CERTIFIKAČNÍ POLITIKA OSOBNÍCH KVALIFIKOVANÝCH CERTIFIKÁTŮ PRO ELEKTRONICKÝ PODPIS

Verze 1.3

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

Obsah

Historie revizí a změn dokumentu

Verze	Datum změny	Důvod změny	Schválil
1.3	14.5.2024	Doplněna politika QCP-n-qscd	Tomáš Prjacha, Manažer PKI KB Digitálně podepsal(a) Tomáš Prjacha dne 16.05.2024 10:11:52
1.2	17.4.2024	Doplnění čipových karet v režimu QSCD	Tomáš Prjacha, Manažer PKI
1.1	1.4.2024	Opraven překlep v OID v kapitole 7.1.2.5	Tomáš Prjacha, Manažer PKI
1.0	29.5.2023	První verze	Tomáš Prjacha, Manažer PKI

1 ÚVOD

Tento dokument představuje certifikační politiku kvalifikovaných certifikátů vydávaných pro klienty společnosti Komerční banka, a.s. (dále jen Komerční banka nebo KB).

1.1 PŘEHLED

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

Certifikáty vydávané podle této CP jsou určeny fyzickým osobám – smluvním klientům Komerční banky. Klíčové páry příslušné k certifikátům vydávaných podle této CP, jsou uloženy v čipových kartách. Čipové karty mají vlastnosti hardwarového kryptografického prostředku a jsou klientům vydávány Komerční bankou.

Komerční banka vydává svým klientům:

- Čipové karty v standardním režimu, které jsou prostředkem pro vytváření elektronických podpisů. Tyto karty chrání soukromé klíče a kvalifikované certifikáty klientů. Pomocí těchto karet lze vytvářet *zaručené* elektronické podpisy a *zaručené* elektronické podpisy založené na kvalifikovaném certifikátu.
- Čipové karty v režimu QSCD, které jsou *kvalifikovaným* prostředkem pro vytváření elektronických podpisů. Tyto karty chrání soukromé klíče a kvalifikované certifikáty klientů. Pomocí těchto karet lze vytvářet *kvalifikované* elektronické podpisy.

Komerční banka může vydávat čipové karty, které jsou schopny pracovat ve standardním režimu i v režimu QSCD. V jednu chvíli však karta může být aktivována právě do jednoho režimu.

Držitelé certifikátů, vydávaných podle této certifikační politiky, využívají soukromé klíče příslušné k vydávaným certifikátům při vytváření zaručených elektronických podpisů založených na kvalifikovaném certifikátu, resp. kvalifikovaných elektronických podpisů – podle toho, v jakém režimu je aktivována čipová karta. Spoléhající se strany používají certifikáty pro ověření elektronického podpisu podepisující osoby.

Jak je uvedeno výše, podle této certifikační politiky se vydávají v zásadě dva typy kvalifikovaných certifikátů: pro vytváření *zaručených* elektronických podpisů založených na kvalifikovaném certifikátu a pro vytváření *kvalifikovaných* podpisů. Oba typy certifikátů se liší v příznaku, uvedeném v datech certifikátu. Certifikát pro vytváření kvalifikovaných podpisů v sobě obsahuje informaci, že soukromý klíč certifikátu je chráněn v *kvalifikovaném* prostředku pro vytváření elektronických podpisů. Kromě tohoto rozdílu platí pro oba typy certifikátů stejná pravidla, stejné postupy pro vydání a správu certifikátu. Pokud není v textu uvedeno jinak, platí uvedené klauzule jak pro certifikáty pro *zaručený* elektronický podpis založený na kvalifikovaném certifikátu, tak pro certifikáty pro *kvalifikovaný* podpis.

1.2 NÁZEV DOKUMENTU A IDENTIFIKACE

Název dokumentu	Certifikační politika osobních kvalifikovaných certifikátů pro elektronický podpis
Verze dokumentu	1.3
OID této certifikační politiky	1.3.154.45317054.1000.1.2.1.1.2
Datum vydání	14.5.2024
Datum platnosti	Do odvolání, resp. do vydání nové verze

Struktura dokumentu odpovídá standardu RFC 3647.

1.3 PARTICIPUJÍCÍ SUBJEKTY

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

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

Kontaktní a identifikační údaje kvalifikovaného poskytovatele služeb vytvářejících důvěru:

Komerční banka, a.s.

IČO 45317054, DIČ CZ699001182

Na Příkopě 33, 114 07 Praha 1

Tel: 800 521 521

e-mail: info_ca@kb.cz

1.3.1 Certifikační autority

PKI Komerční banky je tvořeno třívrstvou hierarchií PKI.

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

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

- Některé z vydávajících CA jsou určeny pro interní použití Komerční banky: vydávají certifikáty pro zaměstnance a infrastrukturu KB.
- Jiné vydávající CA jsou určeny pro vydávání certifikátů klientům Komerční banky. Jednou z certifikačních autorit, které vydávají certifikáty pro klienty KB, je *Komerční banka Qualified CA/RSA*.

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

1.3.1.1 Soulad se standardy

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

- [EIDAS] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- [297/2016] Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce
- [ETSI EN 319 401] Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- [ETSI EN 319 411-1] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- [ETSI EN 319 411-2] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- [ETSI TS 119 312] Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- [ETSI EN 319 412-2] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- [ETSI EN 319 412-5] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
- [GDPR] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- [ISO 27001] ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

- [RFC 6960] Internet X.509 internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- [PKCS10] RSA Laboratories - PKCS#10: Certification Request Syntax Standard.
- [FIPS PUB 140-2] Requirements for Cryptographic Modules.
- [ISO/IEC 15408] Information technology — Security techniques — Evaluation criteria for IT security
- [ISO 3166-1] ISO 3166-1 Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.
- [X.501] ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.
- [X.509] ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.
- [X.520] ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.

1.3.2 Registrační autority

Registrační autority jsou provozovány na pobočkách Komerční banky. Registrační proces zajišťují pracovníci Komerční banky.

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,
- přijímají žádosti o certifikáty, popř. zajišťují předání vydaného certifikátu.

1.3.3 Žadatelé o certifikát

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

- Jsou smluvními klienty Komerční banky.
- Před podáním žádosti byla ověřena jejich osobní identita.
- Jsou držitelem kryptografického prostředku po vytváření elektronických podpisů, který jim vydala Komerční banka.

1.3.4 Držitelé certifikátů

Držitelem certifikátu je žadatel, který požádal o vydání certifikátu, a kterému 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 podle této CP.

1.3.6 Další zúčastněné subjekty

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

1.4 POUŽITÍ CERTIFIKÁTŮ

1.4.1 Přípustné použití certifikátu

Kvalifikované certifikáty vydané podle této certifikační politiky mohou být použity pouze k ověřování elektronického podpisu podepisující osoby v souladu s platnými právními předpisy pro služby vytvářející důvěru.

Pokud je v ověřovaném certifikátu uvedena informace, že soukromý klíč certifikátu je chráněn v kvalifikovaném prostředku pro vytváření elektronických podpisů, pak je elektronický podpis *kvalifikovaným* elektronickým podpisem, v souladu s [eIDAS]. Takový elektronický podpis má (podle Článku 25 [eIDAS]) právní účinek rovnocenný vlastnoručnímu podpisu.

Pokud ověřovaný certifikát neobsahuje informaci, že jeho soukromý klíč je uložen v kvalifikovaném prostředku pro elektronický podpis, pak je elektronický podpis *zaručeným* elektronickým podpisem založeným na kvalifikovaném certifikátu.

1.4.2 Omezení použití certifikátu

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

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

Certifikáty nelze používat v rozporu s platnými právními předpisy.

1.5 SPRÁVA POLITIKY

1.5.1 Organizace pověřená správou dokumentu

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

1.5.2 Kontaktní osoba

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

1.5.3 Osoba odpovědná za soulad CP s odpovídající CPS

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

1.5.4 Postupy při schvalování CP

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

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

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

1.6 DEFINICE A ZKRATKY

Následující tabulka obsahuje definice použitých názvů a zkratek.

Zkratka / pojem	Definice
AIA	Authority Information Access. Rozšíření certifikátu, v němž lze získat informaci o certifikátu vydávající (nadřízené) CA. Popř. lze v tomto rozšíření získat také URL pro ověření stavu certifikátu protokolem OCSP.

Aktivace klíče	Uvedení kryptografického klíče do stavu, kdy lze klíč použít pro aktivní operace. Viz také RFC 3647
Aktivační data	Data, potřebná k aktivaci kryptografického klíče, tzn. uvedení klíče do stavu, kdy lze s klíčem provádět aktivní operace. Viz také RFC 3647.
CA	Certifikační autorita – entita, která vydává certifikáty na základě schválených žádostí, a zveřejňuje seznamy CRL
CDP	CRL Distribution Point. URL adresa, z níž lze stáhnout aktuální seznam zneplatněných certifikátů.
Certifikát (v oblasti PKI)	Je datová struktura, která je vydána CA, spojuje veřejný klíč (=data pro ověřování elektronických podpisů) s podepisující osobou a umožňuje ověřit její identitu.
Common Criteria	Mezinárodní standard ISO/IEC 15408 pro hodnocení IT systémů a komponent.
CP	Certifikační politika, viz RFC3647
CPS	Certifikační prováděcí směrnice, viz RFC3647
CRL	Seznam zneplatněných certifikátů, v souladu s RFC 5280
DNS	Domain Name System. Systém doménových jmen, přidělovaným jednotlivým prvkům síťové komunikace. Jeho hlavním úkolem jsou vzájemné převody doménových jmen a IP adres uzlů sítě.
Držitel certifikátu	Viz kapitolu 1.3.4
EAL	Evaluation Assurance Level. Bezpečnostní hodnocení IT systému nebo komponenty podle mezinárodního standardu Common Criteria security evaluation. Čím vyšší ohodnocení, tím vyšší úroveň jistoty, že jsou bezpečnostní funkce hodnocené komponenty či systému správně implementovány.
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
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 soukromým 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]
Kvalifikovaný podpis	Zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření podpisů a který je založen na kvalifikovaném certifikátu. Více viz [eIDAS].
Kvalifikovaný poskytovatel služeb vytvářejících důvěru	Obecně (podle [eIDAS]): poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele V tomto dokumentu: společnost Komerční banka, a.s., jako kvalifikovaný poskytovatel služeb vytvářejících důvěru, který provozuje certifikační autoritu a vydává kvalifikované certifikáty.
Kvalifikovaný prostředek pro vytváření elektronických podpisů	Prostředek k vytváření elektronických podpisů, který kvalitně chrání soukromé klíče podepisující osoby. Např. čipová karta, která prošla mezinárodně uznávaným procesem bezpečnostní certifikace. Více v Příloze II [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 poskytovatele certifikačních služeb.
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 zneplatnění certifikátu. Protokol je definován v RFC 6960, popř. v RFC 2560.
Operátor registračního místa	Pracovník poskytovatele certifikačních služeb, zodpovědný za ověření identity žadatele o certifikát.
Orgán dohledu	Subjekt dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru, podle [eIDAS] a § 13 zákona č. 297/2016 Sb.
Párové klíče, též párová data	Soukromý a veřejný klíč. Viz také Klíčový pár.
PIN	Personal Identification Number. Číselný kód pro autorizaci operací s čipovou kartou.
Podepisující osoba	Fyzická osoba, která vytváří elektronický podpis. Pro účely této CP se za podepisující osobu pokládá držitel certifikátu vydaného podle této CP, který je zároveň oprávněným držitelem čipové karty se soukromým klíčem daného certifikátu.

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 Certifikát na čipové kartě	Prostředek pro elektronickou identifikaci, vydávaný Komerční bankou pro své klienty. Prostředek je založen na čipové kartě s certifikátem pro autentizaci. (Jde o certifikát vydávaný podle jiné certifikační politiky, než je tato politika pro vydávání kvalifikovaných certifikátů.) Pomocí tohoto prostředku je držitel schopen se přihlásit k informačním systémům KB vzdáleně – přes internet. Je běžné, že klíč a certifikát pro elektronickou identifikaci je uložen ve stejné čipové kartě jako klíč a kvalifikovaný certifikát, vydávaný podle této certifikační politiky.
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 KB. Prostředek má typicky formu čipové karty anebo podobného zařízení. Viz také *Kvalifikovaný prostředek pro vytváření elektronických podpisů*.
PUK	PIN Unblocking Key. Číselný kód, kterým lze odblokovat a nastavit autorizační kód karty: PIN, popř. QPIN.
QPIN	Qualified Personal Identification Number. Číselný kód pro autorizaci operací se soukromými klíči pro vytváření kvalifikovaných elektronických podpisů; klíče uložené na čipové kartě.
ROB	Registr obyvatel; jeden ze základních registrů České republiky. Eviduje občany ČR, cizince s povolením trvalého pobytu a některé další fyzické osoby.
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.
Soukromý klíč	Kryptografický klíč, který podepisující osoba používá k vytváření elektronických podpisů. Viz také *data pro vytváření elektronických podpisů* v [eIDAS].
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).
Zaručený podpis	Elektronický podpis, který je jednoznačně spojen s podepisující osobou. Soukromý klíč, kterým byl podpis vytvořen, má podepisující osoba pod svou výhradní kontrolou. Viz také Článek 26 [eIDAS].
Zneplatněný certifikát	Certifikát, jenž je certifikační autoritou označen jako neplatný a jehož stav zneplatnění je oznámen službou OCSP anebo uvedením na seznamu CRL.
Žadatel	Viz kapitolu 1.3.3.

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

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

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

2.2 ZVEŘEJŇOVÁNÍ INFORMACÍ A DOKUMENTACE

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

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

2.2.1 Zveřejňování informací o certifikátech

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

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

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

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

Certifikáty vydávané podle této CP nejsou volně dostupné pro spoléhající se strany ani pro další subjekty.

2.2.2 Zveřejňování informací o certifikačních autoritách

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

2.3 ČAS NEBO ČETNOST ZVEŘEJŇOVÁNÍ INFORMACÍ

Informace jsou zveřejňovány v následujících intervalech:

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

2.4 ŘÍZENÍ PŘÍSTUPŮ K JEDNOTLIVÝM TYPŮM ÚLOŽIŠŤ

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

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

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

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 v certifikátu odpovídá standardu RFC 5322.

3.1.2 Požadavky na významovost jmen

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

V certifikátech vydávaných podle této CP se uvádí:

- Jméno a příjmení držitele
- Identifikátory držitele platné v informačních systémech KB – viz kapitolu 3.1.5
- E-mailová adresa držitele

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

3.1.3 Anonymita a používání pseudonymu

Certifikáty vydávané podle této CP neobsahují anonymní údaje ani pseudonymy.

3.1.4 Pravidla pro interpretaci různých forem názvů

Identifikační údaje držitele uvedené v žádosti o certifikát musí odpovídat informacím, které o žadateli eviduje KB. Identifikační údaje se do evidence KB shromažďují v rámci procesu ověření totožnosti žadatele, popř. mohou být automaticky aktualizovány z Registru obyvatel ČR. Viz také kapitolu 4.8.1.

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

3.1.5 Jedinečnost jmen

CA zaručuje jedinečnost jmen v předmětu vydávaných certifikátů. Každému žadateli přidělí systémy KB unikátní identifikátor, který se uvádí v předmětu certifikátu.

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

Certifikáty vydávané podle této CP neobsahují obchodní značky ani označení, která představují duševní vlastnictví jiných osob.

3.2 POČÁTEČNÍ OVĚŘENÍ IDENTITY

Počáteční ověření identity se provádí před vydáním prvotního certifikátu.

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

Není relevantní pro certifikáty vydávané podle této CP. Tyto certifikáty se vydávají pouze pro fyzické osoby.

3.2.3 Ověření identity žadatele o certifikát

Držitelem certifikátu vydaného podle této CP může být pouze klient Komerční banky. 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.

Ověření totožnosti musí proběhnout na obchodním místě KB, za osobní přítomnosti klienta. K ověření totožnosti musí klient předložit osobní doklady, obsahující fotografii držitele dokladu.

Při ověření totožnosti jsou ověřovány údaje osoby:

- Jméno a příjmení
- Adresa bydliště
- Datum narození
- Číslo, typ a platnost dokladu

Údaje ztotožněné osoby (klienta) zavede KB do své interní evidence. Klientům dále přidělí KB prostředek pro elektronickou identifikaci, na základě smluvního ujednání.

Před podáním žádosti o certifikát musí být žadatel klientem KB ztotožněným výše uvedeným způsobem. Klient musí mít s KB uzavřenu Smlouvu o elektronickém podpisu a musí v době podání žádosti o kvalifikovaný certifikát dosáhnout věku 15 let

K podání žádosti o certifikát může dojít bezprostředně po ztotožnění klienta, anebo s delším časovým odstupem. Přípustné jsou varianty:

- Žadatel podává žádost osobně na pobočce KB, po kontrole osobního dokladu pracovníkem KB.
- Žadatel podává žádost vzdáleně (přes internet) po úspěšném ověření prostředkem Certifikát na čipové kartě.

3.2.4 Neověřované informace

V kapitole 3.2.3 je uvedeno, které údaje o žadateli jsou ověřovány. Ostatní údaje nejsou ověřovány.

3.2.5 Ověřování oprávnění

Žádost o certifikát může podat pouze osoba, která je klientem KB.

Pokud se žádost o certifikát podává vzdáleně (přes internet), musí být žadatel autentizován pomocí prostředku Certifikát na čipové kartě

3.2.6 Kritéria pro interoperabilitu (spolupráci)

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

3.3 IDENTIFIKACE A AUTENTIZACE PŘI POŽADAVKU NA VÝMĚNU KLÍČE

Žádost o certifikát s novým veřejným klíčem může podat pouze klient KB, který má uzavřenu platnou Smlouvu o elektronickém podpisu.

Pro podání žádosti o certifikát s novým veřejným klíčem jsou podporovány varianty:

- Žadatel podává žádost osobně na pobočce KB, po provedení identifikace pracovníkem KB, pomocí osobního dokladu žadatele.
- Žadatel podává žádost vzdáleně (přes internet) po úspěšném ověření prostředkem Certifikát na čipové kartě.

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Pokud žadatel podává žádost na pobočce KB, ověřuje jeho totožnost pracovník KB na základě osobního dokladu žadatele.

Pokud žadatel podává žádost vzdáleně (přes internet), pak se identita žadatele ověřuje vzdálenou autentizací vůči informačnímu systému KB pomocí prostředku elektronické identifikace, který žadateli vydala KB. Pokud žadatel nemá k dispozici žádný platný prostředek pro elektronickou identifikaci, pak musí podat žádost v souladu s požadavky na počáteční ověření identity – viz kapitolu 3.2.3. Platný certifikát vydaný podle této CP nelze použít pro autentizaci žadatele.

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

Pokud žadatel podává žádost na pobočce KB, ověřuje jeho totožnost pracovník KB, na základě osobního dokladu žadatele.

Pokud žadatel podává žádost vzdáleně (přes internet), pak se identita žadatele ověřuje vzdálenou autentizací pomocí prostředku elektronické identifikace, který žadateli vydala KB. Pokud žadatel nemá k dispozici žádný platný prostředek pro elektronickou identifikaci, pak musí podat žádost v souladu s požadavky na počáteční ověření identity – viz kapitolu 3.2.3.

3.4 IDENTIFIKACE A AUTENTIZACE PŘI POŽADAVKU NA ZNEPLATNĚNÍ CERTIFIKÁTU

Ke zneplatnění certifikátu může dojít:

- Z vůle držitele certifikátu (lze požádat o zneplatnění pouze certifikátu daného držitele).
- Z rozhodnutí pověřených pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru.
- Z rozhodnutí orgánu dohledu dle § 13 odst. 2 zákona č. 297/2016 Sb.
- Automaticky – technickými prostředky kvalifikovaného poskytovatele služeb vytvářejících důvěru, v následujících případech:
  - Pokud žadatel odmítne převzít vydaný certifikát.
  - Pokud informační systém KB zjistí v Registru obyvatel změnu osobních údajů, a držitel si ve stanovené lhůtě nevydá nový certifikát s aktuálními údaji. Viz také kapitolu 4.8.

Držitel certifikátu, který žádá o zneplatnění certifikátu, tak může učinit jedním z následujících postupů:

- Vznese požadavek telefonicky vůči pracovníkům Kontaktního centra KB. V tomto případě se klient autentizuje vzdáleně, pomocí identifikačního prostředku KB.
- Vznese požadavek na obchodním místě KB; v takovém případě se držitel identifikuje svým osobním dokladem.
- Vznese požadavek prostřednictvím samoobslužného portálu MůjProfil. Pro přístup k portálu KB se držitel certifikátu musí identifikovat příslušným prostředkem pro elektronickou identifikaci.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 ŽÁDOST O VYDÁNÍ CERTIFIKÁTU

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu může podle této certifikační politiky podat fyzická osoba, která je klientem Komerční banky, popř. klientem dceřiné společnosti KB. Žadatel musí mít před podáním žádosti s KB uzavřenou Smlouvu o elektronickém podpisu.

Před podáním žádosti musí být žadateli z KB vydán technický prostředek pro vytváření elektronických podpisů (čipová karta), včetně autorizačních kódů. Tento prostředek je určen pro ochranu kryptografických klíčů spojených s vydávanými certifikáty.

4.1.2 Podání žádosti a odpovědnosti poskytovatele a žadatele

4.1.2.1 Podání žádosti na obchodním místě KB

Žadatel může podat žádost o certifikát na pobočce KB.

V případě podání žádosti na pobočce KB je podání žádosti výsledkem interakce žadatele s pracovníkem KB. Žadatel se musí vůči pracovníkovi KB nejprve identifikovat svým osobním dokladem. Proces podání žádosti (a vydání certifikátu) pak probíhá na počítači Komerční banky:

- Pracovník KB vyhledá v evidenci údaje žadatele a zahájí proces podání žádosti.
- Žadatel na vyzvání vloží čipovou kartu do čtečky. Používá se čtečka s klávesnicí a displejem, která umožňuje žadateli plně kontrolovat práci s kartou a zadávat PIN na klávesnici čtečky.
- Obslužný software extrahuje z evidence KB údaje žadatele a zobrazí je. Pracovník KB vyzve žadatele ke kontrole údajů. Jsou-li údaje správné, odsouhlasí žadatel přípravu žádosti.
- Obslužný software vygeneruje v čipové kartě klíčový pár. Žadatel autorizuje operace čipové karty zadáním platné hodnoty PIN, popř. QPIN.
- Obslužný software zakóduje do žádosti o certifikát odsouhlasené identifikační údaje žadatele a podepíše žádost soukromým klíčem z nově vytvořeného klíčového páru. Vytvořená žádost má standardizovaný formát PKCS#10.

  Pokud je klíčový pár generován v kvalifikovaném prostředku pro vytváření elektronických podpisů, pak je součástí žádosti také informace prokazující, že daný klíčový pár byl generován v konkrétním prostředku.
- Obslužný software odešle žádost o certifikát do certifikační autority. Spolu s žádostí se odešle také identifikátor karty, v jejímž čipu byl vygenerován klíčový pár žádosti.
- (Proces nekončí podáním žádosti. Žadatel vyčká na vydání certifikátu a následně mu obslužný software uloží vydaný certifikát do čipové karty. Viz níže.)

Po celou dobu procesu přípravy žádosti má žadatel pod svojí výhradní kontrolou čipovou kartu i kryptografické klíče, které se v čipu karty generují a uchovávají.

4.1.2.2 Samoobslužné podání žádosti

Klient KB, který již byl identifikován za osobní přítomnosti na pobočce může podat žádost o certifikát vzdáleně – přes internet. K elektronické identifikaci pak klient KB použije prostředek Certifikát na čipové kartě pro samoobslužné vydání kvalifikovaného certifikátu.

V případě samoobslužného vydání kvalifikovaného certifikátu za využití čipové karty se postupuje následovně:

- Před započetím přípravy žádosti si musí žadatel nainstalovat do počítače obslužný software, který mu poskytne Komerční banka. Součástí obslužného software jsou ovladače čipové karty a aplikační průvodce pro přípravu žádostí a správu certifikátů.

- Pro podání žádosti se žadatel připojí k webovému portálu KB a identifikuje se.

Po úspěšné identifikaci započne proces podání žádosti o certifikát:

- Na počítači žadatele se spustí obslužný software, který žadatele provede celým procesem vydání certifikátu. Obslužný software v průběhu přípravy žádosti zabezpečeně komunikuje se systémy Komerční banky.
- Žadatel na vyzvání vloží čipovou kartu do čtečky, která je připojena k počítači.
- Obslužný software extrahuje z evidence KB údaje žadatele a zobrazí je žadateli. Žadatel údaje zkontroluje. Jsou-li údaje správné, odsouhlasí žadatel přípravu žádosti.
- Obslužný software vygeneruje v čipové kartě klíčový pár. Žadatel autorizuje operace čipové karty zadáním platné hodnoty PIN, popř. QPIN.
- Obslužný software zakóduje do žádosti o certifikát odsouhlasené identifikační údaje žadatele a podepíše žádost soukromým klíčem z nově vytvořeného klíčového páru. Vytvořená žádost má standardizovaný formát PKCS#10.

  Pokud je klíčový pár generován v kvalifikovaném prostředku pro vytváření elektronických podpisů, pak je součástí žádosti také informace prokazující, že daný klíčový pár byl generován v konkrétním prostředku.
- Obslužný software odešle žádost o certifikát do certifikační autority. Spolu s žádostí se odešle také identifikátor karty, v jejímž čipu byl vygenerován klíčový pár žádosti.
- Žadatel vyčká na vydání certifikátu. Softwarový průvodce potvrdí žadateli, že byl certifikát úspěšně vydán a následně mu uloží vydaný certifikát do čipové karty. Viz kapitolu 4.4.1.

4.1.2.3 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 evidence klientů (žadatelů).
- Ověřovat, zda má s žadatelem uzavřenu platnou smlouvu o elektronickém podpisu.
- Poskytnout žadateli technický prostředek pro vytváření elektronických podpisů (čipovou kartu), včetně autorizačních kódů (PIN). Zajistit, aby hodnoty autorizačních kódů znal pouze příslušný žadatel (držitel čipové karty).
- Poskytnout žadateli obslužný software pro přípravu žádostí a správu certifikátů na čipové kartě.
- 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).

4.1.2.4 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.
- Generovat klíčový pár pouze na čipové kartě, která mu byla přidělena Komerční bankou.
- Zajistit, aby čipová karta, v níž je uložen klíčový pár certifikátu, byla pod výhradní kontrolou držitele. Nesdělovat nikomu přístupové kódy karty.
- Nakládat se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu tak, aby nemohlo dojít k jeho neoprávněnému užití nebo zneužití.
- Zajistit, aby užívání klíčového páru a odpovídajícího certifikátu odpovídalo účelům stanoveným v této certifikační politice.
- V případě podezření na zneužití soukromého klíče neprodleně požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče.
- Seznámit se s certifikační politikou a další dokumentací týkající se používání certifikační služby.

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. Žadatel se identifikuje:

- buď osobním dokladem – v případě podání žádosti na pobočce KB,
- anebo prostředkem Certifikát na čipové kartě – v případě samoobslužného podání žádosti přes internet.

Žádost je po vytvoření předána ke zpracování. Na základě identifikace žadatele se vytvoří elektronické pověření, které reprezentuje identitu žadatele. Vazba mezi identifikovaným žadatelem a žádostí se dále využívá při zpracování žádosti.

Systém CA vyhledá v interní evidenci identifikační údaje žadatele, na základě uživatelského pověření doručeného se žádostí. Porovná, zda údaje v žádosti odpovídají identifikačním údajům autentizovaného žadatele.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Žádost o certifikát je zpracovávána systémem certifikační autority. CA při zpracování využívá informace z evidenčních systémů klientů KB.

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.
- Pokud byla žadateli vydána karta, která je kvalifikovaným prostředkem pro vytváření elektronických podpisů, pak se také prověřuje, zda klíčový pár žádosti vzniknul v čipu karty, která byla žadateli vydána. Ověření se provádí na základě kryptograficky zabezpečených informací, uvedených v elektronické žádosti o certifikát.

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

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

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 zpracování (viz kapitolu 4.2), vydá certifikační autorita na základě žádosti obratem certifikát.

Certifikační autorita zapíše do vydaného certifikátu identifikační údaje žadatele – tak, jak byly dodány v žádosti.

Kromě identifikačních údajů zavede CA do vydaného certifikátu i další údaje (aplikační politiky, účel použití certifikátu, atd…), viz kapitolu 7.1.

Certifikát je elektronicky podepsán soukromým klíčem CA.

4.3.2 Oznámení žadateli o vydání certifikátu

Žadatel je o vydání certifikátu či zamítnutí žádosti informován:

- buď pracovníkem KB, s nímž spolupracuje při podání žádosti – v případě podání žádosti na pobočce 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. Provádí se v aplikaci, která slouží jako průvodce procesem vydání certifikátu a která vygenerovala žádost o certifikát – viz kapitolu 4.1.2.1, resp. 4.1.2.2. Softwarový průvodce potvrdí žadateli, že byl certifikát úspěšně vydán.

Žadatel v okně aplikace zkontroluje údaje vydaného certifikátu. Jsou-li údaje správné, formálně převezme vydaný certifikát:

- Při samoobslužném podání žádosti projeví žadatel souhlas s převzetím kliknutím na příslušnou volbu v okně aplikace.
- Při podání žádosti na obchodním místě projeví žadatel souhlas s převzetím
  - kliknutím na příslušnou volbu v okně aplikace
  - nebo pokynem pracovníkovi KB, aby v okně aplikace odsouhlasil převzetí.

Na základě souhlasu žadatele provede aplikační průvodce elektronický podpis prohlášení jímž žadatel souhlasí s převzetím certifikátu. Podpis prohlášení reprezentuje projev souhlasu žadatele s obsahem certifikátu a podmínkami pro jeho užití. Prohlášení je podepsáno soukromým klíčem příslušejícím k nově vydanému certifikátu.

Elektronicky podepsané prohlášení žadatele se zaznamená do evidence certifikační autority; tímto krokem se certifikát pokládá za převzatý držitelem. Následně držitel provede instalací certifikátu k páru klíčů – certifikát se uloží do čipové karty.

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.

Pokud žadatel odmítne převzít certifikát, učiní tak 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.

4.4.2 Zveřejnění certifikátu certifikační autoritou

Certifikáty vydávané podle této certifikační politiky nejsou zveřejňovány.

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

Držitel certifikátu je povinen generovat klíčový pár žádosti o certifikát v čipu karty, která mu byla vydána Komerční bankou. Technologie čipové karty zajistí dostatečnou a trvalou ochranu soukromého klíče certifikátu.

Držitel certifikátu musí mít pod svou výhradní kontrolou autorizační kódy čipové karty, která mu byla vydána Komerční bankou. Hodnoty autorizačních kódu nesmí držitel sdělit žádnému jinému subjektu.

Držitel certifikátu se zavazuje:

- Dodržovat veškerá relevantní ustanovení této certifikační politiky a dalších souvisejících ujednání KB, jako je smlouva o elektronickém podpisu, obchodní podmínky apod…
  - Nepersonalizovanou dokumentaci je možno najít na adrese https://www.kb.cz/cs/nase-aplikace/ke-stazeni
- Používat soukromý klíč s certifikátem, vydaným podle této CP, pouze pro vytváření zaručených podpisů založených na kvalifikovaném certifikátu, resp. kvalifikovaných elektronických podpisů pro použití popsané v kapitole 1.4.1.
  - Je-li soukromý klíč certifikátu uložen v čipové kartě, která je kvalifikovaným prostředkem pro vytváření elektronických podpisů, pak lze soukromý klíč použít pro vytváření *kvalifikovaných* elektronických podpisů. Viz také kapitolu 1.1.
  - Je-li soukromý klíč certifikátu uložen v čipové kartě, která není kvalifikovaným prostředkem pro vytváření elektronických podpisů, pak lze soukromý klíč použít pro vytváření *zaručených* podpisů založených na kvalifikovaném certifikátu.

    Soukromý klíč lze použít pro vytváření zaručených podpisů založených na kvalifikovaném certifikátu i v případě, kdy je soukromý klíč generován v čipové kartě, která je kvalifikovaným prostředkem pro vytváření elektronických podpisů, ale v příslušném certifikátu není uvedeno, že soukromý klíč vzniknul v kvalifikovaném prostředku.
- Nakládat se soukromým klíčem v souladu s touto certifikační politikou tak, aby nemohlo dojít k jeho zneužití.
- V případě ztráty, odcizení nebo podezření na zneužití čipové karty se soukromým klíčem bezodkladně požádat o zneplatnění certifikátu a ukončit používání takového soukromého klíče.
- V případě změny platnosti údajů, uvedených v certifikátu, oznámit tyto změny kvalifikovanému poskytovateli služeb vytvářejících důvěru.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

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

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

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 klient KB, 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.

Neprodleně po potvrzení převzetí nového certifikátu vymaže softwarový průvodce z karty držitele soukromý klíč odpovídající předchozímu certifikátu. Držitel bude moci dále provádět podpisové operace pomocí soukromého klíče, příslušného k nově vydanému certifikátu. Soukromý klíč předchozího certifikátu nebude moci nadále využívat.

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 žadatele, 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

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 žadateli (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 žadatele.

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. Před změnami atributů certifikátu se vydá nová verze certifikační politiky.

Při kontrole osobních údajů v Registru obyvatel ČR mohou informační systémy KB zaznamenat změnu osobních údajů klienta. Pokud se změnily údaje uvedené v certifikátu, pak aktuální certifikát držitele obsahuje neplatné údaje. KB proto vyzývá klienta k vydání nového certifikátu. Klient má na vydání nového certifikátu lhůtu 30 dní, která počíná běžet okamžikem zjištění změny. Pokud si klient v dané lhůtě nevydá nový certifikát, pak kvalifikovaný poskytovatel služeb vytvářejících důvěru certifikát s neaktuálními údaji držiteli zneplatní. Držitel pak může požádat o vydání nového certifikátu, s platnými údaji.

4.8.2 Subjekty oprávněné žádat změnu údajů

O změnu údajů může požádat držitel certifikátu. Pokud se změní některý z údajů držitele, který je uveden v platném certifikátu, pak je držitel povinen:

- Oznámit změněné údaje Komerční bance, prostřednictvím obchodních míst, popř. elektronických kanálů.
- Požádat o zneplatnění certifikátu, který obsahuje neplatné údaje. Následně lze požádat o vydání nového certifikátů se změněnými údaji.

Změna osobních údajů držitele v evidenci klientů KB může být provedena také Komerční bankou, na základě automatizovaného přístupu do Registru obyvatel ČR.

Pro podání žádosti se změněnými údaji platí stejné požadavky jako pro podání žádosti o následný certifikát – viz kapitolu 4.7.1.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

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

Zpracování certifikátu se změněnými údaji probíhá stejně, jako zpracování žádosti o prvotní certifikát – viz kapitola 4.2.

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.

Neprodleně po potvrzení převzetí nového certifikátu vymaže softwarový průvodce z karty držitele soukromý klíč odpovídající předchozímu certifikátu. Držitel bude moci dále provádět podpisové operace pomocí soukromého klíče, příslušného k nově vydanému certifikátu. Soukromý klíč předchozího certifikátu nebude moci nadále využívat.

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 služba OCSP již vrací informaci o zneplatnění certifikátu, zatímco služba CRL ještě ne. V takovém případě je platná informace o zneplatnění certifikátu ze služby OCSP. Tento rozpor bude trvat nejdéle 1 hodinu a bude automaticky vyřešen v době vydání následujícího CRL.

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

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

4.9.1 Podmínky pro zneplatnění certifikátu

Důvody pro zneplatnění certifikátu jsou následující:

- Podezření z kompromitace či odcizení odpovídajícího soukromého klíče, včetně kompromitace, ztráty, odcizení či zničení čipové karty, která soukromý klíč chrání
- Žádost držitele certifikátu
- Žadatel odmítne převzít vydaný certifikát, resp. nepotvrdí převzetí vydaného certifikátu
- Držiteli je odebráno oprávnění k držení daného certifikátu

- Změní se osobní údaje držitele, uvedené v certifikátu, a držitel ve stanovené lhůtě nepožádá o vydání nového certifikátu s platnými údaji – viz kapitolu 4.8.1
- Porušení ustanovení certifikační politiky či smluvních podmínek ze strany držitele certifikátu
- Ukončení smluvního vztahu mezi držitelem (jako klientem KB) a Komerční bankou
- 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

O zneplatnění certifikátu může požádat:

- Držitel certifikátu
- Osoba oprávněná jednat za držitele certifikátu
- Orgán dohledu dle § 13 odst. 2 zákona č. 297/2016 Sb.
- Kvalifikovaný poskytovatel služeb vytvářejících důvěru:
  - 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 držitelem

Držitel certifikátu může požádat o zneplatnění samoobslužně, prostřednictvím aplikace MůjProfil. Po úspěšné autentizaci vůči aplikaci vyhledá a zneplatní certifikát (provede „blokaci“ či „deaktivaci“ bezpečnostní metody).

4.9.3.2 Žádost 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 označí jej jako zneplatněný (provede „blokaci“ či „deaktivaci“ bezpečnostní metody).

Stejným způsobem jako držitel může na pobočce požádat o zneplatnění certifikátu také osoba, oprávněná jednat za držitele – viz také kapitolu 4.9.2.

4.9.3.3 Žádost o zneplatnění prostřednictvím podpory KB

Držitel může požádat o zneplatnění certifikátu vzdáleně, prostřednictvím Kontaktního centra KB. Pracovník podpory ověří totožnost držitele, 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 Automatizované zneplatnění certifikátu

Zneplatnění certifikátu může provést certifikační autorita (automat) v případech, kdy:

- žadatel odmítne převzít vydaný certifikát, resp. nepotvrdí převzetí vydaného certifikátu,
- certifikát obsahuje neplatné osobní údaje držitele, a držitel v definované lhůtě nepožádá o nový certifikát.

4.9.3.5 Zneplatnění operátorem CA

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. Zneplatnění může být také požadováno orgánem dohledu.

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

CA v takovém případě informuje držitele o zneplatnění certifikátu s udáním důvodu zneplatnění. Pro kontakt držitele použije CA údaje uvedené v evidenci klientů KB.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

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

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

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 bez zbytečného prodlení.
- Pokud držitel požádá o zneplatnění na pobočce KB nebo prostřednictvím Kontaktního centra, 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.
- Pokud se certifikát zneplatňuje na základě požadavku orgánu dohledu, je certifikát označen jako zneplatněný bez zbytečného prodlení od obdržení požadavku.

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

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

- od přijetí požadavku – v případě že o zneplatnění požádal držitel,
- od stanoveného času zneplatnění – v případě, že se certifikát zneplatňuje z vůle kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo na základě požadavku orgánu dohledu.

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 se vydává do 1 hodiny od označení certifikátu jako zneplatněného. Nedojde-li ke zneplatnění žádného certifikátu, je nový seznam zneplatněných certifikátů obvykle vydán

12 hodin od předchozího seznamu, nejvýše však 24 hodin od vydání předchozího seznamu zneplatněných certifikátů.

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

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

4.9.8 Maximální zpoždění při zveřejnění seznamu zneplatněných certifikátů (CRL)

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

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

4.9.9 Možnost ověřování statutu certifikátu online

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

4.9.10 Požadavky na ověřování statutu certifikátu online

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

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

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

4.9.12 Zvláštní postupy při kompromitaci klíče

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

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Certifikátům vydaným podle této CP nelze pozastavit platnost.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu není podporováno.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu není podporováno.

4.9.16 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 zneplatněných 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. 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 kvalifikovaný 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

Poskytování služby vydávání certifikátu je ukončeno zánikem smlouvy o elektronickém podpisu. 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.

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

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 provozovatele certifikačních služeb 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 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. Pro auditní záznamy každého systému jsou definovány specifické skupiny pracovníků, kteří mají k záznamům daného systému přístup.

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

5.4.7 Postup při oznamování událostí subjektu, který ji způsobil

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

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

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

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 a schválení ze strany orgánu dohledu umístěn na publikační místa a dán k dispozici spoléhajícím se stranám. (Seznam publikačních míst je uveden v kapitole 2.2.1). Nově vydaný certifikát 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. O vzniklé situaci bude bezodkladně informován orgán dohledu.

Oznámení o ukončení činnosti, včetně důvodů a dalším postupu, pokud nastane, bude zveřejněno na webové stránce na adrese https://www.kb.cz/pki. Držitelé certifikátů budou na tento stav upozorněni přímými komunikačními kanály pro klienty 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 5.8.3), bude činnost certifikační autority ukončena v okamžiku, kdy:

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

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

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 Odnětí statusu kvalifikovaného poskytovatele služeb vytvářejících důvěru

Pokud orgán dohledu odejme status kvalifikovaného poskytovatele služeb vytvářejících důvěru, pak budou o této skutečnosti informováni držitelé platných certifikátů. Držitelé budou informování prostřednictvím kontaktních údajů uvedených v evidenci klientů KB, zejména e-mailových adres. Informace budou uvedeny také na webové stránce na adrese https://www.kb.cz/pki

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

5.8.3 Mimořádné ukončení činnosti CA

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

- Neprodleně informovat orgán dohledu
- Co nejdříve (pokud možno s předstihem) informovat držitele platných certifikátů o ukončení činnosti CA, prostřednictvím e-mailových zpráv a na webové stránce na adrese.
- 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.

5.8.4 Ukončení činnosti RA

Funkci registrační autority 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.

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.

Klíčový pár žadatele o certifikát musí být generován v technickém prostředku pro vytváření elektronických podpisů (čipové kartě), který byl žadateli dodán kvalifikovaným poskytovatelem služeb vytvářejících důvěru. Žadatel musí na vyzvání autorizovat generování páru klíčů zadáním PIN, popř. QPIN. Za ochranu a uchování klíčových párů je zodpovědný žadatel, resp. držitel 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.

Pokud je klíčový pár generován v kvalifikovaném prostředku pro vytváření elektronických podpisů, pak je součástí žádosti také kryptograficky zabezpečená informace, že daný klíčový pár byl vygenerován v konkrétním prostředku (čipové kartě).

6.1.4 Předání veřejného klíče CA spoléhajícím se stranám

Nadřízené certifikáty jsou zveřejněny způsobem popsaným v kapitole 2.2.

Certifikáty CA jsou také žadatelům a držitelům certifikátů předány jako součást softwarové aplikace pro správu životního cyklu certifikátu.

6.1.5 Délky klíčů

Klíče vydávající certifikační autority 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).

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 jsou generovány v čipu technického prostředku žadatele.

Použité prostředky zajišťují kvalitu generování klíčových párů. Viz také kapitolu 6.1.1.

6.1.7 Účely použití klíčů

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

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+.

Soukromé klíče mají držitelé generovány a chráněny v čipové kartě, což je kryptografický prostředek, certifikovaný podle FIPS 140-2 level 3, popř. podle CC EAL5+.

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, zadáním platné hodnoty PIN, resp. QPIN čipové karty.

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 zašifrované podobě.

Soukromé klíče držitelů certifikátů nejsou zálohovány.

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.

Soukromé klíče držitelů certifikátů vydávaných podle této CP jsou zničeny (vymazány) po vydání novějšího certifikátu držiteli.

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.

Soukromé klíče držitelů certifikátů vznikají a jsou trvale uloženy v čipu technického prostředku, vydaného držiteli Komerční bankou. Soukromé klíče nikdy neopustí chráněné prostředí čipu.

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.

Držitelé certifikátů vydaných podle této CP aktivují soukromý klíč zadáním platné hodnoty PIN, resp. QPIN do softwarového ovladače karty. Softwarový ovladač přenese autorizační kód do čipu karty, kde dojde k jeho ověření. Po úspěšném ověření autorizačního kódu dojde k aktivaci soukromého klíče v čipu karty.

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

Deaktivace soukromého klíče držitele certifikátu se provede automaticky, pokud nastane jedna z následujících podmínek:

- Karta držitele je vyjmuta ze čtečky nebo dojde k přerušení komunikace karty se čtečkou.
- Dojde k ukončení softwarové aplikace, která využívala soukromý klíč.
- Jde-li o soukromý klíč pro vytváření kvalifikovaných elektronických podpisů, dojde k jeho deaktivaci po provedení aktivní operace (např. vytvoření elektronického podpisu). U těchto typů klíčů je nutno provádět aktivaci pro každou operaci – je nutno zadávat QPIN.

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.

Soukromé klíče držitelů certifikátů se zničí vymazáním klíče z čipu technického prostředku (karty). Ke smazání může dojít:

- V rámci procesu vydání nového certifikátu. V takovém případě zajistí vymazání staršího klíče softwarová aplikace, která provádí držitele procesem vydání certifikátu.
- Z vůle držitele technického prostředku, který hostuje soukromý klíč. Držitel pro vymazání může použít softwarovou aplikaci pro správu karty. Tuto aplikaci dodává Komerční banka.

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

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.
- Aktivačními daty certifikátu, vydávaného podle této certifikační politiky, je PIN, resp. QPIN čipové karty. PIN/QPIN je ve výhradním držení držitele certifikátu.

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. Aktivační data mohou být pro další klíčové páry OCSP vygenerována znovu a změněna. Postup generování a instalace aktivačních dat je popsán v interní dokumentaci služby OCSP. Za generování a ochranu aktivačních dat je zodpovědný správce služby OCSP.
- Aktivační data čipové karty, která je žadatelům o certifikát předána pro ochranu soukromých klíčů, jsou nastavena v rámci přípravy karty. Před předáním karty držiteli jsou v čipu karty nastaveny náhodné hodnoty PIN a PUK. Tyto hodnoty jsou vytištěny a uloženy do neprůhledné obálky. Hodnoty aktivačních dat nejsou evidovány v žádných informačních systémech; kvalifikovaný poskytovatel služeb vytvářejících důvěru hodnotu aktivačních dat nezná. Nepoškozená obálka s PIN a PUK je předána žadateli, spolu s čipovou kartou. Žadatel o certifikát získá hodnotu PIN, resp. PUK po rozlepení obálky. Kvalifikovaný poskytovatel služeb vytvářejících důvěru doporučuje, aby si držitel čipové karty změnil hodnoty aktivačních dat, před přípravou první žádosti o certifikát. Držitel čipové karty si může v průběhu používání hodnotu aktivačních dat kdykoli změnit.

  Pokud je používána čipová karta, která je kvalifikovaným prostředkem pro vytváření elektronických podpisů, pak využívá autorizační kód QPIN. QPIN slouží k autorizaci operací se soukromým klíče pro vytváření kvalifikovaných podpisů. Ovladače karty vyzvou držitele k nastavení QPIN před prvním vygenerováním takového klíče.

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.
- Aktivační data čipové karty, používané pro ochranu soukromých klíčů držitele certifikátu, jsou pod výhradní kontrolou držitele certifikátu. Předpokládá se, že si držitel hodnotu aktivačních dat pamatuje, popř. si hodnotu aktivačních dat archivuje do bezpečného úložiště, které je pod jeho výhradní kontrolou.

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.

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 kvalifikovaného 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

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.

6.6.3 Řízení zabezpečení životního cyklu

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

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

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

Certifikát je vydáván klientům Komerční banky, kteří mají uzavřenu smlouvu o elektronickém bankovnictví.

Klíče certifikátů jsou generovány a (po celou dobu života) chráněny v čipové kartě. Soukromé klíče certifikátů lze použít pro vytváření zaručených podpisů založených na kvalifikovaném certifikátu, resp. kvalifikovaných podpisů. Viz také kapitolu 7.1.2.9.

Profil kvalifikovaného certifikátu fyzické osoby je v souladu s normou ETSI EN 319 412-2.

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

Položka	Hodnota	
Verze (Version)	verze 3 *(0x2)*	
Sériové číslo (Serial number)	Jedinečné číslo certifikátu	
Vydavatel (Issuer)	Označení kvalifikovaného poskytovatele služeb vytvářejících důvěru:	
	CN (commonName)	*Komerční banka Qualified CA/RSA*
	O (organisationName)	*Komerční banka, a.s.*
	OID 2.5.4.97 (organizationIdentifier)	*NTRCZ-45317054*
	C (countryName)	*CZ*
Platnost od (Not Before)	Datum počátku platnosti certifikátu, v UTC	
Platnost do (Not After)	Datum konce platnosti certifikátu, v UTC (začátek platnosti + 2 roky)	
Předmět (Subject)	Identifikace držitele certifikátu:	
	CN (commonName)	Jméno a příjmení držitele
	OID 2.5.4.13 (description)	*elektronické podepisování ve vztahu ke třetím stranám a KB*
	G (givenName)	Křestní jméno držitele
	SN (surname)	Příjmení držitele
	OID 2.5.4.5 (serialNumber)	Jednoznačný identifikátor držitele přidělený kvalifikovaným poskytovatelem služeb vytvářejících důvěru

	C (countryName)	Kód země adresy trvalého bydliště držitele, podle ISO 3166
Algoritmus podpisu (Signature Algorithm)	RSASSA-PSS (PKCS #1 v2.1) OID: 1.2.840.113549.1.1.10 hashAlgorithm: SHA512 OID: 2.16.840.1.101.3.4.2.3 maskGenAlgorithm: mgf1 s hash funkcí stejnou jako v hashAlgorithm OID: 1.2.840.113549.1.1.8	
Veřejný klíč (Subject Public Key Info)	Veřejný klíč subjektu certifikátu	
	Algoritmus (Algorithm)	rsaEncryption
	Veřejný klíč (SubjectPublicKey)	Veřejný klíč min. 2048 bitů
Signature	Elektronická pečeť vydavatele certifikátu	

7.1.1 Číslo verze

Vydávané certifikáty odpovídají standardu X.509, verze 3.

7.1.2 Rozšíření certifikátu

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

7.1.2.1 Použití klíče (Key Usage)

Kritické rozšíření.

Toto rozšíření je řešeno nastavením odpovídajícího bitu dle následujícího seznamu:

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

7.1.2.2 Zásady certifikátu (Certificate Policies)

Nekritické rozšíření.

Rozšíření obsahuje sekvenci dvou certifikačních politik:

policyInformation (1)	■ Identifikátor zásad=1.3.154.45317054.1000.1.2.1.1.2 ■ [1,1] Informace o kvalifikátoru zásad: ID kvalifikátoru zásad=userNotice Kvalifikátor (Qualifier): *Tento kvalifikovany certifikat pro elektronicky podpis byl vydan v souladu s narizenim EU c. 910/2014. This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014.* ■ [1,2] Informace o kvalifikátoru zásad: ID kvalifikátoru zásad=cPSuri Kvalifikátor (Qualifier): https://www.kb.cz/pki

policyInformation (2)	Podle úložiště soukromého klíče certifikátu: ■ Je-li soukromý klíč chráněn ve standardní čipové kartě, která *nemá* charakter kvalifikovaného prostředku pro vytváření elektronických podpisů, uvádí se identifikátor zásad OID: 0.4.0.194112.1.0 *QCP-n: certificate policy for EU qualified certificates issued to natural persons* ■ Je-li soukromý klíč chráněn v QSCD čipové kartě, která *je* kvalifikovaným prostředkem pro vytváření elektronických podpisů, uvádí se identifikátor zásad OID: 0.4.0.194112.1.2 *QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a Qualified electronic Signature/seal Creation Device (QSCD)*

7.1.2.3 Základní omezení (Basic Constraints)

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

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

7.1.2.4 Alternativní název předmětu (Subject Alternative Name)

V tomto nekritickém rozšíření se uvádí e-mailová adresa držitele certifikátu (rfc822Name)

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

- id-kp-emailProtection (ochrana e-mailu), OID: 1.3.6.1.5.5.7.3.4
- ms-Document_Signing (podpis dokumentů), OID: 1.3.6.1.4.1.311.10.3.12

7.1.2.6 Distribuční místa zneplatněných certifikátů (CRL Distribution Points)

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

7.1.2.7 Přístup k informacím autority (Authority Information Access)

Toto rozšíření obsahuje:

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

Viz také kap. 2.2.1.

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

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

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

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

7.1.2.9 Rozšíření kvalifikovaných certifikátů (qcStatements)

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

Kvalifikátor	Název / OID	Hodnota, poznámka
Kvalifikovaný certifikát	esi4-qcStatement-1 {0.4.0.1862.1.1}	
Odkazy na dokument PKI Disclosure Statement (PDS)	esi4-qcStatement-5 {0.4.0.1862.1.5}	en: https://www.kb.cz/pki/pds_en.pdf cs: https://www.kb.cz/pki/pds_cs.pdf
Soukromý klíč chráněn v kvalifikovaném prostředku pro vytváření elektronických podpisů	esi4-qcStatement-4 {0.4.0.1862.1.4}	Uvádí se pouze v certifikátech, jejichž klíčový pár byl generován v kvalifikovaném prostředku pro vytváření elektronických podpisů
Typ certifikátu	esi4-qcStatement-6 {0.4.0.1862.1.6}	Obsahuje typ: elektronický podpis {0.4.0.1862.1.6.1}

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

Na vydávané certifikáty není aplikováno omezení jmen.

7.1.6 OID certifikační politiky

Identifikátor této certifikační politiky je uveden v kapitole 1.2, resp. v kapitole 7.1.2.2.

7.1.7 Omezení politiky

Rozšíření Policy Constraints se ve vydaných certifikátech nevyužívá.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz kapitolu 7.1.2.2.

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

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

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, v UTC
Konec platnosti (nextUpdate)	Konec platnosti seznamu CRL, v UTC
Seznam zneplatnění (revokedCertificates)	Přehled zneplatněných certifikátů sestávající ze sériového čísla, data a důvodu zneplatnění (uvedení důvodu je nepovinné).
Rozšíření (CRLExtensions)	Viz kapitolu 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)	Viz kapitola 7.1.2.8
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 zneplatnění 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] 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].

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 provozovatelem certifikačních služeb.

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. Manažer PKI předloží výslednou zprávu orgánu dohledu, a to do 3 pracovních dnů od jejího obdržení. Manažer PKI také rozhodne o případné distribuci zprávy na další příjemce či zveřejnění zprávy.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 POPLATKY

9.1.1 Poplatky za vydání nebo obnovení certifikátu

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

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

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

9.6 ZASTUPOVÁNÍ A ZÁRUKY

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

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 elektronické pečetě
- Správné použití soukromých klíčů příslušných k nadřízeným certifikátům
- Vydávání pouze těch certifikátů, které jsou popsány v některé z platných certifikačních politik
- Shodu identifikačních údajů uvedených v žádosti o vydání certifikátu s těmito údaji obsaženými ve vydaném certifikátu
- Soulad certifikátů, CRL a OCSP s běžně používanými průmyslovými standardy
- Možnost požádat o zneplatnění certifikátu držitelem
- Dostupnost certifikátů certifikačních autorit, CRL a služby OCSP
- Časové limity uvedené v této certifikační politice na vydání CRL
- 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 ze smluvních podmínek KB.

9.6.2 Zastupování a záruky RA

Registrační autority garantují kvalitu ztotožnění klientů KB 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.

KB nevydá certifikát žadateli, 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 vydání certifikátu je v souladu s bezpečnostní politikou Komerční banky
- Zaručuje, že soukromý klíč příslušný k danému certifikátu je pod jeho výhradní kontrolou.
- Zaručuje, že přístup k soukromému klíči vydaného certifikátu nemají neoprávněné osoby či systémy.
- Zaručuje, že aktivační data k soukromým klíčům jeho certifikátů, jsou pod jeho výhradní kontrolou.
- Zaručuje, že bude dodržovat požadavky a pravidla, uvedené v této certifikační politice.

9.6.4 Zastupování a záruky spoléhajících se stran

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

9.6.5 Zastupování a záruky ostatních subjektů

Tato certifikační politika nedefinuje požadavky na zajištění a záruky ostatních subjektů.

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

9.10.2 Ukončení platnosti

Platnost tohoto dokumentu je ukončena:

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

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 daného typu certifikátu zůstávají v platnosti závazky uvedené v této 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.

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

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

9.12.3 Okolnosti, při kterých musí být změněn identifikátor OID

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

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

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

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

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.

9.16.6 Prohlášení o nediskriminaci

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

9.16.7 Přístupnost pro osoby se zdravotním postižením

Zdravotně postižené osoby se předem telefonicky spojí s pobočkou, kterou hodlají navštívit. Pobočka potvrdí termín návštěvy nebo v závislosti na typu zdravotního postižení domluví návštěvu vhodnější pobočky KB.

Seznam poboček, u kterých je zajištěna přístupnost pro osoby se zdravotním postižením, je možno najít na adrese https://www.kb.cz/cs/pobocky-a-bankomaty?isAccessible=true&isDeafFriendly=true.

V případě, že zdravotní postižení neumožňuje manipulovat a přečíst obsah zalepené obálky s čipovou kartou a PIN, pak je nutná přítomnost asistenta (je možné převzatou zalepenou obálku za přítomnosti asistenta otevřít až doma a certifikát vydat vzdáleně, tj. není bezpodmínečně nutná přítomnost asistenta na pobočce). Pracovník KB nesmí zalepenou obálku otevřít.

Prohlášení o přístupnosti je možno najít na adrese https://www.kb.cz/cs/prohlaseni-o-pristupnosti.

9.17 DALŠÍ OPATŘENÍ

Žádná ustanovení.