

CERTIFIKAČNÍ POLITIKA ZAMĚSTNANECKÝCH KVALIFIKOVANÝCH CERTIFIKÁTŮ PRO ELEKTRONICKÝ PODPIS

Verze 1.2

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

1 ÚVOD 9
1.1 Přehled 9
1.2 Název dokumentu a identifikace 9
1.3 Participující subjekty 10
1.3.1 Certifikační autority 10
1.3.2 Registrační autority 11
1.3.3 Žadatelé o certifikát 11
1.3.4 Držitelé certifikátů 11
1.3.5 Informační systémy KB 12
1.3.6 Správa čipových karet KB 12
1.3.7 Spoléhající se strany 12
1.3.8 Další zúčastněné subjekty 12
1.4 Použití certifikátů 12
1.4.1 Přípustné použití certifikátu 12
1.4.2 Omezení použití certifikátu 13
1.5 Správa politiky 13
1.5.1 Organizace pověřená správou dokumentu 13
1.5.2 Kontaktní osoba 13
1.5.3 Osoba odpovědná za soulad CP s odpovídající CPS 13
1.5.4 Postupy při schvalování CP 13
1.6 Definice a zkratky 13
2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE 17
2.1 Úložiště informací a dokumentace 17
2.2 Zveřejňování informací a dokumentace 17
2.2.1 Zveřejňování informací o certifikátech 17
2.2.2 Zveřejňování informací o certifikačních autoritách 17
2.3 Čas nebo četnost zveřejňování informací 17
2.4 Řízení přístupů k jednotlivým typům úložišť 17
3 IDENTIFIKACE A OVĚŘENÍ 19
3.1 Pojmenování 19
3.1.1 Typy jmen 19
3.1.2 Požadavky na významovost jmen 19
3.1.3 Anonymita a používání pseudonymu 19
3.1.4 Pravidla pro interpretaci různých forem názvů 19
3.1.5 Jedinečnost jmen 19
3.1.6 Obchodní značky 19
3.2 Počáteční ověření identity 19
3.2.1 Ověřování vlastnictví soukromého klíče 19
3.2.2 Ověřování identity organizace 20
3.2.3 Ověření identity žadatele o certifikát 20
3.2.4 Neověřované informace 21
3.2.5 Ověřování oprávnění 21
3.2.6 Kritéria pro interoperabilitu (spolupráci) 21
3.3 Identifikace a autentizace při požadavku na výměnu klíče 21
3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče 21
3.3.2 Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu 21
3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu 22
4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU 23
4.1 Žádost o vydání certifikátu 23

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu ... 23
4.1.2 Podání žádosti a odpovědnosti poskytovatele a žadatele ... 23
4.2 Zpracování žádosti o certifikát ... 25
4.2.1 Identifikace a ověření ... 25
4.2.2 Přijetí nebo zamítnutí žádosti o certifikát ... 25
4.2.3 Doba zpracování žádosti o certifikát ... 26
4.3 Vydání certifikátu ... 26
4.3.1 Úkony CA při vydávání certifikátu ... 26
4.3.2 Oznámení žadateli o vydání certifikátu ... 26
4.4 Převzetí vydaného certifikátu ... 26
4.4.1 Úkony spojené s převzetím certifikátu ... 26
4.4.2 Zveřejnění certifikátu certifikační autoritou ... 27
4.4.3 Oznámení o vydání certifikátu jiným subjektům ... 27
4.5 Použití klíčového páru a certifikátu ... 27
4.5.1 Soukromý klíč žadatele a přípustné použití certifikátu ... 27
4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou ... 28
4.6 Obnovení certifikátu ... 28
4.6.1 Podmínky pro obnovení certifikátu ... 28
4.6.2 Subjekty oprávněné požadovat obnovení certifikátu ... 28
4.6.3 Zpracování požadavku na obnovení certifikátu ... 28
4.6.4 Oznámení o obnovení certifikátu držiteli certifikátu ... 28
4.6.5 Úkony spojené s převzetím obnoveného certifikátu ... 28
4.6.6 Zveřejňování obnovených certifikátů ... 28
4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům ... 28
4.7 Vydání následného certifikátu ... 28
4.7.1 Podmínky pro vydání následného certifikátu ... 28
4.7.2 Subjekty oprávněné požadovat následný certifikát ... 29
4.7.3 Podání žádosti o následný certifikát ... 29
4.7.4 Zpracování požadavku o následný certifikát ... 29
4.7.5 Oznámení žadateli o vydání následného certifikátu ... 29
4.7.6 Úkony spojené s převzetím následného certifikátu ... 29
4.7.7 Zveřejnění následného certifikátu certifikační autoritou ... 29
4.7.8 Oznámení o vydání certifikátu jiným subjektům ... 29
4.8 Změna údajů v certifikátu ... 29
4.8.1 Podmínky pro změnu údajů v certifikátu ... 29
4.8.2 Zpracování požadavku na změnu údajů v certifikátu ... 30
4.8.3 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu ... 30
4.8.4 Úkony spojené s převzetím certifikátu se změněnými údaji ... 30
4.8.5 Zveřejňování certifikátů se změněnými údaji ... 31
4.8.6 Oznámení o vydání certifikátu jiným subjektům ... 31
4.9 Zneplatnění a pozastavení platnosti certifikátu ... 31
4.9.1 Podmínky pro zneplatnění certifikátu ... 31
4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu ... 31
4.9.3 Postup zneplatnění certifikátu ... 32
4.9.4 Doba odkladu požadavku na zneplatnění certifikátu ... 33
4.9.5 Doba, ve které musí dojít k zneplatnění certifikátu ... 33
4.9.6 Povinnosti spoléhajících se stran při ověřování, zda byl certifikát zneplatněn ... 33
4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů (CRL) ... 33
4.9.8 Maximální zpoždění při zveřejnění seznamu zneplatněných certifikátů (CRL) ... 33
4.9.9 Možnost ověřování statutu certifikátu online ... 33
4.9.10 Požadavky na ověřování statutu certifikátu online ... 34
4.9.11 Jiné způsoby oznamování zneplatnění certifikátu ... 34

4.9.12 Zvláštní postupy při kompromitaci klíče ... 34
4.9.13 Podmínky pro pozastavení platnosti certifikátu ... 34
4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu ... 34
4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu ... 34
4.9.16 Omezení doby pozastavení platnosti certifikátu ... 34
4.10 Služby související s ověřováním stavu certifikátu ... 34
4.10.1 Funkční charakteristiky ... 34
4.10.2 Dostupnost služeb ... 34
4.10.3 Další charakteristiky služeb stavu certifikátu ... 34
4.11 Ukončení poskytování služeb pro držitele certifikátu ... 35
4.12 Úschova a obnova klíčů ... 35
4.12.1 Zásady a postupy pro úschovu a obnovu soukromých klíčů ... 35
4.12.2 Zásady a postupy zapouzdření klíče a jeho obnovení ... 35
5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST ... 36
5.1 Fyzické zabezpečení ... 36
5.1.1 Umístění a konstrukce ... 36
5.1.2 Fyzický přístup ... 36
5.1.3 Elektřina a klimatizace ... 36
5.1.4 Vliv vody ... 36
5.1.5 Protipožární opatření a ochrana ... 36
5.1.6 Ukládání médií ... 36
5.1.7 Nakládání s odpady ... 37
5.1.8 Zálohy mimo budovu ... 37
5.2 Procesní bezpečnost ... 37
5.2.1 Důvěryhodné role ... 37
5.2.2 Počet osob požadovaných pro jednotlivé činnosti ... 37
5.2.3 Identifikace a ověření pro každou roli ... 37
5.2.4 Role vyžadující rozdělení povinností ... 37
5.3 Personální bezpečnost ... 38
5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost ... 38
5.3.2 Posouzení spolehlivosti osob ... 38
5.3.3 Požadavky na přípravu pro výkon role, vstupní školení ... 38
5.3.4 Požadavky a periodicita školení ... 38
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi ... 38
5.3.6 Postihy za neoprávněné činnosti zaměstnanců ... 38
5.3.7 Požadavky na nezávislé zhotovitele (dodavatele) ... 38
5.3.8 Dokumentace poskytovaná zaměstnancům ... 38
5.4 Auditní záznamy ... 39
5.4.1 Typy zaznamenávaných událostí ... 39
5.4.2 Periodicita zpracování záznamů ... 39
5.4.3 Doba uchování auditních záznamů ... 39
5.4.4 Ochrana auditních záznamů ... 39
5.4.5 Postupy pro zálohování auditních záznamů ... 39
5.4.6 Systém shromažďování auditních záznamů ... 40
5.4.7 Postup při oznamování událostí subjektu, který ji způsobil ... 40
5.4.8 Hodnocení zranitelnosti ... 40
5.5 Uchovávání záznamů ... 40
5.5.1 Typy záznamů ... 40
5.5.2 Doba uchování záznamů ... 40
5.5.3 Ochrana úložiště záznamů ... 41
5.5.4 Postupy při zálohování záznamů ... 41

5.5.5 Požadavky na použití časových razítek při uchovávání záznamů 41
5.5.6 Systém shromažďování uchovávaných záznamů 41
5.5.7 Postup získání a ověření uchovávaných informací 41
5.6 Výměna klíče 41
5.7 Obnova po havárii a kompromitaci 42
5.7.1 Postup v případě incidentu a kompromitace 42
5.7.2 Poškození výpočetních prostředků, softwaru nebo dat 42
5.7.3 Postupy při kompromitaci soukromého klíče 42
5.7.4 Schopnost obnovení činnosti po havárii 42
5.8 Ukončení činnosti CA nebo RA 43
5.8.1 Řádné ukončení činnosti CA 43
5.8.2 Odnětí statusu kvalifikovaného poskytovatele služeb vytvářejících důvěru 43
5.8.3 Mimořádné ukončení činnosti CA 43
5.8.4 Ukončení činnosti RA 43
6 TECHNICKÁ BEZPEČNOST 44
6.1 Generování a instalace klíčového páru 44
6.1.1 Generování klíčového páru 44
6.1.2 Předání soukromého klíče žadateli 44
6.1.3 Předání veřejného klíče kvalifikovanému poskytovateli služeb vytvářejících důvěru 44
6.1.4 Předání veřejného klíče CA spoléhajícím se stranám 44
6.1.5 Délky klíčů 44
6.1.6 Generování parametrů veřejných klíčů a kontrola jejich kvality 44
6.1.7 Účely použití klíčů 45
6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů 45
6.2.1 Standardy a podmínky používání kryptografických modulů 45
6.2.2 Sdílení tajemství 45
6.2.3 Úschova soukromého klíče 45
6.2.4 Zálohování soukromého klíče 45
6.2.5 Uchovávání soukromých klíčů 45
6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu 45
6.2.7 Uložení soukromého klíče v kryptografickém modulu 46
6.2.8 Postup aktivace soukromého klíče 46
6.2.9 Postup deaktivace soukromého klíče 46
6.2.10 Postup ničení soukromého klíče 46
6.2.11 Hodnocení kryptografických modulů 46
6.3 Další aspekty správy páru klíčů 47
6.3.1 Archivace veřejných klíčů 47
6.3.2 Doba platnosti certifikátů a doba platnosti klíčů 47
6.4 Aktivační data 47
6.4.1 Generování a instalace aktivačních dat 47
6.4.2 Ochrana aktivačních dat 48
6.4.3 Ostatní aspekty aktivačních dat 48
6.5 Počítačová bezpečnost 48
6.5.1 Specifické technické požadavky na počítačovou bezpečnost 48
6.5.2 Hodnocení počítačové bezpečnosti 48
6.6 Bezpečnost životního cyklu 49
6.6.1 Řízení vývoje systému 49
6.6.2 Kontroly řízení zabezpečení 49
6.6.3 Řízení zabezpečení životního cyklu 49
6.7 Síťové zabezpečení 49
6.8 Časová razítka 49

7 PROFILY CERTIFIKÁTŮ, SEZNAMŮ CRL A OCSP 50
7.1 Profil certifikátu 50
7.1.1 Číslo verze 51
7.1.2 Rozšíření certifikátu 51
7.1.3 OID algoritmů 53
7.1.4 Zápis jmen a názvů 53
7.1.5 Omezení jmen 53
7.1.6 OID certifikační politiky 53
7.1.7 Omezení politiky 53
7.1.8 Syntaxe a sémantika kvalifikátorů politiky 54
7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies 54
7.2 Profil seznamu zneplatněných certifikátů (CRL) 54
7.2.1 Číslo verze 54
7.2.2 Rozšíření CRL 54
7.3 Profil OCSP 55
7.3.1 Číslo verze 55
7.3.2 Rozšíření OCSP 55
8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ 56
8.1 Periodicita nebo okolnosti hodnocení 56
8.2 Identita a kvalifikace hodnotitele 56
8.2.1 Interní hodnocení shody 56
8.2.2 Externí hodnocení shody 56
8.3 Vztah hodnotitele k hodnocenému subjektu 56
8.3.1 Interní hodnocení shody 56
8.3.2 Externí hodnocení shody 56
8.4 Hodnocené oblasti 56
8.5 Postup v případě zjištění nedostatků 56
8.6 Sdělování výsledků hodnocení 56
9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI 57
9.1 Poplatky 57
9.1.1 Poplatky za vydání nebo obnovení certifikátu 57
9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů 57
9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu 57
9.1.4 Poplatky za další služby 57
9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací) 57
9.2 Finanční odpovědnost 57
9.2.1 Krytí pojištěním 57
9.2.2 Další aktiva a záruky 57
9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele 57
9.3 Důvěrnost obchodních informací 57
9.3.1 Rozsah důvěrných informací 57
9.3.2 Informace mimo rámec důvěrných informací 58
9.3.3 Odpovědnost za ochranu důvěrných informací 58
9.4 Ochrana osobních údajů 58
9.4.1 Osobní údaje 58
9.4.2 Odpovědnost za ochranu osobních údajů 58
9.4.3 Oznámení o používání osobních údajů a souhlas s jejich zpracováním 58
9.4.4 Poskytování osobních údajů pro soudní či správní účely 58
9.5 Práva duševního vlastnictví 58
9.6 Zastupování a záruky 58
9.6.1 Zastupování a záruky CA 59

9.6.2 Zastupování a záruky RA 59
9.6.3 Zastupování a záruky držitele certifikátu 59
9.6.4 Zastupování a záruky spoléhajících se stran 59
9.6.5 Zastupování a záruky ostatních subjektů 59
9.7 Zřeknutí se záruk 59
9.8 Omezení odpovědnosti 59
9.9 Odpovědnost za škodu, náhrada škody 60
9.10 Doba platnosti, ukončení platnosti 60
9.10.1 Doba platnosti 60
9.10.2 Ukončení platnosti 60
9.10.3 Důsledky ukončení a přetrvání závazků 60
9.11 Komunikace mezi zúčastněnými subjekty 60
9.11.1 Komunikace s kvalifikovaným poskytovatelem služeb vytvářejících důvěru 60
9.11.2 Jazyk komunikace 60
9.12 Změny 61
9.12.1 Postup při změnách 61
9.12.2 Postup při oznamování změn 61
9.12.3 Okolnosti, při kterých musí být změněn identifikátor OID 61
9.13 Řešení sporů 61
9.14 Rozhodné právo 61
9.15 Shoda s právními předpisy 61
9.16 Další ustanovení 61
9.16.1 Rámcová dohoda 61
9.16.2 Postoupení práv 61
9.16.3 Oddělitelnost ustanovení 61
9.16.4 Zřeknutí se práv 61
9.16.5 Vyšší moc 62
9.16.6 Prohlášení o nediskriminaci 62
9.16.7 Přístupnost pro osoby se zdravotním postižením 62
9.17 Další opatření 62

Historie revizí a změn dokumentu

Verze	Datum změny	Důvod změny	Schválil
1.0	1.3.2024	První verze	Tomáš Prjacha, Manažer PKI
1.1	24.6.2026	Grafické a textové korekce	Tomáš Prjacha, Manažer PKI
1.2	9.11.2026	Doplnění čipových karet v režimu QSCD	Tomáš Prjacha, Manažer PKI TOMÁŠ PRJACHA Digitálně podepsal TOMÁŠ PRJACHA Datum: 2026.11.09 17:12:21 +01'00'

1 ÚVOD

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

Právní rámec pro poskytování této služby je definován zejména v:

- 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 [EIDAS] v platném znění
- Zákoně č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce [297/2016] v platném znění

1.1 PŘEHLED

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

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

Pro ukládání klíčových párů jsou zaměstnancům vydávány dva druhy čipových karet KB Unipass:

- 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.
- 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.

Držitelé certifikátů, vydávaných podle této certifikační politiky, využívají soukromé klíče příslušné k vydávaným certifikátům při vytváření zaručených, resp. kvalifikovaných elektronických podpisů – podle typu čipové karty. 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* podpisů 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* podpis, tak pro certifikáty pro *kvalifikovaný* podpis.

1.2 NÁZEV DOKUMENTU A IDENTIFIKACE

Název dokumentu	Certifikační politika zaměstnaneckých kvalifikovaných certifikátů pro elektronický podpis
Verze dokumentu	1.2
OID této certifikační politiky	1.3.154.45317054.1000.1.2.1.11.2
Datum vydání	9.11.2026
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 určených pro použití mimo interní prostředí KB. Z těchto CA jsou vydávány certifikáty klientům Komerční banky a také certifikáty pro zaměstnance KB. Jednou z certifikačních autorit, které vydávají certifikáty pro a zaměstnance 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 v platném znění
- [297/2016] Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce v platném znění
- [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. ověřují totožnost žadatelů,
- ověřují, že žadatel je pracovníkem KB anebo dceřiné společnosti,
- ověřují že je žadatel držitelem čipové karty KB Unipass, a že karta žadatele obsahuje data pro autorizaci žádostí (interní certifikát se soukromým klíčem),
- ověří, že žadatel zná PIN k dané kartě
- autorizují data, která mají být uvedena ve vydaném certifikátu,
- podepisují s žadateli dokument, kterým se žadatel zavazuje plnit pravidla držení certifikátu.

1.3.3 Žadatelé o certifikát

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

- Jsou pracovníky Komerční banky nebo dceřiné společnosti Komerční banky.
- Před podáním žádosti byla ověřena jejich osobní identita a výhradní držení autorizačního prostředku (čipové karty s autorizačním certifikátem a příslušným kryptografickým klíčem).
- Jsou držitelem kryptografického prostředku pro vytváření elektronických podpisů (čipové karty KB Unipass), 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. V certifikátu jsou uvedeny také identifikační údaje organizace, která je zaměstnavatelem držitele.

1.3.5 Informační systémy KB

Životní cyklus certifikátů vydávaných podle této CP je do značné míry automatizovaný. Žadatelé provádí velkou část kroků k získání či zneplatnění certifikátu samoobslužně. Při správě certifikátů využívají žadatelé či držitelé technické prostředky a informační systémy Komerční banky, popř. dceřiných společností.
Využívané informační systémy hrají významnou roli v procesu vydání a zneplatnění certifikátu:

- Autentizují žadatele, resp. držitele certifikátu.
- Kontrolují, zda je žadatel, resp. držitel oprávněn k provedení požadovaného úkonu (např. podání žádosti či zneplatnění certifikátu).
- Zprostředkují žadateli, resp. držiteli (elektronický) kontakt s certifikační autoritou.
- Vydávají žadateli certifikát pro autorizaci prvotní žádosti. (Jde o jiný typ certifikátu než certifikát vydávaný podle této CP. Autorizační certifikát se vydává z interní certifikační autority KB.)

1.3.6 Správa čipových karet KB

Certifikáty vydávané podle této CP, a také jejich příslušné kryptografické klíče, jsou chráněny v čipové kartě. Každý žadatel musí mít před vydáním certifikátu v držení čipovou kartu. Držení čipové karty hraje významnou roli při identifikaci žadatele o certifikát.

Čipové karty jsou žadatelům protokolárně vydávány pracovištěm KB pro správu karet. Čipové karty jsou držitelům vydávány osobně. Správa čipových karet vede evidenci vydaných karet. U vydaných karet je jednoznačně evidován oprávněný držitel karty, a také typ karty (zda je karta kvalifikovaným prostředkem pro vytváření elektronických podpisů).

Systém správy čipových karet poskytuje informace o vydaných kartách a jejich držitelích informačním systémům KB, včetně certifikačních autorit KB.

1.3.7 Spoléhající se strany

Spoléhající se stranou je entita spoléhající se na certifikát vydaný podle této CP.

1.3.8 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.

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

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.

Pomocí soukromého klíče certifikátu vydaného podle této certifikační politiky lze vytvářet uznávané elektronické podpisy dle § 6 odstavce 2 zákona č. 297/2016 Sb. Vytvořený elektronický podpis může mít právní účinky úředně ověřeného podpisu dle § 6 odstavce 2 zákona č. 12/2020 Sb.

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 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 Unipass	Čipová karta vydávaná pracovníkům Komerční banky. Karta má charakter hardwarového kryptografického prostředku. Dovede chránit klíčové páry držitele karty. Aktivace soukromého klíče v čipu karty je podmíněna zadání platné hodnoty PIN. Pomocí čipové karty může držitel provádět kryptografické operace asymetrické kryptografie. Karta KB Unipass prošla posouzením shody podle Common Criteria na úroveň EAL 5+, ale není QSCD prostředkem.
Klíčový pár (též párové klíče, párová data)	Vzájemně svázaná dvojice kryptografických 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.)
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.
QSCD	Qualified Signature Creation Device. Kvalifikovaný prostředek pro vytváření elektronických podpisů. Hardwarové zařízení pro vytváření elektronických podpisů založených na principech asymetrické kryptografie, které musí splňovat požadavky stanovené v Příloze II nařízení eIDAS.
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 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: čipové karty KB Unipass. 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.
Registrační proces, též proces registrace	Ověření totožnosti žadatele o certifikát. Registrační proces probíhá formou fyzické interakce mezi žadatelem a operátorem registračního místa. V rámci registračního procesu operátor na základě podkladů předložených žadatelem ověří totožnost žadatele (podle osobních dokladů žadatele), zaměstnanecký poměr žadatele (podle údajů v evidenci pracovníků KB a dceřiných společností), držení konkrétní čipové karty KB Unipass (fyzicky předložené), držení soukromého klíče a certifikátu pro autorizaci prvotní žádosti (vyčtením z čipu karty KB Unipass).
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).
Uznávaný podpis	Zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis; podle § 6 Zákona 297/2016 Sb.
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. Kromě toho se v certifikátu uvádí také identifikace organizace, která je zaměstnavatelem držitele.

V certifikátech vydávaných podle této CP se uvádí:

- Jméno a příjmení držitele
- Identifikátor osobního dokladu držitele
- Identifikace organizace: zaměstnavatele držitele
- E-mailová adresa držitele

Identifikační údaje držitele a organizace 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 odpovídají informacím, které o žadateli eviduje KB. Identifikační údaje pro uvedení v žádosti a certifikátu se shromažďují v rámci procesu registrace, kdy se prování mj. i ověření totožnosti žadatele.

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. Jedinečnost jména se zajišťuje uvedením identifikátoru osobního dokladu žadatele, 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.

Informace, že je vlastníkem daného soukromého klíče konkrétní žadatel, se ověřuje pomocí elektronického podpisu datové obálky žádosti. Žádost o certifikát (ve formátu PKCS#10) musí být žadatelem autorizována, tzn. elektronicky podepsána. K vytvoření elektronického podpisu obálky žádosti musí žadatel použít certifikát a soukromý klíč, který má ve svém výhradním držení a který je s ním jednoznačně spojen. Držení klíče a certifikátu pro autorizaci žádosti se ověřuje a zaznamenává v rámci procesu registrace (před podáním žádosti). Soukromý klíč autorizačního certifikátu musí být generován a uložen v čipu karty KB Unipass, která byla žadateli protokolárně vydána. Bezpečnostní charakteristiky karty KB Unipass garantují, že soukromý klíč chráněný v čipu nelze exportovat. Pouze ověřený držitel čipové karty KB Unipass je schopen vytvořit platný elektronický podpis, který tvoří autorizační obálku žádosti o certifikát, neboť jako jediný zná PIN dané KB Unipass karty. Vytvořením platného elektronického podpisu je prokázána žadatelova znalost PINu k dané KB Unipass kartě.

Karty KB Unipass, které jsou kvalifikovaným prostředkem pro vytváření elektronických podpisů, vytvářejí v průběhu generování klíčového páru a žádosti o certifikát navíc kryptograficky zabezpečená data, která vzniklý klíčový pár jednoznačně spojují s čipem dané karty. Tato data se zakódují do žádosti o certifikát a transportují se spolu s žádostí do zpracování. Data lze použít k prokázání, že veřejný klíč v žádosti je součástí klíčového páru, který prokazatelně vzniknul v konkrétním čipu karty KB Unipass.

Certifikační autorita před vydáním prvotního certifikátu ověřuje jak platnost elektronického podpisu žádosti, tak platnost elektronického podpisu autorizační obálky žádosti. Ověřuje také, že certifikát, jehož soukromý klíč byl použit k vytvoření elektronického podpisu žádosti, byl vydán danému žadateli. Kontrola držitele autorizačního certifikátu se opírá o data zjištěná v rámci procesu registrace. Při zpracování žádosti o certifikát pro vytváření kvalifikovaných podpisu ověřuje certifikační autorita také, že veřejný klíč uvedený v žádosti je součástí klíčového páru, který byl vygenerován v čipu karty, která byla vydána žadateli o certifikát.

3.2.2 Ověřování identity organizace

Do certifikátů vydávaných podle této CP se uvádí informace o organizaci: zaměstnavateli žadatele. Certifikáty jsou vydávány pouze zaměstnancům KB a zaměstnancům dceřiných společností KB. Ověřování informací o organizacích se opírá o interní evidenci pracovníků KB a dceřiných společností.

Před podáním žádosti o certifikát musí žadatel požádat svého nadřízeného o schválení k držení kvalifikovaného zaměstnaneckého certifikátu. Schválení požadavku ze strany nadřízeného se zaznamená do interní evidence KB; tato evidence je k dispozici operátorovi registračního místa.

Příslušnost žadatele k organizaci ověřuje operátor v rámci registračního procesu.

Žadatel musí operátorovi předložit kartu KB Unipass, která slouží jako průkaz zaměstnance. Na těle karty je vytištěna informace o organizaci, která je zaměstnavatelem žadatele a sériové číslo karty. Vytištěno je také jméno, příjmení a barevná fotografie držitele karty KB Unipass – operátor porovná údaje držitele karty s osobními doklady, předloženými žadatelem.

Operátor vyhledá žádost a informace o žadateli v interní adresářové službě KB. Podkladem pro vyhledání jsou údaje z osobního dokladu.

Operátor v interní evidenci ověří, že pro daného žadatele bylo schváleno oprávnění k držení kvalifikovaného zaměstnaneckého certifikátu, a zda podklady předložené žadatelem odpovídají schváleným údajům v interní evidenci KB.

3.2.3 Ověření identity žadatele o certifikát

Držitelem certifikátu vydaného podle této CP může být pouze zaměstnanec Komerční banky nebo zaměstnanec dceřiné společnosti. Před vydáním prvotního certifikátu – v rámci registračního procesu – se ověřuje totožnost žadatele.

Ověření totožnosti musí proběhnout na interní registrační autoritě KB, za osobní přítomnosti žadatele. K ověření totožnosti musí klient předložit osobní doklady, obsahující fotografii držitele dokladu. Přípustné jsou doklady: občanský průkaz, pas, povolení k pobytu.

Při ověření totožnosti jsou ověřovány údaje osoby:

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

Údaje ztotožněné osoby (klienta) zavede KB do své interní evidence.

Ověření identity žadatele probíhá současně s ověřením příslušnosti žadatele k organizaci – viz také kapitolu 3.2.2.

V rámci registračního procesu operátor registrační autority také ověří, že:

- je žadatel držitelem čipové karty KB Unipass
- karta žadatele obsahuje data pro autorizaci žádostí (interní certifikát se soukromým klíčem)
- žadatel zná PIN k dané kartě

Registrační proces a ověření totožnosti žadatele probíhá před podáním žádosti o prvotní certifikát zaměstnance.
Žadatel podává žádost o certifikát po úspěšném absolvování registračního procesu. Žadatel podává žádost samoobslužně, elektronicky, z počítače připojeného do interní sítě KB.

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 fyzická osoba, která je zaměstnancem KB nebo dceřiné společnosti KB.

Žádost o certifikát podává žadatel elektronicky, v rámci interní sítě KB. Před podáním žádosti se žadatel musí autentizovat vůči serveru, provozovaném v interním prostředí KB.

Žádost o prvotní certifikát musí žadatel autorizovat elektronickým podpisem, vytvořeným pomocí soukromého klíče a certifikátu, který má žadatel pod svojí výhradní kontrolou, a jehož držení a uložení na čipové kartě bylo prověřeno v rámci registračního procesu.

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.

Certifikační autorita *Komerční banka Qualified CA/RSA* využívá pro ověření integrity a původu žádostí certifikáty, vydávané z interních certifikačních autorit KB.

3.3 IDENTIFIKACE A AUTENTIZACE PŘI POŽADAVKU NA VÝMĚNU KLÍČE

Žádost o certifikát s novým veřejným klíčem může podat pouze zaměstnanec KB nebo zaměstnanec dceřiné společnosti KB, kterému bylo schváleno držení kvalifikovaného certifikátu zaměstnance.

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Pokud má žadatel v držení platný certifikát vydaný podle této CP, pak podává požadavek na výměnu klíče samoobslužně a elektronicky. Žádost o certifikát s novým klíčem autorizuje elektronickým podpisem, vytvořeným pomocí platného klíče a certifikátu, přičemž autorizační certifikát musí být vydán stejnému žadateli podle této CP. Klíčové páry žádosti i certifikátu použitého pro autorizaci musí být generovány a chráněny ve stejné čipové kartě KB Unipass, která byla žadateli ověřena v rámci registračního procesu.

Pro elektronické podání žádosti s novým klíčem se žadatel musí úspěšně autentizovat vůči interním systémům KB. K autentizaci musí žadatel použít autentizační údaje pracovníka KB, resp. pracovníka dceřiné společnosti KB.

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

Pokud žadatel nemá k dispozici platný certifikát vydaný podle této certifikační politiky, musí pro získání nového certifikátu absolvovat stejný postup, jako pro získání prvotního certifikátu, včetně nového registračního procesu.

Registrační proces i mechanismus identifikace a autentizace pro získání prvotního certifikátu jsou popsány v kapitole 3.2.

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 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:

- Požádá o zneplatnění prostřednictvím samoobslužného webového portálu pro správu certifikátů pracovníka KB. Pro přístup k portálu se držitel musí autentizovat pomocí uživatelského účtu pracovníka KB či dceřiné společnosti. Portál nabízí ke zneplatnění pouze certifikáty, jejichž držitelem je autentizovaný uživatel.
- Vznese požadavek elektronicky prostřednictvím interního systému podpory (Service Manager). Pro přístup k systému podpory se držitel musí autentizovat pomocí uživatelského účtu pracovníka KB či dceřiné společnosti. Vznesený požadavek v sobě nese identitu autentizovaného pracovníka, který požadavek do systému zavedl. Porovnáním této identity s identitou držitele certifikátu zjistí správce certifikátů, který požadavek vypořádává, zda je uživatel oprávněn požadovat zneplatnění (tzn. zda je držitelem daného certifikátu).

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 zaměstnancem Komerční banky, popř. zaměstnancem dceřiné společnosti KB. Nadřízený pracovník musí žadateli schválit oprávnění k držení kvalifikovaného certifikátu zaměstnance. Žadatel musí před podáním žádosti osobně absolvovat registrační proces na pracovišti interní registrační autority KB. Registrační proces je popsán v kapitole 3.2.

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

Před podáním žádosti musí mít žadatel na přidělené kartě KB Unipass vydán certifikát pro autorizaci žádosti o kvalifikovaný certifikát. Autorizační certifikát se vydává z interní certifikační autority KB. Spolu s autorizačním certifikátem musí být v čipu karty generován a uložen také příslušný klíčový pár.

4.1.2 Podání žádosti a odpovědnosti poskytovatele a žadatele

4.1.2.1 Podání žádosti o prvotní certifikát

Žadatel podává žádost o certifikát samoobslužně, elektronicky, z počítače připojeného do interní sítě KB a propojeného s adresářovou službou Active Directory. V operačním systému počítače musí být instalována softwarová aplikace, fungující jako průvodce procesem vydání certifikátu. Tuto aplikaci dává pracovníkům k dispozici KB.

K počítači žadatele musí být připojena čtečka čipových karet. V operačním systému musí být instalovány ovladače čtečky i karty KB Unipass.

Žadatel se autentizuje do interního prostředí KB, vůči adresářové službě Active Directory. Spustí aplikačního průvodce pro vydání certifikátu kliknutím na příslušný odkaz:

- buď v e-mailové zprávě s výzvou k podání žádosti
- anebo na webové stránce samoobslužného portálu pro správu certifikátů pracovníka KB.

Spustí se aplikace, které žadatele provede procesem vydání certifikátu. Aplikační průvodce komunikuje s centrální evidencí KB a se systémem certifikační autority. Zjišťuje informace potřebné k provedení procesu získání certifikátů, zapisuje údaje do evidence a předává žádost o certifikát.

Při komunikaci s centrální evidencí předává aplikační průvodce uživatelská pověření, která žadatel získal autentizací vůči Active Directory. Centrální evidence i systém certifikační autority akceptují uživatelská pověření; pomocí těchto pověření identifikují a autentizují žadatele.

Proces vydání prvotního certifikátu pomocí aplikačního průvodce funguje následovně:

- Aplikační průvodce z evidence zjistí, jaká čipová karta byla přidělena danému žadateli. (Fyzické držení této karty žadatelem bylo ověřeno v rámci registračního procesu.) Vyžádá si vložení příslušné karty.
- Aplikační průvodce z centrální evidence zjistí, jaký klíčový pár s certifikátem by měl být k dispozici pro autorizaci žádosti. (Existence klíčového páru a certifikátu byla ověřena v rámci registračního procesu.)
  Zkontroluje, zda se v čipu karty nachází příslušný certifikát s klíčem.
- Aplikační průvodce zjistí z centrální evidence údaje, které byly ověřeny v rámci registračního procesu a mají být uvedeny ve vydaném certifikátu. Tyto údaje zobrazí žadateli k odsouhlasení:
  - Jméno a příjmení
  - Číslo osobního dokladu

  - Organizace (zaměstnavatel) žadatele
  - E-mailová adresa žadatele
- Žadatel zkontroluje zobrazené údaje. Pokud jsou údaje platné, udělí žadatel souhlas s přípravou a podáním žádosti.
- Aplikační průvodce vygeneruje v čipu karty klíčový pár. Pro autorizaci generování klíčového páru si od žadatele vyžádá zadání platného PIN, popř. QPIN karty.
- Aplikační průvodce vytvoří žádost o certifikát. Do žádosti zakóduje do odsouhlasené identifikační údaje žadatele i organizace 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.
- Aplikační průvodce autorizuje vzniklou žádost. Vytvoří elektronický podpis žádosti, pomocí soukromého klíče příslušného k autorizačnímu certifikátu, zjištěnému z centrální evidence.
- Obslužný software odešle autorizovanou 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.)

4.1.2.2 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:
  - nejprve fyzicky na základě předložených osobních dokladů – v rámci registračního procesu
  - a následně elektronicky, prostřednictvím adresářové služby Active Directory KB – při podání žádosti.
- 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 zaměstnanců (žadatelů).
- Ověřovat, zda žadatel řádně prošel registračním procesem a že údaje v žádosti odpovídají údajům ověřeným při registraci žadatele.
- Poskytnout žadateli technický prostředek pro vytváření elektronických podpisů (čipovou kartu KB Unipass), včetně autorizačních kódů (PIN, resp. QPIN a PUK). 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.
- Ověřovat autorizační obálku žádosti o certifikát. Kontrolovat, zda byl elektronický podpis autorizační obálky žádosti vytvořen soukromým klíčem příslušným k certifikátu, který byl prověřen v rámci registračního procesu. (Tímto způsobem se ověří, že žádost podal konkrétní žadatel – držitel příslušného autorizačního certifikátu.)
- Před vydáním certifikátu pro kvalifikovaný podpis ověřit, že veřejný klíč v žádosti je součástí klíčového páru, který byl vygenerován v čipové kartě, která je kvalifikovaným prostředkem pro vytváření elektronických podpisů, a že tato karta byla vydána žadateli o certifikát.
- 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).

4.1.2.3 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 a potvrdit převzetí vydaného certifikátu.
- Generovat klíčový pár pouze na čipové kartě, která mu byla přidělena Komerční bankou.
- Před generováním první žádosti o certifikát si na přidělené čipové kartě nastavit přístupové kódy na hodnoty, které zná pouze žadatel.
- 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:

- uživatelským účtem, resp. pověřením získaným při autentizaci vůči adresářové službě Active Directory,
- autorizačním certifikátem, kterým je přepodepsána žádost o certifikát.

Žádost je po vytvoření a autorizaci žadatelem předána ke zpracování. Na základě autentizace žadatele vůči Active Directory 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 žadatel řádně absolvoval registrační proces, v rámci nějž byl ztotožněn a byly získány podklady pro podání žádosti.
- 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.)
- Elektronický podpis autorizační obálky žádosti. Ověřuje se nejen platnost podpisu, ale také, zda je použitý autorizační certifikát v držení žadatele o certifikát.
- 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 softwarovou aplikací (aplikačním průvodcem), kterou používá pro přípravu žádosti a zaslání žádosti do CA.

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. 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: projeví žadatel souhlas s převzetím kliknutím na příslušnou volbu v okně aplikace. Na základě souhlasu 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 KB Unipass, 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 související dokumentaci, řídit se pracovním řádem, vnitřními předpisy a směrnicemi zaměstnavatele.
  - 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, 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* elektronických podpisů.

    Soukromý klíč lze použít pro vytváření zaručených podpisů 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.

Držitel typicky žádá obnovu certifikátu žádá před expirací stávajícího certifikátu. Podmínkou pro podání žádosti o následný certifikát je držení platného certifikátu, vydaného podle této certifikační politiky. Soukromým klíčem tohoto certifikátu žadatel autorizuje žádost o následný certifikát. Autorizace žádosti se provádí elektronickým podpisem vytvořeným pomocí soukromého klíče certifikátu, kterému končí platnost.

4.7.1 Podmínky pro vydání následného certifikátu

Podmínky pro vydání následného certifikátu jsou popsány v kapitole 3.3.1.

4.7.2 Subjekty oprávněné požadovat následný certifikát

Žádost o následný certifikát může podat zaměstnanec KB nebo dceřiné společnosti KB, který je oprávněným držitelem platného kvalifikovaného certifikátu zaměstnance, tzn. certifikátu vydaného podle této certifikační politiky. Takový žadatel mj. splňuje tyto podmínky:

- Zaměstnavatelem mu bylo schváleno oprávnění k držení zaměstnaneckého kvalifikovaného certifikátu a toto oprávnění mu nebylo odebráno. (Oprávnění bylo žadateli schváleno před podáním žádosti o prvotní certifikát.)
- Údaje v certifikátu jsou stále platné. Nedošlo ke změně osobních údajů (což by znamenalo povinnost požádat o zneplatnění certifikátu).
- Žadatel má v stále ve výhradním držení čipovou kartu, která byla ověřena v rámci registračního procesu, před podáním žádosti o prvotní certifikát.

4.7.3 Podání žádosti o následný certifikát

Podání žádosti o následný certifikát probíhá takřka shodným způsobem jako podání žádosti o prvotní certifikát – viz kapitolu 4.1.2. Rozdíly od podání žádosti o prvotní certifikát jsou tyto:

- Pro autorizaci žádosti o následný certifikát se vyžaduje elektronický podpis, vytvořený pomocí soukromého klíče předchozího kvalifikovaného certifikátu daného držitele, tzn. soukromým klíčem certifikátu vydaného podle této certifikační politiky.
- Identifikační údaje v žádosti (předmět a alternativní názvy) se v žádosti o následný certifikát musí shodovat s údaji v certifikátu, jehož klíč byl použit k autorizaci žádosti. Tzn. že identifikační údaje v žádosti o následný certifikát se musí shodovat s identifikačními údaji v předchozím certifikátu stejného držitele.

4.7.4 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.

4.7.5 Oznámení žadateli o vydání následného certifikátu

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

4.7.6 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.

4.7.7 Zveřejnění následného certifikátu certifikační autoritou

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

4.7.8 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

Změna údajů v certifikátu může být iniciována jedním z následujících zdrojů:

- 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.
- Dojde ke změně identifikačních údajů držitele certifikátu (jde o údaje, uvedené v předmětu certifikátu anebo v alternativních názvech):
  - Změna jména či příjmení
  - Změna zaměstnavatele
  - Změna osobního dokladu (doklad uvedený v certifikátu)
  - Změna e-mailové adresy
  - Subjekty oprávněné žádat změnu údajů

Pokud kvalifikovaný poskytovatel služeb vytvářejících důvěru rozhodne o dílčích změnách profilu, pak v žádostech o následný certifikát automaticky uvádí změněné údaje. Poskytovatel o změnách informuje na webových stránkách https://www.kb.cz/pki, včetně publikování nové verze certifikační politiky.

Pokud se změní některý z identifikačních údajů držitele, který je uveden v platném certifikátu, pak je držitel povinen:

- Oznámit změněné údaje svému zaměstnavateli, prostřednictvím pracoviště pro správu lidských zdrojů.
- Požádat o zneplatnění certifikátu, který obsahuje neplatné údaje. Následně lze absolvovat nový registrační proces a požádat o vydání nového certifikátů se změněnými údaji.

Změna identifikačních údajů držitele může být také zaznamenána automaticky informačními systémy KB. Pokud se změnily údaje uvedené v certifikátu, pak aktuální certifikát držitele obsahuje neplatné údaje. KB proto informuje držitele o potřebě vydání nového certifikátu s platnými údaji. Certifikační autorita zneplatní certifikát s neaktuálními údaji. Držitel může požádat o nový certifikát.

Pokud chce držitel požádat o nový certifikát se změněnými identifikačními údaji, musí splnit všechny podmínky pro vydání prvotního certifikátu, včetně schvální požadavku nadřízeným pracovníkem, absolvováním registračního procesu atd…

4.8.2 Zpracování požadavku na změnu údajů v certifikátu

Způsob zpracování žádosti o certifikát se změněnými údaji závisí na důvodu provedené změny:

- Je-li změnou úprava profilu certifikátu (iniciovaná certifikační autoritou), pak jsou změny promítnuty automaticky do následně vydaného certifikátu. Zpracování v takovém případě probíhá stejně jako zpracování žádosti o následný certifikát – viz kapitolu 4.7.
- Došlo-li ke změně identifikačních údajů držitele, pak nelze provést obnovu certifikátu. Držitel musí požádat o nový certifikát, stejným postupem jako se vydává prvotní certifikát. Zpracování v takovém případě zahrnuje všechny kroky, jako při zpracování prvotní žádosti. Viz kapitoly 4.1 a 4.2.

4.8.3 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

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

4.8.4 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.

4.8.5 Zveřejňování certifikátů se změněnými údaji

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

4.8.6 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 – viz kapitolu 4.8.1
- Porušení ustanovení certifikační politiky či smluvních podmínek ze strany držitele certifikátu
- Ukončení zaměstnaneckého vztahu mezi držitelem a Komerční bankou, resp. dceřinou společností KB
- Důvody spojené se stavem držitele (úmrtí, 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
- Nadřízený pracovník 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 samoobslužného webového portálu pro správu certifikátů pracovníka KB. Po úspěšné autentizaci vůči aplikaci držitel vyhledá a zneplatní certifikát.

Portál na základě autentizace zkontroluje, zda je autentizovaný uživatel držitelem certifikátu. Pokud ano, pak aplikace portálu označí certifikát jako zneplatněný.

4.9.3.2 Žádost o zneplatnění držitelem prostřednictvím podpory KB

Držitel může požádat o zneplatnění certifikátu prostřednictvím systému aplikační podpory KB (Service Manager). Do požadavku uvede identifikační údaje certifikátu a důvod zneplatnění.

Držitel se před zavedením požadavku musí vůči systému podpory autentizovat. Systém podpory nese s požadavkem na zneplatnění identitu autentizovaného uživatele. Pracovník podpory ověří, zda je autentizovaný uživatel držitelem certifikátu (a zda je tedy oprávněn požádat o zneplatnění). Po úspěšném prověření pracovník podpory (Správce certifikátů) zneplatní certifikát pomocí příslušného softwarového vybavení: pracovník se autentizuje, vyhledá v evidenci certifikát a označí jej jako zneplatněný.

4.9.3.3 Žádost o zneplatnění nadřízeným držitele, prostřednictvím podpory KB

Podobně jako držitel může o zneplatnění certifikátu požádat i nadřízený pracovník držitele. I nadřízený držitele požádá o zneplatnění prostřednictvím systému pro aplikační podporu. I nadřízený se musí před vznesením požadavku autentizovat.

Pracovník podpory v interní evidenci ověří, zda je autentizovaný uživatel nadřízeným držitele certifikátu (a zda je tedy oprávněn požádat o zneplatnění). Po úspěšném prověření pracovník podpory (Správce certifikátů) zneplatní certifikát pomocí příslušného softwarového vybavení: pracovník se autentizuje, vyhledá v evidenci certifikát a označí jej jako zneplatněný.

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,
- držiteli je odebráno oprávnění k držení certifikátu nebo držitel není nadále zaměstnancem organizace.

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 údaj (e-mailovou adresu) ve zneplatněném certifikátu.

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 se o zneplatnění požádá prostřednictvím systému aplikační podpory, 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 může být ukončeno z těchto důvodů:

- Ukončení zaměstnaneckého poměru držitele certifikátu s organizací.
- Odebrání oprávnění zaměstnance k držení tohoto typu certifikátu.
- Zneplatnění certifikátu. (Pokud držitel splní podmínky, lze mu znovu začít poskytovat certifikáty.)
- Rozvázání vztahu Komerční banky a dceřiné společnosti; rozhodnutí, že dané dceřiné společnosti nebudou certifikáty nadále vydávány.

Pokud má držitel v době ukončení poskytování služeb 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.

Žadatelé / držitelé certifikátů mají do prostor KB či dceřiných společností přístup, odpovídající jejich statusu zaměstnance. Přístup na pracoviště registrační autority je žadatelům umožněn buď jako zaměstnancům anebo jako návštěvám kancelářských prostor KB.

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 pracovníkům KB a dceřiných společností jako součást aktualizace operačních systémů.

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 pracovníkům 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 interními komunikačními kanály pro pracovníky KB a pracovníky dceřiných společností 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 certifikační autority, 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

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

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 KB Unipass), který byl žadateli protokolárně vydán zaměstnavatelem (KB či dceřinou společností KB). 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 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 doručeny jako součást operačního systému. (Žadatelé a držitelé jako zaměstnanci KB či dceřiných společností používají operační systémy, které jsou pod správou zaměstnavatele.)

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). Klíče držitelů, generované v kvalifikovaném prostředku pro vytváření elektronický podpisů, mají minimální délku 3072 bitů (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 KB Unipass, což je kryptografický prostředek, certifikovaný podle Common Criteria na úroveň 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, popř. dceřinou společností KB. 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. Aktivační data se liší pro jednotlivé typy karet:
    - Pro karty, které nejsou kvalifikovaným prostředkem pro vytváření elektronických podpisů, jsou před předáním karty držiteli v čipu karty nastaveny náhodná hodnota PIN a konstantní hodnota PUK. Před generováním prvního klíčového páru je držitel karty vyzván k nastavení nové hodnoty PIN. Hodnota PUK se při této operaci zablokuje. Hodnotu PIN zná výhradně držitel karty. Hodnoty PIN nejsou evidovány v žádných informačních systémech; kvalifikovaný poskytovatel služeb vytvářejících důvěru hodnotu aktivačních dat nezná. Držitel čipové karty si může v průběhu používání hodnotu aktivačních dat (PIN) kdykoli změnit.
    - Pro karty, které jsou kvalifikovaným prostředkem pro vytváření elektronických podpisů, je před předáním karty držiteli v čipu karty nastavena hodnota PUK na konstantní hodnotu. Hodnoty PIN a QPIN jsou zablokovány. Před generováním prvního klíčového páru je držitel karty vyzván k nastavení nových hodnot PUK, PIN a QPIN. Hodnotu všech autorizačních kódů zná výhradně držitel karty. Hodnoty autorizačních kódů nejsou evidovány v žádných informačních systémech; kvalifikovaný poskytovatel služeb vytvářejících důvěru hodnotu

aktivačních dat nezná. Držitel čipové karty si může v průběhu používání hodnotu autorizačních kódů kdykoli změnit.

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 pracovníkům Komerční banky a pracovníkům dceřiných společností KB, kterým bylo držení certifikátu schváleno nadřízeným pracovníkem a kteří splnili podmínky pro vydání certifikátu.

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

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)	Identifikátor osobního dokladu držitele certifikátu. Formát identifikátoru je v souladu s normou ETSI EN 319 412-1: • 3 znaky pro identifikaci typu dokladu, podporovány jsou ○ *IDC* pro občanský průkaz ○ *PAS* pro pas

		○ *IR:* pro povolení k pobytu • 2 znaky pro identifikaci státu, který vydal doklad; podle ISO 3166 • znak pomlčka (0x2D (ASCII), U+002D (UTF-8)) • číslo dokladu Např. pro občanský průkaz ČR: *IDCCZ-765434568*
	O (organizationName)	Název organizace, zaměstnavatele držitele
	OID 2.5.4.97 (organizationIdentifier)	Identifikátor organizace, zaměstnavatele držitele, podle normy ETSI EN 319 412-1, ve tvaru: • 3 znaky pro označení typu identifikátoru, podporováno je jen *NTR* pro IČO • 2 znaky pro označení kódu státu, v němž je identifikátor organizace registrován; kód země podle ISO 3166 • znak pomlčka (0x2D (ASCII), U+002D (UTF-8)) • IČO organizace Např. pro KB: *NTRCZ-45317054*
	C (countryName)	Kód státu, který vydal osobní doklad 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. Pro klíče chráněné v kvalifikovaném prostředku pro vytváření elektronických podpisů min. 3072 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=1.3.154.45317054.1000.1.2.1.11.2 ■ [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)	■ Identifikátor zásad=0.4.0.194112.1.0 QCP-n: certificate policy for EU qualified certificates issued to natural persons

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:

- Rozšíření 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}	
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
Odkazy na dokument PKI Disclosure Statement (PDS)	esi4-qcStatement-5 {0.4.0.1862.1.5}	en: https://www.kb.cz/pki/pds_en.pdf cs: https://www.kb.cz/pki/pds_cs.pdf
Typ certifikátu	esi4-qcStatement-6 {0.4.0.1862.1.6}	Obsahuje typ: elektronický podpis {0.4.0.1862.1.6.1}
Označení syntaxe položky SERIALNUMBER, soulad s normou ETSI EN 319 412-1	Id-qcs-pkixQCSyntax-v2 {1.3.6.1.5.5.7.11.2}	Obsahuje sémantiku pro osobní doklad fyzické osoby id-etsi-qcs-SemanticsId-Natural {0.4.0.194121.1.1}

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 jako v 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

Poskytované certifikační služby jsou zaměstnancům KB a dceřiných společností poskytovány bezplatně.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup elektronickou cestou k vydaným certifikátům se neposkytuje.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

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

9.1.4 Poplatky za další služby

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

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Žádné ustanovení.

9.2 FINANČNÍ ODPOVĚDNOST

9.2.1 Krytí pojištěním

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

9.2.2 Další aktiva a záruky

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

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Tato služba není poskytována.

9.3 DŮVĚRNOST OBCHODNÍCH INFORMACÍ

Certifikáty se podle této certifikační politiky vydávají pro zaměstnance Komerční banky, popř. pro zaměstnance dceřiných společností KB. Při poskytování certifikačních služeb se používají

- jak důvěrné údaje,
- tak údaje které lze zjistit z veřejných zdrojů anebo údaje, které nemají charakter důvěrných informací (identifikace zaměstnavatele).

9.3.1 Rozsah důvěrných informací

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

- Osobní údaje žadatelů, pracovníků kvalifikovaného poskytovatele služeb vytvářejících důvěru a dalších osob, které mohou mít spojitost s poskytováním certifikačních služeb
- Informace o osobních dokladech žadatelů
- Interní dokumentace a směrnice

- Interní smluvní ujednání

Žádné z důvěrných informací nejsou kvalifikovaným poskytovatelem služeb vytvářejících důvěru zveřejňovány. Některé z osobních údajů držitelů jsou uváděny ve vydaných certifikátech.

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

Komerční banka poskytuje certifikační služby v rámci vztahu zaměstnavatel – zaměstnanec (analogicky i pro dceřiné společnosti). Vyžaduje se, aby žadatel o certifikát měl vytvořen uživatelský účet v interních systémech KB. V rámci tohoto vztahu KB eviduje a zpracovává celou řadu informací o svých zaměstnancích, zaměstnancích dceřiných společností a uživatelích svých interních systémů. Velká část těchto záznamů se pokládá za osobní údaje.

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

Zaměstnanci KB a dceřiných společností udělují souhlas se zpracováním osobních údajů v průběhu registračního procesu, podpisem protokolu o registraci.

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 z této certifikační politiky.

9.6.2 Zastupování a záruky RA

Registrační autority garantují kvalitu ztotožnění žadatelů prostřednictvím požadovaných osobních dokladů, čipové karty KB Unipass, interních evidencí zaměstnanců KB a dceřiných společností, a dalších interních podkladů. Ztotožnění žadatelů musí být provedeno osobně, za fyzické přítomnosti žadatele na registračním místě.

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 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 zaměstnancům, resp. zaměstnancům dceřiných společností
- Kontaktních údajů, uvedených v kapitole 1.5
- Elektronických kanálů interní aplikační podpory (Service Manager)
- 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 zaměstnancům, kteří komunikují některým z běžně užívaných světových jazyků. Kvalifikovaný poskytovatel služeb vytvářejících důvěru negarantuje, že pro takové žadatele 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

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

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.

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

Přístupnost pro zdravotně postižené osoby je řešena v rámci interních pravidel Komerční banky a dceřiných společností.

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

9.17 DALŠÍ OPATŘENÍ

Žádná ustanovení.