Infrastruktura veřejných klíčů (PKI) v Komerční bance

Certifikační politika (CP)
pro
podřízenou certifikační autoritu Komerční banky

Obsah

1 Úvod

Certifikační politika stanovená pro podřízenou certifikační autoritu zpracovává popis a zásady, které je třeba dodržovat včetně rozsahu odpovědnosti zúčastněných stran. Podřízená certifikační autorita je zařazena do stromu tzv. ROOT CA KB, řídí se jejími pravidly a zároveň umožňuje vydávat certifikáty uživatelům.

1.1 Pojmy

Obsah dokumentů „typ Certifikační politika“ a „typ Certifikační prováděcí směrnice“ vychází z filozofie standardu RFC2527, kde certifikační politika dokumentuje převážně parametry určitého certifikátu a jeho použitelnost, na rozdíl od směrnice, která kodifikuje převážně postupy uplatňované jednotlivými orgány v rámci činností PKI. Hranice mezi oběma typy dokumentů není ostře stanovena.

Certifikační politika (CP) – pravidla, která vymezují použitelnost certifikátů v rámci jednotlivých skupin a/nebo tříd aplikací v souladu s požadavky bezpečnosti a jsou podporována prostřednictvím postupů definovaných v Certifikačních prováděcích směrnicích (CPS).

Certifikační prováděcí směrnice (CPS) – tvoří rámec pravidel stanovených CP. Definují ve svých procedurách, ustanoveních a předpisech požadavky na všechny prvky PKI vstupující do registračního a Certifikačního procesu. Obsahují detailní rozpracování jedné nebo více CP. Rámcově obsahují:

- seznam Certifikačních politik;
- pro každou CP procedury, ustanovení a předpisy, jak SC KB poskytuje služby vyplývající z CP;
- pravidla a postupy při vydávání certifikátů a činnostech spjatých s certifikátem.

Soukromý klíč – data pro vytváření digitálního podpisu.

Veřejný klíč – data pro ověřování digitálního podpisu.

1.2 Zkratky

CA	Certifikační autorita
CP	Certifikační politika
CPS	Certifikační prováděcí směrnice
MRM	místní registrační místo
OMRM	Operátor místního registračního místa
PKI	Public Key Infrastructure - infrastruktura veřejného klíče
SC KB	Správa certifikátů a veřejných klíčů KB, zahrnuje týmy systému PKI.
CS KB	Certifikační služba KB – zahrnuje všechny řídící, organizační a technologické struktury PKI.
AP PKI	Aplikační podpora PKI
OID	číselný identifikátor objektu, slouží pro identifikaci objektu určitého typu v rámci klasifikace objektů podle ISO/ITU (uvnitř certifikátu nebo jiné standardizované datové struktury)
Kořenová CA	Kořenová certifikační autorita ROOT CA KB, počátek stromu certifikačních autorit.

1.3 Identifikace

Název dokumentu:

Certifikační politika pro podřízenou certifikační autoritu.

Název souboru:

PKI_KB_Subordinate_CP_v101.doc

Identifikátor této certifikační politiky:

1.3.0154.45317054.31.1.45.3.0

Tento objektový identifikátor (OID) pro identifikaci objektů v rámci PKI infrastruktury Komerční banky vychází ze základního OID Komerční banky, odvozeného z mezinárodního zatřídění České republiky (1.3.0154…), z identifikačního čísla organizace (IČO - 45317054).

Certifikační politika je v souladu s CPS.

1.4 Aplikovatelnost

1.4.1 Certifikační autorita

Tato certifikační politika platí pro podřízenou certifikační autoritu KB „DCS CA KB“. Tato certifikační autorita je zařazena v certifikačním stromu, dále neumožňuje zřízení a podporu pro sobě podřízené certifikační autority.
Podřízená CA vydává certifikáty pouze pro klienty/uživatele.

1.4.2 Registrační autorita

Tato certifikační politika platí pro technologické registrační autority přímo podřízené DCS CA KB. Organizačně jsou registrační operace prováděny operátory na místních registračních místech. RA, OMRM a MRM jsou organizačně součástmi KB.

1.4.3 Nevhodné využití

Využití certifikátu podřízené CA není vhodné v aplikacích, které neumí ověřit kompletní certifikační cestu.

2 Kontakt

2.1.1 Kontaktní osoby

Všechny otázky a komentáře týkajících se této certifikační politiky, musí být směřovány na pobočku OMRM nebo TC Liberec.

2.1.2 Správa a řízení

Tato certifikační politika je spravována prostřednictvím SC KB a správa je prováděna v souladu s kapitolou 8 CPS.

2.1.3 Orgány odpovědné za CP v KB

Za vydání a údržbu této CP je odpovědná SC KB.

3 Všeobecná ustanovení

3.1 Práva, povinnosti a závazky

3.1.1 KB

Ve zvláštních a výjimečných případech má KB právo zneplatnit/pozastavit platnost certifikátu podřízené CA. Musí o tomto neprodleně informovat všechny klienty a správce podřízené CA. Takový certifikát musí být okamžitě doplněn na seznam zneplatněných certifikátů (CRL).

3.1.2 Správa PKI

SC KB registruje požadavky a schvaluje/zamítá žádosti o zařazení další podřízené certifikační autority do stromu certifikačních autorit KB, v souladu se strategií KB.

3.1.3 Správa certifikátů a veřejných služeb KB (SC KB)

SC KB je odpovědná za vytvoření, popř. ověření obsahu žádosti o vydání certifikátu a za její následné zpracování podle zásad a postupů definovaných v CP, CPS a souvisejících dokumentech vydaných např. KB. Udržuje informace o vydaných, pozastavených a zneplatněných certifikátech podle příslušných ustanovení CP a CPS; zajišťuje ochranu dat podle příslušných právních předpisů a bezpečnostní politiky PKI.
Informuje a uschovává informace uložené v certifikátech podřízených CA.

3.2 Záruky

Jestliže KB prostřednictvím CA vydává certifikát, poskytuje tím záruku, že veškeré postupy jsou realizovány v souladu s dokumenty CP a CPS a že certifikát podřízené CA je správně implementován a jmenné konvence jsou v souladu s požadavky politik a směrnic.

Komerční banka se výslovně zříká všech záruk, které nejsou explicitně definovány v CP.

3.3 Odpovědnost za škody

KB odpovídá za chod systému PKI a odpovídajících struktur prostřednictvím SC KB. KB neodpovídá za nesprávné užití certifikátu nebo klíče na straně klienta nebo strany, která je závislá na certifikátu.
Pokud nastane škoda na straně KB, bude KB vymáhat náhradu škody právní cestou.

3.4 Interpretace a prosazování

3.4.1 Řídící legislativa neboli rozhodné právo

Za směrodatné a rozhodující pro vymáhání, výklad a platnost této CP a těch CPS či smluv, jichž se to týká, budou považovány platné právní předpisy České republiky.

3.4.2 Likvidace, spojení s jiným subjektem, ukončení činnosti

SC KB postupuje dle platných právních předpisů České republiky. Každý klient CS KB bude informován o změně popř. ukončení činnosti včas a dle pravidel stanovených příslušnými právními předpisy.

3.4.3 Postup při řešení sporů

Kterýkoliv spor, jež nelze řešit smírně, bude podléhat soudnímu rozhodnutí. Soudní jednání se bude konat na území České republiky v českém jazyce.

3.5 Poplatky

Cena podřízeného certifikátu není stanovena.

3.6 Zveřejňování informací

SC KB zveřejňuje platné CP na své internetové stránce. CPS je k dispozici na základě písemné žádosti, kromě částí spojené s bezpečností systému PKI. Po ukončení platnosti jsou tyto dokumenty dostupné pouze v tištěné podobě na základě písemné žádosti.
Seznamy zneplatněných certifikátů jsou pravidelně vydávány každých 6 hodin a jsou dostupné ve veřejném registru certifikátů. KB umožňuje přístup k seznamům zneplatněných certifikátu prostřednictvím protokolů HTTP a LDAP.
Veřejný klíč Kořenové i podřízených CA je publikován ve Veřejném registru certifikátů, kde je přístupný prostřednictvím protokolů HTTP a LDAP, a zároveň na své internetové stránce, kde je přístupný prostřednictvím protokolu HTTP(S). Na této stránce je také zveřejněn otisk certifikátu Kořenové a podřízených CA.
SC KB zpřístupní certifikát Kořenové a podřízených CA v rámci svého Veřejného registru Certifikátů po dobu minimálně tří let po uplynutí platnosti všech vydaných certifikátů.
SC KB stanoví v CPS rozsah zveřejňovaných informací a postupy pro jejich publikaci.

3.7 Prověření shody

Pro zajištění odpovídajícího způsobu provozování všech prvků SC KB, zajišťuje KB pravidelný audit jejich činnosti. Auditor je osoba nezávislá na SC KB. CS KB musí projít min. 1x ročně hloubkovým auditem, jehož se účastní externí auditor (mimo KB). KB stanoví termíny auditů a jmenuje auditory.
Pravidla a postupy pro audit shody reálné činnosti s dokumentací jsou definovány v CPS.

3.8 Zajištění důvěrnosti

Informace získané SC KB (v písemné nebo elektronické podobě) v souvislosti s žádostí o certifikát, jsou náležitě archivovány a nebudou zneužity. Použité postupy se řídí právními předpisy České republiky.

3.9 Práva intelektuálního vlastnictví

KB vykonává práva duševního vlastnictví ke všem dokumentům CP a CPS.

4 Identifikace a autentizace

4.1 Prvotní registrace

Podrobnější informace jsou uvedeny v CPS, resp. ve Smlouvě.

4.1.1 Jmenné konvence

Struktura jmenné konvence je založena na schématu normy X.500. Povinnými atributy certifikátů podřízených certifikačních autorit jsou:
- Common Name (pro zadání jména)
- Organizational Unit (pro zadání informací o správci)
- Organization (pro zadání jména organizace)
- Country (pro zadání země)

Common Name:	DCS CA KB
Organization Unit:	KB PKI Executive
Organization:	Komercni banka
Country:	CZ

4.1.2 Využití jmenných konvencí

Údaje v žádosti o certifikát jsou definovány v souladu se jmennými konvencemi KB a SC KB. Použití nepravého jména či pseudonymu není v současnosti povoleno.

4.1.3 Jednoznačnost jmen

SC KB garantuje jednoznačnost jmen podřízených CA.

4.1.4 Ochranné známky

KB není odpovědná za zkoumání ochranných známek žadatelů či třetích stran a neprovádí je.

4.1.5 Metody dokazování vlastnictví soukromého klíče

Všechny žádosti o certifikáty musí být podepsány s využitím soukromého klíče, příslušného k jeho veřejnému klíči (např. využitím PKSC#10). Toto umožní operátorovi CA potvrdit a ověřit vlastnictví soukromého klíče a správnost podané žádosti.

4.1.6 Ověření totožnosti žadatele o podřízený certifikát

SC KB je povinna potvrdit a ověřit, zda žádost odpovídá jmenným konvencím, zda žádost je adekvátní požadovaným procesům KB.

4.2 Pravidelná obnova klíčů

Certifikát je platný po dobu 10 let. Další certifikát je vydán tak, aby délka platnosti certifikátu odpovídala zákonu o elektronickém podpisu. Hodnoty v certifikátu se mohou změnit dle požadavků KB.

4.3 Výměna klíče po zneplatnění

Identifikace a autentizace po zneplatnění certifikátu je prováděna stejným způsobem jako při prvotní registraci.

4.4 Žádost o zneplatnění/pozastavení platnosti

Žádost o zneplatnění se předává prostřednictvím týmu AP PKI..

5 Provozní požadavky

Případné podrobnější informace jsou uvedeny v CPS.

5.1 Žádost o certifikát

1) Přípravný proces

Tým AP PKI má připraven dokument o jmenných konvencích podřízené CA a všechny dostupné informace:

- CP podřízené CA
- CPS podřízené CA
- Bezpečnostní politiku podřízené CA

2) Registrace, ověření

Admin CA před vlastním procesem ověří všechny údaje, přihlásí se k CA a zkontroluje údaje v certifikátu.

5.2 Vydání certifikátu

Po kladném ověření se potvrdí žádost a vydá certifikát. Admin CA certifikát přenese okamžitě do podřízené CA, přímo na místě a zašle kontrolní otisk certifikátu k publikování na webovém serveru KB.

5.3 Akceptace certifikátu

Certifikát je považovaný SC KB akceptovaný a použitelný bezprostředně po implementaci do podřízené CA.

5.3.1 Publikování certifikátu

Jakmile je certifikát vydán, je publikován ve veřejně dostupném registru certifikátů. Tento registr je dostupný dle požadavků a potřeb elektronických bankovních služeb, na základě přesně definovaných přístupových metod.

5.4 Zneplatnění a pozastavení platnosti certifikátu

5.4.1 Okolnosti pro zneplatnění/pozastavení platnosti certifikátu

Certifikát může být zneplatněn/Certifikátu může být pozastavena platnost pouze v následujících situacích:

- Oprávněná osoba požádá o zneplatnění/pozastavení platnosti
- Došlo-li ke kompromitaci soukromého klíče Kořenové CA.
- Došlo-li ke kompromitaci soukromého klíče Podřízené CA.

5.4.2 Kdo může požádat o zneplatnění/pozastavení platnosti certifikátu

Tým AP PKI provede zneplatnění/pozastavení platnosti certifikátu na základě žádosti:

- Komerční banky - zplnomocněných osob;
- Správce PKI;
- subjektů oprávněných ze zákona.

5.4.3 Postup při podání žádosti o zneplatnění certifikátu

a) Žádost o zneplatnění musí být zpracována písemnou formou, ověřena SC KB.
b) Zplnomocněná osoba může požádat o zneplatnění certifikátu pouze osobně, na místě SC KB.

5.4.4 Postup při podání žádosti o pozastavení účinnosti certifikátu

a) Žádost o pozastavení účinnosti musí být doručena v písemné podobě.
b) Musí být ověřena SC KB
c) Zplnomocněná osoba může požádat o pozastavení účinnosti pouze osobně, na místě SC KB.

5.4.5 Lhůty pro zneplatnění/pozastavení platnosti certifikátu

Po ověření žádosti bude certifikát zneplatněn obratem. Pozastavení podřízené CA je uskutečněno obratem.
Podrobnější informace jsou obsaženy v CPS.

5.4.6 Kontroly platnosti certifikátu závislými stranami

Závislé strany jsou povinny ověřit platnost certifikátu před jeho použitím. Možné způsoby ověřování platnosti (využití CRL apod.) jsou definovány v CPS.

5.5 Postupy auditu bezpečnosti

CS KB definuje události na úrovni systémů a poskytovaných služeb, které jsou zaznamenávány pro účely auditu. Zaznamenané události jsou analyzovány pravidelně, min. 1x měsíčně a jsou uchovávány po dobu nejméně 10 let od svého vzniku. Záznamy jsou chráněny způsobem odpovídajícím jejich citlivosti a významu.
Podrobněji jsou opatření a postupy pro ochranu a zpracování záznamů definovány v CPS společně pro všechny relevantní certifikační politiky.

5.6 Archivace záznamů

5.6.1 Archivované záznamy

CS KB archivuje zejména:
- informace pro účely auditu,
- výsledky auditu,
- veškerou výměnu elektronických zpráv mezi klientem a prvky PKI KB,
- současné a předchozí verze CP a CPS;
- migrační protokoly.
- podepsané registrační formuláře a písemnosti,
- písemné žádosti o zneplatnění/pozastavení účinnosti certifikátu.

5.6.2 Lhůta uchování záznamů v archivu

Všechny archívy budou uchovávány po dobu 13 let.

5.6.3 Ochrana archivu

Záznamy jsou chráněny způsobem odpovídajícím jejich citlivosti a významu. Podrobnější údaje o užitých postupech a opatřeních jsou dokumentovány v CPS a v interních předpisech.

5.7 Výměna klíčů

5.7.1 Klíče certifikační autority

Mezi platností starého a nového klíče dojde k překrytí: dle požadavků zákona o elektronickém podpisu. Například při vydání certifikátu podřízené CA platné 10 let, nový certifikát pro podřízenou CA bude vydán tři roky před vypršením platnosti certifikátu podřízené CA a všechny nově vyžádané certifikáty jsou podepisovány novým. Tím se zamezí případům, kdy je certifikát klienta ještě platný a certifikát CA už nikoliv. Nový certifikát je zveřejněn na internetové stránce KB a ve Veřejném registru certifikátů.

5.7.2 Klíče pro křížovou certifikaci CS KB

Křížové certifikáty CS KB jsou, stejně jako kterékoliv jiné, realizovány prostřednictvím žadatelů. Tito jsou SC KB upozorněni, že dochází k výměně klíče. Je nutno projít stejnými procedurami jako při počáteční křížové certifikaci.

5.8 Kompromitace a zotavení po havárii

Podrobnější údaje o užitých postupech a opatřeních jsou dokumentovány v CPS a v interních předpisech.

5.8.1 Výpočetní zdroje, software/nebo data jsou poškozena

Primárním opatřením pro zotavení po poškození výpočetní techniky nebo dat je použití záloh.

5.8.2 Zneplatnění veřejného klíče

Je-li zneplatněn veřejný klíč některého prvku, který je součástí CS KB, musí být podniknuty následující kroky:

1. dojde k aktualizaci a uveřejnění CRL,
2. prvek je vyřazen z provozu,
3. dochází ke generování nového klíčového páru,

5.8.3 Kompromitace klíče prvku CS KB

Je-li poškozen/prozrazen soukromý klíč některého prvku, který je součástí CS KB, musí být podniknuty následující kroky:

1. certifikát je okamžitě zneplatněn (viz odstavec 4.4),
2. všechny certifikáty, které byly vydány pod tímto klíčem, jsou neprodleně zneplatněny,
3. dojde k aktualizaci a zveřejnění CRL,
4. prvek je deaktivován,
5. je vedeno vyšetřování, aby se zjistila příčina znehodnocení/prozrazení, a bylo ji možno v budoucnu vyloučit,
6. dochází k vygenerování nového klíčového páru.

Všechny certifikáty, které byly vydány před znehodnocením klíče, je nutné vydat znovu.
Případné náklady na jejich vydání nese KB.

5.9 Ukončení činnosti CA

Činnost CS KB je svázána např. se službami Komerční banky, které využívají certifikáty. Provoz CS KB může být proto ukončen pouze po včasném oznámení, že končí provoz. Klienti budou o změnách uvědomeni prostřednictvím informačních kanálů těchto služeb 3 měsíce před ukončením činnosti.

6 Fyzická, procedurální a personální opatření

6.1 Fyzická bezpečnostní opatření

Infrastruktura veřejných klíčů vyžaduje pro svoji činnost důslednou ochranu klíčových komponent. Jeden z významných prvků ochrany je fyzické zabezpečení, které zahrnuje tyto oblasti:

1. výběr vhodných prostor
2. ochrana prostor technickými prostředky
3. omezení přístupu - režimová ochrana
4. rozvody inženýrských sítí a klimatizace
5. protipožární opatření

Certifikační autorita je instalována v místě, které splňuje požadavky na nejvyšší stupeň zabezpečení pro ochranu soukromého klíče Certifikační autority z hlediska protipožární, režimové ochrany a z hlediska technického zabezpečení. Přístup je nepřetržitě monitorován a je umožněn pouze oprávněným specialistům.
Podrobnější informace o příslušných opatřeních a postupech jsou pro všechny relevantní certifikační politiky definovány společně v CPS a Interních bezpečnostních směrnicích PKI KB.

6.2 Procedurální opatření

Pracovní náplně v rámci SC KB jsou přiděleny několika odděleným rolím. Rozdělení funkcí mezi role vychází z požadavku oddělení jednotlivých oblastí činnosti, s omezením možnosti zneužití systému. Jednotlivé funkce mohou být rozděleny mezi více pracovníků.
Podrobnější informace o funkcích a rolích jsou pro všechny relevantní certifikační politiky definovány společně v CPS a Interních bezpečnostních směrnicích PKI KB.

6.3 Personální opatření

Pro práci v SC KB jsou vybíráni prověření, maximálně důvěryhodní a spolehliví pracovníci. Pracovníci jsou při nástupu do SC KB vyškoleni a jejich školení jsou v pravidelných intervalech obnovována. Při porušení stanovených zásad a postupů je příslušný pracovník sankcionován.
Podrobnější informace o personálních opatřeních jsou pro všechny relevantní certifikační politiky definovány společně v CPS a Interních bezpečnostních směrnicích PKI KB.

7 Technická bezpečnostní opatření

7.1 Generace a instalace klíčových párů

7.1.1 Generování klíčů

7.1.1.1 Klíče pro certifikační autoritu

Procesu generování klíčů pro Podřízenou CA musí být přítomni: Správce PKI, jeho zástupce, pracovník týmu AP PKI, jeho zástupce, členové auditorského týmu a vedoucí pracovník, do jehož kompetence spadá činnost SC KB. Klíčové páry jsou generovány přímo v zabezpečeném kryptografickém modulu. Ihned po té je vytvořena záložní kopie soukromého klíče CA na čipové kartě, ta je uložena na zabezpečeném místě.

7.1.1.2 Klíče pro administrátory CA

Generování klíčů pro Superadmina CA (SCA) Podřízené CA je prováděno v průběhu její inicializace, případně v procesu prodlužování. Klíče jsou chráněné heslem, které zadává SCA. Tento SCA má možnost toto heslo kdykoliv změnit. Správce PKI má všechna práva a může generovat klíče pro další adminy (ACA) s různými pravomocemi (auditor, monitorování provozu, vydávání CRL).

7.1.2 Doručení veřejného klíče podřízené CA do SC KB

Veřejný klíč je doručován v rámci žádosti o certifikát, zpracován v zóně nejvyššího zabezpečení. Žádost o certifikát je přijímána SC KB ve formátu PKCS#10. SC KB akceptuje pouze osobní doručení na pracoviště SC KB.

7.1.3 Distribuce veřejného klíče

Veřejný klíč Podřízené CA je publikován jako součást certifikátu ve Veřejném registru certifikátů Komerční banky a zároveň na internetové stránce KB http://www.mojebanka.cz. Na této stránce je také zveřejněn otisk certifikátu Kořenové a Podřízené CA.
Otisk certifikátu Kořenové a Podřízené CA Komerční banky je součástí Smlouvy o vydání a použití certifikátu.

7.1.4 Velikosti klíčů

Klíč Podřízené CA používá algoritmus RSA a má délku 2048 bitů.

7.1.5 Generování obsahu klíčů

Pro vytváření náhodných čísel při generování klíčů Kořenové CA i podřízených CA jsou využity algoritmy zabudované v kryptografickém modulu SureWare Keyper. U tohoto zařízení procesy generování klíčů splňují úroveň 4 standardu FIPS 140 – 1.

7.1.6 Omezení použitelnosti certifikátu

Certifikát Podřízené CA je použit pouze k podpisu veřejného klíče klientů/uživatelů CA a k vydávání CRL.

7.1.7 Využití technického a programového vybavení v procesu generování klíčů

Pro generování klíče CA je využit hardwarový kryptografický modul.

7.2 Ochrana soukromých klíčů

7.2.1 Kryptografické moduly

CS KB používá pro generování a uchování soukromého klíče certifikačních autorit kryptografické moduly SureWare Keyper, které splňují standard FIPS 140 – 1, úroveň 4. Modul je akreditován odpovědnými orgány státní správy ČR.

7.2.2 Úschova soukromého klíče

Soukromý klíč Kořenové i podřízených CA je uložen v chráněném prostředí modulu SureWare Keyper.

7.2.3 Povinnost zpřístupnit soukromé klíče

Soukromé klíče klientů generované SC KB nejsou zpřístupněny žádnému dalšímu subjektu.

7.2.4 Zálohování soukromých klíčů

Současně s vygenerováním páru klíčů Podřízené CA je provedeno zálohování soukromého klíče. Klíč je při zálohování zašifrován klíčem modulu a uložen na čipové karty. Karty jsou uloženy na bezpečném místě.

7.2.5 Archivace soukromých klíčů

Způsob archivace soukromých klíčů potřebných pro provoz SC KB je uveden v Interních bezpečnostních směrnicích PKI KB.

7.2.6 Aktivace soukromého klíče

Soukromý klíč certifikační autority je aktivován pouze po dobu činnosti software CS. Aktivace klíče je podmíněna

- odemknutí klávesnice modulu Keyper (klíč operátora modulu)
- aktivováním služeb modulu (čipová karta bezpečnostního správce),
- zadáním hesel k operačnímu systému, k software certifikační autority a k soukromému klíči.

7.2.7 Deaktivace soukromého klíče certifikační autority

Soukromý klíč certifikační autority je deaktivován minimálně v těchto případech:

- kryptografický modul detekoval pokus o narušení bezpečnostních opatření
- činnost softwaru certifikační autority využívající privátní klíč je ukončena. Deaktivaci může uskutečnit pouze SCA (superadmin CA) , ACA (admin CA), po pokynu vydaném Řídící komisí.

7.2.8 Zrušení/smazání soukromých klíčů

V případě Podřízené CA je nutno vynulovat kryptografický modul a inicializovat čipové karty se záložním klíčem.

7.3 Další aspekty správy klíčů

7.3.1 Archivace veřejných klíčů (certifikátů)

Certifikáty jsou archivovány v databázi po dobu minimálně 13 let. Tato databáze je archivována i po ukončení činnosti CA tak, aby podmínka lhůty archivace byla splněna.

7.3.2 Doba platnosti klíčů

Doba platnosti klíče Root Certifikační autority je 20 let.
Doba platnosti podřízené CA je max.10 let.

7.4 Aktivační data

Hesla opravňující k přístupu do modulů, souborů nebo čipových karet se soukromými klíči vzhledem k četnosti použití jsou uchovávána v písemné podobě, dle pravidel.
Rovněž interval a pravidla pro povinnou změnu hesel a tvar hesel je specifikován v *Interních bezpečnostních směrnicích PKI KB*.

7.5 Zabezpečení počítačových systémů

Při návrhu infrastruktury SC KB byl kladen maximální důraz na důkladné zabezpečení všech komponent.
Zabezpečení počítačových systémů SC KB včetně jejich propojení sítěmi je detailně popsáno v *Interních bezpečnostních směrnicích PKI KB*.

7.6 Opatření pro bezpečnost životního cyklu

Oddělení vývoje a rozvoje PKI v KB od produkčního prostředí:

1. Pro vývoj a rozvoj systému PKI v KB je připraveno testovací a vývojové prostředí, které je fyzicky i logicky odděleno od produkčního prostředí.
2. V tomto prostředí jsou testovány nové prvky zabezpečení, nové operační systémy a upgrade a update před nasazením do produkčního prostředí.

Podrobnější informace jsou obsaženy v *Interních bezpečnostních směrnicích PKI KB*.

7.7 Zabezpečení sítí

Kontroly a ověřování stavu a průchodnosti sítě jsou pravidelně prováděny prostřednictvím technických správců v rámci struktury KB.
Podrobnější informace jsou obsaženy v *Interních bezpečnostních směrnicích PKI KB*.

7.8 Technické zabezpečení kryptografického modulu

Pro nasazení v rámci CS KB smí být použity pouze kryptografické moduly splňující úroveň zabezpečení podle standardu FIPS 140-1, úroveň 3. Kryptografické moduly nasazené v certifikačních autoritách musí mít úroveň zabezpečení podle FIPS 140-1, úroveň 4.

8 Profil certifikátu a CRL

8.1 Profil certifikátu

Certifikát DCS CA KB je osvědčení, které propojuje veřejný klíč s objektem CA. Certifikát vydaný podle této CP je v souladu s normou ISO 9594-8 (X.509), verze 3.

8.1.1 Registrační proces

Registrace podřízených CA se uskuteční SC KB na místě implementace certifikátu podřízené CA. Až po ověření je požadavek předán k certifikaci na Kořenové CA.

8.1.2 Tvar certifikátu

V certifikátu jsou uvedeny následující informace:

- verze certifikátu (verze 3)
  - **2**
- jméno CA (atribut Common Name)
  - **DCS CA KB**
- jméno správy Root CA (atribut Organizational Unit)
  - **PKI KB Executive**
- název organizace (atribut Organization)
  - **Komercni banka**
- stát (atribut Country)
  - **CZ**
- délka klíče
  - **2048**
- algoritmus
  - **RSA**
- období platnosti
  - **10** roků
- účel použití certifikátu (rozšíření Key Usage)
  - **Digital Signature**
  - **Non-Repudiation**

    - **CRL Signing**
    - **Certificate Signing**
- identifikace veřejného klíče Root CA (rozšíření Authority Key ID)
    - **160-tibitový SHA-1 otisk veřejného klíče certifikační autority**
    - **DN certifikační autority + seriové číslo certifikátu**
- identifikace veřejného klíče subjektu certifikace (rozšíření Subject Key ID)
    - **160-tibitový SHA-1 otisk veřejného klíče subjektu certifikátu**
- objektový identifikátor této certifikační politiky (rozšíření Policy OID)
    - **1.3.0154.45317054.31.1.45.3.0**
- místo, odkud lze stáhnout tuto certifikační politiku (kvalifikátor rozšíření Policy OID)
    - **www.mojebanka.cz**
- název dokumentu certifikační politiky (kvalifikátor rozšíření User Notice)
    - **Certificate Policy - Root Certification Authority**

8.1.3 Použitelnost certifikátu

(viz též 1.4) Certifikát slouží pro digitální podpis (CRL a certifikátu). Certifikát zajišťuje podpis veřejných klíčů klientů/uživatelů.

8.2 Profil CRL

CA podporuje Seznam zneplatněných certifikátů (CRL) verze 2, dostupných prostřednictvím registru certifikátů dle normy DAP (LDAP). Jako alternativní k CRL v LDAP může CS využít služeb WEB serverů nebo jiné služby sloužící ke kontrole a ověření certifikátů.

8.2.1 Obsah CRL

CRL seznamy jsou vydávány s následujícími standardními položkami (poli, atributy):
- signature algorithm
    - **sha1WithRSAEncryption**
- vydavatel (Issuer) - má stejný obsah jako tento atribut v certifikátu Kořenové CA
- čas vydání tohoto CRL seznamu (This Update)
- předpokládaný čas vydání následujícího CRL seznamu (Next Update)

Vydávané CRL seznamy používají následující rozšíření pro verzi 2:
- alternativní jmény vydavatele certifikátu (Issuer Alternate Name)
    - objekt EmailAddress
    - objekt URI
- identifikace veřejného klíče Kořenové CA (Authority Key ID)
    - **160-tibitový SHA-1 otisk veřejného klíče** Kořenové CA
- pořadové číslo CRL seznamu (CRL Number)

Vydávané CRL seznamy používají následující parametry a položky zneplatněných certifikátů:
- sériové číslo zneplatněného certifikátu (Revoked Certificates)
- datum a čas zneplatnění (Revocation Date)
- důvod zneplatnění (Reason Code)
    - tato položka není povinná, důvod nemusí být oznámen

9 Správa a specifikace

9.1 Specifikace procedur změn a činností

a) SC KB může provést pouze změny opravné nebo editační bez předchozího projednání a schválení (např. změnu kontaktu či adres). Jiné, výrazné změny týkající se prvků PKI v KB, jejich chování a pravidel musí být schváleny Řídící komisí s využitím pravidel KB.
b) Chyby, změny, nebo předpokládané změny těchto dokumentů jsou hlášeny kontaktním osobám, či částem uvedených v části 2.1.1 této CP. Tato komunikace musí zahrnovat popis změny, zdůvodnění změn a kontaktní informace osoby, žádající změnu.

c) Všechny změny v CP vydané v rámci infrastruktury veřejných klíčů mají být SC PKI zaslány na všechna odpovídající kontaktní místa a tam zveřejněny po dobu 1 měsíce. Změny aktuální CP budou distribuovány odpovídajícím a odpovědným složkám využitím technologií Internetu, Intranetu a elektronické pošty.
d) KB může akceptovat, modifikovat nebo odmítnout navrhované změny po vystavení v řádné časové periodě (1 měsíc).
e) Jestliže navrhované změny CP budou mít vliv na určité množství uživatelů, KB smí, v rámci svého výhradního práva, přidělit nový objektový identifikátor pro modifikovanou CP popř. doplnit stávající CPS nebo vytvořit novou CPS.

9.2 Zveřejnění a politika oznámení změn

9.2.1 Údaje nepublikované úmyslně v této CP

Instrukce
Interní směrnice pro provoz SC KB,
Interní bezpečnostní směrnice PKI KB

9.2.2 Šíření a distribuce definovaných CP a CPS

CP jsou šířeny následujícími způsoby:
- přes WWW stránku: http://www.mojebanka.cz

CPS je k prohlédnutí:
- po písemné žádosti na registračním místě

Nebudou poskytnuty informace o procesech spojených s bezpečností CS KB.

9.3 Schvalovací procedury CP

SC KB je odpovědná za přípravu dokumentů a schválení dokumentů.