PKI v České spořitelně, a.s.

Certifikační politika pro zaměstnance ČS

Certifikát pro šifrování

Historie změn

Datum	vydání	status	autor
27. 10. 2010	v0.1	Draft	Marek Hejhal
28.10.2010	V1.0	revize za ČS	Lukáš Lorenc

OBSAH

1. Úvod

1.1 Přehled

Interní certifikační autorita České spořitelny (dále „CSCAINT“) je neveřejná dvojúrovňová hierarchická struktura certifikačních autorit vytvořená a provozovaná pro potřeby zaměstnanců České spořitelny a.s. (dále „ČS“).

Předmětem tohoto dokumentu je definovat certifikační politiku (dále „CP“) k vydávání certifikátů pro šifrování pro zaměstnance ČS. CP popisuje registraci, ověření totožnosti, uplatnění certifikátů a nezbytné postupy, které je zapotřebí uplatňovat v zájmu dodržení přijatých bezpečnostních standardů ČS. Součástí dokumentu je také vymezení rozsahu odpovědnosti zúčastněných stran.

Certifikační politika je v souladu s Certifikační prováděcí směrnicí (dále „CPS“) pro interní větev PKI České spořitelny. Jestliže Správa PKI vydá certifikát podle této CP, poskytuje záruku, že certifikát (veřejný klíč žadatele) je spojen s osobou držitele certifikátu - zaměstnancem ČS a totožnost zaměstnance byla ověřena dle postupů uvedených v kap. 3.2.

Certifikát vystaven podle této CP je osobní certifikát, který poskytuje vysokou záruku vazby mezi osobní totožností zaměstnance ČS a veřejným klíčem. Certifikát v maximální míře zaručuje správnou autentizaci.

Důležité upozornění pro účastníky registračního a certifikačního procesu, kterým má metodika sloužit: Před prvním použitím certifikátů s vysokým stupněm ověření totožnosti je zaměstnanec ČS povinen se prokazatelně seznámit s touto CP a související CPS.

1.2 Název a jednoznačné určení dokumentu

Název dokumentu: Certifikační politika pro zaměstnance ČS – Certifikát pro šifrování

Certifikační politika definována tímto dokumentem nese jednoznačný identifikátor 1.3.0154.45244782.5607.2.2. Tento identifikátor musí být uveden v každém certifikátu vydaném podle této politiky.

CP je v souladu s dokumenty uvedenými v kapitole 9.14.

1.3 Participující subjekty

1.3.1 Certifikační autority (dále „CA“)

Kořenová CA (dále „CAIROOT“) je organizační útvar v rámci systému PKI ČS. Tento útvar vydává a spravuje certifikáty *Certifikačních autorit* v rámci této PKI. Za určitých podmínek přesně definovaných v kapitole 4.9.1 příslušné CP je *Kořenová CA* oprávněna odmítnout vydání certifikátu Certifikační autority. Pouze *Kořenová CA* je oprávněna odvolat nebo pozastavit platnost certifikátu *Certifikační autority* na základě žádosti o odvolání. CAIROOT je organizačně začleněna do úseku bezpečnosti IT/IS České spořitelny.

Vydávající podřízená *Certifikační autorita* (dále „CAIOFF“) je útvar zajišťující vydávání a správu certifikátů koncových držitelů podle této CP na základě žádostí ověřených *Registrační autoritou*. CAIOFF je organizačně začleněna do úseku bezpečnosti IT/IS České spořitelny. Za podmínek přesně definovaných v kapitole 4.9.1 této CP je CA oprávněna odmítnout vydání certifikátu. Certifikát *Registrační autority* a koncového držitele certifikátu je oprávněna odvolat nebo pozastavit platnost na základě jejich žádosti pouze CA.

Certifikační autority jsou zaregistrovány do systému PKI ČS a účty *PKI administrátorů* jsou spravovány *správcem bezpečnosti a správou produkčního forestu Windows ČS*.

1.3.2 Registrační autority (dále „RA“)

Registrační autorita zajišťuje ověřování žádostí o certifikáty a totožnost žadatelů. Operátor RA využívá ke své činnosti primárně aplikaci IRM.

Proces ověření totožnosti žadatele je částečně automatizován. Je svázán s příjmacím procesem zaměstnance, jehož výsledkem je vytvoření účtu uživatele v příslušné doméně Active directory (dále „AD“). Registrační aplikace ověřuje totožnost uživatele při prvotní žádosti o certifikát na základě přihlášení do AD.

1.3.3 Držitelé certifikátů

Koncovými držiteli certifikátů vydávaných podle této CP mohou být pracovníci ČS nebo externí spolupracovníci ČS (dále souhrnně „zaměstnanci“) s přiděleným jednoznačným identifikátorem OIČ a uživatelským účtem v produkčním forestu AD (csin.cz).

1.3.4 Spoléhající se strany

Spoléhajícími stranami jsou fyzické či technické entity, které verifikují podpis koncového certifikátu vydaného podle této CP na základě hierarchie CA až k CAIROOT. Jmenovitě se jedná zejména o:

- Servery a stanice produkčního forestu csin.cz
- Zaměstnanci ČS

1.3.5 Jiné participující subjekty

Personální oddělení – je součástí procesu ověření identity budoucího držitele certifikátu, přiděluje jednoznačné identifikační zaměstnanecké ID na základě něhož se generuje zaváděcí list. Na základě zaváděcího listu je uživateli vytvořen účet v produkčním forestu domény České spořitelny.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Privátní klíč spojený s certifikátem vydávaným podle této CP je určen držitelům certifikátů k šifrování dat zejména v těchto aplikacích:

- šifrování elektronické pošty – např. MS Outlook
- šifrování dat v elektronických distribučních kanálech – prostřednictvím WEB prohlížeče nebo vlastní aplikací ČS

Certifikát vydaný podle této CP je třetími stranami využíván k šifrování zpráv pro držitele certifikátu.

1.4.2 Omezení použití certifikátu

Za nepovolené je považováno takové využití certifikátu/privátního klíče, které není definováno v kapitole 1.4.1. Certifikát/privátní klíč nesmí být využit pro podpis/autentizaci.

1.5 Správa politiky

1.5.1 Organizace spravující CP

Česká spořitelna, a.s., úsek bezpečnosti IS/IT, Řídící komise PKI ČS

Antala Staška 32/1292

Praha 4

1.5.2 Kontaktní osoba organizace spravující CP

Lorenc Lukáš/ Markovič Vilém / Hašek Milan (6510)

Správa PKI České spořitelny

Antala Staška 32/1292

Praha 4, 140 00

1.6 Přehled použitých pojmů a zkratek

Akronym	Plný význam	Vysvětlení
AD	Active Directory	Adresářová služba na jejímž základě je vybudována a funguje enterprise architektura systémů firmy Microsoft.
AIA	Authority Information Access	Extenze certifikátu, která specifikuje umístění CA certifikátu autority, která předmětný certifikát vydala
CA	Certifikační autorita	V úzkém smyslu jde o komponentu, která vlastní privátní klíč pro podpis koncových certifikátů nebo certifikátů podřízených CA a vydává CRL. Certifikační autority jsou vzájemně propojeny vztahy důvěry a to buď hierarchicky nebo explicitně pomocí kroscertifikace.
CAIOFF	CAIOFF	Vydávající certifikační autorita interní větve PKI v ČS, je podřízena CAIROOT a vydává certifkáty dle této CP
CAIROOT	CAIROOT	Kořenová certifikační autorita interní větve PKI v ČS

Certifikát		Datová struktura obsahující veřejný klíč spolu s údaji o držiteli klíče, vydavateli klíče, dovoleném způsbou užití a další relevantní informace definované příslušející CP.
CDP	CRL Distribution Poin	Extenze certifikátu, která specifikuje, kde se nachází aktuální CRL pro daný certifikát
CP	Certifikační politika	Dokument v rámci dokumentační základny CA, který definuje parametry certifikátu vydávaného podle této CP, vymezuje způsob užití certifikátu a definuje životní cyklus certifikátu. Uplatňování CP dále upravuje CPS.
CPS	Certifikační prováděcí směrnice	Definuje způsob aplikace pravidel předepsaných v CP. Určuje požadavky na všechny prvky PKI vstupující do registračního a certifikačního procesu. CPS je vytvářena na základě doporučení v RFC3647.
CRL	Certification Revocation List	Seznam zneplatněných nebo pozastavených certifikátů, jejichž doba platnosti ještě nevypršela.
CSCAINT	Interní certifikační autorita ČS	Dvojúrovňová hierarchická struktura certifikačních autorit včetně podpůrných technologií sloužící k vydávání certifikátů pro zaměstnance a zařízení v rámci ČS
ČS	Česká spořitelna a.s.	
Držitel certifikátu	Držitel certifikátu	Fyzická nebo právnická osoba jež má výhradní právo nakládat se soukromým klíčem, který souvisí s předmětným certifikátem
Žadatel o certifikát	Žadatel o certifikát	Fyzická nebo právnická osoba, žádající o vydání certifikátu. Žadatel o certifikát se stává držitelem certifikátu v okamžiku potvrzení převzetí předmětného certifikátu. Podmínky přijetí certifikátu vymezuje kapitola 4.4.1.
EP	Elektronický podpis	Údaje v elektronické podobě připojené k datové zprávě sloužící k ověření integrity této datové zprávy
IRM	Integrovaný Registrační Modul	Webová aplikace pro operátory RA, zde jsou dostupné všechny funkce, které operátor RA potřebuje ke své činnosti
OCSP	Online Certificate Status Protocol	Protokol pro online ověření platnosti certifikátu dle RFC 2560
OIČ	Osobní identifikační číslo	Jednoznačný identifikátor zaměstnance přiděluje CEN 1631, oddělení personální informační systémy na základě navázání pracovního poměru (přihlašovací ID do AD odpovídá hodnotě OIČ) V případě /externího zaměstnance je identifikátor (číslo EXT) přidělováno odd. CEN 6511, Správa uživatelů na základě e-mailové žádosti zástupce externího pracovníka, který je zaměstnancem ČS, a.s. přihlašovací ID do AD odpovídá hodnotě OIČ)
OID	Object Identifier	Číselná identifikace objektu v rámci jednotné klasifikace objektů podle ISO/ITU
Párová data		Dvojice klíčů privátní a veřejný pro které platí, že

		zpráva zašifrovaná jedním z klíčů lze dešifrovat pouze druhým z této dvojice
PIN	Personal Identification Number	Číselný kód, který chrání přístup na čipovou kartu.
Privátní klíč		Datová struktura pro vytváření elektronického podpisu nebo šifrování datových zpráv.
Veřejný klíč		Datová struktura pro verifikaci nebo dešifrování datových zpráv.
WS	Web Services	Technologie vzdáleného volání funkcí v distribuovaných systémech založená na protokolu pro vzdálená volání SOAP a jazyku pro popis poskytovaných služeb WSDL.

2. Odpovědnost za zveřejňování a úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

ČS zřizuje a udržuje interní úložiště informací a dokumentace formou interního webu (intranetu) interního adresáře (AD)

2.2 Zveřejňování informací a dokumentace

Interní certifikační autorita České spořitelny je neveřejná dvojúrovňová hierarchie certifikačních autorit vytvořená a provozovaná pro potřeby zaměstnanců České spořitelny a.s. (dále „ČS“), dceřiných společností a externích spolupracovníků. Informace jsou proto dostupné zaměstnancům, zařízením a třetím stranám primárně v rámci intranetu ČS.

Základní adresy, kde jsou dostupné CP, CPS a ostatní veřejné dokumenty v elektronické podobě:

- http://www.csas.cz/cp

Základní adresy, kde jsou dostupné CP, CPS a ostatní veřejné dokumenty v tištěné podobě:

- Lorenc Lukáš/ Markovič Vilém
- CEN 6512, odd.standardy a monitoring bezp. IS/IT
  Česká spořitelna, a.s.
  Antala Staška 32/1292
  Praha 4, 140 00

Certifikáty vydávané podlé této CP jsou publikovány do interní AD k objektu koncového uživatele podle jednoznačného identifikátoru, který je obsahem subject Dname vydaného certifikátu (více o mapování do AD viz. 3.1). Dostupnost takto publikovaných certifikátů je odvozena od nastavení přístupových práv do AD.

CA certifikáty jsou dostupné elektronicky na těchto adresách:

ldap:///CN=CAIOFF,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=csin,DC=cz?cACertificate?base?objectClass=certificationAuthority
http://www.csas.cz/caioff.cer

ldap:///CN=CAIROOT,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=csin,DC=cz?cACertificate?base?objectClass=certificationAuthority
http://www.csas.cz/cairoot.cer

Informace o zneplatněných certifikátech (CRL) je dostupná elektronicky na těchto adresách:

ldap:///CN=CAIOFF,CN=CAIOFF,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=csin,DC=cz?certificateRevocationList?base?objectClass=cRLDistributionPoint
http://www.csas.cz/caioff.crl
http://pkiwwwi1.csin.cz/caioff.crl
http://pkiwwwi2.csin.cz/caioff.crl

URL=ldap:///CN=CAIROOT,CN=CAIROOT,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=csin,DC=cz?certificateRevocationList?base?objectClass=cRLDistributionPoint
http://www.csas.cz/cairoot.crl
http://pkiwwwi1.csin.cz/cairoot.crl
http://pkiwwwi2.csin.cz/cairoot.crl

2.3 Periodicita zveřejňování informací

ČS zveřejňuje veškeré jednotlivé typy informací podle následujícího schématu:

- CPS – před vytvořením CSCAINT a po každé změně v procesech touto CPS popsaných
- CP – před vydáním prvního certifikátu podle této CP
- CRL – aktualizace probíhá v pravidelných intervalech nejméně jednou za 4 hodiny.
- Certifikát – je publikován do AD ihned po vydání, z důvodu distribuované topologie AD je avšak ve všech uzlech dostupný nejpozději po uplynutí replikační latence.
- Ostatní informace – není předepsána žádná periodicita, avšak platí, že aktuálně zveřejňené informace musí odrážet reálný stav systému CSCAINT.

2.4 Řízení přístupu k jednotlivým typům úložišť

Přístup ke konkrétním typům úložišť je definován interními směrnicemi ČS. Přístup s právem zápisu mají přidělen správci odpovídajících dat. Veřejné údaje jsou přístupné pro čtení bez omezení. Pro dokumenty s omezeným přístupem je implementováno řízení přístupu.

3. Identifikace a autentizace

Tato kapitola specifikuje požadavky na verifikaci identity držitele certifikátu a způsob zanesení verifikovaných informací do vydávaného certifikátu a souvisejících dokumentů.

3.1 Pojmenování

3.1.1 Typy jmen

Položky žádosti o certifikát:

Atribut	Kódování	Význam	Typ hodnoty	Příklad	Doložení
C	PrintableString	Země	konstanta	CZ	nedokládá se
O	BMPString	Organizace	konstanta	Česká spořitelna a.s.	nedokládá se
OU	PrintableString	OIČ	povinný	CENXXXXX (zaměstnanec) EXTXXXXX (externí pracovník)	generuje personální oddělení, dokládá se zaváděcím listem
RFC822MailBox	OctetString	email adresa žadatele	volitelný	XXXXX@csas.cz	čestné prohlášení
CN	PrintableString BMPString	Příjmení a jméno	povinný	Jan Novák	dokládá se OP nebo pasem

3.1.2 Požadavek na významovost jmen

Jména použitá v rámci PKI ČS musí být srozumitelná všem, kdo se v rámci PKI ČS spoléhají na vydávané certifikáty. Tento požadavek přitom nesmí být v konfliktu s jakýmkoliv právním předpisem včetně právních předpisů upravujících ochranu informací.

- V případě žadatele - zaměstnance, údaje v Rejstříku certifikátů ČS či v certifikátu budou porovnány s údaji uloženými v adresářových službách interní sítě. V nich uvedená data jsou směrodatná a použijí se jako vstupní údaje certifikátu.
- Použití nepravého jména či pseudonymu je zakázáno.
- Všechny další uváděné informace by měly být shodné s mezinárodně akceptovanými standardy a pravidly.

3.1.3 Anonymita a používání pseudonymu

Vydávaný certifikát obsahuje celé jméno držitele a identifikátor OIČ, uvádění pseudonymu ani anonymizace držitele není povolena.

3.1.4 Pravidla pro interpretaci různých forem jmen

Jména a další osobní údaje se do vydávaného certifikátu přenášejí ve formě, jak jsou uvedeny v AD, kam se přenáší ze zaváděcího listu uživatele při zakládání uživatelského účtu.

3.1.5 Jedinečnost jmen

Jednoznačnost je zajištěna uvedením OIČ v subjektu vydávaného certifikátu, které je z podstaty jeho vzniku jednoznačné v rámci ČS.

3.2 Počáteční ověření identity

3.2.1 Ověřování souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů

Generování klíčového páru provádí žadatel.

Vlastnictví soukromého klíče odpovídajícího veřejnému klíči, který bude generovaný certifikát obsahovat, se prokazuje předložením datové zprávy (žádost o vydání certifikátu), elektronicky podepsané tímto soukromým klíčem ve formátu PKCS#10. Systém nebo pracovník, vyřizující předmětnou žádost, kontroluje pravost tím, že pomocí veřejného klíče uvedeného v žádosti o certifikát, ověří platnost elektronického podpisu na této žádosti.

Pokud je ověření platnosti elektronického podpisu negativní, není žádost přijata a řízení k vydání certifikátu je zastaveno.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Není relevantní pro tuto CP

3.2.3 Ověřování identity fyzické osoby

Ověření totožnosti probíhá elektronicky. Žadatel prokáže svou totožnost vlastnictvím podpisového certifikátu na jehož základě žádá o šifrovací certifikát. Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě

3.2.4 Ověřování specifických práv

Není relevantní ve vztahu k této CP.

3.2.5 Kritéria pro interoperabilitu

Případná spolupráce s jinými poskytovateli certifikačních služeb je založen na písemné smlouvě společnosti ČS a.s. s konkrétním poskytovatelem certifikačních služeb.

3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat v certifikátu

3.3.1 Identifikace a autentizace při rutinní výměně párových dat

Žádost se elektronicky podepisuje privátním klíčem náležícím k platnému certifikátu žadatele pro který je výměna párových dat prováděna.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

Výměna párových dat po zneplatnění není podporována a musí být postupováno jako v případě žádosti o prvotní certifikát.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Identifikace a autentizace závisí na způsobu podání žádosti:

- prostřednictvím aplikace Správce Certifikátů – aplikace kontroluje elektronicky platnost zneplatňovaného certifikátu a navíc vyžaduje zadání revokačního hesla, které si žadatel zvolil v procesu žádosti o certifikát (v aplikaci Správce certifikátů).
- elektronicky zasláním emailu na adresu CEN 6510, Správa PKI, ve smyslu předpisu 5603_01_10R , Vyžádání/vrácení podpisové/šifrovací čipové karty

4. Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Certifikáty podle této CP jsou vydávány pouze pracovníkům ČS nebo externí spolupracovníkům ČS s přiděleným jednoznačným identifikátorem OIČ a uživatelským účtem v produkčním forestu AD (csin.cz).

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Registrační proces včetně odpovědností jsou uvedeny v následujících kapitolách.

4.2 Zpracování žádosti o certifikát

Žádost o certifikát se podává elektornicky prostřednictvím aplikace Správce certifikátů nebo pomocí administrátorské aplikace IRM.

4.2.1 Identifikace a autentizace

Při vstupu do aplikace Správce certifikátů je uživatel identifikován a autentizován pomocí přihlášení do domény Microsoft Windows.

Přijetí nebo zamítnutí žádosti o certifikát

Před odesláním je uživateli zobrazena informační obrazovka s údaji, které byly staženy z AD a budou ve výsledném certifikátu. Žadatel je povinen správnost zobrazených údajů potvrdit. V případě, že údaje nesouhlasí, ukončí žadatel generování žádosti a informuje pracovníka odd. CEN 6510, Sprava PKI prostřednictvím e-mailu, případně telefonicky.

Pokud všechny údaje souhlasí, potvrdí žadatel tuto skutečnost odesláním předmětné žádosti na registrační rozhraní CAIOFF, kde proběhne kontrola přijaté žádosti v rozsahu popsaném v bodě 3.2.1.

Žádost o certifikát je zpracovávána automaticky a jsou prováděny následující kontoroly:

- formální kontrola formátu žádosti (PKCS#10)
- ověření důkazu vlastnictví privátního klíče – ověření podpisu PKCS#10
- existence uživatele v AD a shoda údaů v žádosti a údajů v AD

V případě, že všechny kontroly skončí úspěšně, je žádost postoupena k dalšímu zpracování. V případě selhání některé z kontrol je žádost zamítnuta a uživatel je informován v rámci aplikace Správce certifikátů o neúspěšnosti pokusu o vygenerování certifikátu

4.2.2 Doba zpracování žádosti o certifikát

Není stanoven žádný limit pro zpracování žádosti. Obvyklá doba od přijetí žádosti do vydání certifikátu jsou jednotky minut.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V průběhu procesu vydávání certifikátu probíhají na jednotlivých komponentách CAIOFF nezbytné validace tak, aby byla zajištěna integrita a minimalizováno riziko kompromitace. Základní kontroly před vydáním certifiíkátu jsou:

- kontrola duplicity klíče
- kontrola kryptografických parametrů žádosti

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující nebo označující osobě

Žadatel je o vydání certifikátu informován v rámci aplikace Správce certifikátů. Předpokládá se, že žadatel se bude aktivně snažit dokončit proces žádosti o vydání nového certifikátu.

4.4 Převzetí vydaného certifikátu

Řešeno interním předpisem 5603_01_10R

4.4.1 Úkony spojené s převzetím certifikátu

Žadatel si v aplikaci Správce certifikátů vyzvedne certifikát, který je aplikací uložen na čipovou kartu žadatele, kam byl před odesláním žádosti vygenerován soukromý klíč.

Žadatel je povinnen:

- překontrolovat údaje v certifikátu uvedené před prvním použitím tohoto certifikátu, nejpozději však do 7 dní od vyzvednutí certifikátu
- nejsou-li údaje v certifikátu správné, je žadatel povinen neprodleně informovat o této skutečnosti pracovníka odd. CEN 6510, Správa PKI, který následně provede jeho zneplatnění v souladu s postupy pro zneplatnění uvedenými v kap. 4.9 této CP.

Pokud žadatel ve výše uvedené lhůtě nerozporuje obsah certifikátu nebo pokud jej poprvé použije, má se za to, že potvrdil převzetí certifikátu. Po potvrzení převzetí certifikátu je možné jej začít používat pro účely uvedené v bodě 1.4 této CP.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Vydané certifikáty jsou publikovány do AD neprodleně po jejich vydání certifikační autoritou.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Není podporováno.

4.5 Použití párových dat a certifikátu

4.5.1 Použití dat pro vytváření elektronických podpisů držitelem certifikátu nebo podepisující osobou

Párová data musí být generována na čipové kartě schváleného pro použití v interním PKI ČS (5603_01_10R ,Vyžádání/vrácení podpisové/šifrovací čipové karty). Přístup k soukromému klíči uloženému na čipové kartě je chráněn pomocí PIN. Soukromý klíč se generuje mimo čipovou kartu a je uložen v centrálním registru šifrovacích klíčů pro případnou obnovu. Následně je ještě v průběhu registrace nahrán na čipovou kartu uživatele.

Držitelé certifikátů jsou povinni:

- Dodržovat tuto CP
- Používat certifikát k účelu touto CP vymezeným
- V případě změny údajů uvedených v certifikátu o této skutečnosti neprodleně informovat poskytovatele certifikační služby a ve vzájemném souladu podniknout kroky k nápravě. Preferuje se forma vydání následného certifikátu.

Podepisující osoba je povinna:

- od okamžiku vytvoření párových dat je žadatel osobně a výhradně zodpovědný za uložení a a neporušení celistvosti svého soukromého klíče
- chránit PIN pro přístup k soukromému klíči před vyzrazením, zejména je zakázáno PIN sdělovat třetí osobě, mít PIN uložen v blízkosti čipové karty nebo v prostoru pracoviště
- zacházet se soukromým klíčem s náležitou péčí tak, aby nemohlo dojít k jeho zneužití, zejména je zakázáno ponechávat čipovou kartu bez dozoru a to i při krátkodobém opuštění pracoviště.
- uvědomit ČS o tom, že hrozí nebezpečí zneužití soukromého klíče držitele a podniknout kroky vedoucí k zablokování platnosti vydaného certifikátu

4.5.2 Použití dat pro ověřování elektronických podpisů spoléhající se stranou

Spoléhající se strany jsou povinny:

- užívat certifikáty vydané dle této CP v souladu s touto CP a s platnými legislativními normami
- provádět veškeré úkony potřebné k ověření, že elektronický podpis je platný a certifikát nebyl zneplatněn
- kontrolovat elektronický podpis, důvěryhodnost a platnost všech CA certifikátů v hierarchii až po kořenový CA certifikát

4.6 Obnovení certifikátu

Obnovením certifikátu se míní vydání nového certifikátu držiteli beze změny párových dat a dalších údajů v certifikátu.

4.6.1 Podmínky pro obnovení certifikátu

Obnovení certifikátu není pro certifikáty vydané podle této CP za žádných podmínek povoleno.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Nejsou.

4.6.3 Zpracování požadavku na obnovení certifikátu

Požadavek je v každé situaci odmítnut.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu

Není relevantní pro tuto CP.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Není relevantní pro tuto CP.

4.6.6 Zveřejňování vydaného obnoveného certifikátu

Není relevantní pro tuto CP.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

Není relevantní pro tuto CP.

4.7 Výměna veřejného klíče v certifikátu

Výměnou veřejného klíče se myslí generování nových párových dat a vydání certifikátu s nově vygenerovaným veřejným klíčem beze změny ostatních údajů v certifikátu.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Žadatel musí vytvořit novou žádost, která splňuje tyto požadavky:

- žádost je elektronicky podepsaná privátním klíčem, který souvisí s již vydaným platným certifikátem žadatele
- platnost certifikátu žadatele, kterým se ověřuje žádost musí skončit nejpozději 30 dní od data doručení předmětné žádosti
- veřejný klíč v žádosti se liší od veřejného klíče certifikátu, kterým je žádost podepsána

4.7.2 Subjekty oprávněné požadovat výměnu veřejného klíče v certifikátu

O výměnu je oprávněn požádat pouze držitel platného certifikátu, který je nadále veden v AD jako platný uživatel.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

V procesu zpracování je kontrolováno, zda údaje v žádosti jsou shodné s údaji v platném certifikátu žadatele. Pokud jsou nalezeny rozdíly v jiných položkách, než je hodnota veřejného klíče, je žádost zamítnuta.

4.7.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu

Žadatel není přímo informován. Byl-li certifikát vydán, je tento neprodleně publikován do AD.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Žadatel postupuje stejně jako v případě převzetí nového certifikátu, viz. kap. 4.4.1.

4.7.6 Zveřejňování vydaných certifikátů s vyměněným veřejným klíčem

Vydané certifikáty jsou publikovány do AD neprodleně po jejich vydání certifikační autoritou.

4.7.7 Oznámení o vydání certifikátu s vyměněným veřejným klíčem jiným subjektům

Není podporováno.

4.8 Změna údajů v certifikátu

Změnou údajů v certifikátu se míní modifikace údajů v certifikátu při zachování současného veřejného klíče.

4.8.1 Podmínky pro změnu údajů v certifikátu

V případě potřeby změnit údaje v certifikátu musí žadatel nejprve standardní cestou zažádat o změnu těchto údajů v AD a po provedení této změny podnikne stejné kroky jako pro vydání nového certifikátu viz. 4.2.1.

4.8.2 Subjekty oprávněné požádat o změnu údajů v certifikátu

Změna údajů v certifikátu podle této CP je umožněna pouze pracovníkům ČS nebo externí spolupracovníkům ČS s přiděleným jednoznačným identifikátorem OIČ a uživatelským účtem v produkčním forestu AD (csin.cz).

4.8.3 Zpracování požadavků na změnu údajů v certifikátu

Údaje jsou zpracovány stejným způsobem jako v případě vydání nového certifikátu viz. 4.2.2 a 4.3.1.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji

Viz. 4.3.2

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz 4.4

4.8.6 Zveřejňování vydaného certifikátu se změněnými údaji

Viz 4.4.2

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz. 4.4.3

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Podmínky pro zneplatnění certifikátu

Certifikát může být zneplatněn pouze na základě následujících okolností:

- držitel certifikátu nebo jím oprávněná osoba požádá o jeho zneplatnění
- na základě sdělení držitele se věcný obsah certifikátu stane neplatným
- na základě zjištění ČS se věcný obsah certifikátu stane neplatným
- je důvodné podezření, že došlo ke kompromitaci soukromého klíče
- došlo ke kompromitaci soukromého klíče CAIOFF nebo CAIROOT
- držitel certifikátu přestal být oprávněným držitelem certifikátu ve smyslu definice v kapitole 1.3.3.
- držitel certifikátu zemřel

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat:

- držitel certifikátu nebo jím zmocněná osoba
- nadřízená osoba vlastníka certifikátu
- pracovník správy PKI

4.9.3 Požadavek na zneplatnění certifikátu

V případě, že o zneplatnění žádá držitel, musí být požadavek na zneplatnění předán předán způsobem popsaným v kapitole 3.4.

V případě, že se zneplatnění uskutečňuje na žádost nadřízené osoby, případně zmocněného zaměstnance ČS, musí být žádost doručena elektronicky podepsaným emailem na komunikační adresu CEN 6510, Správa PKI

Elektronická žádost o zneplatnění musí obsahovat formulaci: *„Žádám o zneplatnění certifikátu k uživatelskému účtu....“*. Zneplatnění smí provést pouze pracovník oddělení 6511, Správa uživatelů na základě e – mailové žádosti (viz 5603_01_10R Vyžádání/vrácení podpisové/šifrovací čipové karty), který musí provést:

kontrolu identity žadatele

- kontrolu oprávněnosti požadavku

Lhůta na provedení zneplatnění je stanovena na 24 hodin. Skutečná doba zneplatnění certifikátů ovšem probíhá v řádu několika minut od obdržení platné e-mailové žádosti na adresu CEN 6510, Správa PKI.

Doba odkladu požadavku na zneplatnění certifikátu:

Služba se neposkytuje.

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

Lhůta je na 24 hodin. Lhůta se počítá od okamžiku doručení žádosti pověrenému pracovišti a je zajištěna v režimu 7*24. Za realizaci požadavku se považuje publikace nového CRL obsahujícího číslo zneplatňovaného certifikátu ve všech úložišťích definovaných extenzí CDP certifikátu.

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

Spoléhající se strany jsou povinny používat CRL a to z některého z úložišť specifikovaného v CDP extenzi kontrolovaného certifikátu.

4.9.6 Periodicita vydávání seznamu zneplatněných certifikátů

CRL je vydáváno v pravidelných intervalech viz. kap. 2.3.

4.9.7 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Maximální prodlení mezi přijetím požadavku na zneplatnění certifikátu a zveřejněním nového CRL může činit nejvýše 4 hodiny.

4.9.8 Možnost ověřování statutu certifikátu on-line (OCSP)

Služba OCSP je poskytována formou servisního rozhraní WS na níže přiložených adresách vybraným systémům v rámci inetrního prostředí ČS:

http://ASPSFNLB.csin.cz:8831/OCSP/servlet/ResponderServlet
http://BUDSCNLB.csin.cz:8831/OCSP/servlet/ResponderServlet

4.9.9 Požadavky při ověřování statutu certifikátu on-line

Spoléhající se systém/služba je povinna provést ověření integrity odpovědi OCSP serveru formou verifikace elektronického podpisu a stavu certifikátu OCSP serveru proti aktuálnímu CRL pro tento certifikát.

4.9.10 Jiné způsoby oznamování zneplatnění certifikátu

Nejsou definovány.

4.9.11 Případné odlišnosti postupu zneplatnění v případě kompromitace soukromého klíče

Nejsou definovány.

4.9.12 Podmínky pro pozastavení platnosti certifikátu

Certifikát může být pozastaven pouze na základě žádosti držitele certifikátu v těchto případech:

- držitel certifikátu nechce po přechodnou dobu certifikát využívat
- držitel certifikátu má podezření na kompromitaci svého soukromého klíče, ale toto podezření se ještě nestalo důvodným

4.9.13 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

O pozastavení platnosti certifikátu může požádat výhradně držitel certifikátu prostřednictvím k tomu určené aplikace *Správce certifikátů*.

4.9.14 Zpracování požadavku na pozastavení platnosti certifikátu

Žádost o pozastavení certifikátu je zpracována automaticky v nejkratším možném termínu, obvykle v řádu jednotek minut.

4.9.15 Omezení doby pozastavení platnosti certifikátu

Ukončení pozastavení certifikátu může být provedeno pouze pracovníkem oddělení 6511, Správa uživatelů na základě – mailové žádosti (viz 5603_01_10R Vyžádání/vrácení podpisové/šifrovací čipové karty).

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

Služby ověřování statutu certifikátu jsou poskytovány elektronicky těmito službami:

- zveřejňování CRL na adresách definovaných extenzí CDP, viz. kap. 2.2
- zveřejňování CA certifikátů na adresách definovaných extenzí AIA, viz. kap. 2.2
- služba OCSP formou servisního rozhraní pro definované systémy ČS na adrese viz. kap. 4.9.8.
- služba OCSP pro ověření stavu vlastního certifikátu držitele jako funkce v aplikaci Správce certifikátů

- služba OCSP pro ověření stavu certifikátů pro operátory RA jako funkce v aplikaci IRM

4.10.2 Dostupnost služeb

ČS, a.s. zajišťuje dostupnost služeb uvedených v kapitole 4.10.1 v tomto režimu:

- dostupnost CRL distribučních bodů – 24x7
- zveřejňování CA certifikátů při vydání certifikátu– 24x7 (certifikáty uloženy v Active Directory)
- dostupnost úložiště zveřejněných certifikátů AD – 24x7
- dostupnost služby OCSP formou servisního rozhraní – 24x7
- dostupnost služby OCSP pro ověření stavu vlastního certifikátu držitele – 24x7
- dostupnost služby OCSP pro ověření stavu certifikátů pro operátory RA – 24x7

4.10.3 Další charakteristiky služeb statutu certifikátu

Služby OCSP pro držitele certifikátu a operátory RA jsou implementovány jako funkce v aplikacích Správce certifkátů (pro držitele) a IRM (pro operátory). Ověření stavu certifikátu OCSP serveru jak je vyžadováno v kap. 4.9.9 této CP provádí za držitele/RA operátora případě webový server, který aplikace Správce certifikátů/IRM hostuje.

4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující osobu

Ukončení služeb mezi držitelem a ČS, a.s. končí ve chvíli, kdy skončila platnost certifikátu držitele, aniž by držitel předtím nepožádal o vydání následného certifikátu.

4.12 Úschova soukromého klíče u důvěryhodné třetí strany a jejich obnova

Služba není poskytována.

5. Management, provozní a fyzická bezpečnost

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Umístění se zvolí tak, aby bylo možno zajistit ochranu před přístupem nepovolaných osob, ochranu před živelnými pohromami a nehodami v inženýrských sítích.

5.1.2 Fyzický přístup

Objekt musí být nepřetržitě střežen fyzickou ostrahou, přístup do budov, jakož i do prostor CA se zajistí elektronickým bezpečnostním systémem. Prostory CA jsou kontrolovány navíc kamerovým systémem. Přístup do prostor CA je kontrolovaný a omezený na určené zaměstnance České spořitelny. Pro ostatní zaměstnance České spořitelny a cizí osoby je přístup povolen pouze určeným správcem. Tito návštěvníci se zde mohou pohybovat pouze v doprovodu oprávněných zaměstnanců České spořitelny.

5.1.3 Elektřina a klimatizace

V místnostech musí být dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu a vlhkost vyhovující potřebám zde umístěných zařízení. Přívod elektrické energie se zajistní pomocí kombinace UPS a diesel agregátu.

5.1.4 Vliv vody

V prostorách CA nesmí být veden žádný rozvod vody. Budova nesmí být v zátopové oblasti.

5.1.5 Protipožární opatření a ochrana

Vstupní dveře se opatří protipožární vložkou. Místnosti jsou vybaveny požárními hlásiči a samozhášovacím zařízením.

5.1.6 Ukládání médií

Všechna datová media jsou uložena v prostorách se stejným stupněm fyzického zabezpečení jaký má prostor primárního pracoviště. Prostory jsou vybaveny zařízením pro zajištění stálé teploty a vlhkosti a poskytují ochranu proti magnetickému rušení.

5.1.7 Nakládání s odpady

Veškerý papírový kancelářský odpad je před opuštěním pracovišť CA znehodnocen skartováním.

5.1.8 Zálohy mimo budovu

Zařízení certifikační autority musí být geograficky distribuováno do dvou lokalit se stejným stupněm zabezpečení.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Všichni zaměstnanci, kteří mají přístup nebo kontrolu nad kryptografickými operacemi prováděnými v rámci CA nebo RA, jsou zařazeni do důvěryhodných rolí odpovídajících prováděným činnostem. V rámci správy systému CA je důsledně využíváno principu oddělení zodpovědnosti (separation of duties). Zařazování pracovníků do důvěryhodných rolí se řídí interními předpisy ČS.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Počty zaměstnanců na jednotlivých pozicích odpovídají potřebné míře oddělení zodpovědnosti a jsou detailně specifikovány v CPS a související dokumentaci.

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům jsou přiděleny prostředky pro řádnou autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné. Důvěryhodné role související se správou klíčů jsou autentizovány dvoufaktorově na bázi znalosti a držení (čipová karta + PIN + PUK).

5.2.4 Role vyžadující rozdělení povinností

V systému nelze slučovat následující činnosti:

- bezpečnostní dohled systému s žádnou další výkonnou rolí v systému
- použití privátního klíče CA je podmíněno systémem 4 očí

Detailně jsou role a rozdělení pravomocí popsány v CPS a interních směrnicích ČS.

5.3 Personální bezpečnost

Důvěryhodnost a spolehlivost certifikační autority a celé infrastruktury veřejných klíčů je mimo jiné závislá i na kvalitě jejího personálu. Kvalita personálu je dále vnímána jako souhrn důvěryhodnosti a kompetentnosti. ČS se řídí takovými pravidly pro řízení zaměstnanců, jejichž dodržování zajistí potřebnou míru důvěryhodnosti a kompetence pracovníků *Správy PKI* a řádný výkon jejich činností.

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Kandidát musí splňovat podmínky stanovené personálním oddělením ČS,a.s. v rámci interních předpisů banky.

5.3.2 Posouzení spolehlivosti osob

Personální odbor a úsek bezpečnosti ČS provádějí počáteční prověření všech kandidátů ucházejících se o práci v citlivých pozicích. Toto prověření pokrývá osobní a kvalifikační oblast.

Zaměstnanci personálního odboru podle možností ověří předané reference u předchozího zaměstnavatele, nejlépe s využitím jiných zdrojů než těch, které předložil kandidát.

Personální odbor a úsek bezpečnosti ČS provádějí periodické prověření všech zaměstnanců již činných v citlivých pozicích.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Úsek lidské zdroje ČS zajišťuje pro všechny zaměstnance potřebnou úroveň počátečních školení, aby tito byli schopni správně a efektivně zastávat své pozice. Požadavky pro každou roli jsou stanoveny v interních směrnicích pro provoz PKI ČS.

5.3.4 Požadavky a periodicita školení

Úsek lidské zdroje ČS zajišťuje pro všechny zaměstnance potřebnou úroveň pokračovacích školení, aby tito byli schopni správně a efektivně zastávat své pozice.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Nepředepisuje se.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Všichni zaměstnanci podepisují Prohlášení o mlčenlivosti a jednají podle něj a podle dalších interních norem.

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

ČS zajišťuje některé činnosti smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se například o externí zhotovitele programového aplikačního vybavení, dodavatele HW, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími předpisy pro provoz CA. V případě porušení těchto povinností jsou vyžadovány smluvní pokuty, případně je s nimi ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

Všichni zaměstnanci obdrží informaci o existenci a závaznosti bezpečnostní dokumentace. Všichni zaměstnanci mají přístup k bezpečnostní politice ČS, k dokumentu CPS a bezpečnostní dokumentaci svého trvalého pracoviště nebo pobočky.

5.4 Auditní záznamy (logy)

5.4.1 Typy zaznamenávaných událostí

Do elektronického auditního logu jsou zaznamenávány následující typy událostí:

- ***systémové události***. Záznam je vytvořený operačním systémem k zaznamenávání každého úkonu uskutečněného na počítačích, kde jsou nainstalovány procesy *Certifikační autority* nebo *Registrační autority*:
    - instalaci nového software;
    - zapnutí, vypnutí;

  - úkony vykonávané jakoukoliv aplikací;
  - úkony vykonávané jakýmkoliv uživatelem.
- **PKI události**. Záznam je vytvořený systémy Infrastruktury veřejných klíčů České spořitelny
  - záznamy o vydaných certifikátech včetně jejich obsahu;
  - změny v architektuře PKI;
  - údaje o certifikačních politikách;
  - žádosti o certifikáty spolu se záznamy o totožnosti žádajícího, typu žádosti, údajem, zda byla žádost schválena nebo ne, a případně důvod, proč nebyla schválena;
  - záznamy o zneplatnění/pozastavení platnosti certifikátů;
  - soubory s CRL.

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

5.4.2 Periodicita zpracování záznamů

Informace jsou zaznamenávány on-line a záznamy jsou pravidelně analyzovány minimálně jednou denně *Správcem bezpečnosti* tak, aby byly detekovány jakékoliv případné odchylky od běžných činností nebo úmyslné poškozování.

5.4.3 Doba uchování auditních záznamů

Lhůta uchovávání záznamů pro audit je v souladu s kapitolou 5.5.2 . Doba uložení dat pro data publikovaná v rejstříku a data z provozních systémů PKI činí 10 let.

5.4.4 Ochrana auditních záznamů

Elektronické záznamy pro potřeby auditu vytvářené systémy *Infrastruktury veřejných klíčů České spořitelny* obsahují časový údaj o vzniku záznamu a mohou být zabezpečeny před změnou digitálním podpisem.

Soubory obsahující údaje pro audit jsou fyzicky zabezpečeny, stejně jako ostatní části PKI.

Přístup k těmto souborům mají určení členové *Správy PKI* a členové nezávislého týmu auditorů České spořitelny. V průběhu externího auditu PKI ČS zajistí *Řídící komise* přístup i pro externí auditory.

5.4.5 Postupy pro zálohování auditních záznamů

Existují dvě hlavní zálohovací procedury:

- každodenní zálohování pomocí zálohovacího robota;
- kontinuální replikační systém do záložního pracoviště (užívající vysoce zabezpečenou síť) umístěném v bezpečném prostoru se stejnou úrovní zabezpečení jako hlavní místo.

Archivace je popsána v kapitole 5.5..

5.4.6 Systém shromažďování auditních záznamů

Veškeré citlivé auditní záznamy jsou zálohovány do databáze a pravidelných intervalech zálohované. Ostatní bezpečnostní logy jsou kontrolovány v režimu 7*24 odd. CEN 6512, odd.standardy a monitoring bezp. IS/IT

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není standardně informován, v rámci šetření incidentu ale může být vyzván oprávněnou osobou k podání vysvětlení.

5.5 Uchovávání informací a dokumentace

5.5.1 Typy informací a dokumentace, které se uchovávají

Správa PKI v České spořitelně archivuje zejména:

- informace pro účely auditu (popsané v předešlé kapitole);
- výsledky auditu;
- veškerou výměnu elektronických zpráv mezi držitelem a prvky *Infrastruktury veřejných klíčů České spořitelny;*
- písemné dokumenty používané v rámci *Správy PKI*:
    - smluvní dokumenty;
    - písemné žádosti o zneplatnění/pozastavení platnosti certifikátu;
    - předpisovou základnu infrastruktury PKI (současné a předchozí verze bezpečnostních politik, CP a CPS).

5.5.2 Doba uchování informací a dokumentace

Všechny dokumenty v archivech budou uchovávány po dobu nejméně 10 let od vypršení jednotlivých certifikátů nebo ukončení platnosti dokumentů.

5.5.3 Ochrana úložiště informací a dokumentace

Ochrana je zajištěna následujícím souborem opatření:

- Archivy v elektronické formě jsou uloženy v databázi / souborech na nepřepisovatelném záznamovém mediu s dlouhou životností. Všechna data vytvářená systémy *Infrastruktury veřejných klíčů České spořitelny* jsou zabezpečena před změnou elektronickým podpisem.
- Záznamové soubory jsou fyzicky zabezpečeny, stejně jako ostatní části PKI ČS.

- Přístup k těmto souborům mají pouze určení členové *Správy PKI* a členové nezávislého týmu auditorů České spořitelny.
- Při archivaci elektronických záznamů jsou elektronické spoje zabezpečeny v souladu s doporučeními PKIX vydanými organizací IETF.
- Bezpečný transport písemných dokumentů zajišťuje *Správa PKI*.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Zálohovací postupy jsou upraveny interní CPS a další relevantní interní dokumentací ČS.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Nejsou stanoveny.

5.5.6 Systém shromažďování uchovávaných informací a dokumentace

dle standardu ČS, a.s.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Správa PKI ověřuje neporušenost a celistvost archivu jednou ročně. Přístup k archivu mají pouze určení členové *Správy PKI* a členové nezávislého týmu auditorů České spořitelny podle procedur popsaných v interní dokumentaci.

5.6 Výměna veřejného klíče v certifkátu poskytovatele

Postup generování nového klíče CA je definován zvláštní CP pro CA certifkáty. Mezi starým a novým klíčem musí být překrytí minimálně tak dlouhé, jak dlouhá je platnost certifikátů touto CA vydávaných. Všechny nově vyžádané certifikáty jsou podepisovány novým klíčem.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

Konkrétní postup je stanoven relevantní CPS a příslušnou interní prováděcí směrnicí ČS.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Je ošetřeno opatřeními dle kapitol 5.1.8, 5.5 a konkrétní postup je stanoven relevantní CPS a příslušnou interní prováděcí směrnicí ČS.

5.7.3 Postup při kompromitaci soukromého klíče poskytovatele

Je-li zneplatněn klíč CA:

- dojde k aktualizaci a uveřejnění CRL
- CA je odstavena trvale mimo provoz
- dochází k novému generování klíčů CA

- *Správa PKI* rozhodne, zda bude server CA reinstalován nebo ihned spuštěn
- držitelé certifikátů jsou *Správou PKI* upozorněni, že došlo k výměně klíče

Je-li zneplatněn klíč RA, PKI administrátora nebo Registračního pracovníka:

- dojde k aktualizaci a uveřejnění CRL
- daný operátor je odstaven mimo provoz
- dojde k nové generaci klíčů
- *správa PKI* rozhodne, zda bude server RA reinstalován nebo ihned spuštěn
- držitelé certifikátů jsou *Správou PKI* upozorněni, že došlo k výměně klíče

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje ČS v souladu s interními havarijními směrnicemi, provoz CA se může přerušit jen na dobu nezbytně nutnou k migraci postižených subsystémů do záložní lokality.

5.8 Ukončení činnosti CA nebo RA

Činnost PKI ČS je svázána s provozem interních služeb ČS, které využívají certifikáty. Provoz PKI ČS může být proto ukončen buď současně s ukončením provozu všech zabezpečených služeb interních informačních systémů nebo při ekvivalentní funkční náhradě interní PKI jinou infrastrukturou poskytující stejné bezpečnostní funkce. Držitelé certifikátů budou o změnách uvědomeni prostřednictvím informačních kanálů těchto služeb.

Správa PKI přijme opatření pro zajištění archivovaných záznamů po dobu předepsanou v kapitole 5.5.2.

6. Technická bezpečnost

V této kapitole jsou definovány bezpečnostní požadavky a metriky pro hodnocení kvality certifikační autority, která vydává certifikáty podle této CP. Jde zejména o hodnocení párových dat, aktivačních dat, podmínek použití a souboru opatření vedoucích k zajištění potřebného stupně ochrany klíčového materiálu certifikační autority.

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Procesu generování klíčů pro *Certifikační autoritu* České spořitelny musí být přítomni:

- *Hlavní správce PKI* nebo jeho zástupce;
- *PKI auditor*;
- *člen Řídící komise.*

Klíče jsou generovány přímo v zabezpečeném kryptografickém modulu. Konkrétní postup generování je popsán v relevantní interní technické dokumentaci ČS. O procesu generování těchto klíčů je vytvořen písemný protokol obsahující nejméně:

- seznam přítomných pracovníků s uvedením: jména, příjmení, titulu, OIČ
- datum a čas zahájení a ukončení generace párových dat s přesností na minuty
- místo, kde ke generaci párových dat došlo
- popis zařízení, na kterém byla generace prováděna včetně seriového čísla zařízení k jeho jednoznačné identifikaci
- kompletní výpis certifikátu CA
- datum vyhotovení protokolu
- vlastnoruční podpisy všech pracovníků, kteří generaci párových dat prováděli

Ihned po té je vytvořena záložní kopie soukromého klíče CA a uložena na zabezpečeném místě. *PKI auditor* vyhotoví záznam o generování klíčů, v němž potvrdí, že veškeré použité nástroje a postupy odpovídaly dokumentům CP a CPS, schváleným postupům a produktovým doporučením výrobců.

Párová data držitele koncového certifikátu jsou generována výhradně na čipové kartě schválené pro použití v prostředí interního PKI ČS.

6.1.2 Předání soukromého klíče podepisující osobě

Protože proces generování probíhá na zařízení a v prostředí, které je v čase generování pod výhradní kontrolou žadatele, není tento proces definován.

6.1.3 Předání veřejného klíče poskytovateli certifkačních služeb

Žádost o certifikát certifikační autority je přijímána pouze elektronicky přes aplikace Správce certifikátů nebo IRM.

6.1.4 Poskytování veřejného klíče spoléhajícím se stranám

6.1.5 Veřejný klíč je ve formě certifikátu poskytován buď osobně na pracovišti RA nebo elektronicky z AD. Délky párových dat

ČS používá pro CA certifikáty asymetrický algoritmus RSAs délkou klíče (soukromý i veřejný) 2048 bitů.

Certifikáty vydávány pro klíče RSA délky minimálně 1024 bitů.

6.1.6 Generování parametrů veřejného klíče a kontrola jejich kvality

Minimální délka klíče koncového uživatele je 1024.

6.1.7 Omezení pro použití veřejného klíče

Veřejný klíč CA smí být použit pouze pro:

- ověření platnosti podpisu certifikátu vydaného touto CA
- ověření platnosti podpisu CRL vydaného touto CA

6.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů

Soukromý klíč CA vyžaduje nejvyšší stupeň zabezpečení a to jak z hlediska fyzické tak i technické. Detailněji jsou mechanismy ochrany specifikovány v související bezpečnostní dokumentaci a CPS. Požadavky na fyzickou ochranu jsou uvedeny v kapitole 5.1. Tato kapitola specifikuje požadavky na technické prostředky ochrany a nakládání s párovými daty CA.

6.2.1 Standardy a a podmínky používání kryptografických modulů

Párová data jsou generována výhradně na HW zařízení (HSM) splňujícího normu FIPS 140-2 level 3.

6.2.2 Sdílení tajemství

Soukromý klíč je z důvodu dostupnosti sdílen více HSM moduly stejného typu.

6.2.3 Úschova soukromého klíče

Služba úschovy privátní klíče není poskytována.

6.2.4 Zálohování soukromého klíče

Zálohování soukromého klíče se provádí formou jeho rozdělení na části a uložení na více čipových karet. Ke složení soukromého klíče jsou potřeba alespoň 2 různé karty.

6.2.5 Uchování soukromého klíče

Karty s částmi soukromého klíče CA jsou svěřeny členům Správy PKI, kteří znají přístupové heslo pouze ke své kartě. Dvě karty jsou uchovány jako záložní v zabezpečeném prostoru s řízeným přístupem a heslo k těmto kartám je na jiném místě v trezoru v zapečetěné obálce.

6.2.6 Transfer soukromého klíče do kryptografického modulu nebo z kryptografického modulu

K této operaci je nutná přítomnost dvou členů Správy PKI a auditora, který provede o celé operaci zápis. Transfer soukromého klíče do/z modulu je možný pouze pokud je existující HSM nahrazován novým zařízením (např. v případě HW poruchy) nebo pokud byly vygenerovány nová párová data, která je nutno zálohovat.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromý klíč je v kryptografickém modulu uložen v chráněné operační oblasti, veškeré operace jsou prováděny v této oblasti a soukromý klíč tuto oblast za žádných okolností neopustí v nechráněné podobě.

6.2.8 Postup při aktivaci soukromého klíče

Soukromý klíč CA je aktivován pouze po dobu činnosti software CA. Aktivace klíče je podmíněna zadáním hesel k operačnímu systému, k software CA, PINem karty CA operátora, která autorizuje přístup k soukromému klíči CA v HSM, souběžným zadáváním prostřednictvím pověřené osoby v roli CA operátora. Přístup k CA je přísně řízen.

6.2.9 Postup při deaktivaci soukromého klíče

Soukromý klíč CA je deaktivován v těchto případech:

- kryptografický modul detekoval pokus o narušení bezpečnostních opatření
- výpadek napájení CA
- činnost software CA využívající privátní klíč je ukončena

6.2.10 Postup při zničení soukromého klíče

HSM modul, jehož klíč byl zničen musí být resetován a následně do něj může být soukromý klíč obnoven definovaným postupem ze záložních karet.

6.2.11 Hodnocení kryptografických modulů

FIPS 140-2 level 3

6.3 Další aspekty správy párových dat

6.3.1 Uchování veřejného klíče

Pro uchování veřejného klíče platí stejná pravidla jako pro ostatní informace s CA související, viz. kap. 5.5.2.

6.3.2 Maximální doba platnosti certifikátu vydaného podepisující osobě a párových dat

Maximální doba platnosti párových dat je dána zhodnocením aktuální odolnosti párových dat proti známým útokům na použitý algoritmus generování a ochrany těchto dat. Maximání doba platnosti certifikátu je stanovena touto CP na 1 rok.

6.4 Aktivační data

Aktivačními daty se rozumí PINy, hesla a kódy, která je třeba použít k aktivaci soukromého klíče CA.

6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou generována v procesu inicializace CA. Tato skutečnost je zaznamenána na protokolu o vytváření CA spolu s rozdělovníkem, kdo je držitelem jakých aktivačních dat.

6.4.2 Ochrana aktivačních dat

Každý vlastník je zodpovědný za ochranu aktivační dat, zejména je povinen:

- nesdělovat za žádných okolností aktivační data další osobě
- při zadávání aktivačních dat dbát na to, aby nebylo možno tato data odpozorovat
- pravidelně měnit hodnoty aktivačních dat podle daných interními předpisy ČS

6.4.3 Ostatní aspekty aktivačních dat

Nejsou.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Jsou definovány interními směrnicemi pro provoz PKI ČS a řídí se těmito principy:

- Přístup k operačnímu systému počítačů na kterých běží procesy a aplikace PKI ČS je chráněn čipovými kartami a veškeré operace jsou evidovány.
- Kritické systémy PKI ČS jsou umístěny ve fyzicky chráněném prostředí s řízeným přístupem.
- Na těchto počítačích jsou spuštěny nebo instalovány pouze programy související s provozem PKI ČS.
- Provoz systémů je monitorován a pravidelně auditován.
- Testovací a vývojové systémy jsou důsledně odděleny od produkčních systémů.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti je založeno na mezinárodních a národních standardech a je prováděno externí auditorskou společností pravidelných intervalech..

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací a best practice postupy pro vývoj software. Důsledně jsou dodržovány principy:

- oddělení vývojového, testovacího a produkčního prostředí
- implementace principu PDCA (Plan – Do – Check – Act)

6.6.2 Kontroly řízení bezpečnosti

Soulad se standardy je ověřován pravidelnými audity a kontrolami bezpečnostní shody.

6.6.3 Řízení bezpečnosti životního cyklu

Změnové řízení probíhá ve smyslu interního předpisu ČS 6102_02_01R, Řízení změn

6.7 Síťová bezpečnost

Zabezpečení sítí je detailně popsáno v interních směrnicích pro provoz PKI ČS. Při návrhu infrastruktury PKI ČS byl kladen maximální důraz na důkladné zabezpečení všech komponent:

- testovací a vývojové systémy jsou důsledně odděleny od produkčních systémů
- počítačové sítě PKI ČS jsou odděleny od běžné podnikové sítě pomocí interního firewallu
- provoz systémů je monitorován a pravidelně auditován
- kontroly a ověřování průchodnosti sítě jsou pravidelně prováděny prostřednictvím technických správců v rámci struktury České spořitelny

6.8 Časová razítka

Není relevantní.

7. Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

7.1 Profil certifikátu

Certifikáty jsou vydávány v souladu s doporučením ITU-T X.509 z června 1997 a RFC3280. Minimální délka klíče vydávaných certifikátů je 1024 bitů.

Základní položky koncového certifikátu:

Atribut	**Hodnota**
Version	verze 3
Serial Number	jedinečné číslo vydaného certifikátu v rámci CA
Signature	sha1withRSAEncryption
Issuer DN	CN = CAIOFF OU = Správa PKI O = Česká spořitelna a.s. C=CZ
Valid From	UTC čas začátku platnosti certifikátu, formát dle RFC 3280
Valid To	UTC čas konce platnosti certifikátu, formát dle RFC 3280
Subject DN	identifikace držitele certifikátu, viz. kap. 3.1.2
Subject Public Key	veřejný klíč držitele certifikátu, minimálně 1024 bitů
Signature	podpis vydávající CA

7.1.1 Číslo verze

Vydávané certifikáty odpovídají doporučení X.509 verze 3. Certifikační služby poskytované ČS nepodporují certifikáty jiného typu ani jiné verze certifikátu X.509.

7.1.2 Rozšiřující položky v certifikátu

Atribut	**Hodnota**
Subject Alternative Name	
RFC822 Name	automaticky doplněna emailová adresa držitele z objektu uživatele v AD
Principal Name	automaticky doplněna hodnota SAMAccountName z produkčního forestu AD
Certificate policies	
Policy Identifier	OID CP podle které byl certifikát vydán, viz. kap. 1.2
User Notice	See http://www.csin.cz/ or http://www.csas.cz/cp for details.
CPS URI	http://www.csin.cz/
Authority Information Access	
AIA1	ldap:///CN=CAIOFF,CN=AIA,CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=csin, DC=cz?cACertificate?base?objectClass=certificationAuthority

AIA2	http://www.csas.cz/caioff.cer
Enhanced Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)
Authority Key Identifier	
KeyID	hash veřejného klíče vydávající CA
Algoritmus	160-bit SHA-1
CRL Distribution Point	
CDP1	ldap:///CN=CAIOFF, CN=CAIOFF, CN=CDP, CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=csin, DC=cz?certificateRevocationList?base?objectClass=cRLDistributionPoint
CDP2	http://www.csas.cz/caioff.crl
Subject Key Identifier	
KeyID	hash veřejného klíče držitele
Algoritmus	160-bit SHA-1
Basic Constraints	
Subject Type	End Entity
Path Length Constraint	None
Key Usage	Key Encipherment Data Encipherment

7.1.3 OID algoritmů

Jsou používány pouze standardizovaná schémata dle RFC 2437 a RFC 3370.

7.1.4 Způsoby zápisu jmen a názvů

Viz. kapitola 3.1.

7.1.5 Omezení jmen a názvů

Pro položku Subject není žádné omezení s výjimkou omezení vyplývajících z kapitoly 3.1.2. O přípustnosti konkrétního obsahu jednotlivých atributů položky Subject rozhoduje s konečnou platností pracovník registrační autority, který provádí vyřizování požadavku na vydání certifikátu. V případě nesouhlasu může žadatel postupovat podle kapitoly 9.12.

7.1.6 OID certifikační politiky

Viz. kapitola 1.2.

7.1.7 Rozšiřující položka „Policy Constraints“

Viz. tabulka v kapitole 7.1.2

7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“

Neuvádí se.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz. tabulka v kapitole 7.1.2

7.2 Profil seznamu zneplatněných certifikátů

Položky CRL:

Atribut	Hodnota
Version	verze 2
Issuer DN	CN = CAIOFF OU = Správa PKI O = Česká spořitelna a.s. C=CZ
Effective date	UTC čas začátku platnosti CRL, formát dle RFC 3280
Next update	UTC čas nejpozdějšího vydání následujícího CRL, formát dle RFC 3280
Signature algorithm	sha1withRSAEncryption
CRL Number	pořadové číslo seznamu zneplatněných certifikátů
Revocation list	množina atributů popisující revokované certifikáty
Revocation number	seriové číslo revokovaného certifikátu
Revocation date	datum revokace
CRL Reason Code	důvod revokace

7.2.1 Číslo verze

Certifikační služby poskytované ČS využívají revokační seznamy (CRL) podle profilu PKIX (RFC 2459), který je implementací revokačního seznamu X.509 verze 2, definovaného specifikací ISO/IEC/ITU z roku 1997.

7.2.2 Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů

Nejsou.

7.3 Profil OCSP

Profil OCSP odpovídá požadavkům RFC 2560, základní položky certifikátu:

Atribut	Hodnota
Version	verze 3
Serial Number	jedinečné číslo vydaného certifikátu v rámci CA
Signature	sha1withRSAEncryption

Issuer DN	CN = CAIOFF OU = Správa PKI O = Česká spořitelna a.s. C=CZ
Valid From	UTC čas začátku platnosti certifikátu, formát dle RFC 3280
Valid To	UTC čas konce platnosti certifikátu, formát dle RFC 3280
Subject DN	CN = OCSP Server OU = Správa PKI O = Česká spořitelna a.s. C=CZ
Subject Public Key	veřejný klíč držitele certifikátu, minimálně 1024 bitů
Signature	podpis vydávající CA

7.3.1 Číslo verze

Vydávané certifikáty pro OCSP odpovídají doporučení X.509 verze 3. Certifikační služby poskytované ČS nepodporují certifikáty jiného typu ani jiné verze certifikátu X.509.

7.3.2 Rozšiřující položky OCSP

Atribut	**Hodnota**
Subject Alternative Name	
RFC822 Name	SpravaPKI@csas.cz
Certificate policies	
Policy Identifier	OID CP podle které byl certifikát OCSP serveru vydán, aktuální hodnota je 1.3.154.45244782.5607.2.7
User Notice	See http://www.csin.cz/
CPS URI	http://www.csin.cz/
Authority Information Access	
AIA1	ldap:///CN=CAIOFF,CN=AIA,CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=csin, DC=cz?cACertificate?base?objectClass=certificationAuthority
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)
Authority Key Identifier	
KeyID	hash veřejného klíče vydávající CA
Algoritmus	160-bit SHA-1
CRL Distribution Point	
CDP1	ldap:///CN=CAIOFF, CN=CAIOFF, CN=CDP, CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=csin, DC=cz?certificateRevocationList?base?objectClass=cRLDistributionPoint

Subject Key Identifier	
KeyID	hash veřejného klíče držitele
Algoritmus	160-bit SHA-1
Basic Constraints	
Subject Type	End Entity
Path Length Constraint	None
Key Usage	Digital Signature Non-Repudiation
id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5)	doporučený způsob verifikace OCSP certifikátu dle RFC 2650

8. Hodnocení shody a jiná hodnocení

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Koncepční komise je oprávněna vyžádat si pravidelné i nepravidelné inspekce a audity kterékoliv lokality *Infrastruktury veřejných klíčů České spořitelny*. Tyto audity budou provedeny za účelem ověření, zda správa certifikátů je v souladu s bezpečnostními postupy a procedurami, tak jak jsou definovány v této CPS, v příslušných CP a interních předpisech.

Z důvodu kontroly souladu praxe s ustanoveními současné CPS a příslušných CP projde *PKI ČS v pravidelných intervalech* interním auditem.

8.2 Identita a kvalifikace hodnotitele

Odpovědný auditor musí být kvalifikovaný auditor a musí znát principy PKI a procesy probíhající na úrovni CA a RA. Odpovědný auditor musí být držitelem platné certifikace CISA. Odpovědnému auditorovi mohou asistovat další specialisté bez auditorské kvalifikace.

8.3 Vztah hodnotitele k hodnocenému subjektu

Auditor musí být od revidované *Správy PKI* dostatečně organizačně oddělen, aby jeho hodnocení mohlo být skutečně nezávislé a nepředpojaté.

8.4 Hodnocené oblasti

Audit porovnává činnost *Správy PKI* v její psané podobě, jak ji definuje CPS a příslušné CP, s její reálnou podobou. Auditu musí být podrobeny veškeré aspekty činnosti *Správy PKI* tak, jak je specifikuje tato CP, související CPS a další prováděcí dokumentace.

8.5 Postup v případě zjištění nedostatků

Jakékoliv nesrovnalosti mezi činností *Správy PKI* a ustanoveními jejích CP a/nebo CPS musí být zaznamenány a bezodkladně oznámeny *Koncepční komisi.* Právě tato komise určí způsob nápravy, včetně stanovení lhůty, během níž musí být náprava uskutečněna.

Jakákoliv náprava může obsahovat pokyny k trvalému či dočasnému pozastavení činnosti gčásti *Infrastruktury veřejných klíčů České spořitelny*, přičemž je nutno – ještě před přijetím takového rozhodnutí – přihlédnout k několika faktorům, mezi něž se též řadí závažnost nesrovnalostí, vzniklých rizik a újmy, které takové narušení způsobí držitelům certifikátů.

Rozhodnutí o tom, jaké kroky budou podniknuty, se bude též odvíjet od způsobu předchozích reakcí na vzniklé problémy, od závažnosti odchylek a od doporučení auditora.

V závislosti na dané situaci, smluvních dokumentech, příslušných zákonech a předpisech je možné, že *Interní CA ČS* bude muset informovat všechny držitele certifikátů a oznámit jim, jaké kroky hodlá do budoucna podniknout.

8.6 Sdělování výsledků hodnocení

Závěrečné výsledky auditu budou předány *Koncepční komisi* a *Řídící komisi*. Závěrečným výsledkem se zde rozumí informace o veškerých odchylkách, jež by mohly mít vliv na důvěru závislé strany v certifikát, včetně adekvátního ohodnocení závažnosti, nikoliv však podrobné informace, které by šlo použít k napadení systému.

Shodně s ustanoveními odstavce 8.5, jakákoliv součást *Infrastruktury veřejných klíčů České spořitelny* (např.: CA, RA nebo rejstřík), u níž se prokáže, že nepracuje v souladu s touto CPS, musí být ihned, jakmile je audit hotov, informována. Kvůli maximálnímu snížení rizik, je nutno, aby byly pokyny k požadované nápravě určeny i oznámeny co možná nejdříve. O realizaci pokynů k dosažení nápravy je pak nutno zpravit přímo *Komcepční komisi*. Je možné, že pro potvrzení sjednané nápravy a její efektivnosti bude vyžádán zvláštní audit.

9. Ostatní obchodní a právní záležitosti

9.1 Poplatky

Vydávání certifikátu není zpoplatněno

9.2 Důvěrnost obchodních informací

9.2.1 Výčet důvěrných informací

Důvěrnými informacemi CA jsou :

- veškeré soukromé klíče, příslušné k veřejným klíčum CA
- ostatní kryptograficky podstatné informace sloužící k provozu CA
- vybrané obchodní informace
- veškeré informace a dokumentace s ohledem na poskytování certifikačních služeb
- veškeré osobní údaje

Chráněnými - zvláště důvěrnými obchodními informacemi jednotlivých RA jsou:

- Veškeré soukromé klíče, příslušné k veřejným klíčum RA
- ostatní kryptograficky podstatné informace sloužící k provozu RA
- veškeré informace a dokumentace s ohledem na poskytování certifikacních služeb
- veškeré osobní údaje

Za chráněné informace se rovněž považují veškeré další informace označené některým ze subjektů jako zvláště důverné. S chráněnými informacemi, bez ohledu na typ nosiče, je zacházeno tak, aby byla zajištěna jejich důvěrnost a integrita.

9.2.2 Informace mimo rámec důvěrných informací

Za důvěrné nejsou považovány:

- certifikáty
- seznamy CRL
- informace o zneplatnění a pozastavení platnosti
- certifikační politiky

9.2.3 Odpovědnost za ochranu důvěrných informací

Za ochranu důverných informací odpovídá organizační složka nebo osoba, která tyto informace spravuje. Každý pracovník, který přijde do styku s informacemi, které jsou předmětem utajení podle kapitoly 9.2.1 je nesmí poskytnout třetí straně.

Zaměstnanci ČS, spolupracující osoby nebo společnosti, které přicházejí do styku s citlivými informacemi jsou povinni zachovávat mlčenlivost o těchto informacích. Tato povinnost trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení kontrahovaných prací.

Jako organizačně právní opatření vedoucí k naplnění výše uvedených podmínek je se všemi subjekty podepisováno smluvní ujednání (formou dodatku k pracovní smlouvě, dohodě o zachování mlčenlivosti apod).

Ve smyslu i předpisu 5110_00_01R, Pravidla pro spisovou službu, skartaci a archiv (bod 5)

9.3 Ochrana osobních údajů

Ochrana osobních dat se řídí podle zákonů České republiky, hlavně Zákona č. 101/2000 Sb., o ochraně osobních údajů a Zákona č. 21/1992 Sb., o bankách.

9.4 Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek, certifikáty CA, párová data CA, procedury a směrnice jimiž je zajišťován provoz PKI České spořitelny jsou chráněny právy společnosti Česká spořitelna a.s. a představují její významné know-how.

9.5 Zastupování a záruky

9.5.1 Zastupování a záruky CA

ČS a.s. zaručuje prostřednictvím Správy PKI, jakožto výkonné organizační složky stran certifkační autority vymezené popisem v kapitole 1.3.1 že:

- Soukromý klíč CAIOFF užívaný k vydávání certifikátů v souladu s touto CP je užíván výhradně k podepisování certifikátů, seznamů CRL a ostatních adekvátních údajů souvisejících s vydáváním certifikátů
- Vydávané certifikáty splňují všechny náležitosti definované touto CP
- Sériové číslo certifikátu vydaného podle této CP je jedinečné v rámci všech certifkátů vydaných příslušnou certifkační autoritou

9.5.2 Zastupování a záruky RA

RA jak je definována v kapitole 1.3.2 přejímá závazek za správné vyřízení žádostí a ověření údajů podle všech pravidel této CP a příslušné CPS. RA dále přebírá odpovědnost za včasné předání žádostí o zneplatnění na pracoviště CA a včasné a úplné vyřizování připomínek a stížností klientů.

9.5.3 Zastupování a záruky držitele certifikátu

není relevantní v prostředí České spořitelny, a.s.

9.5.4 Zastupování a záruky spoléhajících se stran

není relevantní v prostředí České spořitelny, a.s.

9.5.5 Zastupování a záruky ostatních zúčastněných subjektů

není relevantní v prostředí České spořitelny, a.s.

9.6 Zřeknutí se záruk

není relevantní v prostředí České spořitelny, a.s.

9.7 Omezení odpovědnosti

není relevantní v prostředí České spořitelny, a.s.

9.8 Odpovědnost za škodu, náhrada škody

Řešeno interním předpisem č. 5603_01_10R

9.9 Doba platnosti, ukončení platnosti

9.9.1 Doba platnosti

Tento dokument zůstává v platnosti do skončení platnosti posledního certifikátu, který byl dle této CP vydán.

9.9.2 Ukončení platnosti

Ukončení platnosti této CP musí schválit Koncepční komise písemnou a nezpochybnitelnou formou. Tato skutečnost musí být zveřejněna na místech definovaných v kapitole 2.2.

9.10 Komunikace mezi zúčastněnými subjekty

Individuální komunikace může využívat všechny typy kontaktů, které si zúčastněné subjekty v rámci vzájemné autentizace vyměnili.

Veřejná komunikace probíhá kanály specifikovanými v kapitole 2.2.této CP.

9.11 Změny

9.11.1 Postup při změnách

Česká spořitelna je oprávněna v budoucnosti doplnit tuto CP o ustanovení, jejichž nutnost bude teprve zjištěna. Takové změny budou zveřejněny na místech definovaných v v kapitole 2.2 této CP. Případné změny nebudou mít zpětnou platnost.

Změny nemající materiální povahu vstoupí v platnost okamžikem řádného zveřejnění podle tohoto odstavce.

Změny mající materiální povahu vstoupí v platnost 15 dní po svém řádném zveřejnění, neoznámí-li Česká spořitelna před ukončením 15ti denní lhůty jejich stažení. V případě, že by zpožděným provedením navržené změny mohlo dojít k poškození PKI ČS, České spořitelny nebo její části, vstoupí změna v platnost okamžikem řádného uveřejnění.

Pokud žadatel o certifikát nestáhne svou žádost nebo držitel certifikátu neodvolá svůj certifikát před koncem výše zmíněné 15tidenní lhůty, má se za to, že s doplňky souhlasí.

Změny této CP musí schválit *Koncepční komise.*

9.11.2 Postup při oznamování změn

Řídí se pravidly a postupy uvedenými v kapitole 2.

9.11.3 Okolnosti, při kterých musí být změněn OID

V případě změny v této CP a jí příslušející CPS přidělí pověřená osoba nové verzi tohoto dokumentu číslo verze a nové OID.

9.12 Řešení sporů

není relevantní v prostředí České spořitelny, a.s.

9.13 Rozhodné právo

není relevantní v prostředí České spořitelny, a.s.

9.14 Shoda s právními předpisy

Tento dokument splňuje požadavky stanovené v RFC 3647, legislativě ČR a doporučeních orgánů EU, jmenovitě se jedná o dokumenty:

[1] ETSI TS 102 042 – Electronic Signatures and Infrastructures – Policy requirements for certification authorities issuing public key certificates

[2] RFC3647 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practicies Framework

[3] Vyhláška č. 378/2006 Sb. ze dne 19. července 2006 o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek