CERTIFIKAČNÍ POLITIKA A CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE KOŘENOVÉ CERTIFIKAČNÍ AUTORITY KB ROOT 3

Verze 1.0

Certifikační politika je veřejným dokumentem, který je vlastnictvím společnosti Komerční banka, a.s. Duplikace kterékoli části tohoto dokumentu třetí straně není povolena bez předchozího souhlasu Komerční banky, a.s.

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

Obsah

Historie revizí a změn dokumentu

Verze	Datum změny	Důvod změny	Schválil
1.0	29.5.2023	První verze	Tomáš Prjacha, Manažer PKI  Digitálně podepsal(a) Tomáš Prjacha dne 29.05.2023 10:17:41

1 ÚVOD

1.1 PŘEHLED

Tento dokument slouží jako certifikační politika a certifikační prováděcí směrnice (dále jen Politika) a stanovuje sadu pravidel pro vydávání a používání certifikátu kořenové certifikační autority KB Root 3 a bezpečnostních opatření spojených s vydáváním těchto certifikátů.

Kořenová certifikační autorita KB Root 3 je vytvořena tak, aby splňovala požadavky norem ČSN ETSI EN 319 411-1, ČSN ETSI EN 319 411-2 a ČSN ETSI EN 319 401.

Osnova tohoto dokumentu vychází ze standardu RFC 3647.

1.2 NÁZEV A IDENTIFIKACE DOKUMENTU

Název dokumentu	**Certifikační politika a certifikační prováděcí směrnice Kořenové certifikační autority KB Root 3**
IČO Komerční banka a.s.	45317054
OID Česká republika	1.3.154
OID Komerční banka a.s.	1.3.154.45317054
OID tohoto dokumentu	**1.3.154.45317054.1000.1.1.1.1.1**

1.3 PARTICIPUJÍCÍ SUBJEKTY

1.3.1 Certifikační autority

Certifikační autorita KB Root CA 3 je kořenovou certifikační autoritou, která vydává certifikát sama sobě, a dále výhradně podřízeným certifikačním autoritám.

Certifikační autorita KB Root CA 3 nevydává certifikáty koncovým entitám.

1.3.2 Registrační autority

Certifikační autorita KB Root CA 3 neprovozuje registrační autority. Certifikační autorita KB Root CA 3 vydává certifikáty pouze ceremoniální cestou.

1.3.3 Držitelé certifikátů

Držiteli certifikátů KB Root CA 3 jsou:

- Držitelem kořenového certifikátu KB Root CA 3 je společnost Komerční banka a.s.
- Držiteli ostatních certifikátů jsou provozovatelé podřízených certifikačních autorit KB, kterým KB Root CA 3 vydala certifikáty. Pokud jde o podřízené certifikáty sloužící pro vydávání kvalifikovaného certifikátu jsou vydávány pro společnost Komerční banka,

1.3.4 Spoléhající se strany

Spoléhajícími se stranami jsou fyzické osoby, právnické osoby nebo organizační složky států spoléhající se na kořenový certifikát KB Root CA 3.

1.3.5 Jiné participující strany

Jinými participujícími stranami jsou orgány posuzování shody, orgány dohledu, orgány činné v trestním řízení a další, kterým to přísluší ze zákona.

1.4 POUŽITÍ CERTIFIKÁTU

1.4.1 Přípustné použití

Certifikáty vydané certifikační autoritou KB Root CA 3 je možné používat pouze k ověřování platnosti podřízených certifikačních autorit a certifikátů jimi vydaných.

1.4.2 Omezení použití

Certifikáty nesmí být použity v rozporu s tímto dokumentem, dalšími interními předpisy, platnou legislativou a dalšími právními předpisy.

1.5 SPRÁVA POLITIKY

1.5.1 Organizace pověřená správou dokumentu

Za správu toho dokumentu je zodpovědná Komerční banka, a.s. IČO 45317054. se sídlem Komerční banka, a.s., se sídlem Na příkopě 969/33, Staré Město, 110 00 Praha.

1.5.2 Kontaktní osoba

Kontaktní osobou pro účely správy této Politiky je Manažer bezpečnosti PKI. Další informace je možno získat na emailové adrese info_ca@kb.cz a na webové adrese poskytovatele certifikačních služeb www.kb.cz/pki .

1.5.3 Postup při schvalování Politiky

Tato politika je spravována v souladu s interními pravidly poskytovatele certifikačních služeb. Nové verze této politiky vznikají dle potřeby, zejména však při změně konfigurace CA, vlastností certifikátů či souvisejících postupů, které ovlivní jejich obsah, nebo pokud jakékoli jiné okolnosti její úpravu vyžadují.

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

Politiku schvaluje Manažer bezpečnosti PKI.

1.6 DEFINICE A ZKRATKY

Soukromý klíč – data pro vytváření elektronického podpisu nebo pečeti

Veřejný klíč – data pro ověřování platnosti elektronického podpisu nebo pečeti

Podřízená certifikační autorita – certifikační autorita, jejíž certifikát byl vydán certifikační autoritou KB Root CA 3

OID – identifikátor objektu (*Object Identifier*). Identifikátor, standardizovaný Mezinárodní telekomunikační unií sloužící k jednoznačné identifikaci objektu

PKI – infrastruktura veřejných klíčů (*Public Key Infrastructure*). Označení pro správu a distribuci veřejných klíčů asymetrické kryptografie. PKI umožňuje pomocí přenosu důvěry používat cizí veřejné klíče a ověřovat jimi elektronické podpisy nebo pečeti bez nutnosti jejich individuální kontroly

CRL – seznam odvolaných certifikátů (*Certificate Revocation List*)

HSM – hardwarový modul pro fyzickou ochranu kryptografického materiálu (*Hardware Security Module*)

Registrační autorita – místo, kde dochází k ověření identity uživatele za účelem vydání certifikátu

Koncová entita – entita, které se vystavuje certifikát, a která není zároveň certifikační autoritou

Subjekt certifikátu – entita, pro kterou byl certifikát vystaven nebo je vystavován

Překlenovací certifikát – certifikát certifikační autority, který se vystavuje na dobu, po kterou je platný starý i nový veřejný klíč certifikační autority

1.7 LEGISLATIVNÍ A TECHNICKÉ NORMY

[2015/1502] – Prováděcí nařízení Komise (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

[2015/1506] – Prováděcí nařízení Komise (EU) 2015/1506 ze dne 8. září 2015, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru podle čl. 27 odst. 5 a čl. 37 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

[2016/650] – Prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

[297/2016] - Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce

[ČSN ETSI EN 319 401] – Obecné požadavky politiky pro poskytovatele důvěryhodných služeb

[ČSN ETSI EN 319 411-1] – Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 1: Obecné požadavky

[ČSN ETSI EN 319 411-2] – Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 2: Požadavky na poskytovatele důvěryhodných služeb vydávající kvalifikované certifikáty EU

[ČSN ISO/IEC 27001] – Systém řízení bezpečnosti informací *(best practice)*

[ČSN ISO/IEC 27002] – Soubor postupů pro opatření bezpečnosti informací *(best practice)*

[eIDAS] – Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

[EN 419 261] – Security requirements for trustworthy systems managing certificates and time-stamps

[ETSI TR 103 684] – Global Acceptance of EU Trust Services

[ETSI TS 119 312] – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[ETSI TR 119 411-4] – Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against

[ETSI TS 119 412-1] – Certificate Profiles; Part 1: Overview and common data structures ETSI EN 319 411-1 or ETSI EN 319 411-2

[ETSI EN 319 412-2] – Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[ETSI EN 319 412-3] – Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[ETSI EN 319 412-5] – Certificate Profiles; Part 5: QCStatements

[ETSI EN 319 421] – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-stamps

[ETSI EN 319 422] – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

[ETSI EN 119 495] – Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

[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 (obecné nařízení o ochraně osobních údajů)

[RFC 3647] – Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, DOI 10.17487/RFC3647, November 2003, <https://www.rfc-editor.org/info/rfc3647>

[RFC 5280] – Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>

[X.501] – ITU-T Recommendation X.501 (2005) | ISO/IEC 9594-2:2005, Information technology – Open Systems Interconnection - The Directory: Models

[CEN/TS 419261] – Security requirements for trustworthy systems managing certificates and time-stamps

[FIPS PUB 140-2] – Requirements for Cryptographic Modules.

[ETSI TS 119 312] – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[ITU-T - X.509] – Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ

2.1 PROVOZOVATEL ÚLOŽIŠŤ

Komerční banka a.s. provozuje veškerá úložiště informací a dokumentace spojené s provozem certifikační autority KB Root CA 3.

2.2 ZVEŘEJŇOVÁNÍ INFORMACÍ

Veřejné informace týkající se certifikační autority KB Root CA 3 publikuje Komerční banka a.s. na následující adrese:

- https://www.kb.cz/pki

Mailová adresa pro styk s veřejností je:

- mailto: info_ca@kb.cz

2.3 PERIODICITA ZVEŘEJŇOVÁNÍ INFORMACÍ

Informace a dokumenty jsou zveřejňovány s následující periodicitou:

- Certifikační politiky a certifikační prováděcí směrnice jsou zveřejňovány po jejich schválení, ale vždy před počátkem platnosti těchto dokumentů. Tj. před vydáním prvního certifikátu dle těchto dokumentů.
- Certifikáty vydané certifikační autoritou KB Root CA 3, pokud jsou určeny pro veřejnou publikaci, jsou zveřejněny na adrese https://www.kb.cz/pki.
- Seznamy zneplatněných certifikátů (CRL) certifikační autority KB Root CA 3 jsou vydávány bezprostředně po zneplatnění některého z vydaných certifikátů. Zpracování žádosti o zneplatnění proběhne bez zbytečného prodlení po přijetí žádosti o jejich zneplatnění.
- Ostatní informace jsou zveřejňovány tak, aby odrážely aktuální stav poskytovaných služeb.

2.3.1 Řízení přístupu k úložištím

Veškeré veřejné informace a dokumenty jsou na výše uvedených adresách zveřejňovány bez omezení a bezplatně.

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

Neveřejné informace jsou přístupné výhradně pracovníkům v souladu s interními pravidly Komerční banky a.s.

3 IDENTIFIKACE A OVĚŘENÍ

3.1 POJMENOVÁNÍ

3.1.1 Typy jmen

Jméno vydavatele i subjektu vydávaných certifikátů je konstruováno dle standardu X.501. Atributy mohou být pouze typu `utf8String` nebo `printableString` [RFC 5280].

3.1.2 Smysluplnost jmen

Jména musí být smysluplná, musí se zakládat na skutečnosti, nesmí být zavádějící.

Pokud je to možné, pak se využijí jména vedená v oficiálních registrech. Např. obchodní registr, registr obyvatel atp. V případě zahraničních subjektů se využije obdobný zahraniční registr.

3.1.3 Anonymita a pseudonym

Není povoleno.

3.1.4 Pravidla pro interpretaci různých forem jmen

Transkripce a odstraňování diakritických znaků je zakázáno. Tj. pokud jméno obsahuje jiný znak než kódu US ASCII, pak musí být příslušný atribut typu `utf8String` a musí obsahovat původní znaky.

3.1.5 Jedinečnost jmen

Předmět certifikátu je jedinečný vůči danému subjektu (fyzické nebo právnické osobě). V případě, že by mohlo dojít k nejednoznačnosti, pak certifikační autorita KB Root CA 3 doplní předmět certifikátu tak, aby byla zaručena jednoznačnost subjektu.

3.1.6 Obchodní značky

Vydaný certifikát může obsahovat pouze obchodní značky vlastněné Komerční bankou a.s. nebo ke kterým má Komerční banka a.s. souhlas vlastníka.

3.2 POČÁTEČNÍ OVĚŘENÍ IDENTITY

Je provedeno v souladu s interními dokumenty pro ceremonii, jejichž součástí je vytvoření a předložení žádosti ve formátu PKCS#10. Tato žádost je opatřena elektronickou pečetí za použití tomu odpovídajícímu soukromého klíče, čímž držitel tohoto soukromého klíče prokazuje, že v době vytvoření elektronické pečetě byl jeho vlastníkem.

Pro ověření identity organizace je předkládán originál nebo úředně ověřená kopie výpisu z obchodního rejstříku, živnostenského listu, zřizovací listiny nebo jiného dokladu identické právní povahy.

Pro ověření identity fyzické osoby, která předkládá žádost o vydání certifikátu, předkládá žadatel osobní doklad, který obsahuje fotografii držitele dokladu. Při ověření totožnosti jsou ověřovány údaje osoby:

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

3.3 IDENTIFIKACE A AUTENTIZACE PŘI ZPRACOVÁNÍ POŽADAVKU NA VÝMĚNU KLÍČE

Při výměně klíče je vždy vydáván nový certifikát s novým klíčovým párem, pro jeho vydání platí stejné požadavky jako v případě provedení počátečního ověření identity.

3.4 IDENTIFIKACE A AUTENTIZACE PŘI ZPRACOVÁNÍ POŽADAVKŮ NA ZNEPLATNĚNÍ CERTIFIKÁTU

Postup je určen a popsán v kapitolách 4.9.2 a 4.9.3.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 ŽÁDOST O VYDÁNÍ CERTIFIKÁTU

4.1.1 Žadatel o vydání certifikátu

O vydání certifikátu může požádat zároveň písemně a elektronickou formou Tribe leader – Platforms and Services nebo jím pověřená oprávněná osoba.

4.1.2 Registrační proces

Registrační proces je stanoven interními předpisy Komerční banky, a.s.

4.2 ZPRACOVÁNÍ ŽÁDOSTI O CERTIFIKÁT

4.2.1 Provádění identifikace a autentizace

Viz kapitoly 3.2 a 3.3.

4.2.2 Rozhodnutí o výsledku žádosti o certifikát

Po zpracování žádosti Manažer PKI rozhodne o přijetí či zamítnutí žádosti o certifikát. Toto rozhodnutí je zdokumentováno.

4.2.3 Doba zpracování žádosti o certifikát

Žádost o certifikát bude zpracována bez zbytečného odkladu do pěti pracovních dnů od převzetí žádosti.

4.3 VYDÁNÍ CERTIFIKÁTU

4.3.1 Úkony CA v průběhu vydávání certifikátu

V průběhu vydávání certifikátu provádí pověřený pracovník certifikační autority:

- Identifikaci a autentizaci žadatele dle kapitoly 4.2.1.
- Vizuální kontrolu shody údajů obsažených v žádosti o certifikát.
- Kontrolu formální správnosti údajů.
- Ověření vlastnictví soukromého klíče.

4.3.2 Oznámení o vydání certifikátu

Žadatel o vydání certifikátu je o vydání certifikátu vhodnou formou a bez zbytečného odkladu informován.

4.4 PŘEVZETÍ VYDANÉHO CERTIFIKÁTU

4.4.1 Úkony spojené s převzetím certifikátu

V případě vydání certifikátu má žadatel povinnost tento certifikát přijmout.

4.4.2 Zveřejňování certifikátů certifikační autoritou

Viz kapitola 2.3.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Certifikáty kořenové certifikační autority a certifikáty podřízených certifikačních autorit vydané dle této politiky jsou předány orgánu dohledu.

4.5 POUŽITÍ PÁROVÝCH DAT A CERTIFIKÁTŮ

Párová data svázaná s certifikáty mají stejnou dobu platnosti jako certifikáty. Opětovné použití párových dat je zakázáno.

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Držitel certifikátu může užívat soukromý klíč pouze v souladu s touto Politikou a platnou legislativou.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou povinny:

- Získávat certifikáty a CRL certifikační autority KB Root CA 3 z důvěryhodných zdrojů.
- Provádět veškeré úkony potřebné k tomu, aby si ověřily, že certifikát nebyl zneplatněn.

4.6 OBNOVOVÁNÍ CERTIFIKÁTŮ ZA VYUŽITÍ TÝCHŽ PÁROVÝCH DAT

Obnovením certifikátu za využití týchž párových dat je myšleno vydání nového certifikátu k ještě platnému či již exspirovanému certifikátu za použití stejného veřejného a soukromého klíče.

Obnovování certifikátů za využití týchž párových dat je zakázáno.

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 0.

4.6.2 Kdo může žádat o obnovení

Viz kapitola 0.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 0.

4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 0.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 0.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

Viz kapitola 0.

4.6.7 Oznámení o vydání certifikátu jiným subjektům

Viz kapitola 0.

4.7 OBNOVOVÁNÍ CERTIFIKÁTŮ ZA VYUŽITÍ NOVÝCH PÁROVÝCH DAT

Vydání nového certifikátu pro týž subjekt (fyzickou nebo právnickou osobu) je možné za stejných podmínek, jako vydání prvního certifikátu pro tento subjekt. Původní i nový certifikát mohou mít stejný předmět.

4.7.1 Podmínky pro obnovení certifikátu za využití nových párových dat

Viz kapitola 0.

4.7.2 Kdo může žádat o obnovení certifikátu za využití nových párových dat

Viz kapitola 0.

4.7.3 Zpracování požadavku o obnovení certifikátu za využití nových párových dat

Viz kapitola 0.

4.7.4 Oznámení vydání nového certifikátu držiteli certifikátu

Viz kapitola 0.

4.7.5 Úkony spojené s převzetím certifikátu s novým veřejným klíčem

Viz kapitola 0.

4.7.6 Zveřejnění certifikátu s novým veřejným klíčem

Viz kapitola 0.

4.7.7 Oznámení o vydání certifikátu jiným subjektům

Viz kapitola 0.

4.8 ZMĚNA ÚDAJŮ V CERTIFIKÁTU

V případě požadavku na změny údajů v certifikátu se postupuje stejným způsobem a za stejných podmínek jako při vydání nového certifikátu.

Údaje v původním certifikátu se neberou v úvahu.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Kdo může žádat o změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavků na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu jiným subjektům

Viz kapitola 4.8.

4.9 ZNEPLATNĚNÍ CERTIFIKÁTU

Jestliže se KB Root CA 3 rozhodne určitý certifikát zneplatnit, zaeviduje toto zneplatnění ve své databázi certifikátů a bezodkladně provede zneplatnění certifikátu na CRL, které bezprostředně po vydání zveřejní.

Zneplatnění certifikátu nabývá účinku okamžitě po zveřejnění na CRL.

4.9.1 Podmínky zneplatnění certifikátu

Certifikát může být zneplatněn z vůle držitele certifikátu, certifikační autority KB Root CA 3 nebo z rozhodnutí orgánu dohledu specifikovaném v [eIDAS].

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může žádat držitel certifikátu nebo orgán dohledu dle [eIDAS].

4.9.3 Požadavek na zneplatnění certifikátu

Požadavek na zneplatnění certifikátu vydaného certifikační autoritou KB Root CA 3 podává Manažer bezpečnosti PKI nebo jím pověřená oprávněná osoba písemně nebo elektronickou formou opatřený kvalifikovaným elektronickým podpisem.

Požadavek na zneplatnění musí obsahovat:

- Přesnou identifikaci provozovatele KB Root CA 3
- Přesnou identifikaci provozovatele podřízené CA
- Přesnou identifikaci držitele zneplatněného certifikátu
- Sériové číslo certifikátu v hexadecimálním tvaru.
- Důvod zneplatnění.
- Zodpovědnou osobu za podání zneplatnění. Včetně elektronického kontaktu na tuto osobu.

Požadavek na zneplatnění musí být evidován podatelnou Komerční banky a.s. Poté je bezodkladně předán k vyřízení.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Proces zneplatnění certifikátů vydaných certifikační autoritou KB Root CA 3 se zahajuje bezodkladně.

4.9.5 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu

Vydání CRL se zneplatněným certifikátem se provádí bezodkladně.

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

Spoléhající se strany jsou povinny:

- Získávat certifikáty a CRL certifikační autority KB Root CA 3 z důvěryhodných zdrojů.
- Provádět veškeré úkony potřebné k tomu, aby si ověřily, že certifikát nebyl zneplatněn.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznamy zneplatněných certifikátů (CRL) certifikační autority KB Root CA 3 jsou vydávány bezprostředně po zneplatnění některého z vydaných certifikátů. Nejpozději však po 6 měsících od vydání předchozího CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL se vydává bezodkladně tak, aby byly splněny požadavky paragrafu 4.9.5.

4.9.9 Možnost ověřování statutu certifikátu on-line

Není podporováno.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

Není podporováno.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Není podporováno.

4.9.12 Jiné varianty postupu zneplatňování certifikátů v případě kompromitace soukromého klíče

Postup zneplatňování certifikátu v případě kompromitace soukromého klíče je shodný s obecným postupem zneplatňování certifikátu.

4.9.13 Podmínky pozastavení platnosti certifikátu

Nepodporováno.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Nejsou.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Nepodporováno.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Nepodporováno

4.10 SLUŽBY SOUVISEJÍCÍ S OVĚŘOVÁNÍM STATUTU CERTIFIKÁTU

Status certifikátu je možné ověřit prostřednictvím webových stránek Komerční banky a.s. vůči seznamu zneplatněných certifikátů (CRL). CRL certifikační autority KB Root CA 3 je veřejnou informací.

4.10.1 Funkční charakteristiky

CRL je poskytován prostřednictvím protokolu HTTP:

- Na webových stránkách Komerční banky a.s.

4.10.2 Dostupnost služby ověřování statusu certifikátu

Seznam zneplatněných certifikátů (CRL) je dostupný 24 hodin, 7 dnů v týdnu.

4.10.3 Další charakteristiky služby ověřování statusu certifikátu

Nejsou poskytovány.

4.11 UKONČENÍ POSKYTOVÁNÍ SLUŽEB DRŽITELI CERTIFIKÁTU

V případě ukončení služeb držiteli certifikátu, jsou bezodkladně zneplatněny všechny certifikáty tohoto subjektu.

4.12 ÚSCHOVA A OBNOVOVÁNÍ KRYPTOGRAFICKÉHO MATERIÁLU

Neposkytuje se.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

5.1 FYZICKÉ ZABEZPEČENÍ

Fyzická bezpečnost je určena vnitřními předpisy Komerční banky a.s.

5.2 PROCESNÍ BEZPEČNOST

5.2.1 Důvěryhodné role

Komerční banka, a.s. zaměstnává pracovníky a subdodavatele, kteří mají potřebné odborné znalosti, zkušenosti a kvalifikace, jsou spolehliví a absolvovali odpovídající odbornou přípravu týkající se bezpečnosti a pravidel ochrany osobních údajů, a používá správní a řídicí postupy, které odpovídají evropským nebo mezinárodním normám.

Pro všechny činnosti týkající se provozu a správy certifikační autority KB Root CA 3 jsou určeny důvěryhodné role dle interních předpisů Komerční banky a.s.

Jakékoliv operace týkající se provozu a správy certifikační autority KB Root CA 3 mohou vykonávat výhradně pracovníci k této činnosti pověření.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Účasti více než jedné osoby je mj. vyžadováno při následujících činnostech certifikační autority KB Root CA 3:

- Generování párových dat a vydání kořenového certifikátu.
- Likvidace dat pro vytváření pečeti certifikační autority KB Root CA 3.
- Vydávání certifikátů podřízených certifikačních autorit.
- Zneplatnění certifikátů a vydávání CRL.
- Zálohování a obnova dat pro vytváření pečeti certifikační autority KB Root CA 3.

5.2.3 Identifikace a autentizace pro každou roli

Všichni pracovníci pověření k operacím týkajícím se provozu a správy certifikační autority KB Root CA 3 se před provedením příslušné operace řádně autentizují jim vydanými autentizačními prostředky (čipová karta, heslo atp.).

5.2.4 Oddělení rolí

Role vyžadující oddělení povinnosti jsou specifikovány interními předpisy Komerční banky a.s.

5.3 PERSONÁLNÍ BEZPEČNOST

Personální bezpečnost je určena vnitřními předpisy Komerční banky a.s.

5.4 AUDITNÍ ZÁZNAMY

5.4.1 Typy zaznamenávaných událostí

Zaznamenávají se důležité operace certifikační autority KB Root CA 3, zejména:

- Start vytváření zaznamenávání událostí.
- Veškeré operace s daty pro vytváření pečeti certifikační autority KB Root CA 3.
- Vydání každého certifikátu.
- Zneplatnění certifikátu.
- Vydání CRL.
- Zálohování a obnova dat pro vytváření pečeti certifikační autority KB Root CA 3.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány pověřenými osobami v intervalech stanovených interními předpisy Komerční banky a.s. V případě podezření na bezpečnostní incident se kontrola a vyhodnocení provede okamžitě.

5.4.3 Doba uchovávání auditních záznamů

Auditní záznamy se uchovávají po dobu deseti let od ukončení platnosti certifikátu, nestanoví-li legislativa jinak.

5.4.4 Ochrana auditních záznamů

Ochrana auditních záznamů je stanovena interními předpisy Komerční banky a.s.

5.4.5 Postupy pro zálohování auditních záznamů

Postupy pro zálohování auditních záznamů jsou stanoveny interními předpisy Komerční banky a.

5.4.6 Systém shromažďování auditních záznamů

Systém shromažďování auditních záznamů je stanoven interními předpisy Komerční banky a.s.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt, který událost způsobil, není o této skutečnosti informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti probíhá pravidelně dle interních předpisů Komerční banky a.s.

5.5 UCHOVÁVÁNÍ INFORMACÍ A DOKUMENTACE

5.5.1 Typy informací a dokumentace, které se uchovávají

Uchovávají se následující informace:

- Certifikační politika a certifikační prováděcí směrnice.
- Protokol o generování párových dat vystavení kořenového certifikátu.
- Protokol o likvidaci párových dat pro pečeť certifikátu a CRL.
- Protokol o vydání certifikátu
- Protokol o zneplatnění certifikátu
- Vydané CRL a certifikáty
- Auditní záznamy

5.5.2 Doba uchovávání uchovávaných informací a dokumentace

Informace a dokumentace se uchovávají po dobu deseti let, nestanoví-li legislativa jinak.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Ochrana je stanovena interními předpisy Komerční banky a.s.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou stanoveny interními předpisy Komerční banky a.s.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Časová razítka se v případě uchovávání informací a dokumentace nepoužívají.

5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní, externí)

Informace se uchovávají v interních systémech Komerční banky a.s.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Informace a dokumentace jsou udržovány v určených trezorech. O každém přístupu do trezoru je veden záznam.

5.6 ZMĚNA DAT PRO VYTVÁŘENÍ PEČETI KOŘENOVÉ CERTIFIKAČNÍ AUTORITY KB ROOT CA 3

Nejpozději po době určené vydáváním nejdéle platného certifikátu podřízené certifikační autority jsou vygenerována nová párová data a vystaven nový kořenový certifikát.

Nevytváří se překlenovací certifikáty.

V případě poškození dat pro vytváření pečeti kořenové certifikační autority KB Root CA 3 s následným selháním obnovy těchto dat se rovněž vygenerují nová párová data a nový kořenový certifikát. Tato skutečnost je neprodleně oznámena všem kontaktům podřízených certifikačních autorit a orgánu dohledu.

V případě, že dojede k takovému vývoji kryptografických metod, že by mohla být zpochybněna párová data svázaná s certifikátem certifikační autority KB Root 3, se změna dat pro vytváření pečeti kořenové certifikační autority KB Root CA 3 provede bezodkladně.

O vytvoření nového kořenového certifikátu jsou informovány kontaktní osoby podřízených certifikačních autorit a orgánu dohledu.

5.7 OBNOVA PO HAVÁRII NEBO KOMPROMITACI

5.7.1 Postup v případě incidentu a kompromitace

V případě incidentu a kompromitace se postupuje dle interních předpisů Komerční banky a.s.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

V případě incidentu a kompromitace se postupuje dle interních předpisů Komerční banky a.s.

5.7.3 Postup při kompromitaci dat pro vytváření pečeti certifikační autority KB Root CA 3

V případě důvodného podezření z kompromitace dat pro vytváření pečeti certifikační autority KB Root CA 3 se:

- Zneplatní všechny vydané a dosud platné certifikáty.
- Publikuje poslední CRL s hodnotou další aktualizace rovnou původní době platnosti kořenového certifikátu.
- Bezodkladně informují kontaktní osoby podřízených certifikačních autorit.
- V případě, že mezi podřízenými certifikačními autoritami byla autorita pro vydávání kvalifikovaných certifikátů nebo kvalifikovaných pečetí, se rovněž informuje orgán dohledu.

5.7.4 Schopnost obnovit činnost po havárii

Po havárii se postupuje dle interních předpisů Komerční banky a.s.

5.8 UKONČENÍ ČINNOSTI CA

5.8.1 Ukončení činnosti kořenové certifikační autority

O záměru ukončení činnosti se s předstihem informují kontaktní osoby podřízených certifikačních autorit a orgán dohledu.

Vlastní ukončení činnosti probíhá dle postupu stanoveného interním předpisem Komerční banky a.s.

6 TECHNICKÁ BEZPEČNOST

6.1 GENEROVÁNÍ A INSTALACE KLÍČOVÉHO PÁRU

Postup generování a instalace je specifikován v interním dokumentu Komerční banky, a.s.

6.1.1 Generování párových dat

Certifikační autora KB Root CA 3 generuje párová data výhradně pro vydání kořenového certifikátu. Párová data podřízených certifikačních autorit si generují tyto podřízené certifikační autority.

6.1.2 Poskytnutí dat pro vytváření pečetí

Není poskytováno.

6.1.3 Poskytnutí dat pro ověřování elektronických pečetí

Poskytován je pouze kořenový certifikát KB Root CA. Poskytování certifikátů podřízených certifikačních autorit je v kompetenci těchto certifikačních autorit.

6.1.4 Poskytnutí certifikátu KB Root CA 3

Certifikát certifikační autority KB Root CA 3 je poskytován při vydání certifikátu podřízené certifikační autority společně s aktuálním CRL na webových stránkách Komerční banky a.s.

6.1.5 Délky párových dat

Viz kapitola 7.

6.1.6 Kvalita generovaných párových dat

Párová data jsou generována certifikovaným HSM. Součástí této certifikace je rovněž hodnocení kvality generátoru náhodných čísel.

6.1.7 Omezení pro použití párových dat

Párová data certifikační autority KB Root CA 3 je možné využívat výhradně k pečetění certifikátů a CRL certifikační autority KB Root CA 3.

6.2 OCHRANA DAT PRO VYTVÁŘENÍ PEČETI AUTORITY KB ROOT CA 3 A BEZPEČNOST KRYPTOGRAFICKÝCH MODULŮ

6.2.1 Standardy a podmínky používání kryptografických modulů

Párová data certifikační autority KB Root CA 3 jsou generována v HSM, kde jsou i uložena data pro vytváření pečeti certifikační autority KB Root CA 3.

6.2.2 Sdílená tajemství

Sdílená tajemství se používají k aktivování kryptografického modulu v HSM. Sdílená tajemství jsou rozestřena na sady čipových karet tak, aby bylo vždy nutné minimální kvorum karet dané sady k sestavení sdíleného tajemství. Čipově karty jsou pak přiděleny konkrétním zodpovědným pracovníkům.

Pro aktivaci sdíleného tajemství je třeba alespoň dvou pověřených pracovníků vybavených příslušnou čipovou kartou.

6.2.3 Úschova dat pro vytváření elektronických pečetí nebo dat pro vytváření elektronických značek

Není poskytováno.

6.2.4 Zálohování dat pro vytváření elektronické pečeti certifikační autority KB Root CA 3

Data pro vytváření elektronické pečeti jsou uložena v HSM a nikdy jej neopouští.

Při vytváření záloh jsou zálohovaná data šifrována za pomocí bezpečných kryptografických algoritmů. Šifrovací klíč je odvozen od sdíleného tajemství.

6.2.5 Uchovávání dat pro vytváření elektronické pečeti certifikační autority KB Root CA

Data pro vytváření elektronické pečeti jsou po vydání posledního CRL protokolárně zničena.

6.2.6 Přenos dat pro vytváření elektronické pečeti certifikační autority KB Root CA

Data pro vytváření elektronické pečeti neopouští HSM kromě situace, kdy jsou data zálohována.

Jiný přenos je vyloučen.

6.2.7 Uložení dat pro vytváření elektronické pečeti certifikační autority KB Root CA

Data pro vytváření pečeti jsou po aktivaci HSM uložena v nešifrovaném stavu.

6.2.8 Aktivace HSM

K aktivování HSM je třeba součinnosti minimálně dvou osob vybavených příslušnou čipovou kartou.

6.2.9 Deaktivace dat pro vytváření pečeti certifikační autority KB Root CA

Deaktivace dat pro vytváření pečeti certifikační autority KB CA 3 provádějí určení pracovníci prostřednictvím kryptografického modulu HSM za využití sdíleného tajemství rozloženého na příslušné čipové karty.

6.2.10 Likvidace dat pro vytváření pečeti certifikační autority KB Root CA

Likvidaci dat pro vytváření pečeti certifikační autority KB CA 3 provádějí určení pracovníci prostřednictvím kryptografického modulu HSM za využití sdíleného tajemství rozloženého na příslušné čipové karty.

Likvidace dat pro vytváření pečeti certifikační autority KB Root CA 3 je provedena uvedením HSM do inicializovaného stavu, kdy je pomocí mechanismů HSM bezpečně vymazán veškerý kryptografický materiál uložený v HSM. Likvidace dat pro vytváření pečeti certifikační autority KB Root CA zahrnuje i smazání zálohovaných kopií klíčů a deaktivaci karet použitých pro přístup ke klíčům.

O likvidaci se provede písemný zápis.

6.2.11 Hodnocení kryptografického modulu

Kryptografický modul uložený v HSM je certifikovaný dle standardu Bezpečnostní požadavky pro kryptografické moduly FIPS PUB 140-2 na úroveň 3.

HSM je dále certifikováno na Common Criteria Evaluation Assurance Level (EAL) level 4+.

6.3 DALŠÍ ASPEKTY SPRÁVY PÁROVÝCH DAT

6.3.1 Archivace veřejného klíče certifikační autority KB Root CA 3

Certifikát certifikační autority KB Root CA 3 a jí vydané certifikáty podřízených CA jsou archivovány v souladu se Spisovým a skartačním řádem Komerční banky a.s.

6.3.2 Doba platnosti vydávaných certifikátů

Viz kapitola 7.1.

6.4 AKTIVAČNÍ DATA

6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou vytvářena v průběhu procesu instalace. Postup generovaní aktivačních dat je popsán v příslušné dokumentaci.

6.4.2 Ochrana aktivačních dat

Ochrana aktivačních dat je specifikována v příslušné dokumentaci.

6.4.3 Ostatní aspekty aktivačních dat

Ostatní aspekty aktivačních dat jsou popsány v příslušné dokumentaci.

6.5 IT BEZPEČNOST

IT bezpečnost a její hodnocení je specifikováno interními předpisy Komerční banky a.s.

6.6 BEZPEČNOST ŽIVOTNÍHO CYKLU

Bezpečnosti životního cyklu a její hodnocení je specifikováno interními předpisy Komerční banky a.s.

6.7 SÍŤOVÁ BEZPEČNOST

Síťová bezpečnost a její hodnocení je specifikováno interními předpisy Komerční banky a.s.

6.8 ČASOVÁ RAZÍTKA

Pro potřeby certifikační autority KB Root CA 3 nejsou časová razítka využívána.

7 PROFILY CERTIFIKÁTŮ, CRL A OCSP

7.1 PROFIL CERTIFIKÁTU

Formát certifikátu vychází ze standardu RFC 5280.

7.1.1 Základní položky certifikátů

Položka dle RFC 5280	**Význam**	**Kořenový certifikát**	**Certifikát podřízené CA**
`version`	Verze struktury certifikátu	3	
`serialNumber`	Jednoznačné číslo certifikátu	Přiděluje CA	
`signature`	Algoritmus podpisu certifikátu	SHA512RSA	SHA512RSA
`issuer`	Vydavatel	CN = KB Root 3 CA, O="Komerční banka, a.s.", 2.5.4.97 = NTRCZ-45317054, C = CZ	
`validity`	Platnost od doby vydání	Po dobu 20 let	Po dobu 10 let
`subject`		CN = KB Root 3 CA, O="Komerční banka, a.s.", 2.5.4.97 = NTRCZ-45317054, C = CZ	Z žádosti o certifikát
`subjectPublicKeyInfo`	Veřejný klíč	Z žádosti o certifikát	
`issuerUniqueID`	Není využito		
`subjectUniqueID`			
`extensions`	Viz paragraf 7.1.2		
`signatureAlgorithm`	Stejná hodnota jako položka `signature`		
`signatureValue`	Elektronická pečeť KB Root CA 3		

7.1.2 Rozšíření certifikátů

Ve vydaných certifikátech se smí výhradně vyskytovat pouze rozšíření uvedená v následující tabulce.

Rozšíření	Význam	Kritické	Kořenový certifikát	Certifikát podřízené CA
`Authority Key Identifier`	Identifikátor klíče úřadu	Ne	Nepoužit	Plní CA
`Subject Key Identifier`	Identifikátor klíče předmětu	Ne	Plní CA	
`Key Usage`	Základní použití klíče	Ano	Podpis certifikátu, podpis CRL	
`Basic Constraints`	Základní omezení	Ano	cA:true	
`CRL Distribution Points`	Distribuční místo zneplatněných certifikátů	Ne	Nepoužito	Specifikuje žadatel o certifikát
`Authority Information Access`	Přístup k informacím CA	Ne		
`Certificate Policies`	Zásady certifikátu	Ne	Všechny zásady	
`CA Version`	Verze certifikátu	Ne	V0.0	

7.1.3 Konec platnosti certifikátu podřízené CA

Konec platnosti vystaveného certifikátu podřízené CA nesmí nastat později, než je konec platnosti kořenového certifikátu, kterým je tento podřízení certifikát podepsán.

7.2 PROFIL CRL CERTIFIKAČNÍ AUTORITY KB ROOT CA 3

Formát CRL vychází ze standardu RFC 5280.

7.2.1 Základní položky CRL

Položka dle RFC 5280	Význam	Hodnota
`version`	Verze struktury CRL	2
`signature`	Algoritmus podpisu CRL	sha512RSA
`issuer`	Vydavatel	CN = KB Root 3 CA, O="Komerční banka, a.s.", 2.5.4.97 = NTRCZ-45317054, C = CZ
`thisUpdate`	Datum a čas vydání CRL	Aktuální datum a čas
`nextUpdate`	Datum a čas o 7 měsíců pozdější, než je uveden v `thisUpdate`	
`revokedCertificates`	Zneplatněné certifikáty, viz paragraf 7.2.2	

crlExtensiions	Rozšíření CRL, viz paragraf 7.2.3
signatureAlgorithm	Algoritmus pečeti CRL
signatureValue	Pečeť CRL

7.2.2 Zneplatnění certifikáty

Položka zneplatněné certifikáty (revokedCertificates) obsahuje sekvenci nesoucí informace o jednotlivých zneplatněných certifikátech. Informace o konkrétním zneplatněném certifikátu mohou obsahovat následující údaje:

Položka dle RFC 5280	Význam	Hodnota
userCertificate	Jednoznačné číslo certifikátu	serialNumber
revocationDate	Datum a čas zneplatnění	
crtEntryExtension	Rozšíření položky CRL	

Přípustná jsou pouze následující volitelná rozšíření položky CRL:

Položka dle RFC 5280	Kritické	Význam
invalidityDate	Ne	Datum a čas vzniku události vedoucí ke zneplatnění certifikátu
reasonCode	Ne	Důvod zneplatnění

7.2.3 Rozšíření CRL

Používají se pouze následující rozšíření CRL:

Rozšíření	Kritické	Význam
Authority Key Identifier	Ne	Viz stejnojmenné rozšíření certifikátu
CRL Number	Ne	Číslo seznamu CRL

7.3 PROFIL OCSP

OCSP není využíváno.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

Kořenová certifikační autorita KB Root CA 3 je pravidelně auditována tak, aby byla zajištěna shoda s [ČSN ETSI EN 319 401], [ČSN ETSI EN 319 411-1] a [ČSN ETSI EN 319 411-2].

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].

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 POPLATKY

Není využíváno.

9.2 FINANČNÍ ODPOVĚDNOST

Komerční banka a.s. má k dispozici finanční zdroje předepsané bankovní legislativou a uzavřené pojištění pokrývající případné škody.

9.3 CITLIVOST OBCHODNÍCH INFORMACÍ

Ochrana a odpovědnost za citlivé obchodní informace je předepsána bankovní legislativou.

9.4 OCHRANA OSOBNÍCH ÚDAJŮ

Certifikáty vydané certifikační autoritou KB Root CA 3 neobsahují žádné osobní údaje. Listinné dokumenty opravňující k vydání certifikátu obsahují osobní údaje použité pro identifikaci žadatele.

9.5 PRÁVA DUŠEVNÍHO VLASTNICTVÍ

Tato certifikační politika a ostatní dokumenty týkající se certifikačních autorit provozovaných Komerční bankou a.s. představují významné know-how Komerční banky, která je rovněž nositelem výlučných práv k informačnímu systému pro provoz certifikačních autorit Komerční banky a.s. A to včetně struktury, organizaci, vzhledů obrazovek a obsahu webových stránek Komerční banky a.s.

9.6 ZASTUPOVÁNÍ A ZÁRUKY

9.6.1 Zastupování a záruky CA

Komerční banka a.s. prohlašuje, že splní veškeré povinnosti uložené touto Politikou a povinnými ustanoveními příslušných právních předpisů.

9.6.2 Zastupování a záruky registrační autority

Certifikační autorita KB Root CA 3 nevyužívá registrační autority.

9.6.3 Zastupování a záruky držitele certifikátu

Držitel certifikátu podřízené certifikační autority postupuje v souladu s platnou legislativou vztahující se k problematice elektronické pečeti a ručí za informace uvedené ve vydaném certifikátu.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s touto Politikou a platnou legislativou.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není využito.

9.7 ZŘEKNUTÍ SE ZÁRUK

Komerční banka se řídí platnou legislativou České republiky.

9.8 OMEZENÍ ODPOVĚDNOSTI

Komerční banka nezodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti požadované touto certifikační politikou nebo porušily zákon.

9.9 ODPOVĚDNOST ZA ŠKODU, NÁHRADA ŠKODY

Komerční banka a.s. zodpovídá za škody způsobené porušením této Politiky ze strany Komerční banky a.s.

9.10 DOBA PLATNOSTI, UKONČENÍ PLATNOSTI

9.10.1 Doba platnosti

Tato CP platí po dobu platnosti posledního podle ní vydaného certifikátu.

9.10.2 Ukončení platnosti

Ukončení platnosti této certifikační politiky nastane v případě, že:

- Byla vydána nová certifikační politika.
- Z rozhodnutí soudu nebo orgánu dohledu.
- Rozhodnutím Tribe leadera – Platforms and Services.

9.10.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti tohoto dokumentu v důsledku ukončení poskytování služeb zůstávají v platnosti omezení a ustanovení uvedená v kapitole 9, která se týkají obchodních a právních záležitostí.

9.11 KOMUNIKACE MEZI ZÚČASTNĚNÝMI SUBJEKTY

Komunikace subjektů Komerční banky a.s. a jimi vlastněných subjektů se řídí interními předpisy banky.

9.12 ZMĚNY

9.12.1 Postup při změnách

Tato Politika je spravována v souladu s interními pravidly poskytovatele certifikačních služeb a příslušnými právními předpisy. Nové verze dokumentu vznikají v případě, že nastanou změny v systému, které Manažer bezpečnosti PKI posoudí a případně rozhodne o vydání nové Politiky.

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

9.12.2 Postup při oznamování změn

Vydání nové verze certifikační politiky je vždy oznámeno formou popsanou v kapitole 2.2.

9.12.3 Okolnosti, při kterých musí být změněno OID

V případě změn majících vliv na obsah vydávaného certifikátu je vždy změněno i OID.

9.13 ŘEŠENÍ SPORŮ

Není využito.

9.14 ROZHODNÉ PRÁVO

Právní řád České republiky.

9.15 SHODA S PRÁVNÍMI PŘEDPISY

Činnost Komerční banky, a.s. je ve shodě s právními předpisy České republiky.

9.16 DALŠÍ USTANOVENÍ

9.16.1 Rámcová dohoda

Není využito.

9.16.2 Postoupení práv

Není využito.

9.16.3 Oddělitelnost ustanovení

Není využito.

9.16.4 Zřeknutí se práv

Není využito.

9.16.5 Vyšší moc

Komerční banka a.s. neodpovídá za porušení svých povinností vyplývající ze zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu.

9.17 DALŠÍ OPATŘENÍ

Není využito.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato Politika nabývá platnosti a účinnosti dnem jejího vydání.