavku na změnu údajů v certifikátu

Zpracování certifikátu se změněnými údaji probíhá stejně, jako zpracování žádosti o prvotní certifikát – viz kapitolu 3.2.

3.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Platí stejné ustanovení, jako pro vydání prvního certifikátu – viz kapitolu 3.3.2.

3.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Platí stejné ustanovení, jako pro převzetí prvního certifikátu – viz kapitolu 3.4.1.

3.8.6 Zveřejňování certifikátů se změněnými údaji

Stejně jako první vydané certifikáty nejsou zveřejňovány ani certifikáty se změněnými údaji – viz také kapitolu 3.4.2.

3.8.7 Oznámení o vydání certifikátu jiným subjektům

Platí stejné ustanovení, jako pro první vydaný certifikát – viz kapitolu 3.4.3.

3.9 ZNEPLATNĚNÍ A POZASTAVENÍ PLATNOSTI CERTIFIKÁTU

Platnost certifikátu je ukončena v okamžiku jeho zneplatnění certifikační autoritou. Od okamžiku zneplatnění v CA poskytuje služba OCSP spoléhajícím se stranám informaci, že byl daný certifikát zneplatněn. Informace o zneplatnění certifikátu se také objeví na dalším vydaném seznamu zneplatněných certifikátů (CRL).

V době mezi zneplatněním certifikátu a vydáním dalšího seznamu zneplatněných certifikátů (CRL) tedy služba OCSP již vrací informaci o zneplatnění certifikátu, zatímco služba CRL ještě ne. V takovém případě je platná informace o zneplatnění certifikátu ze služby OCSP. Tento rozpor bude trvat nejdéle 1 hodinu a bude automaticky vyřešen vydáním následujícího CRL.

Pokud nedojde ke zneplatnění certifikátu po dobu jeho platnosti, skončí platnost certifikátu v čase uvedeném v certifikátu.

Zneplatnění certifikátu je nevratné. Certifikát, který byl zneplatněn, nelze uvést zpět do platného stavu.

3.9.1 Podmínky pro zneplatnění certifikátu

Důvody pro zneplatnění certifikátu jsou následující:

- Podezření z kompromitace či odcizení odpovídajícího soukromého klíče, včetně kompromitace, ztráty, odcizení či zničení technického prostředku, který soukromý klíč chrání
- Ukončení provozu zařízení, v němž je obsažen soukromý klíč, resp. ukončení potřeby generovat časová razítka
- Žádost držitele certifikátu
- Porušení ustanovení certifikační politiky ze strany držitele certifikátu

- Zánik právnické osoby držitele, popř. podstatná změna legálního statusu držitele
- Změna jména právnické osoby držitele, nebo jiných identifikačních údajů držitele, uvedených v certifikátu
- Dojde ke kompromitaci soukromého klíče CA, která certifikát vydala
- Rozhodnutí CA ve zdůvodněných případech, např.
  - když nastanou skutečnosti uvedené v právní úpravě pro služby vytvářející důvěru nebo příslušných technických standardech a normách,
  - při neočekávaném vývoji kryptoanalytických metod,
  - z důvodu vyšší moci.
- Požadavek orgánu dohledu, na základě § 13 odst. 2 zákona č. 297/2016 Sb.

3.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat:

- Kvalifikovaný poskytovatel služeb vytvářejících důvěru, ve zdůvodněných případech:
  - Správce TSA serveru (pracovník kvalifikovaného poskytovatele služeb vytvářejících důvěru), pro který byl vydán certifikát
  - Správce certifikátů
  - Manažer PKI
  - Manažer bezpečnosti PKI
  - Orgán dohledu, na základě § 13 odst. 2 zákona č. 297/2016 Sb.

3.9.3 Postup zneplatnění certifikátu

1 O zneplatnění certifikátu může rozhodnout kvalifikovaný poskytovatel služeb vytvářejících důvěru, jako držitel certifikátu, např. pokud získá věrohodnou informaci o některém z důvodů uvedených v kapitole 3.9.1. Zneplatnění může být také požadováno orgánem dohledu.

Pověřený pracovník kvalifikovaného poskytovatele služeb vytvářejících důvěru v takovém případě zneplatní certifikát držitele: pracovník se autentizuje k příslušné softwarové aplikaci, vyhledá certifikát a označí jej jako zneplatněný.

CA v takovém případě informuje držitele o zneplatnění certifikátu s udáním důvodu zneplatnění. Pro kontakt držitele použije CA údaje žadatele, popř. oficiální kontaktní údaje držitele (tzn. organizace).

3.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Požadavek na zneplatnění je třeba vznést bezodkladně po identifikaci skutečnosti, která je důvodem pro zneplatnění certifikátu.

V případě, že o zneplatnění rozhodnul kvalifikovaný poskytovatel služeb vytvářejících důvěru, může být součástí rozhodnutí i plánovaná doba zneplatnění (odklad).

3.9.5 Doba, ve které musí dojít k zneplatnění certifikátu

Doba mezi vznesením požadavku a zneplatněním certifikátu, se pro jednotlivé postupy liší (viz také kapitolu 3.9.3):

- Pokud se certifikát zneplatňuje z vůle kvalifikovaného poskytovatele služeb vytvářejících důvěru, je certifikát označen jako zneplatněný k určenému budoucímu datu zneplatnění.
- Pokud se certifikát zneplatňuje na základě požadavku orgánu dohledu, je certifikát označen jako zneplatněný bez zbytečného prodlení od obdržení požadavku.

Od okamžiku, kdy je certifikát v evidenci označen jako zneplatněný, poskytuje služba OCSP informaci o zneplatnění certifikátu.

Po označení certifikátu jako zneplatněného je daný certifikát uveden na nejbližším publikovaném CRL. Seznam zneplatněných certifikátů (CRL) s tímto certifikátem bude zveřejněn nejpozději 24 hodin

- od přijetí požadavku – v případě že o zneplatnění požádal orgán dohledu,
- od stanovaného času zneplatnění – v případě, že o zneplatnění rozhodnul kvalifikovaný poskytovatel služeb vytvářejících důvěru.

3.9.6 Povinnosti spoléhajících se stran při ověřování, zda byl certifikát zneplatněn

Spoléhající se strany musí při ověřování platnosti certifikátu provádět úkony popsané v kapitole 3.5.2.

3.9.7 Periodicita vydávání seznamu zneplatněných certifikátů (CRL)

Seznam zneplatněných certifikátů se vydává do 1 hodiny od označení certifikátu jako zneplatněného. Nedojde-li ke zneplatnění žádného certifikátu, je nový seznam zneplatněných certifikát obvykle vydán 8 hodin od předchozího seznamu, nejvýše však 24 hodin od vydání předchozího seznamu zneplatněných certifikátů.

Seznam zneplatněných certifikátů (CRL) je vydáván s dobou platnosti 1 den.

Pokud vyprší platnost zneplatněného certifikátu, je z následných CRL vypuštěn.

3.9.8 Maximální zpoždění při zveřejnění seznamu zneplatněných certifikátů (CRL)

Seznamy zneplatněných certifikátů (CRL) jsou zveřejňovány bez zbytečného odkladu ihned po jejich vydání.

CRL je vždy vydán nejvýše 24 hodin od vydání předchozího CRL.

3.9.9 Možnost ověřování statutu certifikátu online

Služba OCSP pro ověřování stavu certifikátu je spoléhajícím se stranám dostupná po síti, na adrese uvedené v certifikátu. Viz také kapitolu 3.10.2.

Formát OCSP odpovědí je v souladu s normami RFC 2560 a RFC 6960.

Certifikát služby OCSP obsahuje rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 2560. Nevyžaduje se ověřování stavu zneplatnění certifikátu služby OCSP.

3.9.10 Požadavky na ověřování statutu certifikátu online

Ověření stavu certifikátu službou OCSP mohou použít všechny participující subjekty i spoléhající se strany.

3.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Informace o zneplatnění jsou poskytovány službou OCSP a prostřednictvím seznamu zneplatněných certifikátů (CRL). Jiné formy poskytování informací o zneplatnění nejsou podporovány.

3.9.12 Zvláštní postupy při kompromitaci klíče

Postup pro zneplatnění certifikátu v případě kompromitace soukromého klíče se neliší od výše popsaného postupu pro zneplatnění certifikátu.

3.9.13 Podmínky pro pozastavení platnosti certifikátu

Certifikátům vydaným podle této CP nelze pozastavit platnost.

3.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu není podporováno.

3.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu není podporováno.

3.9.16 Omezení doby pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu není podporováno.

3.10 SLUŽBY SOUVISEJÍCÍ S OVĚŘOVÁNÍM STAVU CERTIFIKÁTU

Pro ověření stavu vydaných certifikátů lze využít:

- seznam zneplatněných certifikátů (CRL)
- online službu pro zjišťování stavu certifikátu (OCSP).

Uvedené mechanismy jsou dostupné všem participujícím subjektům i spoléhajícím se stranám.

3.10.1 Funkční charakteristiky

Platný seznam zneplatněných certifikátů (CRL) je dostupný ke stažení protokolem HTTP z webového serveru provozovaného Komerční bankou. Adresa (URL), z níž lze získat aktuální CRL, je uvedena ve vydaném certifikátu.

Služba OCSP je dostupná na adrese uvedené ve vydaném certifikátu. Ke komunikaci se službou OCSP se využívá protokol HTTP.

3.10.2 Dostupnost služeb

Seznam zneplatněných certifikátů je k dispozici nepřetržitě v režimu provozu 24 hodin denně 7 dní v týdnu.

Služba OCSP je dostupná nepřetržitě v režimu provozu 24 hodin denně 7 dní v týdnu.

3.10.3 Další charakteristiky služeb stavu certifikátu

V případě, že se kvalifikovaný poskytovatel služeb vytvářejících důvěru rozhodne ukončit provozování služby CRL, bude poslední CRL obsahovat v položce nextUpdate hodnotu „99991231235959Z“.

3.11 UKONČENÍ POSKYTOVÁNÍ SLUŽEB PRO DRŽITELE CERTIFIKÁTU

Certifikáty podle této certifikační politiky jsou vydávány pro Komerční banku, jako kvalifikovaného poskytovatele služeb vytvářejících důvěru. (Certifikáty podle této CP vydává kvalifikovaný poskytovatel služeb vytvářejících důvěru pouze sám pro sebe.)

Kvalifikovaný poskytovatel služeb vytvářejících důvěru může rozhodnout o ukončení vydávání certifikátů podle této CP. Pokud bude v době ukončení poskytování služby existovat platný certifikát vydaný podle této CP, bude takový certifikát zneplatněn.

CA bude poskytovat informace o stavu certifikátu i po ukončení poskytování služeb držiteli, a to nejméně po dobu platnosti, uvedené v certifikátu.

3.12 ÚSCHOVA A OBNOVA KLÍČŮ

Kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje službu úschovy klíčů.

3.12.1 Zásady a postupy pro úschovu a obnovu soukromých klíčů

Kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje službu úschovy klíčů.

3.12.2 Zásady a postupy zapouzdření klíče a jeho obnovení

Kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje službu úschovy klíčů.

4 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

4.1 FYZICKÉ ZABEZPEČENÍ

4.1.1 Umístění a konstrukce

Certifikační autority, TSA servery a podpůrné centrální systémy jsou umístěny v prostorách datových center kvalifikovaného poskytovatele služeb vytvářejících důvěru. Tato pracoviště jsou proti neoprávněnému vniknutí chráněna mechanickými prostředky a bezpečnostní službou. Je zpracována bezpečnostní dokumentace stanovující požadavky na fyzickou bezpečnost těchto prostor.

Klíčové části systémů kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou duplikovány do dvou geograficky oddělených lokalit. V případě výpadku systémů v jedné lokalitě převezmou provoz systémy v druhé lokalitě.

Mimo datová centra se nacházejí pouze administrátorské a operátorské počítače, které umožňují dálkový přístup k centrálním systémům kvalifikované poskytovatele služeb vytvářejících důvěru.

4.1.2 Fyzický přístup

Všechny části systému kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou rozděleny do bezpečnostních perimetrů s definovanými vlastnostmi a požadavky na bezpečnost. Pro ochranu každého z perimetrů jsou přijata příslušná opatření pro řízení přístupu.

Přístup do datových center, která hostují certifikační autority a podpůrné centrální systémy, 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 pracovníkovi udělen na základě dvoustupňového schvalování. Seznam oprávněných uživatelů je průběžně aktualizován.

Pracoviště administrátorů a operátorů, včetně registračního místa jsou umístěna v kancelářských budovách kvalifikovaného poskytovatele služeb vytvářejících důvěru. Přístup do prostor kvalifikovaného poskytovatele je řízený a chráněný. Pro přístup je vyžadována identifikace bezkontaktní čipovou kartou. Seznam akceptovaných čipových karet je průběžně aktualizován.

4.1.3 Elektřina a klimatizace

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

4.1.4 Vliv vody

Datová centra kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou umístěna mimo zátopové oblasti.

4.1.5 Protipožární opatření a ochrana

Datová centra kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou vybavena elektronickou požární signalizací. Signalizace je vyvedena na pracoviště obsazené nepřetržitě 24x7.

4.1.6 Ukládání médií

Záložní fyzická média jsou uchovávána v chráněných skříních datových center.

4.1.7 Nakládání s odpady

Papírové dokumenty a média používaná v souvislosti s certifikačními službami jsou v případě nepotřebnosti likvidována bezpečným způsobem.

4.1.8 Zálohy mimo budovu

Všechny podstatné systémy kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou provozovány redundantně ve dvou datových centrech. Duplikace je primárním mechanismem pro zajištění kontinuity provozu v případě výpadku jednoho datového centra.

Zálohy vybraných aktiv jsou uloženy mimo datová centra, v souladu s interními pokyny Manažera PKI.

4.2 PROCESNÍ BEZPEČNOST

4.2.1 Důvěryhodné role

Pro správu a provoz certifikačních služeb jsou definovány bezpečnostní role, které vycházejí z příslušných technických standardů. Kvalifikovaný poskytovatel služeb vytvářejících důvěru má vytvořena pravidla pro obsazování osob do těchto rolí, pro jmenování a odvolávání pracovníků. Oprávnění přístupu (na úrovni fyzického a logického přístupu k informačním aktivům certifikačních autorit) jsou založena na těchto bezpečnostních rolích.

4.2.2 Počet osob požadovaných pro jednotlivé činnosti

Nominace pracovníků do rolí pro správu a provoz certifikačních služeb 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 certifikačních služeb mohou pracovníci v definovaných rolích provádět samostatně s výjimkou následujících kroků (v závorce uvedený nutný počet osob potřebných k provedení operace):

- Vydání / obnova certifikátu certifikační autority (2 osoby)
- Start / restart / aktivace certifikační autority (2 osoby)
- Start / restart / aktivace služby pro generování CRL (2 osoby)
- Rušení soukromých klíčů certifikační autority (2 osoby)

4.2.3 Identifikace a ověření pro každou roli

Představitel každé bezpečnostní role se musí před přístupem k informačním aktivům kvalifikovaného poskytovatele služeb vytvářejících důvěru nejprve identifikovat a autentizovat. Každý z pracovníků má přiděleny jednoznačné identifikační údaje k systémům, k nimž má z titulu své role přístup.

Pro přístup k systémům se používá ověření pomocí jména a hesla a/nebo dvoufaktorové ověření. Pro použití hesel jsou nastaveny politiky, které vynucují délku, kvalitu a pravidelnou obnovu hesel. Pro kritické části informačních systémů se navíc vyžaduje aktivní spolupráce více pracovníků (tzv. princip 4 očí, zajišťující vzájemnou kontrolu nad prováděnou operací).

4.2.4 Role vyžadující rozdělení povinností

V interní dokumentaci kvalifikovaného poskytovatele služeb vytvářejících důvěru 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.

Administrátorské role pro správu certifikační autority jsou personálně odděleny od operátorských rolí pro správu certifikátů.

4.3 PERSONÁLNÍ BEZPEČNOST

4.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Role zajišťující chod a správu certifikačních služeb jsou dle existujících procedur obsazovány důvěryhodnými a zkušenými pracovníky. Tito pracovníci nesmějí být ve střetu zájmů, který by ohrozil nestrannost kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Obdobné procedury platí i pro spolupráci s externími subjekty (dodavateli).

4.3.2 Posouzení spolehlivosti osob

Do rolí správy certifikačních služeb jsou jmenovány osoby, které patří mezi zaměstnance provozovatele certifikačních služeb a které mají dobré pracovní i osobní reference. U externích dodavatelů se uplatňují stejná měřítka zakotvená ve smluvním vztahu.

4.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

4.3.4 Požadavky a periodicita školení

Školení pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru je organizováno při změnách v nástrojích, konfiguraci či postupech správy a pro rutinní či základní činnosti v pravidelných intervalech s odstupem maximálně 2 let.

Školení pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru týkající se aktuálních bezpečnostních postupů a nových hrozeb je uskutečňováno s odstupem maximálně 1 roku.

Forma školení je buď osobní, nebo e-learning, ve vybraných případech je zakončena testem znalostí.

4.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Nestanovuje se.

4.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

4.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

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

4.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci udržující chod a spravující certifikační služby mají k dispozici následující dokumentaci:

- Certifikační prováděcí směrnice
- Certifikační politiky
- Provozní dokumentace
- Havarijní plány a plány obnovy
- Specifikace systému
- Příručky pro obsluhu
- Technické normy

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

4.4 AUDITNÍ ZÁZNAMY

4.4.1 Typy zaznamenávaných událostí

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

Mezi auditovanými událostmi jsou např. systémové změny v klíčových modulech, start/restart služeb, podání žádosti o certifikát, vydání certifikátu či CRL, atd…

Významné operace, prováděné ceremoniálně, jsou zaznamenávány na papírových protokolech podepsaných účastníky operace.

Auditní události umožňují prokázat účast a zodpovědnost jednotlivých pracovníků na vzniklých událostech. Umožňují také dohledat a vyhodnotit sled a návaznosti událostí.

Kromě auditních záznamů jsou shromažďovány také záznamy o provozu významných částí systému kvalifikovaného poskytovatele služeb vytvářejících důvěru. Provozní záznamy slouží primárně pro detekci a analýzu problémových stavů systému.

4.4.2 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.

V případě zjištění bezpečnostního incidentu jsou auditní události bezodkladně kontrolovány a vyhodnocovány pověřenými pracovníky kvalifikovaného poskytovatele služeb vytvářejících důvěru.

4.4.3 Doba uchování auditních záznamů

Auditní i provozní záznamy vznikají v jednotlivých částech infomačního systému CA. Bezprostředně po vzniku ve zdrojovém systému jsou auditní záznamy automaticky přeneseny do nezávislého centrálního úložiště.

Auditní i provozní záznamy jsou v centrálním úložišti ponechány do doby, než jsou archivovány v souladu s kapitolou 5.5.2.

4.4.4 Ochrana auditních záznamů

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

Elektronické auditní záznamy jsou uloženy v dedikovaném systému s řízeným přístupem. Záznamy nelze v úložišti modifikovat. Mazání auditních záznamů je povoleno výhradně pověřeným pracovníkům a v souladu se skartačním řádem. Pracovníci, kteří jsou oprávněni mazat auditní záznamy, nesmí být členy žádné jiné role kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Papírové auditní záznamy jsou uloženy u pověřených pracovníků, v chráněném úložišti.

4.4.5 Postupy pro zálohování auditních záznamů

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

Po přenesení do centrálního úložiště jsou auditní záznamy hostovány na dvou geograficky oddělených úložištích. Úložiště je navíc pravidelně zálohováno do nezávislého média.

Auditní události v papírové formě se archivují. Podstatné papírové protokoly jsou vytvořeny ve více originálech a chráněny v odlišných úložištích.

4.4.6 Systém shromažďování auditních záznamů

Auditní záznamy jsou shromažďovány v dedikované centrální databázi. Centrální úložiště je provozováno Komerční bankou v rámci interních systémů. Kromě záznamů kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou v centrální databázi uloženy také auditní záznamy jiných systémů, provozovaných v Komerční bance. Jsou implementována pravidla pro oddělení auditních záznamů, vzniklých v různých systémech. Pro auditní záznamy každého systému jsou definovány specifické skupiny pracovníků, kteří mají k záznamům daného systému přístup.

Každý auditní záznam obsahuje alespoň informace o serveru, který jej generoval, času, datu a identifikaci události. Většina záznamů obsahuje také rozšiřující informace.

4.4.7 Postup při oznamování událostí subjektu, který ji způsobil

Subjektu, který způsobil událost zaznamenanou v auditním logu, není taková skutečnost kvalifikovaným poskytovatelem služeb vytvářejících důvěru oznamována.

4.4.8 Hodnocení zranitelnosti

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

4.5 UCHOVÁVÁNÍ ZÁZNAMŮ

4.5.1 Typy záznamů

Uchovávají se následující typy záznamů:

- Záznamy související s životním cyklem certifikátů, vč. žádostí o certifikáty, vydaných certifikátů a metadat spojených s žádostí a certifikátem
- Vydané CRL
- Papírové protokoly, např. předávací protokoly aktiv, záznam ceremonií apod…
- Relevantní dokumentace
- Provozní záznamy a auditní záznamy
- Programové vybavení a konfigurace klíčových částí informačního systému kvalifikovaného poskytovatele služeb vytvářejících důvěru

4.5.2 Doba uchování záznamů

Kvalifikovaný poskytovatel služeb vytvářejících důvěru uchovává dokumenty a data související s vydáváním a životním cyklem certifikátů na základě paragrafu 3 zákona 297/2016 Sb., O službách vytvářejících důvěru pro elektronické transakce po dobu 10 let. Po ukončení této doby uchovává kvalifikovaný poskytovatel po dobu následujících 15 let údaje na základě kterých byla ověřena totožnost žadatele.

Dokumentace, certifikáty CA, CRL a programové vybavení se uchovává minimálně po dobu provozu certifikační autority *Komerční banka Qualified CA/RSA*.

Provozní záznamy jsou uchovány po dobu, po kterou lze předpokládat použití těchto záznamů k řešení provozních problémů. (Přesná doba je definována interními směrnicemi Komerční banky.)

4.5.3 Ochrana úložiště záznamů

Způsoby ochrany úložiště záznamů se pro jednotlivé typy záznamů liší. Vždy je ale zajištěno řízení přístupu k záznamům, vč. ochrany proti neoprávněné manipulaci či smazání záznamů:

- Záznamy související s životním cyklem certifikátů jsou uloženy redundantně v centrálním systému certifikační autority. Přístup k údajům mají výhradně pověření pracovníci.
- Vydané CRL jsou uloženy redundantně v centrálním systému certifikační autority. Přístup k údajům mají výhradně pověření pracovníci.
- Papírové protokoly jsou uloženy u pracovníků, pověřených archivací jednotlivých typů protokolů.
- Dokumentace je uložena v interních úložištích Komerční banky, vyhrazených pro dokumentaci.
- Provozní záznamy a auditní záznamy jsou uloženy redundantně v centrálním úložišti Komerční banky. Přístup k záznamům je řízený.
- Verze programového vybavení a konfigurace jsou uloženy v dedikovaném úložišti s řízeným přístupem. Úložiště je vybaveno mechanismem sledování změn.

4.5.4 Postupy při zálohování záznamů

Elektronické záznamy jsou ukládány redundantně ve dvou datových centrech Komerční banky, v geograficky oddělených lokalitách. Každé úložiště elektronických záznamů je navíc pravidelně zálohováno na nezávislá média. Přístup k záložním médiím mají výhradně pověření pracovníci. Zálohovací procedury se řídí interními směrnicemi Komerční banky.

4.5.5 Požadavky na použití časových razítek při uchovávání záznamů

Všechny uchovávané záznamy obsahují informaci o času vzniku události. Pro generování časových údajů o vzniku událostí se používá interní časový zdroj, synchronizovaný v rámci prostředí Komerční banky nejméně jednou za 24 hodin.

Při označování časových údajů v záznamech se nepoužívají časová razítka.

4.5.6 Systém shromažďování uchovávaných záznamů

Elektronické záznamy jsou uchovávány v datacentrech Komerční banky. Zálohy elektronických záznamů jsou ukládány v souladu s interními směrnicemi Komerční banky.

4.5.7 Postup získání a ověření uchovávaných informací

Přístup k uchovávaným záznamům mají pověření pracovníci kvalifikovaného poskytovatele služeb vytvářejících důvěru a subjekty vykonávající audit či kontrolu. Přístup je umožněn po úspěšné autentizaci a ověření oprávnění.

Záznamy týkající se provozu služeb budou zpřístupněny za účelem poskytnutí důkazu o správném fungování certifikačních služeb pro účely soudního řízení.

4.6 VÝMĚNA KLÍČE

Doba platnosti certifikátu certifikační autority *Komerční banka Qualified CA/RSA* je 10 let. Maximální doba platnosti certifikátů vydávaných z *Komerční banka Qualified CA/RSA* je 6 let.

CA nevydá certifikát, který by měl platnost delší než platnost certifikátu CA. Klíče certifikační autority *Komerční banka Qualified CA/RSA* jsou nahrazeny novými klíči (tzn. je vydán nový certifikát) nejpozději 6 let před vypršením platnosti certifikátu. Pokud je rozhodnuto o ukončení činnosti CA, pak se další výměna klíčů neprovede.

Certifikáty pro *Komerční banka Qualified CA/RSA* jsou vydávány z kořenové *KB Root 3 CA*.

Každý nový certifikát certifikační autority *Komerční banka Qualified CA/RSA* je po svém vydání a schválení orgánem dohledu umístěn na publikační místa a dán k dispozici spoléhajícím se stranám. (Seznam publikačních míst je uveden v kapitole 2.2.1).

Nově vydaný certifikát CA je aktivován a uveden do provozu na základě pokynu Manažera PKI – poté, co uplyne dostatečně dlouhá doba pro distribuci nově vydaného certifikátu spoléhajícím se stranám.

V období mezi vydáním nového certifikátu CA a uvedením tohoto certifikátu do produkčního provozu, jsou koncové certifikáty podepisovány soukromým klíčem předchozího certifikátu CA. Po uvedení nově vydaného certifikátu CA do produkčního provozu jsou koncové certifikáty podepisovány soukromým klíčem příslušným k novému certifikátu CA.

V nestandardních případech (např. vývoj kryptoanalytických metod) může být certifikát CA obnoven dříve, než je výše uvedený interval.

4.7 OBNOVA PO HAVÁRII A KOMPROMITACI

Pro poskytování certifikačních služeb 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 kvalifikovaného poskytovatele služeb vytvářejících důvěru.

4.7.1 Postup v případě incidentu a kompromitace

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

4.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Všechny podstatné části systému kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou pravidelně zálohovány. Podstatné části jsou provozovány redundantně. Vytvořené zálohy obsahují jednotlivé součásti certifikačních služeb, 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.

4.7.3 Postupy při kompromitaci soukromého klíče

V případě důvodného podezření na kompromitaci soukromého klíče certifikační autority *Komerční banka Qualified CA/RSA* bude mimořádně ukončena její činnost. O vzniklé situaci bude bezodkladně informován orgán dohledu.

Oznámení o ukončení činnosti, včetně důvodů a dalším postupu, pokud nastane, bude zveřejněno na webové stránce na adrese https://www.kb.cz/pki. Držitelé certifikátů budou na tento stav upozorněni prostřednictvím kontaktních údajů žadatelů a také prostřednictvím oficiálních kontaktních údajů dané organizace.

Obratem bude zneplatněn certifikát certifikační autority a všech vydaných platných certifikátů. Bude zveřejněn nový seznam CRL, což zneplatní všechny certifikáty vydané touto CA.

Certifikační autorita *Komerční banka Qualified CA/RSA* bude poté zničena (odinstalovány certifikační služby a operační systém, bezpečně zničeny soukromé klíče CA, včetně záloh soukromých klíčů). O ukončení činnosti a zničení CA bude pořízen zápis.

Popsaný postup bude použit také v případě náhlého rozvoje kryptoanalytických metod, které by mohly oslabit používané kryptografické algoritmy a zpochybnit důvěryhodnost vydávaných certifikátů.

4.7.4 Schopnost obnovení činnosti po havárii

Při zvládání havárie a uvádění CA zpět do rutinního provozu se postupuje v souladu s havarijními plány a plány kontinuity.

Pokračování procesů certifikační autority po havárii závisí na typu havárie a jejích následcích a je věcí rozhodnutí Manažera PKI.

4.8 UKONČENÍ ČINNOSTI CA NEBO RA

4.8.1 Řádné ukončení činnosti CA

Nenastanou-li mimořádné okolnosti (viz kapitola 4.8.3), bude činnost certifikační autority ukončena v okamžiku, kdy:

- Všem vydaným certifikátům vypršela platnost
- Vypršela platnost posledního (nejnovějšího) certifikátu CA

O ukončení činnosti bude informován orgán dohledu, s nejméně tří-měsíčním předstihem.

Držitelům se s dostatečným předstihem dá na vědomí, že CA přestává vydávat certifikáty. Vydané certifikáty zůstanou v platnosti, dokud nedojde k jejich expiraci, příp. k jejich zneplatnění. CA bude po celou dobu (do expirace certifikátu CA) pravidelně vydávat CRL a poskytovat službu OCSP.

Po expiraci certifikátu CA budou komponenty certifikační služby odebrány (odinstalovány certifikační služby a operační systém, bezpečně zničeny soukromé klíče CA, včetně záloh soukromých klíčů). O ukončení činnosti a zničení klíčů CA bude pořízen zápis.

Záznamy CA budou uchovány v souladu s ustanovením kapitoly 4.5.

4.8.2 Odnětí statusu kvalifikovaného poskytovatele služeb vytvářejících důvěru

Pokud orgán dohledu odejme status kvalifikovaného poskytovatele služeb vytvářejících důvěru, pak budou o této skutečnosti informováni držitelé platných certifikátů. Držitelé budou informováni

prostřednictvím kontaktních údajů dodaných v podkladech žádostí, zejména e-mailových adres žadatele a držitele. Informace budou uvedeny také na webové stránce na adrese https://www.kb.cz/pki

Součástí publikovaných informací bude také plán dalšího postupu, včetně informací o příp. dopadech na platnost certifikátů.

4.8.3 Mimořádné ukončení činnosti CA

V případě mimořádného ukončení činnosti bude snahou kvalifikovaného poskytovatele služeb vytvářejících důvěru:

- Neprodleně informovat orgán dohledu.
- Co nejdříve (pokud možno s předstihem) informovat držitele platných certifikátů o ukončení činnosti CA, prostřednictvím e-mailových zpráv a na webové stránce na adrese https://www.kb.cz/pki.
- K určenému datu zneplatnit všechny platné certifikáty a vydat finální CRL

Kvalifikovaný poskytovatel služeb vytvářejících důvěru zajistí prokazatelné zničení certifikační autority (odinstaluje certifikační služby a operační systém, bezpečně zničeny soukromé klíče CA, včetně záloh soukromých klíčů). O ukončení činnosti a zničení CA bude pořízen zápis.

Záznamy CA budou uchovány v souladu s ustanovením kapitoly 4.5.

4.8.4 Ukončení činnosti RA

Registrační místo, jehož prostřednictvím se vydávají certifikáty podle této certifikační politiky, zůstává v provozu po celou dobu poskytování tohoto typu certifikátů. Umístění registračního místa se může v čase měnit; držitelé a žadatelé jsou o umístění informování interními komunikačními kanály KB.

5 TECHNICKÁ BEZPEČNOST

5.1 GENEROVÁNÍ A INSTALACE KLÍČOVÉHO PÁRU

5.1.1 Generování klíčového páru

Kryptografický pár klíčů vydávající certifikační autority je generován a uložen v externím hardwarovém modulu (HSM) certifikovaném podle standardu Common Criteria na úroveň EAL4+.

Pro generování i aktivaci soukromého klíče CA v HSM jsou nutné dvě čipové karty a autorizace pomocí kódu PIN. Při aktivaci soukromého klíče musí aktivně spolupracovat držitelé dvou čipových karet. Soukromý klíč certifikační autority nelze exportovat mimo modul HSM.

Klíčový pár pro certifikát OCSP služby je také generován v hardwarovém modulu certifikovaném dle standardu Common Criteria na úroveň EAL4+. Generování i aktivace soukromého klíče OCSP služby jsou chráněny aktivačním heslem.

Klíčový pár TSA serveru, pro který se vydává certifikát podle této CP, je generován a uložen v externím hardwarovém modulu (HSM) certifikovaném podle standardu Common Criteria na úroveň EAL4+. HSM modul je kvalifikovaným prostředkem pro vytváření elektronických pečetí. Procesu generování klíčů a žádosti musí být osobně přítomen zástupce kvalifikovaného poskytovatele služeb vytvářejících důvěru. O vygenerování klíčového páru musí být vyhotoven protokol. Viz také kapitolu 3.1.2.1. Podrobnosti o správě klíčů TSA serveru jsou uvedeny v dokumentaci TSA serveru.

- Předání soukromého klíče žadateli

Kvalifikovaný poskytovatel služeb vytvářejících důvěru, jako provozovatel TSA serveru, pro který se vydává certifikát podle této CP, generuje klíčový pár v hardwarovém modulu (HSM). Soukromý klíč zůstává chráněn v HSM modulu.

5.1.2 Předání veřejného klíče poskytovateli služeb vytvářejících důvěru

Žadatel o certifikát předává veřejný klíč v žádosti o certifikát, ve formátu PKCS#10.

5.1.3 Předání veřejného klíče CA spoléhajícím se stranám

Nadřízené certifikáty jsou zveřejněny způsobem popsaným v kapitole 2.2.

Držitel může nadřízené certifikáty získat také na registračním místě.

5.1.4 Délky klíčů

Klíče vydávající certifikační autority mají délku 4096 bitů (algoritmus RSA).

Klíče OCSP služby mají minimální délku 2048 bitů (algoritmus RSA).

Klíče TSA serverů mají minimální délku 2048 bitů (algoritmus RSA).

5.1.5 Generování parametrů veřejných klíčů a kontrola jejich kvality

Klíče CA, služby OCSP i TSA serverů jsou generovány hardwarovým prostředkem, garantujícím kvalitu vygenerovaných kryptografických klíčů. Viz také kapitolu 5.1.1.

5.1.6 Účely použití klíčů

Veřejné klíče držitelů mohou být použity pouze v souladu s pravidly popsanými v kapitole 1.4.1. Možnosti použití klíče jsou dále upřesněny v rozšíření certifikátu.

5.2 OCHRANA SOUKROMÉHO KLÍČE A BEZPEČNOST KRYPTOGRAFICKÝCH MODULŮ

5.2.1 Standardy a podmínky používání kryptografických modulů

Klíče certifikační autority, služby OCSP i TSA serverů jsou generovány a chráněny pomocí hardwarového modulu (HSM) certifikovaného dle standardu Common Criteria na úroveň EAL4+.

HSM, v němž se generují klíčové páry TSA serverů, je kvalifikovaným prostředkem pro vytváření elektronických pečetí, v souladu s požadavky článku 39 a přílohy II [EIDAS] a s dalšími požadavky, které pro kvalifikované prostředky pro vytváření elektronických pečetí plynou z [EIDAS] a návazných prováděcích aktů.

5.2.2 Sdílení tajemství

Soukromý klíč certifikační autority je během provozu chráněn v aktivovaném a konfigurovaném hardwarovém modulu. Pro aktivaci soukromého klíče CA v hardwarovém modulu je vyžadována aktivní spolupráce dvou pověřených pracovníků vybavených čipovými kartami, k nimž je nutno zadat platný PIN.

Soukromý klíč služby OCSP je během provozu chráněn v aktivovaném a konfigurovaném hardwarovém modulu. Pro aktivaci soukromého klíče CA je třeba jednoho pověřeného pracovníka, který je držitelem aktivačního hesla.

Soukromý klíč TSA serveru je během provozu chráněn v aktivovaném a konfigurovaném hardwarovém modulu. Způsob aktivace soukromého klíče je popsán v dokumentaci TSA serveru.

5.2.3 Úschova soukromého klíče

Kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje službu úschovy klíčů.

5.2.4 Zálohování soukromého klíče

Soukromé klíče CA, služby OCSP i TSA serverů jsou zálohovány s využitím nativních prostředků kryptografického modulu. Zálohované klíče jsou uchovávány v zašifrované podobě.

5.2.5 Uchovávání soukromých klíčů

Soukromé klíče CA jsou uchovávány minimálně po dobu platnosti příslušného certifikátu CA. Po ukončení provozu certifikační autority jsou klíče včetně záloh zničeny; o zničení klíčů je vyhotoven záznam.

Soukromé klíče služby OCSP i TSA serverů jsou uchovávány minimálně po dobu platnosti příslušného OCSP certifikátu, resp. certifikátu TSA serveru. Po náhradě certifikátu OCSP jsou nepotřebné klíče OCSP služby zničeny. Totéž platí i pro klíče TSA serverů.

5.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Pro aktivaci soukromého klíče CA, služby OCSP i TSA serveru je třeba příslušný klíč zavést do hardwarového kryptografického modulu ze zašifrovaného souboru.

Při aktivaci soukromého klíče CA musí aktivně spolupracovat dva pověření pracovníci s přidělenými aktivačními čipovými kartami. Každý z pracovníků musí zadat platnou hodnotu PIN karty.

Aktivaci soukromého klíče služby OCSP může provést jeden pověřený pracovník.

Postup aktivace klíče TSA serveru je popsán dokumentaci TSA serveru.

V rámci zavedení a aktivace je soukromý klíč dešifrován v chráněném prostředí HSM. Operace se soukromým klíčem probíhají výhradně v chráněném prostředí HSM. Soukromý klíč v otevřené podobě nikdy neopustí prostředí kryptografického modulu HSM.

5.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče CA, služby OCSP i TSA serverů jsou (po aktivaci) uloženy v hardwarovém kryptografickém prostředku v otevřené podobě. Bezpečnostní certifikace použitého HSM garantuje, že soukromé klíče z HSM nelze přečíst ani exportovat v otevřené podobě.

5.2.8 Postup aktivace soukromého klíče

Před započetím použití soukromých klíčů CA, služby OCSP i TSA serverů je nutno tyto klíče v HSM aktivovat. Aktivaci klíčů mohou provést výhradně pověření pracovníci kvalifikovaného poskytovatele služeb vytvářejících důvěru. Postup aktivace klíčů je zjednodušeně popsán v kapitole 5.2.2. Podrobný popis aktivace soukromých klíčů v HSM je popsán v interní provozní dokumentaci.

Po aktivaci jsou soukromé klíče CA, služby OCSP i TSA serveru použitelné, dokud se neukončí spojení mezi službou a HSM, anebo dokud nedojde k ukončení činnosti HSM.

5.2.9 Postup deaktivace soukromého klíče

Deaktivace soukromého klíče CA, služby OCSP nebo TSA serveru se provede automaticky, pokud nastane jedna z podmínek:

- Je ukončena činnost služby, využívající klíče v HSM (CA, OCSP či TSA server)
- Je přerušeno spojení mezi službou a HSM
- Je ukončena či restartována činnost HSM

5.2.10 Postup ničení soukromého klíče

Soukromé klíče CA, služby OCSP i TSA serveru se zničí deaktivací klíče v HSM a vymazáním všech záložních kopií klíče. Zničení klíče mohou provádět pouze pověření pracovníci kvalifikovaného poskytovatele služeb vytvářejících důvěru. O zničení klíče CA je proveden písemný záznam.

5.2.11 Hodnocení kryptografických modulů

Soukromé klíče CA, služby OCSP i TSA serverů jsou chráněny v hardwarovém kryptografickém prostředku (HSM), který podle bezpečnostního hodnocení Common Criteria dosahuje úrovně EAL4+. HSM je inicializováno a používáno v souladu s doporučením výrobce a schválenou bezpečnostní politikou.

HSM je kvalifikovaným prostředkem pro vytváření elektronických pečetí, je certifikován v souladu s článkem 39 [EIDAS], a splňovat i další relevantní požadavky, které pro kvalifikované prostředky pro vytváření elektronických pečetí plynou z [EIDAS] a návazných prováděcích aktů.

Pověření pracovníci kvalifikovaného poskytovatele služeb vytvářejících důvěru průběžně sledují a vyhodnocují rizika, plynoucí z použití HSM, a reagují na případná rizika.

5.3 DALŠÍ ASPEKTY SPRÁVY PÁRU KLÍČŮ

5.3.1 Archivace veřejných klíčů

Veřejné klíče (ve formě certifikátů) jsou uchovávány po dobu provozu a archivace certifikátu CA, která tyto certifikáty vystavila.

5.3.2 Doba platnosti certifikátů a doba platnosti klíčů

Doba platnosti certifikátů, vydaných podle této certifikační politiky, je uvedena v certifikátu. Doba platnosti páru klíčů je shodná s platností certifikátu.

5.4 AKTIVAČNÍ DATA

Aktivační data se pro jednotlivé participující subjekty liší:

- Aktivačními daty klíče CA je kryptografický klíč uložený na čipových kartách, chráněných pomocí PIN. Pro složení aktivačního klíče jsou zapotřebí 2 aktivační karty. Držiteli aktivačních karet jsou

oprávnění pracovníci kvalifikovaného poskytovatele služeb vytvářejících důvěru. Jedna osoba může mít v držení pouze jednu aktivační kartu. Držitel aktivační karty má ve výhradním držení PIN dané karty. Pomocí PIN se aktivuje tajemství uložené v čipu aktivační karty. Při aktivaci klíče CA musí aktivně spolupracovat 2 držitelé aktivačních karet.

- Aktivačními daty klíče služby OCSP je heslo, které je v držení pověřených pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru. Heslo je chráněno prostředky hostitelského operačního systému služby OCSP.
- Aktivační data klíčů TSA serveru jsou popsána v dokumentaci TSA serveru.

5.4.1 Generování a instalace aktivačních dat

Generování a instalace aktivačních dat se liší podle technologických možností prostředků, jimiž jsou aktivační data chráněna:

- Aktivační data klíče CA jsou generována a instalována v rámci procesu zprovoznění certifikační autority, před vygenerováním prvního klíčového páru CA. Postup generování a instalace aktivačních dat je popsán v interní dokumentaci CA. Za generování a ochranu aktivačních dat je zodpovědný správce CA spolu s držiteli aktivačních karet.
- Aktivační data klíče služby OCSP jsou generována a instalována v rámci procesu zprovoznění služby OCSP, před vygenerováním prvního klíčového páru pro certifikát služby OCSP. Aktivační data mohou být pro další klíčové páry OCSP vygenerována znovu a změněna. Postup generování a instalace aktivačních dat je popsán v interní dokumentaci služby OCSP. Za generování a ochranu aktivačních dat je zodpovědný správce služby OCSP.
- Generování a instalace aktivačních dat TSA serveru jsou popsány v dokumentaci TSA serveru.

5.4.2 Ochrana aktivačních dat

Aktivační data musí být chráněna před prozrazením neoprávněným osobám. Adekvátní ochranu aktivačních dat musí zajistit příslušný držitel aktivačních dat:

- Aktivační data klíče CA jsou chráněna v čipu aktivačních karet. Použití aktivačních dat je podmíněno držením aktivační karty a znalostí platné hodnoty PIN aktivační karty. Aktivační karty i hodnoty PIN jsou ve výhradním držení pověřených pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru. V době nečinnosti jsou aktivační karty uloženy v chráněném úložišti s řízeným přístupem.
- Aktivační data klíče služby OCSP jsou v držení pověřených pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru. Přístup k aktivačním datům mají pouze pověření pracovníci, oprávnění manipulovat s aktivačními daty služby OCSP.
- Aktivační data TSA serveru jsou pod kontrolou pověřených správců TSA serveru. Podrobný popis správy a ochrany aktivačních dat je uveden v dokumentaci TSA serveru.

V případě podezření na kompromitaci musí držitel aktivačních dat bezodkladně zahájit kroky pro eliminaci rizik:

- Správce TSA serveru musí změnit aktivační data a požádat o zneplatnění certifikátu.
- Držitelé aktivačních dat klíče CA a OCSP musí postupovat podle provozní dokumentace kvalifikovaného poskytovatele služeb vytvářejících důvěru.

5.4.3 Ostatní aspekty aktivačních dat

Aktivační data klíče CA nejsou nikdy přenášena či uchovávána v otevřené podobě.

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

5.5 POČÍTAČOVÁ BEZPEČNOST

5.5.1 Specifické technické požadavky na počítačovou bezpečnost

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

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

Technické řešení pro zajištění počítačové bezpečnosti je popsáno v interní dokumentaci kvalifikovaného poskytovatele služeb vytvářejících důvěru.

5.5.2 Hodnocení počítačové bezpečnosti

Počítačová bezpečnost systému certifikačních služeb vychází ze standardů pro poskytovatele služeb vytvářejících důvěru. Jde zejména o pravidla, zakotvená v normách:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

Kvalita počítačové bezpečnosti podléhá hodnocení podle interních postupů Komerční banky.

Systém certifikačních služeb prošel při uvedení do provozu penetračními testy. Výsledky penetračních testů byly zohledněny, byla přijata odpovídající opatření pro eliminaci rizik.

Penetrační testy systému certifikačních služeb jsou prováděny nejméně jednou ročně.

5.6 BEZPEČNOST ŽIVOTNÍHO CYKLU

5.6.1 Řízení vývoje systému

Systém certifikačních služeb byl navržen tak, aby splňoval bezpečnostní požadavky, kladené na kvalifikované poskytovatele služeb vytvářejících důvěru. Ve fázi návrhu byly zohledněny bezpečnostní zásady a mechanismy fyzického i logického zabezpečení. Byla také provedena analýza rizik a navrženy mechanismy ochrany aktiv. Byly navrženy procesy, role a oprávnění. Vše je zdokumentováno v interních dokumentech KB.

Na základě schváleného návrhu byl systém certifikačních služeb implementován. Pro dílčí části systému byly vyvinuty specifické softwarové komponenty. Implementace systému certifikačních služeb byla provedena podle bezpečnostních zásad kvalifikovaného poskytovatele služeb vytvářejících důvěru pro oblast změnového řízení.

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

5.6.2 Kontroly řízení zabezpečení

V rámci implementace systému certifikačních služeb 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.

5.6.3 Řízení zabezpečení životního cyklu

Systém certifikačních služeb je předmětem kontroly a auditu dle standardních postupů kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Kvalita a funkčnost provozu certifikačních služeb je průběžně vyhodnocována. Hodnoceny jsou také zranitelnosti. Na nalezená zjištění jsou aplikovány adekvátní reakce, např. ve formě instalace, odinstalace či upgrade komponent, anebo také úpravy konfigurací či politik.

5.7 SÍŤOVÉ ZABEZPEČENÍ

Systém certifikačních služeb je provozován v interní síti Komerční banky s ostatními servery, počítači a dalšími zařízeními. Komponenty systému certifikačních služeb jsou rozděleny do segmentů sítě, s definovanými komunikačními prostupy do dalších síťových segmentů.

V interní dokumentaci je pro každou komponentu systému certifikačních služeb navržen seznam povolených komunikací. Je definováno, se kterými adresami a porty může daná komponenta komunikovat. Na úrovni síťových prvků a firewallů jsou schválené komunikační vazby povoleny, ostatní komunikace je zakázána.

Komunikační pravidla jsou nastavena restriktivně. Jsou povoleny pouze komunikační vazby nezbytné pro provoz certifikačních služeb, resp. pro komunikaci spojenou se zasíláním žádostí a vydáváním certifikátů.

Systém certifikačních služeb je od sítě internet oddělen firewallem.

5.8 ČASOVÁ RAZÍTKA

Časová razítka nejsou při poskytování certifikačních služeb používána.

Časové údaje, přiřazené k certifikátům i všem dalším záznamům, jsou synchronizovány v rámci prostředí Komerční banky. Čas je synchronizován proti internímu serveru, který je sdíleným zdrojem přesného času. Čas se synchronizuje nejméně jednou za 24 hodin.

TSA servery generují časová razítka, ta však nejsou využívána pro podporu provozu certifikačních služeb.

6 PROFILY CERTIFIKÁTŮ, SEZNAMŮ CRL A OCSP

6.1 PROFIL CERTIFIKÁTU

Profil kvalifikovaného certifikátu pro elektronickou pečeť je v souladu s normami ETSI EN 319 412-3 a ETSI EN 319 412-5.

Profily vydávaných certifikátů odpovídají RFC 5280 (*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*). Certifikáty pro koncové subjekty jsou vydávány s následujícími položkami:

Položka	Hodnota	
Verze (Version)	verze 3 *(0x2)*	
Sériové číslo (Serial number)	Jedinečné číslo certifikátu	
Vydavatel (Issuer)	Označení kvalifikovaného poskytovatele služeb vytvářejících důvěru:	
	CN (commonName)	*Komerční banka Qualified CA/RSA*
	O (organisationName)	*Komerční banka, a.s.*
	OID 2.5.4.97 (organizationIdentifier)	*NTRCZ-45317054*
	C (countryName)	*CZ*
Platnost od (Not Before)	Datum počátku platnosti certifikátu, v UTC	
Platnost do (Not After)	Datum konce platnosti certifikátu, v UTC (začátek platnosti + 3 roky)	
Předmět (Subject)	Identifikace držitele certifikátu:	
	CN (commonName)	Identifikace TSA serveru
	OID: 2.5.4.5 (serialNumber)	Identifikátor technického prostředku, který hostuje TSA server
	OID: 2.5.4.97 (organizationIdentifier)	Identifikátor organizace, pro kterou se certifikát vydává, ve formátu: NTR<kód země>-<IČO> kde: <kód země> je kód země dle ISO 3166, podle sídla organizace <IČO> je IČO organizace
	O (organizationName)	Název organizace, pro kterou se certifikát vydává
	C (countryName)	Kód země adresy sídla organizace, pro kterou se certifikát vydává, podle ISO 3166
Algoritmus podpisu (Signature Algorithm)	RSASSA-PSS (PKCS #1 v2.1)	

	OID: 1.2.840.113549.1.1.10 hashAlgorithm: SHA512 OID: 2.16.840.1.101.3.4.2.3 maskGenAlgorithm: mgf1 s hash funkcí stejnou jako v hashAlgorithm OID: 1.2.840.113549.1.1.8	
Veřejný klíč (Subject Public Key Info)	Veřejný klíč subjektu certifikátu	
	Algoritmus (Algorithm)	rsaEncryption
	Veřejný klíč (SubjectPublicKey)	Veřejný klíč min. 2048 bitů
Signature	Elektronická pečeť vydavatele certifikátu	

6.1.1 Číslo verze

Vydávané certifikáty odpovídají standardu X.509, verze 3.

6.1.2 Rozšíření certifikátu

V následujících podkapitolách jsou uvedena rozšíření, uváděná ve vydávaných certifikátech.

6.1.2.1 Použití klíče (Key Usage)

Kritické rozšíření.

Toto rozšíření je řešeno nastavením odpovídajícího bitu dle následujícího seznamu:

- digitalSignature (digitální podpis)
- nonRepudiation (neodmítnutelnost odpovědnosti)

6.1.2.2 Zásady certifikátu (Certificate Policies)

Nekritické rozšíření.

Rozšíření obsahuje sekvenci dvou certifikačních politik:

policyInformation (1)	■ Identifikátor zásad= 1.3.154.45317054.1000.1.2.1.6.1 ■ [1,1]Informace o kvalifikátoru zásad: ID kvalifikátoru zásad=userNotice Kvalifikátor (Qualifier): *Tento kvalifikovany certifikat pro elektronickou pecet byl vydan v souladu s narizenim EU c. 910/2014. This is a qualified certificate for electronic seal according to Regulation (EU) No 910/2014.* ■ [1,2]Informace o kvalifikátoru zásad: ID kvalifikátoru zásad=cPSuri Kvalifikátor (Qualifier): https://www.kb.cz/pki
policyInformation (2)	Identifikátor zásad=0.4.0.194112.1.3 QCP-l-qscd: certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in QSCD

6.1.2.3 Základní omezení (Basic Constraints)

Obsahuje informaci, že jde o certifikát koncového subjektu (cA = false):

- Subject type = End entity
- Path length constraint = None

6.1.2.4 Alternativní název předmětu (Subject Alternative Name)

V tomto nekritickém rozšíření se uvádí e-mailová adresa držitele certifikátu (rfc822Name). Údaj je nepovinný, nemusí být uveden.

6.1.2.5 Rozšířené použití klíče (Extended Key Usage) a aplikační politiky (Application Policies)

- id-kp-timeStamping (svázání hash s časovou značkou), OID: 1.3.6.1.5.5.7.3.8

- Distribuční místa zneplatněných certifikátů (CRL Distribution Points)

Toto rozšíření obsahuje cestu URL k platnému seznamu CRL - viz kap. 2.2.1.

6.1.2.6 Přístup k informacím autority (Authority Information Access)

Toto rozšíření obsahuje:

- cestu URL k certifikátu CA
- URL služby OCSP, na níž lze ověřit stav certifikátu.

Viz také kap. 2.2.1.

6.1.2.7 Identifikátor klíče předmětu (Subject Key Identifier) a Identifikátor klíče autority (Authority Key Identifier)

Tato rozšíření obsahují 160 bitový řetězec (hash spočítaný algoritmem SHA1 z veřejného klíče). Přičemž:

- Rozšířeni Subject Key Identifier obsahuje hash z veřejného klíče z vlastního certifikátu (certifikátu, který má být ověřován).
- Rozšíření Authority Key Identifier obsahuje hodnotu z rozšíření Subject Key Identifier certifikátu, kterým má být tento certifikát ověřován. (Rozšíření AKI obsahuje hash veřejného klíče vydávající CA.)

Vazba Subject Key Identifier a Authority Key Identifier slouží k sestavení certifikační cesty pro ověření certifikátu.

6.1.2.8 Rozšíření kvalifikovaných certifikátů (qcStatements)

Toto nekritické rozšíření obsahuje sekvenci identifikátorů, které upřesňuje vlastnosti kvalifikovaného certifikátu:

Kvalifikátor	Název / OID	Hodnota, poznámka
Kvalifikovaný certifikát	esi4-qcStatement-1 {0.4.0.1862.1.1}	
Soukromý klíč chráněn v QSCD prostředku	esi4-qcStatement-4 {0.4.0.1862.1.4}	
Odkazy na dokument PKI Disclosure Statement (PDS)	esi4-qcStatement-5 {0.4.0.1862.1.5}	en: https://www.kb.cz/pki/pds_en.pdf cs: https://www.kb.cz/pki/pds_cs.pdf
Typ certifikátu	esi4-qcStatement-6 {0.4.0.1862.1.6}	Obsahuje typ: elektronická pečeť {0.4.0.1862.1.6.2}

6.1.3 OID algoritmů

Objektové identifikátory algoritmů jsou používány v souladu s obecně užívanými standardy a normami.

6.1.4 Zápis jmen a názvů

Jména a názvy se používají v souladu s pravidly v odstavci 2.5.

6.1.5 Omezení jmen

Na vydávané certifikáty není aplikováno omezení jmen.

6.1.6 OID certifikační politiky

Identifikátor této certifikační politiky je uveden v kapitole 1.2, resp. v kapitole 6.1.2.2.

6.1.7 Omezení politiky

Rozšíření Policy Constraints se ve vydaných certifikátech nevyužívá.

6.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz kapitolu 6.1.2.2.

6.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Není relevantní pro tento dokument – položka není označena jako kritická.

6.2 PROFIL SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ (CRL)

Vydávající CA vydává CRL s následujícím profilem:

Položka	Hodnota
Verze (version)	v2 (0x1)
Podpisové schéma (Signature Algorithm)	RSASSA-PSS (PKCS #1 v2.1) OID: 1.2.840.113549.1.1.10 hashAlgorithm: SHA512 OID: 2.16.840.1.101.3.4.2.3 maskGenAlgorithm: mgf1 s hash funkcí stejnou jakov hashAlgorithm OID: 1.2.840.113549.1.1.8
Vydavatel (issuer)	CN = Komerční banka Qualified CA/RSA, O = Komerční banka, a.s., 2.5.4.97 = NTRCZ-45317054, C = CZ
Datum začátku platnosti (thisUpdate)	Datum a čas vydání seznamu CRL, v UTC
Konec platnosti (nextUpdate)	Konec platnosti seznamu CRL, v UTC

Seznam zneplatnění (revokedCertificates)	Přehled zneplatněných certifikátů sestávající ze sériového čísla, data a důvodu zneplatnění (uvedení důvodu je nepovinné).
Rozšíření (CRLExtensions)	Viz kapitolu 6.2.2
Podpis (signature)	Elektronická pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru

6.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X.509 verze 2.

6.2.2 Rozšíření CRL

Rozšíření (crlExtensions)	Hodnota
Identifikátor klíče CA (není kritické) (authorityKeyIdentifier)	Viz kapitola 6.1.2.7
Číslo seznamu CRL (není kritické) (CRLNumber)	Pořadové číslo aktuálního seznamu CRL

6.3 PROFIL OCSP

Stav platnosti certifikátu lze ověřit prostřednictvím OCSP protokolu. Server OCSP služby je provozován v režimu autorizovaného respondéru (Authorized Responder).

Profily OCSP žádosti i odpovědi jsou v souladu s RFC 6960 a RFC 2560.

OCSP podporuje zpracování dotazů a generování odpovědí typu basic (id-pkix-ocsp-basic).

Pro nevydané certifikáty (non-issued certificates) je vrácena odpověď se stavem revoked. Údaje o stavu certifikátu (SingleResponse) obsahují v tomto případě výchozí hodnoty: revocationReason = certificateHold (6), revocationTime = 1.1.1970. Navíc je do rozšíření odpovědi (responseExtensions) doplněno nekritické rozšíření id-pkix-ocsp-extended-revoke (OID = 1.3.6.1.5.5.7.48.1.9).

Je-li znám důvod zneplatnění certifikátu, pak se tento důvod uvádí v sekci SingleResponse, ve struktuře RevokedInfo.

Jako transportní protokol se používá HTTP.

6.3.1 Číslo verze

V žádosti i odpovědi OCSP se uvádí verze 1.

6.3.2 Rozšíření OCSP

Kromě rozšíření, uvedených v úvodu kapitoly 6.3, je v odpovědích OCSP podporováno rozšíření Nonce (pokud je uvedeno ve vstupním požadavku).

7 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

PKI systém Komerční banky je auditován v souladu s interními směrnicemi kvalifikovaného poskytovatele služeb vytvářejících důvěru.

7.1 PERIODICITA NEBO OKOLNOSTI HODNOCENÍ

Interní audit je prováděn nejméně jednou ročně, v případě vzniku bezpečností události je proveden bezodkladně.

Externí audit je prováděn subjektem posuzování shody [EIDAS] nejméně jednou za dva roky. V případě podezření na vznik bezpečnostního incidentu nebo podezření na neplnění požadavků [EIDAS] může subjekt posuzování shody nebo orgán dohledu provést mimořádný audit v souladu s [EIDAS].

7.2 IDENTITA A KVALIFIKACE HODNOTITELE

7.2.1 Interní hodnocení shody

Interní hodnocení shody provádí pracovníci oddělení interního auditu Komerční banky. Hodnocení shody se provádí v souladu s interní metodikou Komerční banky.

7.2.2 Externí hodnocení shody

Externí hodnocení shody provádí subjekt posuzování shody [EIDAS].

7.3 VZTAH HODNOTITELE K HODNOCENÉMU SUBJEKTU

7.3.1 Interní hodnocení shody

Subjekt provádějící hodnocení shody není ve vztahu nadřízenosti ani podřízenosti vůči organizační jednotce, která provozuje certifikační služby.

Subjekt provádějící hodnocení shody se nepodílí na provozu certifikačních služeb.

7.3.2 Externí hodnocení shody

Subjekt, který provádí externí hodnocení shody, není žádným způsobem (majetkově ani personálně) svázán s provozovatelem certifikačních služeb.

7.4 HODNOCENÉ OBLASTI

Pro každé hodnocení shody je předem specifikováno, jaké oblasti budou předmětem hodnocení.

Oblasti hodnocení shody obecně vycházejí se standardu ETSI TR 119 411-4. Metodika hodnocení shody vychází ze standardu ETSI EN 319 403.

7.5 POSTUP V PŘÍPADĚ ZJIŠTĚNÍ NEDOSTATKŮ

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

7.6 SDĚLOVÁNÍ VÝSLEDKŮ HODNOCENÍ

Výstupem hodnocení shody je písemná zpráva, která je předána Manažeru PKI. Manažer PKI předloží výslednou zprávu orgánu dohledu, a to do 3 pracovních dnů od jejího obdržení. Manažer PKI také rozhodne o případné distribuci zprávy na další příjemce či zveřejnění zprávy.

8 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 POPLATKY

8.1.1 Poplatky za vydání nebo obnovení certifikátu

Certifikáty podle této CP vydává kvalifikovaný poskytovatel služeb vytvářejících důvěru pro zařízení (TSA servery), která sám provozuje. Poplatky za vydání certifikátů jsou stanoveny interními pravidly kvalifikovaného poskytovatele služeb vytvářejících důvěru.

8.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup elektronickou cestou k vydaným certifikátům se neposkytuje.

8.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Zneplatnění certifikátu ani přístup k informacím o stavu certifikátu není zpoplatněno.

8.1.4 Poplatky za další služby

Certifikáty podle této CP vydává kvalifikovaný poskytovatel služeb vytvářejících důvěru pro zařízení (TSA servery), která sám provozuje. Poplatky za služby spojené se správou certifikátů jsou stanoveny interními pravidly kvalifikovaného poskytovatele služeb vytvářejících důvěru.

8.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Žádné ustanovení.

8.2 FINANČNÍ ODPOVĚDNOST

8.2.1 Krytí pojištěním

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

8.2.2 Další aktiva a záruky

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

8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Tato služba není poskytována.

8.3 DŮVĚRNOST OBCHODNÍCH INFORMACÍ

Komerční banka poskytuje certifikační služby v rámci svých dalších služeb, jako jsou bankovní či finanční služby. V rámci bankovních (a dalších) služeb KB eviduje a zpracovává celou řadu informací o svých klientech, včetně osobních a finančních záznamů. Velká část těchto záznamů se pokládá za důvěrné obchodní údaje. Všechny tyto informace KB eviduje a zpracovává v souladu s bankovním tajemstvím, právními předpisy, obchodními podmínkami a smlouvami s klienty.

8.3.1 Rozsah důvěrných informací

Certifikáty se podle této certifikační politiky vydávají pro Komerční banku. Při poskytování certifikačních služeb se používají především údaje, které lze zjistit z veřejných zdrojů anebo údaje, které nemají charakter důvěrných informací (identifikace držitele, identifikace systému či prostředku který hostuje vydaný certifikát).

Za důvěrné informace se pokládají technické údaje o prostředku či systému, který hostuje soukromý klíč TSA serveru. Za důvěrné informace se pokládají také procesy pro správu soukromého klíče a certifikátu, aktivační data soukromého klíče atd…

Za důvěrné informace, k nimž má kvalifikovaný poskytovatel služeb vytvářejících důvěru přístup, jsou dále pokládány:

- Osobní údaje žadatelů, pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru a dalších osob, které mohou mít spojitost s poskytováním certifikačních služeb
- Soukromé klíče
- Interní dokumentace a směrnice
- Interní smluvní ujednání

Žádné z důvěrných informací nejsou kvalifikovaným poskytovatelem služeb vytvářejících důvěru zveřejňovány.

8.3.2 Informace mimo rámec důvěrných informací

Za veřejné informace se označují pouze takové údaje, které kvalifikovaný poskytovatel služeb vytvářejících důvěru určil ke zveřejnění.

8.3.3 Odpovědnost za ochranu důvěrných informací

Pracovníci kvalifikovaného poskytovatele služeb vytvářejících důvěru, i všichni případní dodavatelé, jsou povinni chránit důvěrné informace a neposkytovat takové informace třetím stranám.

8.4 OCHRANA OSOBNÍCH ÚDAJŮ

Kvalifikovaný poskytovatel služeb vytvářejících důvěru zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb.

8.4.1 Osobní údaje

Za osobní údaje jsou považovány informace stanovené Nařízením 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 – dále jen [GDPR].

Při poskytování certifikačních služeb se využívají osobní a identifikační údaje zástupců právnické osoby, která je držitelem certifikátu. Převážná většina těchto zástupců jsou pracovníci KB nebo smluvní dodavatelé.

Zástupci organizací (typicky žadatelé), kteří participují na procesech správy certifikátů tak činí s vědomím, že jejich osobní údaje budou zpracovávány kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

8.4.2 Odpovědnost za ochranu osobních údajů

Odpovědnost za ochranu osobních údajů zpracovávaných v systémech certifikačních služeb nese Komerční banka, jakožto kvalifikovaný poskytovatel služeb vytvářejících důvěru, všichni její zaměstnanci a smluvní partneři.

Odpovědnosti za ochranu osobních údajů jsou podrobněji rozpracovány v interních směrnicích Komerční banky.

8.4.3 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Osoba, která zastupuje organizaci držitele certifikátu, bere na vědomí, že její osobní údaje budou zpracovávány v systémech kvalifikovaného poskytovatele služeb vytvářejících důvěru.

8.4.4 Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů pro soudní, resp. správní účely je řešeno v souladu s požadavky příslušných právních předpisů.

8.5 PRÁVA DUŠEVNÍHO VLASTNICTVÍ

Kvalifikovaný poskytovatel služeb vytvářejících důvěru plně respektuje zákon č. 121/2000 Sb., autorský zákon, a zákon č. 441/2003 Sb., o ochranných známkách.

Obsah certifikační politiky, i dalších dokumentů kvalifikovaného poskytovatele služeb vytvářejících důvěru, je chráněn autorskými právy kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Autorskými právy jsou chráněny také softwarové aplikace, které Komerční banka používá v souvislosti s poskytováním certifikačních služeb.

8.6 ZASTUPOVÁNÍ A ZÁRUKY

Komerční banka, a.s. zaručuje, že splní veškeré povinnosti uložené touto certifikační politikou.

8.6.1 Zastupování a záruky CA

Certifikační autorita poskytuje u certifikátů vydaných podle této certifikační politiky záruky na:

- Jednoznačnost sériového čísla vydaných certifikátů
- Kryptografickou odolnost použitých algoritmů pro výpočet hashe a elektronické pečetě
- Správné použití soukromých klíčů příslušných k nadřízeným certifikátům
- Vydávání pouze těch certifikátů, které jsou popsány v některé z platných certifikačních politik
- Shodu identifikačních údajů uvedených v žádosti o vydání certifikátu s těmito údaji obsaženými ve vydaném certifikátu
- Soulad certifikátů, CRL a OCSP s běžně používanými průmyslovými standardy
- Možnost požádat o zneplatnění certifikátu držitelem
- Dostupnost certifikátů certifikačních autorit, CRL a služby OCSP
- Časové limity uvedené v této certifikační politice na vydání CRL

8.6.2 Zastupování a záruky RA

Registrační autorita garantuje kvalitu ztotožnění žadatelů prostřednictvím požadovaných osobních dokladů. Registrační autorita také ověřuje údaje právnické osoby, pro kterou se žádá o certifikát.

KB nevydá certifikát podle této CP, pokud:

- identita žadatele nebyla dostatečným způsobem prokázána a ověřena, nebo
- nebylo prokázáno, že daný žadatel je zastupovat danou právnickou osobu při podání žádosti o certifikát, nebo
- nebyly prověřeny identifikační údaje právnické osoby pro kterou se žádá o certifikát, nebo
- nebylo prověřeno, že právnická osoba, pro kterou se žádá o certifikát, je oprávněna k držení daného typu certifikátu.

8.6.3 Zastupování a záruky držitele certifikátu

Držitelem certifikátu, vydaného podle této CP, je Komerční banka jako kvalifikovaný poskytovatel služeb vytvářejících důvěru. Držitel:

- Zaručuje, že pro získání certifikátu pověří důvěryhodného zástupce (žadatele), který je pracovníkem kvalifikovaného poskytovatele služeb vytvářejících důvěru. Tento žadatel zastupuje kvalifikovaného poskytovatele služeb vytvářejících důvěru při procesu registrace žádosti.
- Zaručuje, že identifikační údaje uvedené v žádosti jsou pravdivé a odpovídají jeho identifikačním údajům organizace a také identifikačním údajům prostředku či systému, který hostuje soukromý klíč certifikátu.
- Zaručuje, že vydání certifikátu je v souladu s bezpečnostní politikou Komerční banky.
- Zaručuje, že soukromý klíč příslušný k danému certifikátu je pod jeho výhradní kontrolou.

- Zaručuje, že přístup k soukromému klíči vydaného certifikátu nemají neoprávněné osoby či systémy.
- Zaručuje, že aktivační data k soukromým klíčům jeho certifikátů, jsou pod jeho výhradní kontrolou.
- Zaručuje, že bude dodržovat požadavky a pravidla, uvedené v této certifikační politice.

8.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající strana musí při využití certifikátů jednat v souladu s touto certifikační politikou.

8.6.5 Zastupování a záruky ostatních subjektů

- Není relevantní pro tento dokument.

8.7 ZŘEKNUTÍ SE ZÁRUK

Komerční banka poskytuje pouze záruky uvedené v odstavci 8.6.

8.8 OMEZENÍ ODPOVĚDNOSTI

Komerční banka neodpovídá za škodu vyplývající z použití certifikátu, pokud nebyly dodrženy podmínky jeho použití uvedené v certifikační politice, certifikační prováděcí směrnici a souvisejících dokumentech.

Odpovědnost za škodu, náhrada škody

Komerční banka, a.s., odpovídá držiteli certifikátu za vzniklou škodu dle platných právních předpisů. Komerční banka odpovídá za škodu způsobenou porušením povinností kvalifikovaného poskytovatele certifikačních služeb, uvedených v této certifikační politice a návazných dokumentech.

8.9 DOBA PLATNOSTI, UKONČENÍ PLATNOSTI

8.9.1 Doba platnosti

Doba platnosti této certifikační politiky je od data vydání do odvolání, resp. vydání nové verze.

8.9.2 Ukončení platnosti

Platnost tohoto dokumentu je ukončena:

- Jeho nahrazením novější verzí,
- Rozhodnutím kvalifikovaného poskytovatele služeb vytvářejících důvěru o ukončení vydávání tohoto typu certifikátu nebo
- Ukončením poskytování certifikačních služeb

8.9.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti tohoto dokumentu z důvodu ukončení poskytování certifikačních služeb zůstávají v platnosti ustanovení uvedená v kapitole 8 týkající se obchodních a právních záležitostí.

V případě rozhodnutí kvalifikovaného poskytovatele o ukončení vydávání daného typu certifikátu zůstávají v platnosti závazky uvedené v této CP, minimálně do ukončení platnosti všech certifikátů vydaných podle této CP.

8.10 KOMUNIKACE MEZI ZÚČASTNĚNÝMI SUBJEKTY

8.10.1 Komunikace s poskytovatelem služeb vytvářejících důvěru

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

Spoléhající se strany mohou s kvalifikovaným poskytovatelem služeb vytvářejících důvěru komunikovat elektronicky, prostřednictvím kontaktních údajů, uvedených v kapitole 1.5.

8.10.2 Jazyk komunikace

Primárním komunikačním jazykem je čeština. Certifikační služby však mohou být poskytovány i držitelům a žadatelům, kteří komunikují některým z běžně užívaných světových jazyků. Kvalifikovaný poskytovatel služeb vytvářejících důvěru negarantuje, že pro takové klienty budou k dispozici dokumenty v jiném než českém jazyce.

8.11 ZMĚNY

8.11.1 Postup při změnách

Postupy pro změny probíhají podle ustanovení kapitoly1.5.4.

8.11.2 Postup při oznamování změn

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

Nová verze CP je zveřejněna vždy předtím, než je započato vydávání certifikátů podle dané CP.

8.11.3 Okolnosti, při kterých musí být změněn identifikátor OID

OID je přiřazeno certifikační politice, podle níž se vydávají certifikáty.

OID certifikační politiky se změní v případě změny certifikační politiky, která se týká zásadních bezpečnostních aspektů certifikátů, jako jsou např.:

- Změna profilu certifikátu
- Změna délky platnosti certifikátů
- Změna kryptografických vlastností (použité algoritmy, velkosti klíčů, hashovací funkce)
- Změna záruk za důvěryhodnost certifikátu
- Změna akceptovatelnosti certifikátu vzhledem ke službám vytvářejícím důvěru

V případě jakýchkoliv změn v tomto dokumentu je vždy změněna verze dokumentu.

8.12 ŘEŠENÍ SPORŮ

Všechny strany případného sporu jsou součástí organizační struktury Komerční banky. Případné spory se řeší v rámci interních pravidel Komerční banky.

8.13 ROZHODNÉ PRÁVO

Rozhodným právem je právo České republiky.

8.14 SHODA S PRÁVNÍMI PŘEDPISY

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

8.15 DALŠÍ USTANOVENÍ

8.15.1 Rámcová dohoda

Žádná ustanovení.

8.15.2 Postoupení práv

Není stanoveno.

8.15.3 Oddělitelnost ustanovení

Dohoda o poskytování certifikačních služeb zůstává platná i v případě, že jakákoliv její dílčí část pozbude platnost, pokud se obě strany nedohodnou jinak.

8.15.4 Zřeknutí se práv

Žádná ustanovení.

8.15.5 Vyšší moc

Žádná ze stran nenese odpovědnost za porušení svých povinností způsobeným vyšší mocí, jako jsou například přírodní katastrofy velkého rozsahu, stávky, občanské nepokoje nebo válečný stav.

8.16 DALŠÍ OPATŘENÍ

Žádná ustanovení.