Infrastruktura veřejných klíčů (PKI) v Komerční bance

Certifikační politika (CP)
s vysokým stupněm ověření osobní totožnosti žadatele/klienta

Osobní certifikát na čipové kartě

Obsah

1 Úvod

Certifikační politika s uvedenou metodikou vydávání certifikátů s vysokým stupněm ověření klienta zpracovává popis registrace, ověření, uplatnění certifikátů a zároveň zásady, které je třeba dodržovat včetně rozsahu odpovědnosti zúčastněných stran.

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.

Klient – fyzická i právnická osoba, uzavírá smlouvu s KB. Podílí se na registračním procesu, žádá o vydání certifikátu, její totožnost je ověřována. Vlastní soukromý klíč a k němu odpovídající certifikát. Zodpovídá za ochranu a použití soukromého klíče a odpovídajícího certifikátu.
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
ČK	Čipová karta
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
OID	číselný identifikátor objektu, slouží pro identifikaci objektu určitého typu v rámci klasifikace objektů podle ISO/ITU (uvnitř certifikátu nebo jiné standardizované datové struktury)
CS	Certifikační služba KB – zahrnuje všechny řídící, organizační a technologické struktury

1.3 Identifikace

Název dokumentu:
Certifikační politika osobního certifikátu vydaného do čipové karty s vysokým stupněm ověření totožnosti.
Název souboru:
PKI_KB_CP_E_Os_vys_cip_cl_v501.doc
Identifikátor této certifikační politiky:
1.3.0154.45317054.131.1.25.0.3

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.

Důležité upozornění pro účastníky registračního a Certifikačního procesu, kterým má metodika sloužit:

Před prvním použitím certifikátů s vysokým stupněm ověření totožnosti je klient povinen se seznámit s touto Certifikační politikou a jí odpovídajícími CPS.

1.4 Aplikovatelnost

1.4.1 CA

Tato certifikační politika platí pro externí certifikační autoritu KB „DCS CA KB“. Tato certifikační autorita je zařazena v certifikačním stromu KB, jehož kořenem je kořenová certifikační autorita KB „Root CA KB“. DCS CA KB již nezřizuje ani nepodporuje sobě podřízené certifikační autority.

1.4.2 RA

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 Klienti

Klientem může být pouze taková fyzická osoba, která je způsobilá k právním úkonům a pro kterou je možné ověřit totožnost.

1.4.4 Vhodné aplikace

K využití tohoto typu certifikátu jsou doporučené a otestované následující aplikace (viz též 7.1.3):

- elektronické bankovní systémy – dodané popř. realizované Komerční bankou, např. s využitím prostředí prohlížeče WEB (Internet bankovnictví) nebo vlastní aplikace KB.
- ověření totožnosti uživatele – prostřednictvím protokolu SSL, např. prohlížeče WEB (Internet Explorer, Netscape Navigator) nebo tzv. vzdáleně přistupujícího klienta (VPN)
- lze je využít i v prostředí elektronické pošty – Outlook, Exchange, samostatně popř. prostřednictvím dodávaných modulů pro zabezpečení elektronické pošty.

1.4.5 Nevhodné aplikace

Jako nevhodné aplikace jsou chápány všechny, které nejsou schváleny touto CP.

1.5 Kontakt

1.5.1 Kontaktní osoby

Se všemi otázkami a komentáři týkající se této certifikační politiky se obracejte na OMRM, který zajistí potřebné informace.

1.5.2 Správa a řízení

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

1.5.3 Orgány odpovědné za CP v KB

Za vydání a údržbu této CP je odpovědný správce PKI.

2 Všeobecná ustanovení

2.1 Práva, povinnosti a závazky

Komerční banka
Ve zvláštních případech má SC KB právo zneplatnit/pozastavit platnost certifikátu klienta a musí o tomto neprodleně informovat klienta a vydat takový certifikát na seznam zneplatněných certifikátů (CRL).
Certifikační autorita
Vydává certifikáty PKI entit a klientů podle zásad a postupů definovaných v CP, CPS a souvisejících dokumentech vydaných KB; udržuje informace o vydaných, pozastavených a zneplatněných certifikátech podle příslušných ustanovení CP a CPS; zajišťuje ochranu dat podle příslušných právních předpisů.
Registrační autorita
Registruje žadatele/klienty a předává jejich žádosti o certifikáty ke zpracování podle zásad a postupů definovaných v CP, CPS a souvisejících dokumentech vydaných KB
Držitel certifikátu
Používá vydaný certifikát pouze v souladu s touto CP a souvisejícími dokumenty vydanými KB; zajišťuje ochranu svého soukromého klíče podle příslušných ustanovení CP a CPS resp. Smlouvy.
Závislá strana
Ověřuje platnost certifikátu při každém použití.
Úložiště
Informuje klienty/žadatele a závislé strany o informacích uložených v certifikátech a o pozastavení či zneplatnění certifikátu podle příslušných ustanovení CP/S.

2.2 Záruky CA a RA

Certifikační autorita
Jestliže KB prostřednictvím CA vydává certifikát, poskytuje tím záruku, že veškeré postupy jsou realizovány v souladu s dokumenty CP a CPS a že certifikát (veřejný klíč klienta) je spojen s osobou klienta.
Registrační autorita
Všechny postupy registrace klienta/žadatele jsou v souladu s příslušnou CP, CPS a souvisejícími dokumenty vydanými KB.
Komerční banka se výslovně zříká všech záruk, které nejsou explicitně definovány v CPS.

2.3 Odpovědnost za škody

KB odpovídá za chod systému PKI a za činnost SC KB. KB neodpovídá za nesprávné užití certifikátu nebo klíče na straně klienta nebo závislé strany.
Pokud nastane škoda na straně KB, bude KB vymáhat náhradu škody právní cestou.
Podrobně je finanční odpovědnost definována v CPS.

2.4 Interpretace a prosazování

2.4.1 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.

2.4.2 Likvidace, spojení s jiným subjektem, ukončení činnosti

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

2.4.3 Postup při řešení sporů

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

2.5 Poplatky

Případná cena certifikátů je zveřejňována v oficiálním ceníku certifikátů. Ceník může být k dispozici i na internetové stránce Komerční banky. Může být rovněž zaslán na požádání.

2.6 Zveřejňování informací

KB zveřejňuje platné CP na své internetové stránce. Dále je možné tyto dokumenty získat v tištěné podobě na základě písemné žádosti. Po ukončení platnosti jsou tyto dokumenty dostupné pouze v tištěné podobě na základě písemné žádosti, předané na pobočce OMRM.
Některé části CPS odpovídají pravidlům o citlivé informaci a jako takové nebudou součástí zveřejněných dokumentů. CPS lze získat pouze na základě písemné žádosti, předané na pobočce OMRM.
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.
Veřejné klíče kořenové i podřízené CA jsou publikovány jako součást CA certifikátu ve Veřejném registru certifikátů, kde jsou přístupné prostřednictvím protokolů HTTP a LDAP, a zároveň na internetové stránce KB, kde jsou přístupné prostřednictvím protokolu HTTP(S). Na této stránce jsou také zveřejněny otisky certifikátu kořenové i podřízené CA.
Otisky certifikátu podřízené CA a kořenové CA jsou součástí Smlouvy o vydání a použití certifikátu.
SC KB zpřístupní certifikáty Certifikační služby KB v rámci svého Veřejného registru Certifikátů po dobu minimálně tří let po uplynutí platnosti všech vydaných certifikátů.
KB stanoví v CPS rozsah zveřejňovaných informací a postupy pro jejich publikaci.

2.7 Prověření shody

Pro zajištění odpovídajícího způsobu provozování všech prvků SC KB, zajišťuje KB pravidelný audit jejich činnosti. Auditor je osoba nezávislá na SC KB. SC 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.

2.8 Zajištění důvěrnosti

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

2.9 Práva intelektuálního vlastnictví

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

3 Identifikace a autentizace

3.1 Prvotní registrace

Případné podrobnější informace jsou uvedeny v CPS, resp. ve Smlouvě.

3.1.1 Jmenné konvence

Struktura jmenné konvence je založena na schématu normy X.500. Povinnými atributy jména v certifikátu jsou:

- Common Name (pro zadání jména držitele)
- Organizational Unit (pro zadání bydliště a data narození)
- Country (pro zadání státu bydliště)
- Locality (pro zadání města bydliště)
- Subject Alternate Name-RFC822Name (pro zadání adresy elektronické pošty)

3.1.2 Využití jmenných konvencí

Údaje v žádosti o certifikát jsou porovnávány s identifikačním dokladem.
Použití pseudonymu není v současnosti povoleno.

3.1.3 Jednoznačnost jmen

Registrační místa nemohou garantovat jednoznačnost jmen.

3.1.4 Jmenné tvrzení, prohlášení a pochybnosti v proceduře rozlišování

Tyto nesrovnalosti budou řešeny SC PKI.

3.1.5 Ochranné známky

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

3.1.6 Metody dokazování vlastnictví soukromého klíče

Všechny elektronické žádosti o certifikáty musí být klientem podepsány s využitím jeho soukromého klíče, příslušného k jeho veřejnému klíči (např. využitím PKSC#10). Toto umožní operátorovi RM případně systému PKI ověřit vlastnictví soukromého klíče.

3.1.7 Ověření totožnosti klienta

RA je povinna ověřit totožnost žadatele pomocí postupů definovaných dále v této CP resp. v CPS.
Před vydáním certifikátu s vysokým stupněm ověření totožnosti klienta se ověřují následující informace (viz oddíl 4):

- Stát;
- město/obec;
- ulice/místo, číslo popisné, PSČ;
- příjmení klienta;
- křestní jméno klienta (příp. iniciály dalších jmen);
- rok, měsíc a den narození;
- kontaktní e-mail adresa klienta;
- kontaktní telefonní číslo;
- telefonní číslo pro zaslání jednorázového hesla prostřednictvím SMS.

Do elektronické žádosti o certifikát a poté do certifikátu je rovněž doplněn identifikační údaj klienta v systému KB.
Pro ověření totožnosti klienta je vyžadován platný doklad totožnosti, případně doplňkový doklad, přičemž jsou upřednostňovány doklady s fotografií.

3.2 Pravidelná obnova klíčů

Probíhá před uplynutím doby platnosti původního certifikátu, závisí na typu certifikátu.

a) Žádost o certifikát je podepsaná platnými daty pro vytváření digitálního podpisu. Změní se data pro ověřování digitálního podpisu, údaje uvedené k jednoznačné identifikaci zůstávají stejné. Je vydán nový certifikát, s novou dobou platnosti. Ověření údajů jednoznačné identifikace proběhne v rámci systému SC KB.

b) Pokud budou změněny údaje jednoznačné identifikace, pro které je nutné předložit průkazy totožnosti, je nutná osobní účast klienta na MRM. Po ověření je vydán nový certifikát.

c) Pokud je změněna jiná hodnota než v jednoznačné identifikaci – např. e-mail adresa – nový certifikát lze vydat na základě doručené žádosti o certifikát, podepsané platnými daty pro vytváření digitálního podpisu. Mění se data pro vytváření digitálního podpisu. Platí, že hodnoty jednoznačné identifikace musí být stejné jako při osobním předání žádosti, kromě hodnoty např. e-mail adresy.

Hodnoty v jednoznačné identifikaci jsou porovnány s hodnotami uvedenými v záznamech SC KB.

3.3 Vydání klíče po zneplatnění

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

3.4 Žádost o zneplatnění/pozastavení platnosti

a) V případě, že klient nebo třetí pověřená osoba žádá o zneplatnění, musí potvrdit svoji žádost následujícími dokumenty:
   - klient – vyplněný a podepsaný formulář (žádost o zneplatnění), totožnost je ověřena dle platného průkazu totožnosti. Před odesláním žádosti o zneplatnění je nutná znalost hesla pro zneplatnění/pozastavení certifikátu;
   - pověřená osoba - vyplněný a podepsaný formulář (žádost o zneplatnění), totožnost je ověřena dle platného průkazu totožnosti a plné moci. Před odesláním žádosti o zneplatnění je nutná znalost hesla pro zneplatnění/pozastavení certifikátu;

b) V případě, že klient nebo třetí ověřená strana žádá o pozastavení platnosti certifikátu, lze toto uskutečnit prostřednictvím k tomu určené aplikace, vzdáleně, na registračních místech nebo prostřednictvím Telefonního centra.

3.5 Základní pravidla pro práci s ČK

SC KB zaručuje, že jsou splněna základní kritéria určená pro práci s ČK:

a) klíče jsou generovány na ČK
b) soukromá klíč nikdy neopustí ČK

4 Provozní požadavky

Případné podrobnější informace jsou uvedeny v CPS.

4.1 Žádost o certifikát

1) Přípravný proces

a) Klient si může ze stránky KB www.mojebanka.cz kopírovat odpovídající soubory pro certifikát nejvyššího stupně (Certifikační politiku) a vytiskne si ji. Klient si rovněž může CP vyzvednout na místních registračních místech KB.
b) Klient se osobně dostaví na místní registrační místo KB s doklady totožnosti.

Schůzka s operátorem registračního místa může být předem sjednaná. Seznam místních registračních míst je uveden na www.mojebanka.cz.

2) Registrace, ověření a předání jednorázového hesla na registračním místě:

a) Operátor místního registračního místa předá klientovi ČK. Je žádoucí změna PINu, lze před i po procesu vydání certifikátu.
b) Operátor místního registračního místa (OMRM) ověřuje totožnost klienta podle průkazu totožnosti popř. podle doplňkového dokladu;
c) OMRM zpracuje s klientem údaje do žádosti o certifikát;
d) Klíče jsou generovány v přítomnosti klienta. Klient potvrzuje zobrazené informace zadáváním svého PINu.

e) OMRM předá klientu výtisk schváleného certifikátu k provedení kontroly. Pokud klient s údaji souhlasí, schválí a potvrdí svoji žádost o certifikát.
f) OMRM zpracuje smlouvu o používání certifikátu.

4.2 Vydání certifikátu

Po přijetí ověřené žádosti o certifikát, SC KB generuje certifikát a připraví jej k vyzvednutí. Po akceptaci (viz. odst. 4.3) si klient poté svůj certifikát vyzvedne a importuje do ČK.

4.3 Akceptace certifikátu

a) Celý proces probíhá na registračním místě.
b) Certifikát je považovaný klientem za akceptovaný a použitelný bezprostředně po ověření certifikátu prostřednictvím aplikace dodané SC KB k ověření certifikátu. Klient je zodpovědný za ověření správnosti obsahu svého certifikátu. Jestliže klient zjistí rozpor mezi údaji smluvního ujednání a obsahem certifikátu, musí bez prodlení informovat KB.
c) OMRM provede zneplatnění certifikátu.
d) Není-li certifikát ověřen, nepovažuje se za akceptovaný a použitelný.
e) Jestliže není certifikát ověřen, může být aplikací odmítnut.

4.3.1 Publikování certifikátu

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

4.4 Zneplatnění a pozastavení platnosti certifikátu

4.4.1 Okolnosti pro zneplatnění/pozastavení platnosti certifikátu

Certifikát může být zneplatněn/Certifikátu může být pozastavena platnost pouze v následujících situacích:
- klient nebo zplnomocněná osoba požádá o zneplatnění/pozastavení platnosti;
- certifikát byl vydán na základě chybných či nepravdivých údajů nebo údaje, na jejichž základě byl vydán, přestaly platit;
- klient (držitel certifikátu) porušil závažným způsobem Smlouvu;
- došlo-li ke kompromitaci soukromého klíče CS KB.

4.4.2 Kdo může požádat o zneplatnění/pozastavení platnosti certifikátu

CS KB provede zneplatnění/pozastavení platnosti certifikátu na základě žádosti:
- klienta (držitele certifikátu) nebo jím pověřené osoby;
- Operátora MRM, který certifikát vydal;
- SC KB;
- subjektů oprávněných ze zákona.

4.4.3 Postup při podání žádosti o zneplatnění certifikátu

a) Žádost o zneplatnění musí být zpracována písemnou formou, potvrzena heslem a ověřena SC KB.
   - Klient musí být ověřen prostřednictvím procedur ověření a potvrzení skutečného vlastnictví certifikátu (viz odst. 3.4).
   - Klient/pověřená osoba může požádat o zneplatnění certifikátu těmito způsoby:
     – osobně – se žádostí o zneplatnění certifikátu, na MRM, se znalostí hesla pro zneplatnění certifikátu

b) Klient/pověřená osoba může nejprve požádat o pozastavení platnosti certifikátu telefonickým, faxovým nebo elektronickým kanálem (viz násl. odstavec), s následným doručením žádosti o zneplatnění či zrušení pozastavení.

4.4.4 Postup při podání žádosti o pozastavení platnosti certifikátu

a) Klient/pověřená osoba může požádat o pozastavení platnosti těmito způsoby:
- telefonicky – se žádostí o pozastavení platnosti,
- osobně – se žádostí o pozastavení platnosti certifikátu, na MRM,
- faxem – žádostí o pozastavení platnosti na pobočku KB,
- elektronickou poštou – se žádostí o pozastavení platnosti na OMRM,
- Prostřednictvím aplikace vytvořené SC KB a dostupné na Internetu, doplněnou heslem pro zneplatnění/pozastavení platnosti certifikátu.

4.4.5 Lhůty pro zneplatnění/pozastavení platnosti certifikátu

Po ověření žádosti bude certifikát zneplatněn/pozastaven obratem, nejpozději během SC KB stanoveného časového limitu.
Podrobnější informace jsou obsaženy v CPS.

4.4.6 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.

4.5 Postupy auditu bezpečnosti

SC KB definuje události na úrovni systémů a poskytovaných služeb, které jsou zaznamenávány pro účely auditu. Zaznamenané události jsou analyzovány pravidelně, min. 1x týdně a jsou uchovávány po dobu minimálně 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.

4.6 Archivace záznamů

4.6.1 Archivované záznamy

SC 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.

MRM archivuje zejména písemné dokumenty používané v rámci služeb prostřednictvím elektronických distribučních kanálů:
- podepsané registrační formuláře - Smlouva o poskytnutí a používání certifikátu,
- písemné žádosti o zneplatnění/pozastavení platnosti certifikátu.

4.6.2 Lhůta uchování záznamů v archivu

Všechny archívy budou uchovávány po dobu minimálně 10 let.

4.6.3 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.

4.7 Výměna klíčů

4.7.1 Klíče uživatelů

Klient je automaticky upozorněn emailem 30 a 15 dní před vypršením platnosti. Nový certifikát není automaticky znovu vystaven na základě předchozích dat. Klient musí požádat o nový certifikát nebo prodloužení platnosti certifikátu. Doporučuje se, aby všechny druhy nově vytvářených certifikátů byly založeny na novém páru klíčů, neboť období platnosti certifikátu bylo stanoveno z bezpečnostních důvodů.

4.7.2 Klíče certifikační autority

Mezi platností starého a nového klíče dojde k překrytí: tři roky a jeden měsíc před vypršením platnosti klíče je vydán nový 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.

4.7.3 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.

4.8 Kompromitace a zotavení po havárii

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

4.8.1 Výpočetní zdroje, software/nebo data jsou poškozena

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

4.8.2 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,

4.8.3 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.

4.9 Ukončení činnosti CA

Činnost CS KB je svázána s ostatními službami Komerční banky, které využívají certifikáty. Provoz CS KB může být proto ukončen pouze po zrušení těchto služeb nebo pokud přejdou na jinou technologii zabezpečení. Klienti budou o změnách uvědomeni prostřednictvím informačních kanálů těchto služeb 3 měsíce před ukončením činnosti.

5 Fyzická, procedurální a personální opatření

5.1 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.

5.2 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.

5.3 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.

6 Technická bezpečnostní opatření

6.1 Generace a instalace klíčových párů

V případě definování požadavků na kryptografické klíče je třeba rozlišit dvě oblasti vlastníků klíčů:

- klíče pro vnitřní potřebu SC KB - do této kategorie patří např. klíče certifikačních a registračních autorit,
- klíče pro klienty.

6.1.1 Generování klíčů

6.1.1.1 Klíče pro certifikační autoritu

Procesu generování klíčů pro Root CA KB i DCS CA KB musí být přítomni: Správce PKI, jeho zástupce, člen týmu aplikační podpory PKI, jeho zástupce, členové auditorského týmu, externí nezávislý auditor 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 CS na čipové kartě, ta je uložena na zabezpečeném místě.

6.1.1.2 Klíče pro ostatní moduly Infrastruktury veřejných klíčů Komerční banky

Generování klíčů pro Registrační autority a ostatní moduly Infrastruktury veřejných klíčů Komerční

banky (RA, RAO, WebRAO,....) je prováděno členem týmu aplikační podpory Infrastruktury veřejných klíčů Komerční banky v přítomnosti operátora odpovědného za příslušný modul, pro který jsou klíče generovány. Klíče jsou chráněné heslem, které zadává operátor. Tento operátor má možnost toto heslo kdykoliv změnit.

6.1.1.3 Generování klíčů pro klienta jeho vlastními prostředky

Klient je odpovědný za proces generování páru klíčů a elektronické žádosti o certifikát na svém HW. Může být použit software dodaný nebo doporučený SC KB. Klient je též odpovědný za bezpečné uložení soukromého klíče. Heslo/PIN umožňující přístup k použití soukromého klíče nesmí být uchováváno v otevřené formě ani sdělováno cizí osobě.

6.1.1.4 Generování klíčů pro klienty prostředky SC KB

Klíče jsou generovány operátory MRM v prostředí SC KB, na Č s využitím odpovídajících technologií splňujících normy PKCS a zásady zabezpečení**. Heslo/PIN umožňující přístup k použití soukromého klíče zadává klient na MRM osobn**ě. Je žádoucí změna PINu po odchodu z obchodního místa, z vlastního HW.

6.1.2 Předání soukromého klíče klienta

Soukromý klíč klienta je mu předán:

- na čipové kartě chráněné heslem/PIN, dle formátu PKCS#11.

6.1.3 Doručení veřejného klíče klienta do SC KB

Veřejný klíč klienta je doručován v rámci elektronické žádosti o certifikát. Tato žádost je přijímána SC KB ve formátu PKCS#10, PEM, REQ nebo DER. SC KB akceptuje následující způsoby doručení žádostí:

- Při osobní registraci, v rámci generování klíčů a elektronické žádosti na čipové kartě.

6.1.4 Distribuce veřejného klíče (certifikátu)

6.1.4.1 Distribuce veřejného klíče CS (CS certifikátu)

Veřejný klíč CS (kořenové i podřízené) je publikován jako součást CS certifikátu ve Veřejném registru certifikátů Komerční banky a zároveň na internetové stránce KB http://www.mojebanka.cz. Na této stránce jsou také zveřejněny otisky certifikátů.
Otisky certifikátů CS KB jsou součástí Smlouvy o vydání a použití certifikátu.

6.1.4.2 Distribuce veřejného klíče klienta (certifikátu klienta)

Certifikát klienta je publikován do Veřejného registru certifikátů KB.

6.1.5 Velikosti klíčů

Klíč Certifikační autority používá algoritmus RSA a má délku 2048 bitů.
Klíče ostatních modulů Infrastruktury veřejných klíčů Komerční banky mají délku 2048 bitů, algoritmus RSA.
Minimální délka klíče uživatele je 1024 bitů, uživatel může pro podpis používat algoritmus RSA.

6.1.6 Generování obsahu klíčů

Pro vytváření náhodných čísel při generování klíčů CA jsou využity algoritmy zabudované v kryptografickém modulu. U tohoto zařízení je certifikován i proces generování klíčů.

Při generování klíčů dalších modulů PKI KB a klientů je pro počáteční nastavení generátoru náhodných čísel po určitou dobu snímán pohyb myši a činnost klávesnice.

6.1.7 Omezení použitelnosti certifikátu

Certifikáty vydávané SC KB obsahují podle normy X.509v3 rozšíření upravující způsoby použití certifikátu.
Certifikáty vydávané podle této CP smí být použit pouze k účelům:
- šifrování, odšifrování, digitální podpis a pro určení nepopiratelné odpovědnosti.

6.1.8 Využití technického a programového vybavení v procesu generování klíčů

6.1.8.1 CA

Pro generování klíče CA je využit hardwarový kryptografický modul.

6.1.8.2 Jádro PKI

Klíče pro uživatele certifikačních autorit jsou generovány na čipové kartě resp. v zabezpečeném souboru.

6.1.8.3 Klient

Klíče pro klienty jsou generovány v souboru typu PKCS#11 na ČK.

6.2 Ochrana soukromých klíčů

6.2.1 Kryptografické moduly

SC KB používá pro generování a uchování soukromého klíče certifikačních autorit kryptografické moduly SureWare Keyper, které splňují standard FIPS 140 – 1, úroveň 4.
Pro jádro Infrastruktury veřejných klíčů Komerční banky jsou pro ochranu privátního klíče použity i čipové karty, které umožňují nejenom bezpečné uschování klíče, ale i generaci klíčů uvnitř karty.

6.2.2 Úschova soukromého klíče

Pouze záložní soukromý klíč certifikační autority je rozdělen na dvě části a uložen na dvě čipové karty. Obě karty jsou uloženy v zabezpečeném prostoru s řízeným fyzickým přístupem.
Logický přístup ke kartám je chráněn hesly, přičemž každý ze dvou členů týmu SC KB zná přístupové heslo pouze k jedné kartě.
Soukromý klíč klienta je uložen na ČK, nikdy neopustí tuto ČK.

6.2.3 Povinnost zpřístupnit soukromé klíče

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

6.2.4 Zálohování soukromých klíčů

Současně s vygenerováním páru klíčů certifikační autority je provedeno zálohování soukromého klíče. Klíč je při zálohování rozdělen do dvou čipových karet (viz. 6.2.2).
SC KB nezajišťuje zálohování soukromých klíčů klientů.

6.2.5 Archivace soukromých klíčů

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

6.2.6 Aktivace soukromého klíče

Soukromý klíč certifikační autority je aktivován pouze po dobu činnosti software CS. Aktivace klíče je podmíněna zadáním hesel k operačnímu systému, k software certifikační autority a k soukromému klíči, souběžným zadáváním prostřednictvím 2 osob.
Soukromý klíč klienta je aktivován pouze po dobu činnosti klientské aplikace, která ho využívá. Aktivace klíče je podmíněna zadáním hesel/PIN.

6.2.7 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.

6.2.8 Zrušení/smazání soukromých klíčů

V případě certifikační autority je nutno vynulovat kryptografický modul a inicializovat čipové karty se záložním klíčem. Pro ostatní prvky Infrastruktury veřejných klíčů Komerční banky se pouze inicializují čipové karty obsahující jejich soukromé klíče.
V případě jádra PKI smí deaktivaci uskutečnit pouze SCA (Superadmin CA) , ACA (Admin CA)I.
Zrušení privátního klíče klienta provede sám klient, zničením čipu a okamžitým zneplatněním certifikátu.

6.3 Další aspekty správy klíčů

6.3.1 Archivace certifikátů (veřejných klíčů)

Certifikáty (veřejné klíče) jsou archivovány v databázi CS po dobu minimálně 10 let. Tato databáze je archivována i po ukončení činnosti CS tak, aby podmínka lhůty archivace byla splněna.

6.3.2 Doba platnosti klíčů

Doba platnosti klíče Certifikační autority je 10 let.
Doba platnosti klientského certifikátu a odpovídajícího soukromého klíče jsou 2 roky.

6.4 Aktivační data

Hesla opravňující k přístupu do souborů nebo čipových karet se soukromými klíči pro moduly Infrastruktura veřejných klíčů Komerční banky jsou uchovávána v písemné podobě, dle Interních bezpečnostních směrnic PKI KB.
Interval a pravidla pro povinnou změnu hesel a tvar hesel je specifikován v *Interních bezpečnostních směrnicích PKI KB*.

6.5 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.*

6.6 Opatření pro bezpečnost životního cyklu

Oddělení vývoje a rozvoje PKI v KB od produkčního prostředí:
- Pro vývoj a rozvoj systému PKI v KB je připraveno testovací a vývojové prostředí, které je fyzicky i logicky odděleno od produkčního prostředí.
- Přístup do tohoto prostředí má pouze Správce PKI, členové týmu aplikační podpory PKI a testovací specialisté.
- 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*.

6.7 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*.

6.8 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.

7 Profil certifikátu a CRL

7.1 Profil certifikátu

Certifikát vysokého stupně ověření totožnosti je osvědčení, které propojuje veřejný klíč s osobou klienta. Jde o osobní certifikát, který poskytuje vysokou záruku vazby mezi osobní totožností klienta a veřejným klíčem. Certifikát vydaný podle této CP je v souladu s normou ISO 9594-8 (X.509), verze 3.

7.1.1 Registrační proces

Registrace k certifikátu nejvyššího stupně se uskuteční na místních registračních místech (MRM) prostřednictvím operátorů místních registračních míst (OMRM).
Klient se dostaví na registrační místo KB, osobně prokáže na MRM svoji totožnost (viz 4.1, 4.2 a 4.3).

7.1.2 Tvar certifikátu

V certifikátu jsou uvedeny následující informace:
- verze certifikátu (verze 3)
  - **2**
- jméno, příjmení, popř. titul (atribut Common Name)
- datum narození ve tvaru RRRRMMDD (atribut Organizational Unit)
- bydliště – místo/obec (atribut Locality)
- adresa bydliště – ulice, číslo popisné (atribut Organizational Unit)
- e-mail adresa (rozšíření RFC822Mailbox)
- délka klíče
  - **1024**
- algoritmus
  - **RSA**
- období platnosti
  - **2 roky**
- účel použití certifikátu (rozšíření Key Usage)
  - **digitální podpis**
  - **šifrování**
  - **autentizaci**
- identifikace veřejného klíče DCS CA (rozšíření Authority Key ID)
  - **160-tibitový hash veřejného klíče certifikační autority**
  - **DN certifikační autority + seriové číslo certifikátu**
- identifikace veřejného klíče subjektu certifikace (rozšíření Subject Key ID)
  - **160-tibitový hash veřejného klíče subjektu certifikátu**
- objektový identifikátor bezpečnostní politiky (rozšíření Policy OID)
  - **1.3.154.45317054.131.1.25.0.2**
- místo, odkud lze stáhnout tuto Certifikační politiku (kvalifikátor rozšíření Policy OID)
  - **www.mojebanka.cz**
- identifikátor zákazníka - identifikátor klienta (generické rozšíření, OID)
  - **1.3.0154.45317054.1.4.0**
  - parametr = číselná hodnota

7.1.3 Použitelnost certifikátu

(viz též 1.4) Certifikát slouží pro digitální podpis, šifrování dat a autentizaci.
Certifikát zajišťuje vysokou úroveň ověření osobní totožnosti a proto může být použit v aplikacích, které uskutečňují bankovní transakce odpovídající úrovně a zajišťuje bankovní transakce prostřednictvím digitálního podpisu. Lze jej využít při elektronickém nebo obchodním styku s Komerční bankou, a.s.

7.2 Profil CRL

CS 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.

7.2.1 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 DCS 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 DCS CA (Authority Key ID)
    - **160-tibitový hash veřejného klíče DCS SA**
- 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

8 Specifikace správy

8.1 Specifikace procedur změn a činností

a) SC PKI 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 a procesů KB.
b) Chyby, změny, nebo předpokládané změny těchto dokumentů jsou hlášeny kontaktním osobám, či částem uvedených v části 1.5 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.

8.2 Zveřejnění a politika oznámení změn

8.2.1 Údaje nepublikované úmyslně v této CP

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

8.2.2 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.

8.3 Schvalovací procedury CP

SC PKI je odpovědná za přípravu dokumentů a schválení dokumentů.