CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE KOMERČNÍ BANKA QUALIFIED CA/RSA

Verze 1.0

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 10:24:27

1 ÚVOD

Tento dokument představuje certifikační prováděcí směrnici certifikační autority *Komerční banka Qualified CA/RSA*, provozované společnosti Komerční banka, a.s. (dále jen Komerční banka nebo KB).

1.1 PŘEHLED

Tato certifikační prováděcí směrnice (dále CPS) deklaruje pravidla a praktiky, které jsou používány při správě, provozu a fungování *Komerční banka Qualified CA/RSA*.

Certifikační autorita *Komerční banka Qualified CA/RSA* (dále CA) je provozována v interním prostředí Komerční banky. Slouží k vydávání certifikátů pro potřeby Komerční banky a spřízněných organizací.

Certifikáty vydávané z *Komerční banka Qualified CA/RSA* jsou vydávány:

- Primárně klientům Komerční banky, popř. klientům dceřiných společností KB.
- Případně pro vnitřní použití KB, např. pro technické prostředky a infrastrukturu KB.

Pro každý typ certifikátu, vydávaného z *Komerční banka Qualified CA/RSA* je zpracována samostatná certifikační politika (CP). Informace v CP upřesňují a doplňují informace, uvedené v této CPS. Zatímco CPS se primárně zabývá fungováním, správou a bezpečností certifikační autority, dokumenty CP se zaměřují na vlastnosti vydávaných certifikátů, jejich životní cyklus a podmínky pro získání daného typu certifikátu.

CA je vybudována a provozována v souladu s obecně platnými standardy, platnými pro certifikační autority.

CA je provozována v režimu *kvalifikovaného poskytovatele služeb vytvářejících důvěru*, v souladu s *Nařízením 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* (eIDAS). Z *Komerční banka Qualified CA/RSA* jsou vydávány kvalifikované certifikáty, ve smyslu eIDAS.

Informace, publikované v této CPS, mají přispět k důvěryhodnosti:

- Komerční banky, jako kvalifikovaného poskytovatele certifikačních služeb,
- certifikační autority *Komerční banka Qualified CA/RSA*
- a certifikátů vydávaných z *Komerční banka Qualified CA/RSA*.

1.2 NÁZEV DOKUMENTU A IDENTIFIKACE

Název dokumentu	Certifikační prováděcí směrnice Komerční banka Qualified CA/RSA
Verze dokumentu	1.0
OID tohoto dokumentu	není přidělováno
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, Praha 1, 114 07

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. Jednou z certifikačních autorit, které vydávají certifikáty pro klienty KB je *Komerční banka Qualified CA/RSA*.

Tato CPS (tento dokument) se vztahuje k certifikační autoritě *Komerční banka Qualified CA/RSA*.

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 autority:

- za Komerční banku, a.s. uzavírají s žadateli smlouvy o poskytování certifikačních služeb,
- ověřují totožnost žadatelů,
- vydávají žadatelům prostředky pro vytváření elektronických podpisů (pouze pro některé typy certifikátů),
- přijímají žádosti o certifikáty, popř. zajišťují předání vydaného certifikátu.

Komerční banka Qualified CA/RSA využívá v zásadě dva typy registračních autorit:

- Registrační autority na pobočkách Komerční banky. Na pobočkách KB se realizuje registrační proces klientů KB. Žadateli o certifikáty jsou v tomto případě fyzické osoby nebo zástupci právnických osob, které jsou klienty KB. Registrační proces zajišťují pracovníci pobočky Komerční banky.
- Interní registrační autority KB. Tato registrační pracoviště nejsou přístupná veřejnosti. Provádí se na nich registrační proces žadatelů o certifikáty, které mají sloužit pro interní potřeby KB. Žadateli o certifikát jsou typicky pracovníci KB či dceřiných společností KB.

Postup registračního procesu a fungování registrační autority je pro každý typ certifikátu upřesněn v příslušné certifikační politice.

1.3.3 Žadatelé o certifikát

Žadatelé o certifikáty se dělí na dvě podmnožiny:

- O některé typy certifikátů mohou požádat pouze smluvní klienti KB nebo jejich oprávnění zástupci.
- O jiné certifikáty mohou požádat pouze pracovníci KB anebo pracovníci dceřiných společností.

Před podáním žádosti o certifikát se provádí ověření identity žadatele.

Pokud se žádá o certifikát fyzické osoby, pak může o tento certifikát požádat pouze daná fyzická osoba. Tato osoba je následně také držitelem certifikátu. .

Pokud se žádá o certifikát organizace, pak může být žadatelem také pověřená osoba, pokud tato pověřená osoba splnila všechny podmínky pro zastupování dané organizace. Přesnější definice žadatelů o jednotlivé typy certifikátů jsou uvedeny v příslušné certifikační politice.

1.3.4 Držitelé certifikátů

Držitelem certifikátu je fyzická či právnická osoba, pro kterou se žádalo o certifikát, a které byl certifikát vydán. Ve vydaném certifikátu jsou uvedeny identifikační údaje držitele.

1.3.5 Spoléhající se strany

Spoléhající se stranou je entita spoléhající se na certifikát vydaný z *Komerční banka Qualified CA/RSA*.

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

Certifikát certifikační autority *Komerční banka Qualified CA/RSA* může být používán pouze k ověřování platnosti certifikátů a seznamu zneplatněných certifikátů (CRL), vydaných z této CA.

Certifikáty vydávané z *Komerční banka Qualified CA/RSA* jsou kvalifikovanými certifikáty ve smyslu [eIDAS].

Certifikáty vydávané z *Komerční banka Qualified CA/RSA* mohou být použity:

- k ověření elektronických podpisů (zaručených i kvalifikovaných) v souladu s [eIDAS]
- k ověření elektronických pečetí (zaručených i kvalifikovaných) v souladu s [eIDAS].

Přípustné použití certifikátů vydaných z *Komerční banka Qualified CA/RSA* je uvedeno v certifikační politice daného typu certifikátu. Certifikáty nelze používat v rozporu s platnými právními předpisy.

1.4.2 Omezení použití certifikátu

Certifikáty vydávané z *Komerční banka Qualified CA/RSA* nelze používat k jiným účelům, než je stanoveno v kapitole 1.4.1.

Omezení použití certifikátů, vydaných z *Komerční banka Qualified CA/RSA* je uvedeno v certifikační politice pro daný typ certifikátu.

1.5 SPRÁVA POLITIKY

1.5.1 Organizace pověřená správou dokumentu

Za správu této certifikační prováděcí směrnice i souvisejících certifikačních politik 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

Z Komerční banka Qualified CA/RSA se vydává několik typů certifikátů; pro jednotlivé typy certifikátů je zpracována certifikační politika.

Kontaktní osobou pro účely správy této CPS je Manažer PKI. Další informace je možné získat:

- na webových stránkách https://www.kb.cz/pki
- na e-mailové adrese info_ca@kb.cz.

1.5.3 Osoba odpovědná za soulad CPS s certifikační politikou

Za soulad této certifikační prováděcí směrnice s certifikačními politikami vydávaných certifikátů odpovídá Manažer PKI.

1.5.4 Postupy při schvalování CPS

Tato certifikační prováděcí směrnice je spravována v souladu s interními pravidly kvalifikovaného poskytovatele služeb vytvářejících důvěru. Nové verze vznikají podle potřeby, např. při změně konfigurace CA, postupů pro správu a provoz CA, zavedení podpory nových typů certifikátů. Obecně dochází ke změně CPS v případě, že by dosavadní verze byla v rozporu se skutečnou implementací PKI KB, anebo v případě vzniku skutečností, které je třeba zohlednit v CPS. Certifikační prováděcí směrnici schvaluje Manažer PKI.

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.
Certifikační služba	Kvalifikovaná služba vytvářející důvěru provozovaná za účelem vydávání kvalifikovaných 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
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.
Kvalifikovaný certifikát	Certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky přílohy 1 [EIDAS]
Manažer bezpečnosti PKI	Osoba zodpovědná za administraci poskytovatele a implementaci bezpečnostních pravidel kvalifikovaného poskytovatele služeb vytvářejících důvěru. Osoba je zodpovědná za schvalování změn, které mají dopad na úroveň bezpečnosti kvalifikovaného poskytovatele služeb vytvářejících důvěru.
Manažer PKI	Osoba zodpovědná za akreditaci poskytovatele, interní audit, certifikaci a provoz certifikačních autorit i autorit pro vydávávání časových razítek. Osoba schvaluje dokumenty poskytovatele (certifikační politiky, havarijní plány atd.)
MůjProfil	Webové stránky KB, které slouží žadatelům a držitelům k samoobslužné správě certifikátů. Prostřednictvím webových stránek může např. žadatel požádat o vydání nového certifikátu. Držitel může také zjistit informace o držených certifikátech, požádat o zneplatnění (blokaci) certifikátu.
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 odvolání 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.
Párové klíče, též párová data	Soukromý a veřejný klíč. Viz také Klíčový pár.
Kvalifikovaný poskytovatel služeb vytvářejících důvěru	Společnost Komerční banka, a.s., jako společnost, která provozuje certifikační autoritu a vydává certifikáty.
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 podpisů	Technické zařízení, které slouží k přímému provádění operací s kryptografickými klíči, např. k vytváření elektronických podpisů, ale i k jiným kryptografickým operacím. Držitelé certifikátů, vydaných podle této CP, musí být držitelem prostředku, vydaného kvalifikovaný poskytovatelem služeb vytvářejících důvěru. Prostředek má typicky formu čipové karty anebo podobného zařízení.
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.
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).
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 z *Komerční banka Qualified CA/RSA*. Úložiště informací jsou hostována v rámci interních informačních systémů KB.

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 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 odvolání pomocí OCSP je veřejně dostupné z internetu.

Certifikáty vydávané z certifikační autority *Komerční banka Qualified CA/RSA* nejsou volně dostupné pro spoléhající se strany ani pro další subjekty.

2.2.2 Zveřejňování informací o certifikačních autoritách

Certifikační prováděcí směrnice, 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. 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 politiky jsou zveřejňovány 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, před započetím platnosti dané verze.

2.4 ŘÍZENÍ PŘÍSTUPŮ K JEDNOTLIVÝM TYPŮM ÚLOŽIŠŤ

Certifikační prováděcí směrnice, certifikační politiky, certifikáty CA, seznamy odvolaných 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. V případě neplánovaného výpadku vyvine poskytovatel maximální úsilí, aby obnovil dostupnost nejpozději na konci pracovního dne, který následuje po vzniku výpadku.

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

Vydané certifikáty nejsou zveřejňovány. Jsou přístupné pracovníkům kvalifikovaného poskytovatele služeb vytvářejících důvěru, na základě interních pravidel.

3 IDENTIFIKACE A OVĚŘENÍ

3.1 POJMENOVÁNÍ

3.1.1 Typy jmen

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

E-mailová adresa (je-li v certifikátu obsažena) odpovídá standardu RFC 5322 (historicky RFC 822).

DNS jméno (je-li v certifikátu obsaženo) odpovídá standardu RFC 1035.

3.1.2 Požadavky na významovost jmen

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

Komerční banka Qualified CA/RSA vydává několik typů certifikátů. Identifikační údaje, obsažené ve vydávaných certifikátech, se pro jednotlivé typy certifikátů liší. Pro každý podporovaný typ certifikátu jsou používané identifikační údaje popsány v příslušné certifikační politice.

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

3.1.3 Anonymita a používání pseudonymu

Komerční banka Qualified CA/RSA vydává několik typů certifikátů. Použití pseudonymů je pro každý typ certifikátu specifikováno v příslušné certifikační politice.

3.1.4 Pravidla pro interpretaci různých forem názvů

Pravidla pro interpretaci názvů jsou pro jednotlivé typy certifikátů uvedeny v příslušné certifikační politice.

3.1.5 Jedinečnost jmen

CA zaručuje jedinečnost jmen v předmětu certifikátů, které jsou vydávány klientům KB. Každému klientovi přidělí systémy KB unikátní identifikátor, který se uvádí v předmětu certifikátu.

U certifikátů, které z *Komerční banka Qualified CA/RSA* vydává KB pro svou interní potřebu je jedinečnost názvu předmětu zajištěna procesní kontrolou žádostí. Podrobnosti jsou uvedeny v příslušné certifikační politice.

Pokud je danému držiteli vydáno z PKI KB několik certifikátů (i různého typu), mohou tyto certifikáty obsahovat shodná jména, resp. shodný předmět certifikátu.

3.1.6 Obchodní značky

Použití obchodních značek je pro každý podporovaný typ certifikátu popsán v příslušné certifikační politice.

3.2 POČÁTEČNÍ OVĚŘENÍ IDENTITY

Počáteční ověření identity se provádí před vystavením prvotního certifikátu.

Komerční banka Qualified CA/RSA vydává několik typů certifikátů. Způsob ověření identity je pro každý typ certifikátu specifikován v příslušné certifikační politice.

3.2.1 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 žadatel měl v době vytváření žádosti pod kontrolou soukromý klíč odpovídající veřejnému klíči v žádosti.

3.2.2 Ověřování identity organizace

Způsob ověřování identity organizace je pro jednotlivé typy certifikátu popsán v příslušné certifikační politice. (Pro některé typy certifikátu je ověřování identity organizace irelevantní.)

3.2.3 Ověření identity žadatele o certifikát

Ověřování identity žadatele je pro jednotlivé typy certifikátu popsáno v příslušné certifikační politice.

Obecně platí, že se způsob ověřování identity žadatele liší pro certifikáty vydávané klientům KB a pro certifikáty, které KB vydává pro svou interní potřebu či pro potřebu svých dceřiných společností:

- Pro certifikáty vydávané klientům (včetně právnických osob) je ověření identity spojeno s uzavřením smlouvy mezi klientem a KB. Před navázáním smluvního vztahu KB ověřuje totožnost klienta, v souladu s:
  - Obchodními podmínkami KB
  - Zákonem o bankách č. 21/1992 Sb., resp. č. 353/2021 Sb.
  - Zákonem o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu č. 253/2008 Sb.
- Pro certifikáty vydávané pro potřebu KB jsou definovány interní postupy ověření identity žadatele. Žadateli o certifikáty jsou typicky pracovníci KB, pracovníci dceřiných společností, popř. pracovníci dodavatelských společností. Postupy identifikace žadatele se mohou opírat o autentizaci pracovníků vůči interním informačním systémům KB, a/nebo může být identita žadatele ověřována na základě kontroly osobních dokladů.

3.2.4 Neověřované informace

Neověřované informace jsou pro jednotlivé typy certifikátu uvedeny v příslušné certifikační politice.

3.2.5 Ověřování oprávnění

Mechanismy ověřování oprávnění jsou pro jednotlivé typy certifikátu popsány v příslušné certifikační politice.

Obecně platí rozdílné mechanismy ověřování pro certifikáty vydávané klientům KB a pro interní potřebu KB:

- V případě certifikátů pro klienty KB se provádí ověřování pomocí mechanismů autentizace klientů KB a evidence klientů KB. Klienti se mohou autentizovat vzdáleně, pomocí prostředků pro elektronickou identifikaci uznávaných Komerční bankou. Klienti mohou být také identifikováni pobočkovým pracovníkem KB, pomocí osobních dokladů. Po identifikaci, resp. autentizaci jsou údaje klienta vyhledány v evidenčních systémech KB. Pro vydávání certifikátu je např. ověřováno, zda je klient evidován, splnil všechny náležitosti, má s KB uzavřenu příslušnou smlouvu. Pokud se žádá o certifikát pro organizaci, ověřuje se v evidenci také, zda je identifikovaný klient oprávněn zastupovat danou organizaci.
- V případě certifikátů, vydávaných pro potřeby KB či dceřiných společností, se k ověřování oprávnění používají interní informační systémy KB a/nebo kontrola osobních dokladů. Žadatel o certifikát musí být zmocněn k podání žádosti. Pro zmocnění se obvykle využívá elektronický systém KB (Service Manager). Pověřený pracovník (obvykle nadřízený) v systému elektronicky odsouhlasí, že daný pracovník může požádat o daný certifikát. V rámci registračního procesu se pak musí žadatel identifikovat: buď elektronicky uživatelským účtem proti interním systémům KB anebo pomocí osobních dokladů.

3.2.6 Kritéria pro interoperabilitu (spolupráci)

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

3.3 IDENTIFIKACE A AUTENTIZACE PŘI POŽADAVKU NA VÝMĚNU KLÍČE

Požadavky na identifikaci a autentizaci při požadavku na výměnu klíče jsou pro jednotlivé typy certifikátu stanoveny v příslušné certifikační politice.

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Při běžném požadavku na výměnu klíče jsou obecně podporovány tyto možnosti:

- Postupovat stejně jako v případě počátečního ověření identity při vydání prvního certifikátu – viz kapitolu 3.2.3.
- Doručit žádost o nový certifikát elektronicky; žádost musí být opatřena elektronickým podpisem, resp. pečetí vytvořeným pomocí soukromého klíče certifikátu, k němuž se žádá o nový (následný) certifikát. Identifikační údaje v žádosti se v takovém případě musí shodovat s údaji v certifikátu, jehož soukromým klíčem je žádost autorizována. (Žadatel tímto způsobem mj. potvrzuje, že se identifikační údaje nezměnily.) Certifikát, jehož soukromým klíčem je nová žádost autorizována, musí být platný, a musí být stejného typu, jako je nově požadovaný certifikát.

  Tento mechanismus identifikace je podporován jen pro některé typy certifikátů – viz příslušnou certifikační politiku.

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

Nemá-li žadatel k dispozici platný certifikát, musí při podání žádosti postupovat stejně jako v případě počátečního ověření identity při vydání prvního certifikátu – viz kapitolu 3.2.3.

3.4 IDENTIFIKACE A AUTENTIZACE PŘI POŽADAVKU NA ZNEPLATNĚNÍ CERTIFIKÁTU

Požadavky na identifikaci a autentizaci pro zneplatnění certifikátu jsou pro jednotlivé typy certifikátů stanoveny v příslušné certifikační politice.

Obecně platní, že ke zneplatnění certifikátu může dojít:

- Z vůle držitele certifikátu nebo zmocněného žadatele (lze požádat o zneplatnění pouze u certifikátů daného držitele).
- Z rozhodnutí pověřených pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru.
- Automaticky – technickými prostředky kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Pokud o zneplatnění žádá držitel certifikátu či zmocněný žadatel, pak je postup závislý na typu certifikátu, o jehož zneplatnění se žádá:

- Pokud se žádá o zneplatnění certifikátu vydávaného pro klienty KB, pak osoba, která žádá o zneplatnění, může postupovat jednou z následujících variant:
  - Vznese požadavek telefonicky vůči pracovníkům Kontaktního centra KB. V tomto případě se autentizuje vzdáleně, pomocí identifikačního prostředku KB.
  - Vznese požadavek na obchodním místě KB; v takovém případě se identifikuje svým osobním dokladem.
  - Vznese požadavek prostřednictvím samoobslužného portálu MůjProfil. Pro přístup k portálu KB se klient musí identifikovat příslušným prostředkem pro elektronickou identifikaci.
- Pokud se žádá o zneplatnění certifikátu, vydávaného pro potřeby KB či dceřiných společností, musí žadatel využít interní elektronický systém KB (Service Manager). Žadatel o zneplatnění zavede požadavek na zneplatnění do systému Service Manager; pro přístup do tohoto systému se musí autentizovat svým uživatelským účtem. Vytvořený požadavek na zneplatnění pak zašle správci certifikátů. Správce certifikátů nejprve v evidenci prověří, zda je odesílatel požadavku oprávněn žádat zneplatnění daného certifikátu; pokud je odesílatel oprávněn, provede správce certifikátů zneplatnění certifikátu.

V certifikační politice může být definováno, že o zneplatnění certifikátu mají právo žádat i jiné subjekty, než je uvedeno výše. V takovém případě certifikační politika popisuje také podporované způsoby identifikace a autentizace, potřebné pro vznesení požadavku na zneplatnění certifikátu.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 ŽÁDOST O VYDÁNÍ CERTIFIKÁTU

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Subjekty oprávněné podat žádost o certifikát jsou pro jednotlivé typy certifikátů stanoveny v příslušné certifikační politice.

Obecně lze oprávněné žadatele rozdělit do následujících podmnožin:

- Žadatel je klientem KB, popř. dceřiné společnosti KB. Žadatel musí mít před podáním žádosti s KB uzavřenou Smlouvu o elektronickém podpisu. Žadatelem může být fyzická či právnická osoba.

  Žadatelé v této skupině žádají typicky o certifikát pro sebe (fyzickou osobu) anebo pro organizaci kterou zastupují.

- Žadatel je pracovníkem KB, pracovníkem dceřiné společnosti KB anebo externím spolupracovníkem KB či dceřiné společnosti.

  Žadatelé v této skupině žádají typicky o certifikát, využívaný technickým zařízením KB nebo dceřiné společnosti.

4.1.2 Podání žádosti a odpovědnosti poskytovatele a žadatele

Způsob podání žádosti se pro jednotlivé typy certifikátů liší. Způsob podání je pro každý typ popsán v příslušné certifikační politice.

Obecně platí, že:

- Žadatel podává žádost ve formátu PKCS#10. Žádost obsahuje identifikační údaje subjektu, pro který se žádá o certifikát, a veřejný klíč subjektu. Žádost je opatřena podpisem či pečetí, vytvořeným pomocí soukromého klíče, který se váže k veřejnému klíči v žádosti.
- Před podáním žádosti se provádí identifikace žadatele; ta může být provedena buď v rámci osobní interakce žadatele s poskytovatelem, anebo elektronicky.

Obecně platí, že žádost lze podat některým z následujících způsobů:

- Na obchodním místě KB; tímto způsobem mohou podat žádost smluvní klienti KB.
- Elektronicky přes internet; tímto způsobem mohou podat žádost smluvní klienti KB, kteří mají v držení prostředek pro elektronickou identifikaci a jsou schopni se identifikovat vůči systémům KB.
- Na interním registračním místě KB; tímto způsobem podávají žádost pracovníci KB či dceřiných společností.

4.1.2.1 Odpovědnosti kvalifikovaného 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: buď fyzicky na základě předložených osobních dokladů anebo elektronicky, pomocí prostředku pro elektronickou identifikaci.
- Evidovat identifikační údaje žadatele a další informace, spojené se správou certifikátů žadatele.
- Ověřovat platnost identifikačních údajů držitele, zapisovaných do certifikátu, na základě identifikace žadatele a interní evidence.

- Ověřovat, zda má s žadatelem uzavřenu platnou smlouvu o elektronickém podpisu. (Platí pouze pro certifikáty vydávané smluvním klientům).
- 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).

Další odpovědnosti kvalifikovaného poskytovatele služeb vytvářejících důvěru mohou být uvedeny v certifikační politice daného typu certifikátu.

4.1.2.2 Odpovědnosti žadatele

Žadatel je povinen zejména:

- 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.
- 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 příslušné 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.

Další odpovědnosti žadatele mohou být uvedeny v certifikační politice daného typu certifikátu.

4.2 ZPRACOVÁNÍ ŽÁDOSTI O CERTIFIKÁT

4.2.1 Identifikace a ověření

Identifikace žadatele se provádí v rámci procesu podání žádosti – viz kapitolu 4.1.2.

Výsledkem procesu identifikace žadatele jsou tzv. registrační data. Registrační data jsou souborem datových položek, obsahující mimo jiné:

- Informace o požadovaném typu certifikátu,
- identifikační údaje žadatele,
- identifikační údaje, které mají být zapsány do certifikátu (informace o držiteli certifikátu),
- popř. identifikaci technického prostředku, v němž má být chráněn klíčový pár certifikátu.

Vznik registračních dat je důkazem, že

- úspěšně a korektně proběhlo ztotožnění a identifikace žadatele,
- žadatel splnil všechny podmínky pro podání žádosti,
- proběhlo úspěšné prověření údajů, které mají být zapsány do certifikátu.

Vznik registračních dat se pro jednotlivé typy certifikátů liší:

- Při podání žádosti klientem KB vznikají registrační data v systému KB pro evidenci, identifikaci a autorizaci klientů. Údaje registračních dat jsou exportovány z interní evidence klientů KB.
- Při podání žádosti pracovníkem KB či dceřiné společnosti vznikají registrační data v aplikaci operátora registračního místa. Část registračních dat se extrahuje z podané žádosti a zbylou část kompletuje operátor registračního místa na základě dokladů žadatele a interní evidence KB.

Před vložením do systému CA musí být registrační data autorizována elektronickým podpisem či elektronickou pečetí. Autorizace je důkazem, že:

- buď proběhla korektní elektronická identifikace žadatele a na základě této identifikace byly v interních systémech KB nalezeny platné údaje pro vydání certifikátu,
- anebo proběhla úspěšná osobní identifikace žadatele operátorem registračního místa; na základě identifikace byly zkompletovány platné údaje pro vydání certifikátu.

Autorizovaná registrační data jsou uložena do systému CA. Uložením registračních dat dochází k předschválení žádosti o certifikát. Doručení autorizovaných registračních dat jsou pro systém CA důkazem, že proběhly všechny náležitosti potřebné pro schválení žádosti a vydání certifikátu.

Do systému musí doputovat registrační data, musí být autorizována podpisem či pečetí. Registrační data obsahují údaje žadatele i schválené identifikační údaje, které mají být zapsány do certifikátu. Vznik a mechanismus autorizace registračních se pro jednotlivé typy certifikátů liší.

Po doručení registračních dat může být do CA zaslána i příslušná žádost certifikát. (Elektronická žádost ve formátu PKCS#10). Pro doručení žádosti se využívají tyto způsoby:

- Klienti KB či dceřiné společnosti podávají žádost prostřednictvím softwarové aplikace, kterou jim za tím účelem poskytuje KB. Žádost se z aplikace transportuje elektronicky do systému CA.
- Pracovníci KB předávají datový soubor s žádostí operátorovi registračního místa. Operátor registračního místa vkládá soubor se žádostí do systému CA.

Každá žádost je při vkládání do systému CA autorizována elektronickým podpisem či elektronickou pečetí. Elektronický podpis či pečeť je důkazem, že žádost byla korektně validována a transportována do CA schváleným elektronickým kanálem.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Žádost o certifikát je zpracovávána systémem certifikační autority. CA zpracovává žádost automaticky, při zpracování žádosti využívá registrační data, pro daného žadatele a typ certifikátu. (Vznik a autorizace registračních dat jsou popsány v kapitole 4.2.1.)

V rámci zpracování provádí CA celou řadu kontrol, mimo jiné:

- Kontroluje, zda je žádost korektně autorizována elektronickým podpisem či pečetí. Tzn. zda byla žádost do zpracování doručena důvěryhodným způsobem.
- Kontroluje integritu žádosti PKCS#10. Tzn. ověřuje, zda je žádost opatřena podpisem či pečetí pomocí soukromého klíče, odpovídajícího veřejnému klíči v žádosti.
- Kontroluje, zda jsou registrační data korektně autorizována elektronickým podpisem či pečetí. Tzn. zda registrační data vznikla důvěryhodným způsobem a pocházejí z důvěryhodného zdroje.
- Porovnává, zda schválené údaje registračních dat odpovídají údajům v žádosti.
- Porovnává, zda původce žádosti odpovídá očekávané identitě ve schválených registračních datech.
- Ověřuje, zda registrační data schvalují vydání daného typu certifikátu pro daného žadatele.

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

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

CA při zpracování žádosti prověřuje především:

- Zda má žadatel s KB uzavřenu platnou smlouvu o elektronickém podpisu.
- Zda byl žadatel dostatečně kvalitně identifikován a byla dostatečně kvalitně 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.)
- Zda identifikační údaje uvedené v žádosti odpovídají osobním údajům žadatele v evidenčních systémech KB.
- Zda identifikátor karty, v jejímž čipu byl vygenerován klíčový pár žádosti, odpovídá kartě, která byla Komerční bankou vydána žadateli.

4.2.3 Doba zpracování žádosti o certifikát

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

4.3 VYDÁNÍ CERTIFIKÁTU

4.3.1 Úkony CA při vydávání certifikátu

Pokud žádost projde úspěšně procesem kontrol a zpracování (viz kapitolu 4.2), vydá certifikační autorita na základě žádosti obratem certifikát:

- CA extrahuje z žádosti veřejný klíč a identifikační údaje
- CA příp. doplní část identifikačních údajů ze své interní evidence, resp. z registračních dat.
- CA doplní obvyklé atributy certifikátu (např. rozšíření, sériové číslo atd…).
- CA opatří certifikát elektronickou pečetí, vytvořenou pomocí soukromého klíče CA.

4.3.2 Oznámení žadateli o vydání certifikátu

Žadatel je o vydání certifikátu či zamítnutí žádosti informován:

- buď operátorem registračního místa, s nímž spolupracuje při podání žádosti – v případě podání žádosti na obchodním, resp. registračním místě KB
- anebo softwarovou aplikací, kterou používá pro přípravu žádosti a zaslání žádosti do CA – v případě samoobslužného podání žádosti.

4.4 PŘEVZETÍ VYDANÉHO CERTIFIKÁTU

4.4.1 Úkony spojené s převzetím certifikátu

Převzetí certifikátu bezprostředně navazuje na proces přípravy a podání žádosti – viz kapitolu 4.1.2.

Přesný popis úkonů, spojených s převzetím certifikátu, je pro jednotlivé typy certifikátů popsán v příslušné certifikační politice. Obecně platí:

- Pokud žádost podává klient KB pomocí softwarové aplikace, pak se vydaný certifikát formálně převezme kliknutím na příslušnou volbu v okně aplikace.
- Pokud žádost podává pracovník KB či dceřiné společnosti na interním registračním místě, pak převzetí potvrdí podpisem protokolu.

Převzetím certifikátu držitel potvrzuje:

- že přijímá závazky vyplývající z certifikační politiky, podle které byl certifikát vydán,
- že má v držení a pod svou kontrolou soukromý klíč odpovídající veřejnému klíči v certifikátu,
- že údaje ve vydaném certifikátu jsou platné.

Žadatel může odmítnout převzít certifikát:

- Klient KB může odmítnout převzetí certifikátu kliknutím na příslušnou volbu v softwarové aplikaci, která slouží jako průvodce procesem vydání certifikátu. Projev vůle žadatele se zaznamená do evidence certifikační autority. CA na základě odmítnutí certifikát zneplatní.
- Pracovník KB může odmítnout převzetí certifikátu tím, že odmítne podepsat protokol o převzetí. Operátor registračního místa v takovém případě zajistí zneplatnění certifikátu.

4.4.2 Zveřejnění certifikátu certifikační autoritou

Certifikáty vydávané z certifikační autority *Komerční banka Qualified CA/RSA* nejsou zveřejňovány. Vydané certifikáty jsou evidovány v interních systémech KB a využívány interními systémy KB.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Informace o vydaném certifikátu je zaznamenána do interní evidence klientů Komerční banky.

Informace o vydání certifikátu není oznamována jiným subjektům.

4.5 POUŽITÍ KLÍČOVÉHO PÁRU A CERTIFIKÁTU

4.5.1 Soukromý klíč žadatele a přípustné použití certifikátu

Informace o soukromém klíči žadatele a přípustném použití certifikátu jsou pro jednotlivé typy certifikátu popsány v příslušné certifikační politice.

Držitel certifikátu se zavazuje:

- Dodržovat veškerá relevantní ustanovení příslušné certifikační politiky a dalších souvisejících ujednání KB, jako je smlouva o elektronickém podpisu, obchodní podmínky apod…
- Používat soukromý klíč s certifikátem, pouze pro účely stanovené v příslušné certifikační politice.
- Nakládat se soukromým klíčem v souladu s příslušnou certifikační politikou tak, aby nemohlo dojít k jeho zneužití
- V případě ztráty, odcizení nebo podezření na zneužití soukromého klíče bezodkladně požádat o zneplatnění certifikátu a ukončit používání takového soukromého klíče.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strana je před použitím certifikátu 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 certifikační politiky, podle které byl certifikát vydán; především ustanovení která se vztahují k používání certifikátu.

4.6 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.

4.6.1 Podmínky pro obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.3 Zpracování požadavku na obnovení certifikátu

Služba obnovení certifikátu není poskytována.

4.6.4 Oznámení o obnovení certifikátu držiteli certifikátu

Služba obnovení certifikátu není poskytována.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Služba obnovení certifikátu není poskytována.

4.6.6 Zveřejňování obnovených certifikátů

Služba obnovení certifikátu není poskytována.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

Služba obnovení certifikátu není poskytována.

4.7 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 žadatele. Žádost o nový certifikát není autorizována podpisem, vytvořeným pomocí soukromého klíče stávajícího certifikátu žadatele. 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.

4.7.1 Podmínky pro vydání následného certifikátu

Podmínky pro vydání následného certifikátu jsou popsány v kapitole 3.3.

4.7.2 Subjekty oprávněné požadovat následný certifikát

Žádost o následný certifikát může podat žadatel, který splňuje podmínky uvedené v kapitole 4.1.1.

4.7.3 Zpracování požadavku o následný certifikát

Postup zpracování požadavku o následný certifikát je shodný s postupem zpracování prvního certifikátu – viz kapitoly 4.2 a 4.3.1.

4.7.4 Oznámení žadateli o vydání následného certifikátu

Platí stejné ustanovení, jako pro vydání prvního certifikátu – viz kapitolu 4.3.2.

4.7.5 Úkony spojené s převzetím následného certifikátu

Platí stejné ustanovení, jako pro převzetí prvního certifikátu – viz kapitolu 4.4.1.

4.7.6 Zveřejnění následného certifikátu certifikační autoritou

Stejně jako první vydané certifikáty nejsou zveřejňovány ani následné certifikáty – viz také kapitolu 4.4.2.

4.7.7 Oznámení o vydání certifikátu jiným subjektům

Platí stejné ustanovení, jako pro první vydaný certifikát – viz kapitolu 4.4.3.

4.8 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…).

4.8.1 Podmínky pro změnu údajů v certifikátu

Podmínky pro změnu údajů v certifikátu jsou pro jednotlivé typy certifikátů popsány v příslušné certifikační politice. Základní podmínky jsou uvedeny v následujících podkapitolách.

Kvalifikovaný poskytovatel služeb vytvářejících důvěru může rozhodnout o dílčích změnách profilu certifikátů, jako jsou např. účel použití, aplikační politiky atd… Po změně těchto charakteristik jsou v nově vydávaných certifikátech uvedeny změněné hodnoty.

4.8.1.1 Podmínky pro změnu údajů v certifikátech klientů KB

KB eviduje informace o svých klientech v interních informačních systémech. Údaje o klientech jsou evidovány a aktualizovány v rámci smluvního vztahu a dohodnutých obchodních podmínek. Ke změnám údajů dochází buď na základě informací od klientů anebo automatizovaným přístupem KB do Správy základních registrů ČR, konkrétně Registru obyvatel ČR.

Do vydávaných certifikátů se uvádějí údaje, aktuálně evidované o klientovi v evidenci KB. Obslužný software, který žadatel používá pro vytvoření žádosti, komunikuje s evidenci KB a vloží do žádosti aktuálně evidované údaje. Tyto údaje se při zpracování žádosti kontrolují proti evidenci KB; pokud se údaje neshodují, je žádost zamítnuta. Údaje, které úspěšně projdou ověřením, jsou uvedeny i ve vydaném certifikátu. Identifikační údaje žadatele se tedy při vydání každého certifikátu koncipují nově, bez vazby na jiné certifikáty stejného držitele.

4.8.1.2 Podmínky pro změnu údajů v certifikátech pro interní potřebu KB

Žádosti o certifikáty pro vnitřní potřebu se podávají na interním registračním místě KB. Každá podaná žádost se zpracovává nově, bez vazby na jiné (předchozí) certifikáty. Každá žádost o certifikát daného držitele může obecně obsahovat jiné údaje. Žadatel musí doložit platnost údajů žádosti vždy pro každou podanou žádost. Při zpracování žádosti se nepřihlíží k údajům v jiném certifikátu daného držitele.

4.8.2 Subjekty oprávněné žádat změnu údajů

Žadatel nemusí žádat o vydání nového certifikátu kvůli změně údajů. Může využít standardní interval vydání následného certifikátu.

Při vydání se do certifikátu zapíší vždy aktuální informace:

- Po změně údajů klienta v evidenci KB se nově evidované informace automaticky promítnou do příštího certifikátu, o který žadatel požádá.
- U certifikátů vydávaných pro interní potřebu KB musí žadatel vždy doložit platnost údajů v podané žádosti.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Zpracování certifikátu se změněnými údaji probíhá stejně, jako zpracování žádosti o prvotní certifikát – viz kapitolu 4.2. Údaje v žádosti se kontrolují oproti registračním datům. Registrační data se pro každou žádost kompletují nově, na základě aktuálních, resp. nově prokázaných údajů.

Při vydání certifikátu klientům KB se vždy použijí aktuálně platné identifikační údaje, uvedené v evidenci klientů Komerční banky. Případné změny se tedy do vydaného certifikátu promítnou automaticky.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Platí stejné ustanovení, jako pro vydání prvního certifikátu – viz kapitolu 4.3.2.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Platí stejné ustanovení, jako pro převzetí prvního certifikátu – viz kapitolu 4.4.1.

4.8.6 Zveřejňování certifikátů se změněnými údaji

Stejně jako první vydané certifikáty nejsou zveřejňovány ani certifikáty se změněnými údaji – viz také kapitolu 4.4.2.

4.8.7 Oznámení o vydání certifikátu jiným subjektům

Platí stejné ustanovení, jako pro první vydaný certifikát – viz kapitolu 4.4.3.

4.9 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 služby 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 24 hodin a bude automaticky vyřešen v době vydání následujícího CRL.

V okamžiku, kdy dojde k vypršení platnosti již zneplatněného certifikátu, není tento certifikát nadále uváděn na následných CRL. Služba OCSP o takovém certifikátu vrací stále informaci, že byl zneplatněn, čím vzniká rozdíl mezi výstupem CRL a OCSP: V tomto případě je platná informace ze služby OCSP.

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.

4.9.1 Podmínky pro zneplatnění certifikátu

Důvody pro zneplatnění certifikátu jsou pro jednotlivé typy certifikátů uvedeny v příslušné certifikační politice.

Obecně platí následující podmínky pro zneplatnění certifikátu:

- Podezření z kompromitace či odcizení odpovídajícího soukromého klíče, včetně kompromitace, ztráty, odcizení či zničení čipové karty, která soukromý klíč chrání
- Žádost držitele certifikátu anebo žádost pověřeného zástupce držitele
- Držiteli je odebráno oprávnění k držení daného certifikátu
- Porušení ustanovení certifikační politiky či smluvních podmínek ze strany držitele certifikátu
- Ukončení smluvního vztahu mezi držitelem (jako klientem KB) a Komerční bankou
- Ukončení provozování zařízení, pro které byl vydán certifikát
- Důvody spojené se stavem držitele (úmrtí, zánik, zbavení nebo omezení právní způsobilosti)
- 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.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Subjekty oprávněné žádat o zneplatnění certifikátu jsou pro jednotlivé typy certifikátů uvedeny v příslušné certifikační politice.

Obecně může o zneplatnění certifikátu požádat:

- Držitel certifikátu
- Osoba oprávněná jednat za držitele certifikátu
- Kvalifikovaný poskytovatel služeb vytvářejících důvěru, ve zdůvodněných případech:
    - Správce certifikátů
    - Manažer PKI
    - Manažer bezpečnosti PKI

- Informační systém certifikační autority (automat)

4.9.3 Postup zneplatnění certifikátu

Postup zneplatnění je závislý na tom, kdo o zneplatnění žádá, popř. jakým kanálem doručí požadavek na zneplatnění.

4.9.3.1 Samoobslužné podání žádosti o zneplatnění klientem KB

Klient KB může požádat o zneplatnění certifikátu, jehož je držitelem anebo oprávněným žadatelem. Klient certifikátu může požádat o zneplatnění samoobslužně, prostřednictvím aplikace MůjProfil. Po úspěšné autentizaci vůči aplikaci vyhledá certifikát a požádá o jeho zneplatnění (provede „blokaci“ či „deaktivaci“ bezpečnostní metody). Požadavek se elektronickým kanálem předá do systému certifikační autority a ten provede zneplatnění.

4.9.3.2 Žádost klienta KB o zneplatnění na pobočce KB

Držitel může požádat o zneplatnění certifikátu na pobočce KB. Pro vznesení požadavku se držitel musí identifikovat svým osobním dokladem. Po úspěšné identifikaci pracovník KB zneplatní certifikát pomocí příslušného softwarového vybavení: pracovník se autentizuje, vyhledá v evidenci certifikát a požádá o jeho zneplatnění (provede „blokaci“ či „deaktivaci“ bezpečnostní metody). Požadavek se elektronickým kanálem předá do systému certifikační autority a ten provede zneplatnění.

Stejným způsobem jako držitel může na pobočce požádat o zneplatnění certifikátu také osoba, oprávněná jednat za držitele.

4.9.3.3 Žádost klienta KB o zneplatnění prostřednictvím podpory KB

Klient KB může požádat o zneplatnění svého certifikátu vzdáleně, prostřednictvím Kontaktního centra KB. Pracovník podpory ověří totožnost klienta, pomocí identifikačních prostředků banky. Po úspěšné identifikaci pracovník KB zneplatní certifikát pomocí příslušného softwarového vybavení: pracovník se autentizuje, vyhledá v evidenci certifikát a označí jej jako zneplatněný (provede „blokaci“ či „deaktivaci“ bezpečnostní metody).

4.9.3.4 Žádost o zneplatnění certifikátu, vydaného pro technický prostředek KB

Pro certifikáty, vydávané technickým prostředkům KB či dceřiných společností, může o zneplatnění požádat správce daného zařízení anebo pověřený pracovník. Pracovník KB zavede požadavek na zneplatnění do systému interní podpory KB (Service Manager). Požadavek se doručí správci certifikátů.

Správce certifikátů v interní evidenci prověří, zda byl požadavek vznesen pracovníkem, oprávněným požadovat zneplatnění daného certifikátu. Po úspěšném prověření se správce certifikátů autentizuje vůči aplikaci pro správu certifikátů, vyhledá příslušný certifikát a označí jej jako zneplatněný.

4.9.3.5 Automatizované zneplatnění certifikátu

Zneplatnění certifikátu může provést certifikační autorita (automat) v případech, kdy žadatel odmítne převzít vydaný certifikát, resp. nepotvrdí převzetí vydaného certifikátu.

4.9.3.6 Zneplatnění správcem certifikátů

O zneplatnění certifikátu může rozhodnout rovněž kvalifikovaný poskytovatel služeb vytvářejících důvěru, např. pokud získá věrohodnou informaci o některém z důvodů uvedených v kapitole 4.9.1.

Správce certifikátů v takovém případě zneplatní certifikát: autentizuje se k příslušné softwarové aplikaci, vyhledá certifikát a označí jej jako zneplatněný.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Požadavek na zneplatnění certifikátu musí být vznesen bezodkladně, v co nejkratší době 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 odvolání (odklad).

4.9.5 Doba, ve které musí dojít k zneplatnění certifikátu

Doba mezi vznesením požadavku a zneplatněním certifikátu, se pro jednotlivé postupy liší (viz také kapitolu 4.9.3):

- Pokud držitel požádá o zneplatnění samoobslužně, je certifikát označen jako zneplatněný bezodkladně.
- Pokud držitel požádá o zneplatnění na pobočce KB, prostřednictvím Kontaktního centra anebo prostřednictvím systému podpory (Service Manager), je certifikát označen jako zneplatněný bez zbytečného prodlení po zpracování pracovníkem KB.
- Pokud se certifikát zneplatňuje z vůle kvalifikovaného poskytovatele služeb vytvářejících důvěru, je certifikát označen jako zneplatněný k určenému budoucímu datu zneplatnění.

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 držitel,
- od stanovaného času zneplatnění – v případě, že o zneplatnění rozhodnul kvalifikovaný poskytovatel služeb vytvářejících důvěru.

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

Spoléhající se strany musí při ověřování platnosti certifikátu provádět úkony popsané v kapitole 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů (CRL)

Seznam zneplatněných certifikátů (CRL) je vydáván dle potřeby CA minimálně však jedenkrát denně s dobou platnosti 1 den.

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

4.9.8 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 4.10.2.

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 odvolání certifikátu služby OCSP.

4.9.9 Požadavky na ověřování statutu certifikátu online

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

4.9.10 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.

4.9.11 Zvláštní postupy při kompromitaci klíče

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

4.9.12 Podmínky pro pozastavení platnosti certifikátu

Certifikační autorita *Komerční banka Qualified CA/RSA* neposkytuje podporu pozastavení platnosti certifikátu.

4.9.13 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu není podporováno.

4.9.14 Zpracování požadavku na pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu není podporováno.

4.9.15 Omezení doby pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu není podporováno.

4.10 SLUŽBY SOUVISEJÍCÍ S OVĚŘOVÁNÍM STAVU CERTIFIKÁTU

Pro ověření stavu vydaných certifikátů lze využít:

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

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

4.10.1 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. Služba OCSP je hostována na serveru, provozovaného Komerční bankou. Ke komunikaci se službou OCSP se využívá protokol HTTP.

4.10.2 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.

4.10.3 Další charakteristiky služeb stavu certifikátu

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

4.11 UKONČENÍ POSKYTOVÁNÍ SLUŽEB PRO DRŽITELE CERTIFIKÁTU

Podmínky pro ukončení poskytování služeb jsou pro jednotlivé typy certifikátů uvedeny v příslušné certifikační politice.

V následujících podkapitolách jsou uvedeny základní principy ukončení poskytování služeb pro držitele certifikátu.

CA poskytuje informace o stavu certifikátu i po ukončení poskytování služeb držiteli, a to nejméně po dobu platnosti certifikátu.

4.11.1 Ukončení poskytování služeb klientům KB

Poskytování služby vydávání certifikátu klientům KB je vázáno na platnost smlouvy o elektronickém podpisu. Zánikem této smlouvy je ukončeno poskytování služby. Smlouva o elektronickém podpisu může být ukončena z vůle klienta, KB anebo jiných důvodů (úmrtí apod…)

Pokud má držitel v době ukončení smlouvy o elektronickém podpisu v držení platný certifikát, je takový certifikát zneplatněn.

4.11.2 Ukončení poskytování služby interním držitelům certifikátu

Část certifikátů vydává *Komerční banka Qualified CA/RSA* pro interní účely KB, popř. dceřiných společností KB. Certifikáty jsou vydávány na základě jednotlivých žádostí, nikoli na základě smluvního vztahu.

O certifikáty žádají pověření pracovníci KB, popř. dceřiných společností KB. Pracovník, který žádá o certifikát, k tomuto úkonu musí být oprávněn (zmocněn). Odebráním oprávnění se ukončí poskytování služby danému pracovníkovi. Daný pracovník nemůže požádat o další certifikát. (O certifikát ale může požádat jiný oprávněný pracovník.)

Ukončením poskytování služeb nemusí dojít ke zneplatnění certifikátu, o který žádal pracovník, jemuž bylo odebráno oprávnění. (Certifikát je typicky vydán pro technické zařízení. Toto zařízení může certifikát i nadále používat, pokud nenastala některá z podmínek pro zneplatnění.)

4.12 ÚSCHOVA A OBNOVA KLÍČŮ

Kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje službu úschovy klíčů.

4.12.1 Zásady a postupy pro úschovu a obnovu soukromých klíčů

Kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje službu úschovy klíčů.

4.12.2 Zásady a postupy zapouzdření klíče a jeho obnovení

Kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje službu úschovy klíčů.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

5.1 FYZICKÉ ZABEZPEČENÍ

5.1.1 Umístění a konstrukce

Certifikační autority 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 uživatelské a operátorské počítače, které umožňují dálkový přístup k centrálním systémům kvalifikovaného poskytovatele služeb vytvářejících důvěru.

5.1.2 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 jsou umístěna v kancelářských budovách kvalifikovaného poskytovatele služeb vytvářejících důvěru. Přístup do prostor poskytovatele je řízený a chráněný. Pro přístup je vyžadována identifikace bezkontaktní čipovou kartou. Seznam akceptovaných čipových karet je průběžně aktualizován.

Obchodní místa KB (pobočky apod…), na kterých se poskytuje podpora správy certifikátů, jsou přístupná veřejnosti s tím, že klienti nemají volný přístup k bezpečnostně citlivým zařízením.

5.1.3 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.

5.1.4 Vliv vody

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

5.1.5 Protipožární opatření a ochrana

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

5.1.6 Ukládání médií

Záložní fyzická média jsou uchovávána v chráněných skříních datových center.

5.1.7 Nakládání s odpady

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

5.1.8 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.

5.2 PROCESNÍ BEZPEČNOST

5.2.1 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.

5.2.2 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)

5.2.3 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).

5.2.4 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.

5.3 PERSONÁLNÍ BEZPEČNOST

5.3.1 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).

5.3.2 Posouzení spolehlivosti osob

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

5.3.3 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.

5.3.4 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.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Nestanovuje se.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

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

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

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

5.3.8 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 jsou pracovní směrnice, metodické pokyny, apod.

5.4 AUDITNÍ ZÁZNAMY

5.4.1 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.

5.4.2 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.

5.4.3 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.

5.4.4 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.

5.4.5 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.

5.4.6 Systém shromažďování auditních záznamů

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

5.4.7 Postup při oznamování událostí subjektu, který ji způsobil

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

5.4.8 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.

5.5 UCHOVÁVÁNÍ ZÁZNAMŮ

5.5.1 Typy záznamů

Uchovávají se následující typy záznamů:

- Záznamy související s životním cyklem certifikátů, vč. žádosti 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

Kromě údajů, které uchovává kvalifikovaný poskytovatel služeb vytvářejících důvěru (jako logická jednotka v rámci Komerční banky), se uchovává celá řada dalších záznamů o klientech, kterým jsou poskytovány certifikáty. Tyto záznamy jsou uchovávány v příslušných systémech a úložištích Komerční banky. Mezi těmito záznamy jsou také smlouvy (včetně smlouvy o elektronickém podpisu), obchodní podmínky, protokoly o předání technických prostředků (čipových karet) atd…

5.5.2 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 poskytovatel po dobu následujících 15 let údaje, na základě kterých byla ověřena totožnost žadatele, a také vydané certifikáty.

Dokumentace, 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.)

5.5.3 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.

5.5.4 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.

5.5.5 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.

5.5.6 Systém shromažďování uchovávaných záznamů

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

5.5.7 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.

5.6 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 *Komerční banka Qualified CA/RSA* je po svém vydání umístěn na publikační místa a dán k dispozici spoléhajícím se stranám. (Seznam publikačních míst je uveden v kapitole 2.2.1). Nově vydaný certifikát je také distribuován klientům KB jako součást aktualizace programového vybavení.

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 klientům a 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.

5.7 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.

5.7.1 Postup v případě incidentu a kompromitace

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

5.7.2 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.

5.7.3 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. Oznámení o tomto kroku, 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 přímými komunikačními kanály pro klienty KB, resp. interními komunikačními kanály KB.

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.

5.7.4 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.

5.8 UKONČENÍ ČINNOSTI CA NEBO RA

5.8.1 Řádné ukončení činnosti CA

Nenastanou-li mimořádné okolnosti (viz kapitola 5.8.2), bude činnost certifikační autority ukončena v okamžiku, kdy:

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

Žadatelům 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 5.5.

5.8.2 Mimořádné ukončení činnosti CA

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

- 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 5.5.

5.8.3 Ukončení činnosti RA

Funkci registrační autority pro klienty KB zastávají obchodní místa KB. Ukončením činnosti obchodního místa KB se ukončuje také činnost příslušného registračního místa. Žadatelé o certifikáty se mohou obracet na jiné pobočky KB.

Interní registrační místo (pro vydávání certifikátů k internímu použití v KB a dceřiných společnostech) je dostupné po celou dobu fungování kvalifikovaného poskytovatele služeb vytvářejících důvěru.

6 TECHNICKÁ BEZPEČNOST

6.1 GENEROVÁNÍ A INSTALACE KLÍČOVÉHO PÁRU

6.1.1 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.

Postupy pro generování klíčových párů na straně kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou popsány v instalační příručce dané komponenty, popř. v provozní příručce dané komponenty.

Požadavky na generování klíčových párů žadatelů o certifikáty jsou uvedeny v certifikační politice pro daný typ certifikátu.

6.1.2 Předání soukromého klíče žadateli

Služba generování soukromého klíče pro žadatele není podporována. Žadatel musí generovat soukromý klíč sám.

6.1.3 Předání veřejného klíče kvalifikovanému poskytovateli služeb vytvářejících důvěru

Žadatelé o certifikát předávají veřejné klíče v žádosti o certifikát, ve formátu PKCS#10.

6.1.4 Předání veřejného klíče CA spoléhajícím se stranám

Certifikát certifikační autority *Komerční banka Qualified CA/RSA* i nadřízený (kořenový) certifikát jsou zveřejněny způsobem popsaným v kapitole 2.2.

6.1.5 Délky klíčů

Klíče vydávající certifikační autority *Komerční banka Qualified CA/RSA* mají délku 4096 bitů (algoritmus RSA).

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

Klíče držitelů certifikátů mají minimální délku 2048 bitů (algoritmus RSA). Požadované délky klíčů mohou být upřesněny v příslušné certifikační politice.

6.1.6 Generování parametrů veřejných klíčů a kontrola jejich kvality

Klíče CA a služby OCSP jsou generovány hardwarovým prostředkem, garantujícím kvalitu vygenerovaných kryptografických klíčů.

Klíčové páry žadatelů (včetně veřejných klíčů) jsou generovány technickými prostředky žadatele.

Komerční banka Qualified CA/RSA kontroluje povolenou délku klíčů a možný dvojí výskyt veřejného klíče ve vydávaných certifikátech. V případě duplicitního výskytu veřejného klíče je žádost s tímto klíčem odmítnuta.

6.1.7 Účely použití klíčů

Veřejné klíče držitelů mohou být použity pouze v souladu s příslušnou certifikační politikou. Možnosti použití klíče jsou dále upřesněny v rozšíření certifikátu.

6.2 OCHRANA SOUKROMÉHO KLÍČE A BEZPEČNOST KRYPTOGRAFICKÝCH MODULŮ

6.2.1 Standardy a podmínky používání kryptografických modulů

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

Standardy a podmínky pro ochranu klíčů žadatelů jsou popsány v příslušné certifikační politice.

6.2.2 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.

Držitelé certifikátů aktivují své soukromé klíče sami, podle technických možností použitého úložiště. Podmínky pro ochranu klíčů jednotlivých typů certifikátů jsou uvedeny v příslušné certifikační politice.

6.2.3 Úschova soukromého klíče

Kvalifikovaný poskytovatel služeb vytvářejících důvěru neposkytuje službu úschovy klíčů.

6.2.4 Zálohování soukromého klíče

Soukromé klíče CA i služby OCSP jsou zálohovány s využitím nativních prostředků kryptografického modulu. Zálohované klíče jsou uchovávány v zašifrovaných souborech. Přístup k šifrovaným souborům se zálohou klíčů mají pouze pověření správcové CA. Provedení zálohy, popř. obnovy klíče ze zálohy může provést jedna osoba v roli správce CA.

6.2.5 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 jsou uchovávány minimálně po dobu platnosti příslušného OCSP certifikátu. Po náhradě certifikátu OCSP jsou nepotřebné klíče OCSP služby zničeny.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Pro aktivaci soukromého klíče CA i služby OCSP 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.

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.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče CA a služby OCSP 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.

6.2.8 Postup aktivace soukromého klíče

Před započetím použití soukromých klíčů CA a služby OCSP 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 6.2.2. Podrobný popis aktivace soukromých klíčů v HSM je popsán v interní provozní dokumentaci.

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

6.2.9 Postup deaktivace soukromého klíče

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

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

6.2.10 Postup ničení soukromého klíče

Soukromé klíče CA či služby OCSP 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.

6.2.11 Hodnocení kryptografických modulů

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

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

6.3 DALŠÍ ASPEKTY SPRÁVY PÁRU KLÍČŮ

6.3.1 Archivace veřejných klíčů

Veřejné klíče (ve formě certifikátů) jsou uchovávány po dobu stanovenou v kapitole 5.5.2.

6.3.2 Doba platnosti certifikátů a doba platnosti klíčů

Doba platnosti certifikátů, vydávaných z *Komerční banka Qualified CA/RSA*, je uvedena v příslušném certifikátu. Doba platnosti páru klíčů je shodná s platností certifikátu.

Komerční banka Qualified CA/RSA vydává certifkáty s maximální dobou platnosti 6 let. Doba platnost jednotlivých typů vydávaných certifikátů je stanovena v příslušné certifikační politice.

6.4 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 certifikátů, vydávaných z *Komerční banka Qualified CA/RSA*, jsou pro jednotlivé typy certifikátů stanovena v příslušné certifikační politice.

6.4.1 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. 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 certifikátů, vydávaných z *Komerční banka Qualified CA/RSA*, je pro jednotlivé typy certifikátů popsáno v příslušné certifikační politice.

6.4.2 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.
- Ochrana aktivačních dat certifikátů, vydávaných z *Komerční banka Qualified CA/RSA*, vychází z technologických možností pro uložení klíčů. Pro jednotlivé typy certifikátů je popsáno v příslušné certifikační politice.

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

- Držitel certifikátu 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.

6.4.3 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.

6.5 POČÍTAČOVÁ BEZPEČNOST

6.5.1 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.

V systému certifikačních služeb probíhá pravidelná kontrola konfigurace. Tato kontrola probíhá nejméně jednou za 6 měsíců.

6.5.2 Hodnocení počítačové bezpečnosti

Počítačová bezpečnost systému certifikačních služeb vychází ze standardů pro kvalifikovaného 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.

6.6 BEZPEČNOST ŽIVOTNÍHO CYKLU

6.6.1 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.

6.6.2 Kontroly řízení zabezpečení

Na systém certifikačních služeb byly aplikovány restrikce, používané pro bezpečnostně citlivé serverové komponenty Komerční banky. Na citlivé části systému byly aplikovány bezpečnostní restrikce v souladu s *Microsoft security baseline for Windows Server 2019*, které jsou součástí *Microsoft Security Compliance Toolkit*. Tam, kde byly bezpečnostní politiky KB v nesouladu s *Microsoft Security Compliance Toolkit,* bylo zvoleno přísnější nastavení.

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. Nastavení komponent systému certifikačních služeb je detailně popsáno v příslušné instalační příručce.

6.6.3 Řízení zabezpečení životního cyklu

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

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.

Uživatelské i technické účty, potřebné pro provoz certifikačních služeb, jsou pravidelně vyhodnocovány. V rámci hodnocení jsou účtům odebírána nepotřebná oprávnění. Všechny účty jsou klasifikovány do kategorií podle rizika zneužití. Na jednotlivé kategorie účtů jsou aplikovány omezení, podle interních bezpečnostních politik KB.

6.7 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.

6.8 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.

7 PROFILY CERTIFIKÁTŮ, SEZNAMŮ CRL A OCSP

7.1 PROFIL CERTIFIKÁTU

Profily vydávaných certifikátů odpovídají RFC 5280 (*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*).

Profily jednotlivých typů vydávaných certifikátů jsou uvedeny v příslušné certifikační politice.

7.1.1 Číslo verze

Certifikáty vydávané z *Komerční banka Qualified CA/RSA* odpovídají standardu X.509, verze 3.

7.1.2 Rozšíření certifikátu

Ve vydávaných certifikátech se používají rozšíření; specifikace těchto rozšíření je uvedena v příslušné certifikační politice.

7.1.3 OID algoritmů

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

7.1.4 Zápis jmen a názvů

Jména a názvy se používají v souladu s pravidly v odstavci 3.1.

7.1.5 Omezení jmen

Omezení jmen je pro jednotlivé typy certifikátů stanoveno v příslušné certifikační politice.

7.1.6 OID certifikační politiky

V každém certifikátu, vydaném z *Komerční banka Qualified CA/RSA* je uvedeno rozšíření s definici certifikační politiky, podle níž byl certifikát vydán. Součástí rozšíření je i jednoznačný identifikátor (OID) dané certifikační politiky.

7.1.7 Omezení politiky

Rozšíření Policy Constraints se ve vydaných certifikátech nevyužívá.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Komerční banka Qualified CA/RSA zapisuje do vydávaných certifikátů rozšíření s kvalifikátorem certifikační politiky, podle níž byl certifikát vydán. Podrobný popis tohoto kvalifikátoru je pro jednotlivé typy certifikátů uveden v příslušné certifikační politice. Typicky se v rámci kvalifikátoru uvádí:

- Odkaz na webové stránky kvalifikovaného poskytovatele služeb vytvářejících důvěru, odkud lze získat dokument s příslušnou certifikační politikou.
- Textová informace, že daný certifikát je vydán jako kvalifikovaný certifikát pro elektronický podpis, popř. pro elektronickou pečeť, podle [eIDAS].

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Způsob zápisu rozšíření Certificate Policies je pro jednotlivé typy certifikátů popsán v příslušné certifikační politika. Toto rozšíření není označováno jako kritické.

7.2 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, UTC
Konec platnosti (nextUpdate)	Datum a čas nejpozdějšího vydání dalšího CRL, UTC
Seznam odvolání (revokedCertificates)	Přehled zneplatněných certifikátů sestávající ze sériového čísla, data a důvodu odvolání (uvedení důvodu je nepovinné).
Rozšíření (CRLExtensions)	Viz kapitolu 7.2.2
Podpis (signature)	Elektronická pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru

7.2.1 Číslo verze

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

7.2.2 Rozšíření CRL

Rozšíření (crlExtensions)	Hodnota
Identifikátor klíče CA (není kritické) (authorityKeyIdentifier)	Obsahuje hodnotu z rozšíření Subject Key Identifier certifikátu, kterým má být tento certifikát ověřován. (Obsahuje hash veřejného klíče vydávající CA.)
Číslo seznamu CRL (není kritické) (CRLNumber)	Pořadové číslo aktuálního seznamu CRL

7.3 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 odvolání certifikátu, pak se tento důvod uvádí v sekci SingleResponse, ve struktuře RevokedInfo.

Jako transportní protokol se používá HTTP.

7.3.1 Číslo verze

V žádosti i odpovědi OCSP se uvádí verze 1.

7.3.2 Rozšíření OCSP

Kromě rozšíření, uvedených v úvodu kapitoly 7.3, je v odpovědích OCSP podporováno rozšíření Nonce (pokud je uvedeno ve vstupním požadavku).

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

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

8.1 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] nebo orgánem dohledu [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].

8.2 IDENTITA A KVALIFIKACE HODNOTITELE

8.2.1 Interní hodnocení shody

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

8.2.2 Externí hodnocení shody

Externí hodnocení shody provádí subjekt posuzování shody [eIDAS] nebo orgán dohledu [eIDAS].

8.3 VZTAH HODNOTITELE K HODNOCENÉMU SUBJEKTU

8.3.1 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.

8.3.2 Externí hodnocení shody

Subjekt, který provádí externí hodnocení shody, není žádným způsobem (majetkově ani personálně) svázán s kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

8.4 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.

8.5 POSTUP V PŘÍPADĚ ZJIŠTĚNÍ NEDOSTATKŮ

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

8.6 SDĚLOVÁNÍ VÝSLEDKŮ HODNOCENÍ

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

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 POPLATKY

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za poskytované certifikační služby klientům KB jsou stanoveny v platném Sazebníku KB.

Pro interní použití v KB nebo v dceřiných společnostech jsou certifikáty vydávány bezplatně.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup elektronickou cestou k vydaným certifikátům se neposkytuje.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

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

9.1.4 Poplatky za další služby

Poplatky za další poskytované certifikační služby jsou stanoveny v rámci Všeobecných obchodních podmínek KB.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Žádné ustanovení.

9.2 FINANČNÍ ODPOVĚDNOST

9.2.1 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.

9.2.2 Další aktiva a záruky

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Tato služba není poskytována.

9.3 DŮVĚRNOST OBCHODNÍCH INFORMACÍ

Komerční banka poskytuje certifikační služby v rámci svých dalších služeb klientům, 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.

9.3.1 Rozsah důvěrných informací

Při poskytování certifikačních služeb se využívají osobní a identifikační údaje klientů KB. Informační systémy pro poskytování certifikačních služeb využívají identifikační údaje klientů KB, které byly získány primárně za účelem bankovních a finančních služeb. Identifikační údaje jsou využívány pro ověření totožnosti žadatele o certifikát a pro uvedení pravdivých údajů do vydávaných certifikátů.

Finanční a obchodní údaje nejsou při poskytování certifikačních služeb využívány, ani k nim systémy pro poskytování certifikačních služeb nemají přístup.

Žádné z důvěrných obchodních informací nejsou kvalifikovaným poskytovatelem služeb vytvářejících důvěru zveřejňovány. Veškeré takové údaje jsou evidovány, popř. vyměňovány v souladu s obchodními podmínkami v systémech Komerční banky, popř. jejich dceřiných společností.

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

- Osobní údaje
- Soukromé klíče
- Interní dokumentace
- Interní smluvní ujednání

9.3.2 Informace mimo rámec důvěrných informací

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

9.3.3 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.

9.4 OCHRANA OSOBNÍCH ÚDAJŮ

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

9.4.1 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].

9.4.2 Odpovědnost za ochranu osobních údajů

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

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

9.4.3 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Klienti KB udělují souhlas se zpracováním osobních údajů při navazování smluvního vztahu s Komerční bankou. Tento souhlas se vztahuje i na poskytování certifikačních služeb.

Informace o ochraně osobních údajů jsou uvedeny ve Všeobecných obchodních podmínkách KB, a návazných dokumentech.

9.4.4 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.

9.5 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 certifikačních politik, certifikační prováděcí směrnice, i dalších dokumentů kvalifikovaného poskytovatele služeb vytvářejících důvěru, jsou chráněny autorskými právy kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Autorskými právy jsou chráněny také softwarové aplikace, které Komerční banka poskytuje žadatelům a držitelům pro správu certifikátů.

9.6 ZASTUPOVÁNÍ A ZÁRUKY

Komerční banka, a.s. zaručuje, že splní veškeré povinnosti uložené touto certifikační prováděcí směrnicí, a také povinnosti uložené certifikačními politikami, podle kterých se z *Komerční banka Qualified CA/RSA* vydávají certifikáty.

9.6.1 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 digitálního podpisu
- 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 CPS na vydání CRL
- Bezpečnost osobních údajů o uživatelích, které byly využity při vydání certifikátů

Veškeré záruky je možné uznat jen tehdy, pokud žadatel či držitel neporušil povinnosti plynoucí z certifikační politiky a ze smluvních podmínek KB.

Certifikační autorita dále zaručuje, že:

- Údaje v této CPS jsou platné a pravdivé
- Provozuje certifikační služby zodpovědně, v souladu s CPS, certifikačními politikami, interní dokumentací a běžně platnými technickými i bezpečnostními standardy.
- Zveřejňuje dokumenty certifikačních politik, podle kterých vydává certifikáty
- Zveřejňuje v režimu 24x7 certifikáty certifikačních autorit, potřebné k ověření důvěryhodnosti vydávaných certifikátů
- Umožňuje v režimu 24x7 ověřit stav certifikátu, buď pomocí veřejně přístupného seznamu CRL anebo službou OCSP
- Používá soukromý klíč CA pouze k vystavování certifikátů a CRL
- Používá soukromý klíč služby OCSP pouze k autorizaci odpovědí na stav certifikátu

9.6.2 Zastupování a záruky RA

Registrační autority garantují kvalitu ztotožnění žadatelů prostřednictvím požadovaných osobních dokladů, popř. dalšími způsoby zajišťující stejnou kvalitu ztotožnění.

Ke ztotožnění klientů nemusí dojít v přímé souvislosti s poskytováním certifikačních služeb. Klienti mohou být ztotožněni v souvislosti s poskytováním bankovních a finančních služeb Komerční bankou; získané identifikační údaje pak mohou být akceptovány pro poskytování certifikačních služeb.

Registrační autority fungují v souladu s touto CPS a také s příslušnými certifikačními politikami.

Registrační autority nepřijmou žádost žadatele, jehož identita nebyla dostatečným způsobem prokázána a ověřena.

9.6.3 Zastupování a záruky držitele certifikátu

Držitel certifikátu:

- Zaručuje, že identifikační údaje uvedené v žádosti jsou pravdivé a odpovídají jeho osobním údajům.
- 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 certifikační politice, podle níž byl certifikát vydán.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající strana musí při využití certifikátů jednat v souladu s certifikační politikou, podle níž byl daný certifikát vydán. Viz také kapitolu 4.5.2.

9.6.5 Zastupování a záruky ostatních subjektů

Viz příslušná certifikační politika.

9.7 ZŘEKNUTÍ SE ZÁRUK

Komerční banka poskytuje pouze záruky uvedené v odstavci 9.6.

9.8 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.

Komerční banka neodpovídá za škodu vyplývající z použití certifikátu v období po přijetí žádosti o jeho zneplatnění, učinila-li všechny kroky vyplývající z certifikační prováděcí směrnice a certifikační politiky.

9.9 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 služeb vytvářejících důvěru, uvedených v této certifikační politice a návazných dokumentech.

9.10 DOBA PLATNOSTI, UKONČENÍ PLATNOSTI

9.10.1 Doba platnosti

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

9.10.2 Ukončení platnosti

Platnost tohoto dokumentu je ukončena:

- Jeho nahrazením novější verzí nebo
- Ukončením poskytování certifikačních služeb

9.10.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti tohoto dokumentu z důvodu ukončení poskytování certifikačních služeb zůstávají v platnosti ustanovení uvedená v kapitole 9 týkající se obchodních a právních záležitostí.

V případě rozhodnutí poskytovatele o ukončení vydávání některého typu certifikátu zůstávají v platnosti závazky uvedené v příslušné CP, minimálně do ukončení platnosti všech vydaných certifikátů.

9.11 KOMUNIKACE MEZI ZÚČASTNĚNÝMI SUBJEKTY

9.11.1 Komunikace s kvalifikovaným 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.

Žadatelé a držitelé certifikátů mohou s kvalifikovaným poskytovatelem služeb vytvářejících důvěru komunikovat prostřednictvím:

- Softwarových aplikací, které za tím účelem poskytuje Komerční banka svým klientům
- Kontaktních údajů, uvedených v kapitole 1.5
- Elektronických kanálů klientské podpory Komerční banky
- Pobočkových pracovišť Komerční banky

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

Pracovníci KB, kteří žádají či využívají certifikáty, vydávané z *Komerční banka Qualified CA/RSA*, mohou s kvalifikovaným poskytovatelem služeb vytvářejících důvěru komunikovat prostřednictvím interních kanálů KB, jako je např. systém Service Manager.

9.11.2 Jazyk komunikace

Primárním komunikačním jazykem je čeština. Certifikační služby však mohou být poskytovány i klientům, 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.

Kvalifikovaný poskytovatel služeb vytvářejících důvěru dává žadatelům k dispozici softwarové nástroje v české a anglické lokalizaci.

9.12 ZMĚNY

9.12.1 Postup při změnách

Postupy pro změny probíhají podle ustanovení kapitoly1.5.4.

9.12.2 Postup při oznamování změn

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

9.12.3 Okolnosti, při kterých musí být změněn identifikátor OID

Tomuto dokumentu (CPS) není přiřazován identifikátor OID. V případě změny CPS dochází ke změně verze dokumentu.

Každé certifikační politice, podle níž se z *Komerční banka Qualified CA/RSA* vydávají certifikáty, je přiřazen identifikátor OID. Okolnosti, za kterých se mění hodnota OID, jsou uvedeny v příslušné certifikační politice.

9.13 ŘEŠENÍ SPORŮ

V případě vzniku sporu mezi klientem a kvalifikovaným poskytovatelem služeb vytvářejících důvěru se klient může obrátit na kontaktní údaje uvedené v kapitole 1.3.

Pokud se v rámci jednání nesjedná ukončení sporu, bude se spor mezi klientem a kvalifikovaným poskytovatelem služeb vytvářejících důvěru řešit u místně a věcně příslušného soudu.

9.14 ROZHODNÉ PRÁVO

Rozhodným právem je právo České republiky.

9.15 SHODA S PRÁVNÍMI PŘEDPISY

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

Komerční banka poskytuje certifikační služby v souladu se smluvními ujednáními s klienty, včetně Všeobecných obchodních podmínek a dalších závazných dokumentů.

9.16 DALŠÍ USTANOVENÍ

9.16.1 Rámcová dohoda

Žádná ustanovení.

9.16.2 Postoupení práv

Není stanoveno.

9.16.3 Oddělitelnost ustanovení

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

9.16.4 Zřeknutí se práv

Žádná ustanovení.

9.16.5 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.

9.17 DALŠÍ OPATŘENÍ

Žádná ustanovení.