

SMĚRNICE

Věc:	Certifikační politika k certifikátu šifrování dat pro pracovníka PČS nebo externího uživatele PKI-PČS
Číselná řada:	6/2006
Ruší se interní předpis č.:	
Odborný garant:	Ing. Antonín Pacák
Datum vydání:	1. 2. 2006
Datum platnosti do:	31. 12. 2999
Aktualizovat:	ANO <u>NE</u> *
Účinnost:	1. 1. 2006
Vydávající útvar:	Oddělení vnitřní kontroly a bezpečnosti – bezpečnostní manažer
Počet stran:	12
Počet příloh:	0
Určeno:	členové představenstva zaměstnanci společnost externisté
Přístup pro exter:	<u>ANO</u> <u>NE</u> *
- úroveň přístupu	<u>EOZ</u> * <u>Výhradní agenti</u> <u>Agenti</u> <u>Makléři</u> <u>Asistenční služby</u>

* podtrhněte správnou variantu

Ing. František Mareš
člen představenstva
a náměstek generálního ředitele

OBSAH

1.	Úvod	3
1.1	Účel dokumentu	3
1.2	Definice pojmů a zkratk	3
2.	Použití certifikátu	5
2.1	Použitelnost certifikátu pro šifrování dat.	5
2.2	Vhodné aplikace	5
2.3	Způsob využití CRL	5
2.4	Ukončení platnosti certifikátů	5
3.	Metodika vydávání certifikátu žadatelům	6
3.1	Medium pro uložení certifikátů a klíčů	6
3.2	Registrační proces	6
3.3	Získání šifrovacího certifikátu	6
3.4	Délka klíče	6
3.5	Platnost certifikátu	6
3.6	Převzetí certifikátu žadatelem	6
3.7	Žádost o následný certifikát	6
3.8	Způsob ověřování platnosti	6
3.9	Závazky a povinnosti stran	7
4.	Obsah certifikátu	8
4.1	Ověřované údaje	8
4.2	Údaje a parametry uvedené v certifikátu	8
5.	Žádost o zneplatnění šifrovacího certifikátu	9
5.1	Podání žádosti o zneplatnění certifikátu	9
5.2	Ověření žádosti o zneplatnění / obnovení	9
5.3	Způsob předání požadavku o zneplatnění na CAPojCS	9
5.4	Způsob vyrozumění o provedení zneplatnění certifikátu	9
6.	Podání žádosti o vydání následných certifikátů	10
6.1	Podání žádosti	10
6.2	Ověření totožnosti	10
6.3	Vydání certifikátu	10
6.4	Vyzvednutí certifikátu	10
6.5	Potvrzení převzetí certifikátu	10
7.	Dostupnost seznamu zneplatněných certifikátů (CRL)	11
7.1	Způsob publikování	11
7.2	Zajištění dostupnosti	11
8.	Zajištění důvěrnosti	12

1. Úvod

1.1 Účel dokumentu

Předmětem tohoto dokumentu je definovat certifikační politiku k vydávání certifikátů pro šifrování dat pracovníka PČS nebo externího uživatele *PKI-PČS*. Certifikační politika popisuje registraci, ověření totožnosti, uplatnění certifikátů a nezbytné postupy, které je zapotřebí uplatňovat v zájmu dodržení přijatých bezpečnostních standardů PČS. Součástí dokumentu je také vymezení rozsahu odpovědnosti zúčastněných stran.

Certifikační politika je v souladu s Obecnou certifikační politikou a Certifikační prováděcí směrnicí (CPS) Pojišťovny České spořitelny. Jestliže Správa PKI vydá certifikát podle této certifikační politiky, poskytuje záruku, že certifikát (veřejný klíč žadatele) je spojen s osobou držitele certifikátu - pracovníka PČS nebo se smluvním externím uživatelem.

Jde o osobní certifikát, který poskytuje vysokou záruku vazby mezi osobní totožností a veřejným klíčem.

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

Před prvním použitím certifikátu je držitel povinen se seznámit s Obecnou certifikační politikou Pojišťovny České spořitelny a touto konkrétní certifikační politikou.

Obecná certifikační politika a konkrétní politiky pro jednotlivé typy certifikátů jsou publikovány na Intranetu Pojišťovny České spořitelny a na stránkách <http://www.pojistovnacs.cz/ca>.

1.2 Definice pojmů a zkratk

AD	Active directory
CA	Certifikační autorita
CAPOJCS	Certifikační autorita Pojišťovna České spořitelny, a.s.
Certifikát	Elektronické osvědčení vydané certifikační autoritou (datová zpráva), které propojuje data pro ověřování podpisů (veřejný kryptografický klíč) s podepisujícím subjektem (určitou osobou) a umožňuje ověřit jeho totožnost.
Certifikační autorita (CA)	Součást PKI, softwarová aplikace pracující na zvláštním zabezpečeném hardwaru, která transformuje elektronické požadavky na certifikát (request) předložené žadatelem či registrační autoritou do tvaru elektronického certifikátu podepsaného soukromým klíčem vydávající certifikační autority.
Certifikační prováděcí směrnice (CPS)	Interní směrnice Pojišťovny České spořitelny definující ve svých ustanoveních pravidla a postupy, které jsou uplatňovány na všechny prvky PKI vstupující do registračního a certifikačního procesu. Tvoří rámec pro uplatňování pravidel stanovených v Obecné certifikační politice Pojišťovny České spořitelny. CPS je vytvářena na základě doporučení dokumentu RFC 2527.
Certifikační politika (CP)	Dokument obsahující souhrn pravidel pro vydávání určitého typu certifikátů v systému PKI PČS, který současně stanoví jeho použitelnost pro určitou aplikaci nebo skupinu aplikací v souladu s požadavky na bezpečnost.
CRL	(Certificate Revocation List) seznam certifikátů, které byly zneplatněny
Držitel certifikátu	pracovník PČS nebo externí uživatel, kterému byl vydán CAPOJCS certifikát
Externí uživatel	fyzická nebo právnická osoba, která poskytuje PČS služby na základě obchodního smluvního vztahu, k jehož realizaci využívá i smluvně dojednaných služeb CAPOJCS.

Hlavní správce PKI	Pracovník odpovědný za základní parametry certifikační autority, za řízení a správu klíčů administrátorů a registračních pracovníků a celkový běh systému PKI
Infrastruktura	Technologické prvky a jejich propojení zajišťující služby spojené s vydáváním a správou certifikátů
Klient CA Kořenová CA (RCA)	pracovník Pojišťovny České spořitelny nebo externí uživatel. Jedinečná součást v rámci určité PKI, která vydává a spravuje certifikáty podřízených certifikačních autorit v rámci této PKI.
Obecná certifikační politika (CP)	Dokument obsahující obecná pravidla platná pro vydávání certifikátů všech typů v systému PKI PČS. Uplatňování obecné certifikační politiky dále upravuje certifikační prováděcí směrnice (CPS).
Párová data	Data pro vytváření elektronického podpisu spolu s odpovídajícími daty pro ověřování elektronického podpisu (odpovídající si soukromý a veřejný klíč). Klíčový pár vytvořený na principu asymetrické kryptografie, jedním klíčem se šifruje a druhým dešifruje.
PČS PKI PČS	Pojišťovna České spořitelny, a.s. Souhrnný pojem zahrnující technologii, soubor organizačních norem a personál zajišťující služby spojené s provozováním CAPojCS, to je s vydáváním a správou certifikátů pro zaměstnance Pojišťovny České spořitelny a externí smluvní partnery. Obsahuje infrastrukturu veřejných klíčů Pojišťovny České spořitelny a Správu PKI.
Podřízená CA	Součást určité PKI, zajišťující vydávání a správu certifikátů vydávajících certifikačních autorit. Podřízená CA může být současně i vydávající CA.
Požadavek na certifikát	formální, standardní dokument elektronického požadavku na certifikát vyplněný dle požadavků definovaných v příslušné politice
Pracovník PČS	fyzická osoba, která má pracovní smluvní vztah s PČS nebo pracuje v PČS na základě smlouvy uzavřené mezi jeho zaměstnavatelem (pracovní agenturou) a PČS.
Registrační autorita (RA)	Součást PKI, přijímá žádosti o certifikát, odpovídá za ověření totožnosti žadatelů o certifikát.
Soukromý klíč Správa PKI	Data pro vytváření elektronického podpisu Organizační struktura v rámci úseku IT zajišťující služby spojené s vydáváním a správou certifikátů
Subjekt	fyzická osoba, právnická osoba nebo softwarový modul s odpovědností konkrétní fyzické osoby
Veřejný klíč Vydávající CA Žadatel	Data pro ověřování elektronického podpisu Součást určité PKI, zajišťující vydávání a správu certifikátů. fyzická osoba nebo oprávněný jednatel právnické osoby podávající na RA žádost o službu (certifikát). Po vydání certifikátu se žadatel stává držitelem certifikátu.
Žádost o službu	formální dokument žádosti o některou ze služeb poskytovaných CAPojCS, např. žádost o zneplatnění certifikátu.

2. Použití certifikátu

2.1 Použitelnost certifikátu pro šifrování dat.

Tyto certifikáty zajišťují vysokou úroveň důvěrnosti komunikace mezi odesílatelem a adresátem, vlastníkem soukromého klíče. Totožnost adresáta je ověřena použitým certifikátem. Certifikát lze využít k šifrování zpráv při elektronickém obchodním styku (prostřednictvím elektronické pošty) v rámci Finanční skupiny České spořitelny nebo se smluvními partnery Pojišťovny České spořitelny, a.s.

2.2 Vhodné aplikace

K využití certifikátu, vydaného v souladu s certifikační politikou jsou doporučeny a otestované následující aplikace:

- šifrování elektronické pošty – MS Outlook;

2.3 Způsob využití CRL

- a) Závislé strany kontrolují *CRL* na vlastní zodpovědnost. To platí zejména o frekvenci vyhledávání *CRL*, jejíž volba je výhradně zodpovědností závislé strany.
- b) *CRL* lze kontrolovat s pomocí patřičného software (např. www prohlížeč) přístupem do Active directory či <http://klicenka.pojcs.cz/certsrv/> (pouze z interní sítě) nebo <http://www.pojistovnacs.cz/ca/capojcs.crl> (např. protokoly LDAP nebo HTML).
- c) Správa *PKI-PČS* doporučuje všem uživatelům konfigurovat použité aplikace tak, aby kontrolovaly platnost certifikátu s využitím všech příslušných *CRL* před každým použitím certifikátu.

2.4 Ukončení platnosti certifikátů

Certifikát pozbývá platnosti po vypršení doby platnosti uvedené v certifikátu. Doba platnosti je daná typem certifikátu a je specifikována v odpovídající *CP*.

Automaticky generované certifikáty jsou automaticky obnovovány.

3. Metodika vydávání certifikátu žadatelům

3.1 Medium pro uložení certifikátů a klíčů

Soukromé klíče a certifikáty vystavené podle certifikační politiky šifrování dat pro pracovníka PČS nebo externího uživatele *CAPOJCS*. jsou ukládány na čipových kartách odpovídajících standardu PKCS#11. Čipová karta je zaměstnanci přidělena v rámci přijímacího řízení. Při předávacím procesu je vyhotoven a podepsán žadatelem a oprávněným pracovníkem správy PKI protokol o vydání čipové karty a čtečky čipových karet. Čipová karta je opatřena sériovým číslem unikátním v rámci daného výrobce karet. Toto číslo je uvedeno v Protokolu o vydání čipové karty a čtečky čipových karet.

Přístup k soukromému klíči uloženému na čipové kartě je chráněn pomocí PIN (Personal Identification Number). Soukromý klíč si žadatel generuje přímo na čipové kartě a klíč nikdy neopustí kartu.

3.2 Registrační proces

Požadavek na certifikát podle této politiky je možno uskutečnit po registraci uživatele do AD, vydání certifikátu pro podpis a ověření klienta a na základě autentizace uživatele v AD.

3.3 Získání šifrovacího certifikátu

Požadavek na certifikát podle této politiky je možno uskutečnit po ověření uživatele v AD. Po prvním úspěšném přihlášení do systému se novému uživateli na základě jeho členství ve skupině *PKI_Autoenroll_Users* zobrazí v pravém dolním rohu obrazovky ikona Certificate Managera.

Po zasunutí čipové karty do čtečky, poklepání na ikonu Certificate Managera a následné volbě typu šablony *POJCS_User_Encrypt* a zadání přístupového PINu k čipové kartě, se vygeneruje do čipové karty klíčový pár a požadavek na certifikát, který přejímá údaje z AD. Tento požadavek je automaticky odeslán na *CAPOJCS* a po ověření na *CAPOJCS* se automaticky uloží šifrovací certifikát na čipovou kartu. Současně je na *CAPOJCA* bezpečně zálohován soukromý klíč pro případ obnovy při eventuální ztrátě čipové karty.

3.4 Délka klíče

Tento typ certifikátu má klíč o délce 1024 bitů a je určen k použití s algoritmem RSA.

3.5 Platnost certifikátu

Tento typ certifikátu má platnost 1 rok ode dne vydání.

3.6 Převzetí certifikátu žadatelem

Žadatel, který vyzvedl certifikát, je povinen přezkontrolovat údaje v něm uvedené před prvním použitím certifikátu, a to nejpozději do 7 dní od vyzvednutí certifikátu. Nejsou-li údaje v certifikátu správné, žadatel v nejkratší možné době informuje pověřeného pracovníka Správy PKI, který provede potřebné operace. Pokud žadatel ve výše uvedené lhůtě nespornuje 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 bodu [2.1](#) tohoto dokumentu.

3.7 Žádost o následný certifikát.

Žádost o následný certifikát se generuje na základě členství ve skupině *PKI_Autoenroll_Users* automaticky a proces získání certifikátu je obdobný procesu získání původního certifikátu

3.8 Způsob ověřování platnosti

Stav certifikátu se ověřuje vůči seznamu zneplatněných certifikátů. *CAPOJCS* vydává tento seznam každých 60 hodin. Je podepsán soukromým klíčem *CAPOJCS* a zveřejněn v adresářových službách na místě definovaném v rozšíření CRL Distribution Points (CDP) certifikátu koncového držitele. Tento

seznam je možné z adresářových služeb získat protokolem LDAP. Pro potřeby externích uživatelů je CRL publikován na <http://www.pojistovnacs.cz/ca/capoics.crl>, odkud je možno jej získat protokolem HTTP. Seznam zneplatněných certifikátů má určenou dobu platnosti, mimo niž informace v něm obsažené nemusí být platné. Pro určení stavu certifikátu je vždy zapotřebí použít aktuální seznam zneplatněných certifikátů. Všechny certifikáty, jejichž číslo je uvedeno na seznamu zneplatněných certifikátů jsou momentálně neplatné. Důvod ukončení platnosti a čas této změny jsou součástí záznamů v seznamu zneplatněných certifikátů. Všechny ostatní certifikáty, jejichž sériové číslo se nenachází na seznamu neplatných certifikátů, jsou platné.

3.9 Závazky a povinnosti stran

Práva, povinnosti, odpovědnost a závazky jsou definovány v Obecné certifikační politice.

4. Obsah certifikátu

4.1 Ověřované údaje

Při registraci žadatele podle této CP se ověřují následující informace:

- příjmení klienta a křestní jméno klienta (CN)
- osobní identifikátor používaný k přihlášení do AD (alternativní název předmětu)

4.2 Údaje a parametry uvedené v certifikátu

Vydaný certifikát obsahuje tyto informace:

- verze protokolu X509=V3
- unikátní číslo certifikátu
- typ podepisovacího algoritmu (sha1RSA)
- jméno podepisující certifikační autority (CN=CAPojCS,DC=pojcs,DC=cz)
- platnost od
- platnost do
- předmět (uživatel)
 - e-mail adresa žadatele E=(ID@pojstovnacs.cz
 - jméno uživatele (CN)
 - organizační jednotka (OU)
 - doména (DC=zam, DC=pojcs, DC=cz)
- Veřejný klíč
- použití klíče
 - zakódování klíče
 - zakódování dat
- identifikátor klíče předmětu (Subject Key ID)
- informace o šabloně certifikátu (Šablona=POJCS_User_Encrypt)
- identifikátor klíče certifikační autority (Authority Key ID)
- distribuční místa seznamu odvolaných certifikátů pro protokoly ldap i http
- údaje o certifikační politice
 - umístění CP (<http://www.pojstovnacs.cz/ca>)
- Použití rozšířeného klíče
 - zabezpečená pošta
- politiky aplikování
- alternativní název předmětu: ID@pojstovnacs.cz
- algoritmus miniatury (sha1)
- miniatura (otisk certifikátu)

Volitelně může certifikát obsahovat

- popisný název (zadaný při generaci, možno měnit)
- popis

5. Žádost o zneplatnění šifrovacího certifikátu

5.1 Podání žádosti o zneplatnění certifikátu

Držitel certifikátu může požádat *RA PKI PČS* o zneplatnění certifikátu.

5.2 Ověření žádosti o zneplatnění / obnovení

Žádost o pozastavení/změna údajů se ověřuje na základě elektronického podpisu držitele certifikátu nebo neelektronickými formami ověření, zpětné telefonické volání, osobní návštěva, dopis).

5.3 Způsob předání požadavku o zneplatnění na CAPojCS

Pracovník *RA PKI-PČS* po ověření žádosti tento požadavek předá dohodnutým způsobem dle interní směrnice na *CAPojCS*.

5.4 Způsob vyrozumění o provedení zneplatnění certifikátu

RA PKI-PČS informuje držitele o zneplatnění certifikátu mailem odeslaným bezprostředně po zadání požadavku o zneplatnění na *CAPojCS*.

6. Podání žádosti o vydání následných certifikátů

6.1 Podání žádosti

Držitel platného certifikátu může požádat o vydání následných certifikátů. Následné certifikáty se vydávají na základě autoenrollmentu, bez potřeby přímého ověření osobní totožnosti žadatele.

6.2 Ověření totožnosti

Žádost o následný certifikát je podepsána soukromým klíčem držitele platného podpisového certifikátu. Osobní totožnost žadatele je odvozena z vlastnictví soukromého podepisovacího klíče k již vystavenému platnému podpisovému certifikátu.

6.3 Vydání certifikátu

CA PojCS přijímá ověřené požadavky na certifikát a na jejich základě vydává elektronické certifikáty podepsané svým soukromým podepisovacím klíčem. Vydané certifikáty publikuje do AD.

6.4 Vyzvednutí certifikátu

Certifikát se automaticky uloží na čipovou kartu v procesu autoenrollmentu, kde byl před odesláním žádosti vygenerován soukromý podepisovací klíč žadatele. Předchozí šifrovací certifikát je na čipové kartě zachován.

6.5 Potvrzení převzetí certifikátu

Žadatel, který vyzvedl certifikát, je povinen přezkontrolovat údaje v něm uvedené před prvním použitím certifikátu, a to nejpozději do 7 dní od vyzvednutí certifikátu. Nejsou-li údaje v certifikátu správné, žadatel v nejkratší možné době informuje oprávněného pracovníka, který provede potřebné operace. Pokud žadatel ve výše uvedené lhůtě nespornuje 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 bodu [2.1](#) tohoto dokumentu.

7. Dostupnost seznamu zneplatněných certifikátů (CRL)

7.1 Způsob publikování

Seznam zneplatněných certifikátů (CRL) je publikován pravidelně každých 60 hodin. Seznam zneplatněných certifikátů je podepsán soukromým klíčem **CApójCS** a zveřejněn v adresářových službách na místě definovaném v rozšíření CRL Distribution Point (CDP) certifikátu vystaveného podle této politiky. Tento seznam je možné z adresářových služeb získat protokolem LDAP. Pro potřeby externích uživatelů je CRL publikován na <http://www.pojistovnacs.cz/ca/capojcs.crl>, odkud je možno jej získat protokolem HTTP

7.2 Zajištění dostupnosti

Seznamy zneplatněných certifikátů jsou dostupné nepřetržitě 24 hodin 7 dní v týdnu.

8. Zajištění důvěrnosti

Informace získané Správou PKI od žadatele v souvislosti s jeho žádostí o certifikát, jsou náležitě archivovány a budou použity pouze pro účely, pro které byly pořízeny. Použité postupy se budou řídit zákony České republiky.

Pro zajištění odpovídajícího chodu všech prvků infrastruktury veřejných klíčů v PČS je zajištěn pravidelný audit činnosti.

Podrobnosti jsou uvedeny v Obecné certifikační politice a Certifikační prováděcí směrnici.