

SMĚRNICE

Věc:	Obecná certifikační politika Pojišťovny České spořitelny a.s.
Číselná řada:	4/2006
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. 2. 2006
Vydávající útvar:	Oddělení vnitřní kontroly a bezpečnosti bezpečnostní manažer pro ICT
Počet stran:	9
Počet příloh:	0
Určeno:	členové představenstva zaměstnanci společnost externí partneři
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	Výchozí dokumenty..... 3
1.2	Definice pojmů a zkratk..... 3
2. OBECNÁ USTANOVENÍ	5
2.1	Závazky a povinnosti stran 5
2.2.	Typy certifikátů a metodika vydávání certifikátu žadatelům 6
2.3	Využitelnost certifikátů 6
2.4	Zneplatnění certifikátu..... 6
2.4.1	Podmínky zneplatnění 7
2.4.2	Kdo může žádat o zneplatnění platnosti..... 7
2.4.3	Postup při žádosti o zneplatnění certifikátu 7
2.4.4	Frekvence vydávání seznamu zneplatněných certifikátů (CRL) 8
2.4.5	Způsob využití CRL 8
2.4.6	Formy oznamování zneplatnění 8
2.5	Zajištění důvěrnosti 8
2.6	Proces schvalování základních materiálů..... 8
2.7	Zveřejňování a kontaktní informace..... 8

1. ÚVOD

Tento dokument představuje Certifikační politiku (dále též CP) platnou pro Certifikační autoritu Pojišťovny České spořitelny, a.s. (dále též CA PójCS).

Certifikační autorita Pojišťovny České spořitelny plní roli „Zprostředkujícího vydávajícího certifikačního úřadu“ ve struktuře certifikačních autorit České spořitelny a.s. Je podřízenou certifikační autoritou kořenové certifikační autority České spořitelny. Certifikáty vydané CA PójCS jsou uznávány uvnitř Finanční skupiny České spořitelny.

Tato certifikační politika se zabývá skutečnostmi, které se vztahují na CA PójCS, žadatele, klienty, uživatele, a smluvní partnery, a které souvisí s vydáváním certifikátů, jejich další správou, použitím, akceptací, a všemi aspekty souvisejícími s nakládáním s párovými daty (dvojicí klíčů).

1.1 Výchozí dokumenty

Certifikační politika odpovídá požadavkům stanoveným v RFC 2527 s přihlédnutím k doporučením orgánů EU a k legislativě ČR v daném oboru.

CP vychází zejména z následujících legislativních předpisů, norem, standardů a doporučení:

- Zákon č.227/2000Sb. v platném znění o elektronickém podpisu a o změně některých dalších zákonů.
- Certifikační politika a Prováděcí certifikační směrnice České spořitelny, a.s.
- RFC 2527 – Internet X 509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework (dále též RFC 2527)
- RFC 3280 – Internet X 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (dále též RFC 3280)

1.2 Definice pojmů a zkratk

CA	Certifikační autorita
CA PójCS	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.
Certifikát externího uživatele	Certifikát, jehož držitelem je externí uživatel CA PójCS
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	uživatel, který má párová data, a kterému CA PójCS vydala certifikát
Externí uživatel CA PójCS	fyzická nebo právnická osoba, která poskytuje PČS služby na základě obchodního smluvního vztahu, k jehož realizaci využívá i smluvně dojednaných služeb CA PójCS.
Hlavní správce PKI-PČS	Pracovník odpovědný za základní parametry certifikační autority, za řízení a správu klíčů administrátorů a registračních pracovníků a celkový běh systému PKI-PČS
Infrastruktura	Technologické prvky a jejich propojení zajišťující služby spojené s vydáváním a správou certifikátů

Klient CA PojCS 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.
Následný certifikát	certifikát, který byl vydán na základě nového požadavku (requestu) na vydání certifikátu podepsaného platným soukromým klíčem souvisejícím s již vydaným certifikátem, ke kterému je vydáván tento následný certifikát. Údaje ověřované CA PójCS musí být stejné. Data pro ověřování elektronického podpisu (veřejný klíč) musí být jiná. Ostatní položky následného certifikátu podléhají aktuálním pravidlům pro vydávání certifikátů.
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 CA PójCS, 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 (Request)	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-PČS	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 Zneplatněný certifikát	Data pro ověřování elektronického podpisu Součást určité PKI, zajišťující vydávání a správu certifikátů. certifikát, u nějž byla ukončena platnost bez možnosti obnovení této platnosti
Žadatel	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 CA PójCS, např. žádost o zneplatnění certifikátu.

2. OBECNÁ USTANOVENÍ

2.1 Závazky a povinnosti stran

Veškeré subjekty, které při své činnosti používají nebo využívají certifikáty vydané CAJCS jsou povinny dodržovat tuto Obecnou certifikační politiku a konkrétní Certifikační politiku platnou pro používaný typ certifikátu a jsou povinny dodržovat legislativní normy platné v ČR.

Vydavatel certifikátu

- CA pověřená k vydání certifikátu Pojišťovny České spořitelny se nazývá **CAJCS**, a její přesné charakteristiky jsou definovány v CPS.
- Certifikační autorita Pojišťovny České spořitelny plní roli Zprostředkujícího vydávajícího úřadu ve struktuře certifikačních autorit ČS, certifikát CAJCS je podepsán kořenovou certifikační autoritou České spořitelny.
- CAJCS zaručuje, že její postupy a procedury jsou uplatňovány v souladu s interní Certifikační prováděcí směrnicí (CPS), v souladu s Certifikační politikou České spořitelny a že každý vydaný certifikát byl vydán v souladu s ustanovením této CPS a příslušnou CP
- CAJCS je instalována v místě, které splňuje požadavky na zabezpečení pro ochranu privátního klíče certifikační autority z hlediska protipožární, režimové ochrany a z hlediska technického zabezpečení. Přístup je nepřetržitě monitorován a je umožněn pouze oprávněným specialistům.
- Soukromý a veřejný klíč CAJCS jsou generovány výhradně v prostředí hardwarového kryptografického modulu splňujícího normu FIPS 140-1 – úroveň 3.
- Při vytváření digitálního podpisu soukromý podepisovací klíč CAJCS nikdy neopustí tento hardwarový kryptografický modul.
- Kryptografické operace spojené s vydáváním certifikátů jsou prováděny výhradně v hardwarovém kryptografickém modulu bez možnosti ovlivnění obsluhou
- CAJCS zveřejňuje na své WWW adrese informace o zneplatněných certifikátech včetně odkazů na další adresy, na nichž je možno získat aktuální seznamy zneplatněných certifikátů. CAJCS vydává seznam zneplatněných certifikátů nejméně jednou za 60 hodin
- Ve zvláštních případech má Správa PKI právo zneplatnit certifikátu a musí o tomto neprodleně informovat držitele certifikátu a zapsat takový certifikát na seznam neplatných certifikátů (CRL).
- Správa PKI není odpovědná za použití certifikátu nebo klíčového páru, které je v rozporu s příslušnou certifikační politikou ani za používání párů klíčů.

Žadatel

- Žadatel souhlasí s danou certifikační politikou (CP) a zavazuje se ji dodržovat
- Žadatel se zavazuje používat certifikáty výhradně v souladu s příslušnou Certifikační politikou, podle které byl konkrétní certifikát vydán.
- V této souvislosti žadatel zvláště akceptuje, že:
 - smluvní ujednání vztahené k danému typu certifikátu se řídí zákony České republiky;
 - musí, po celou dobu používání, chránit svůj soukromý podepisovací klíč před ztrátou, vyrazení jiné, třetí straně či osobě, před úpravami či neoprávněným použitím, a to v souladu s danou CPS a CP. Od vytvoření svého soukromého a veřejného klíče je žadatel osobně a výhradně zodpovědný za uložení a neporušení celistvosti svého soukromého klíče. Každé použití soukromého klíče bude plně pod kontrolou žadatele a je považováno za akt žadatele. PIN, použitý k ochraně neautorizovaného užití soukromého klíče nesmí být nikdy uložen na stejném místě jako soukromý podepisovací klíč samotný, ani v blízkosti médií, na kterých je klíč uložen. Žadatel nesmí ponechat svůj soukromý podepisovací klíč v nechráněném stavu (pracovní stanice je přístupná komukoliv) a v odblokované pozici (PIN je zadán v paměti pracovní stanice). Žadatel je výhradně zodpovědný za užití svého soukromého klíče. PČS není zodpovědná za použití a využití páru klíčů žadatele;
 - je zodpovědný za generování své dvojice podepisovacích klíčů;
 - je zodpovědný za úplnost a správnost údajů, které nahlásil Správě PKI;
 - požádá Správu PKI o pozastavení platnosti nebo zneplatnění svého certifikátu, kdykoliv je to žádoucí a nutné podle dané CP. Procedury zneplatnění jsou popsány v článku 2.3 této CP;
 - musí okamžitě informovat Správu PKI při jakémkoliv změně údajů, zahrnutých ve svém certifikátu;
 - je povinen informovat Správu PKI při jakémkoliv změně údajů, které sice nejsou zahrnuty v certifikátu, ale které byly nahlášený Správě PKI při registračním procesu. Správa PKI si upraví registrované údaje;
 - je odpovědný za kontrolu a ověření správnosti obsahu zveřejněného certifikátu před jeho prvním použitím nejpozději do 7 dnů od vydání certifikátu. Zjistí-li žadatel rozpor mezi obsahem

- certifikátu a údaji v protokolu, musí o tom bezprostředně uvědomit Správu PKI. Správa PKI zabezpečí zneplatnění certifikátu a učiní opatření k nápravě;
- o souhlasí s právy, povinnostmi a závazky jak jsou popsány v účastnické smlouvě.

2.2. Typy certifikátů a metodika vydávání certifikátu žadatelům

CAPojCS vydává následující typy komerčních certifikátů pro zaměstnance i externí uživatele:

- certifikát pro ověření klienta a digitální podpis.
- v případě potřeby další certifikát určený pro šifrování dat.

Dále pro použití pouze na interní síti vydává CAPojCS certifikáty:

- pro server
- pro počítač
- pro zařízení
- pro podpis kódu

Postup podávání žádosti o určitý typ certifikátu, postup identifikace a autentizace žadatele při registraci, metodika pro jeho vydání a doporučené aplikace pro jeho použití jsou definovány v certifikační politice pro konkrétní typ certifikátu. Certifikační politiky pro certifikát pro ověření klienta a certifikát pro šifrování dat jsou pro potřeby externích uživatelů zveřejněny též na www.pojistovnacs.cz/ca

2.3 Využitelnost certifikátů

Vydaný certifikát lze použít pouze pro interní účely uvnitř Finanční skupiny ČS, v souladu s definovanými parametry certifikátu a ustanoveními příslušné certifikační politiky, na základě které byl certifikát vydán. Rozsah použití certifikátů externími partnery Pojišťovny České spořitelny musí být stanoven smluvním ujednáním.

Touto certifikační politikou se řídí vydávání certifikátů:

- pro autentizaci držitele při přihlášení do systémů provozovaných Pojišťovnou České spořitelny
- pro šifrování zprávy a podpis zprávy při komunikaci prostřednictvím elektronické pošty ve vnitřním styku uvnitř Finanční skupiny České spořitelny
- pro šifrování zprávy a podpis zprávy při komunikaci prostřednictvím elektronické pošty ve styku s externími partnery Pojišťovny České spořitelny, pokud byl tento způsob komunikace smluvně dohodnut.
- pro použití v serverových aplikacích (autentizace a/nebo šifrování)
- pro ochranu dat uložených na počítačích Pojišťovny České spořitelny
- pro podpis kódu užívaných uvnitř Pojišťovny České spořitelny.
- certifikátů pro počítače a zařízení (pouze uvnitř infrastruktury PČS)

Vydávané certifikáty a příslušné páry kryptografických klíčů lze použít k těmto účelům

- zajištění integrity dat
- zajištění důvěrnosti
- ustanovení sdíleného tajemství (klíče) v rámci protokolu pro bezpečnou výměnu dat
- přímé šifrování a dešifrování dat
- přímé podepisování dat

Protože CAPojCS nesplňuje podmínky stanovené pro kvalifikovaného poskytovatele certifikačních služeb dle zákona 227/2000 Sb. v platném znění, certifikáty vydané CA PojČS nesplňují podmínky pro kvalifikovaný certifikát, a proto podpisový certifikát nelze použít pro vytvoření zaručeného elektronického podpisu dle výše citovaného zákona. V případě certifikátu vydaného CA PojČS se jedná o komerční certifikát.

Vydávané certifikáty NELZE použít pro elektronický styk s orgány veřejné správy podle Zákona č. 227/2000 Sb., o elektronickém podpisu.

Použití certifikátu pro jiné účely nebo aplikace je na vlastní riziko držitele certifikátu a Pojišťovna České spořitelny se předem zříká jakékoli odpovědnosti za následky takového použití.

2.4 Zneplatnění certifikátu

- a) Podmínky a postupy zneplatnění jsou definovány CPS a příslušnou CP;
- b) Pokud je držiteli vydán kromě šifrovacího certifikátu navíc vyhrazený certifikát pro elektronický podpis, musí být zneplatněny všechny relevantní certifikáty najednou;
- c) Žádost o zneplatnění a veškeré s ní související dokumenty jsou archivovány.

2.4.1 Podmínky zneplatnění

Certifikát musí být zneplatněn v těchto případech:

- a) na žádost držitele certifikátu, resp. jeho nadřízeného;
- b) na žádost pracovníků *Správy PKI-PČS*, existují-li vážné a podložené důvody k tomu, aby bylo možné stanovit, že:
 - certifikát byl vydán na základě nepravdivých nebo zfalšovaných informací;
 - certifikát byl vydán způsobem, který neodpovídal *CPS*;
 - ověřené a certifikované informace již nejsou platné;
 - důvěrnost soukromého klíče již není zaručena;
 - media obsahující soukromý klíč jsou ztracena nebo zničena;
 - držitel certifikátu používá prostředky pro podepisování, které vykazují bezpečnostní nedostatky a umožnily by zfalšování údajů v certifikátu nebo změnu podepisovaných údajů. Doporučené prostředky pro podepisování jsou specifikovány v navazujících dokumentech;
 - držitel certifikátu nedodrжуje své závazky nebo hrubě porušil smluvní ujednání s Pojišťovnou České spořitelny;
- c) v případě, kdy daná *CA* *PojCS* ukončí svou činnost, aniž by její aktivity převzala nějaká jiná *CA* v rámci *PKI-PČS*;
- d) na pokyn státních orgánů v souladu s relevantními právními předpisy.

Nadřízený je oprávněn požádat o zneplatnění certifikátu podřízeného zaměstnance v situacích závažného porušení pracovní kázně zaměstnancem, při přechodu zaměstnance na jinou pozici, při ukončení pracovního poměru.

Případy zneplatnění z rozhodnutí *Správy PKI-PČS* jsou vždy způsobeny porušením závazků držitelem certifikátu nebo působením vyšším mocí. V těchto případech je riziko plně na straně držitele. V případě zneplatnění certifikátu z důvodu duplicity klíčů nabídne *Správa PKI-PČS* držiteli ihned nové vydání certifikátu.

Pro detailnější náhled viz příslušné *CP*.

2.4.2 Kdo může žádat o zneplatnění platnosti

O zneplatnění mohou požádat dále jmenované osoby, přičemž se ověřuje jejich totožnost:

- držitel certifikátu nebo jeho nadřízený;
- pracovník *Správy PKI-PČS*;
- státní orgány v souladu s relevantními právními předpisy.

2.4.3 Postup při žádosti o zneplatnění certifikátu

- a) O zneplatnění lze požádat v souladu s relevantní *CP*:
 - telefonicky, přičemž se ověřuje zpětným voláním identita žadatele;
 - elektronicky, přičemž se ověřuje elektronický podpis žádosti.
Podrobněji viz příslušná *CP*.
- b) Žádost o zneplatnění bude následována zneplatněním certifikátu v nejkratší možné době, nejpozději do 24 hodin od přijetí požadavku registrační autoritou. Zneplatnění podpisového certifikátu bude provedeno současně se zveřejněním nové, v případě potřeby mimořádné verze seznamu CRL, která bude bezprostředně publikována do AD, na <http://klicenka.pojcs.cz/certsrv/> a na www.pojistovnacs.cz/ca/capojcs.crl.
- c) O zneplatnění certifikátu informuje držitele certifikátu *RA PKI-PČS*.
- d) Zneplatnění certifikátu nemůže být zrušeno. Zneplatnění je proces nevratný.

2.4.4 Frekvence vydávání seznamu zneplatněných certifikátů (CRL)

Frekvence vydávání *CRL* závisí na typu certifikátu a proto je jedním z parametrů stanovených v příslušné *CP*. V každém případě jsou *CRL* seznamy vydávány pravidelně, minimálně jednou za 60 hodin a přírůstkový (delta) *CRL* je vydáván každé 4 hodiny.

V případě nutnosti může *CA* vydat i mimořádný *CRL* seznam.

2.4.5 Způsob využití CRL

- Závislé strany kontrolují *CRL* na vlastní zodpovědnost. To platí zejména o frekvenci vyhledávání *CRL*, jejíž volba je výhradně zodpovědností závislé strany.
- CRL* lze kontrolovat s pomocí patřičného software (např. Outlook, 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).
- Správa *PKI-PČS* doporučuje všem uživatelům konfigurovat použité aplikace tak, aby kontrolovaly platnost certifikátu s využitím všech příslušných *CRL* před každým použitím certifikátu.
- Pokud závislá strana obdrží podepsaný dokument, jehož obsah zavazuje odesílatele, nebo Pojišťovnu České spořitelny k jakémukoli plnění, je příjemce takového dokumentu povinen ověřit platnost certifikátu, jímž je dokument podepsán, momentálně nejaktuálnější platným *CRL* publikovaným na adrese <http://www.pojistovnacs.cz/ca/capojcs.crl>.
- Přírůstkové *CRL* jsou generovány pro urychlení ověřování komunikace v některých novějších aplikacích, avšak pro ověřování pravosti podpisů na dokumentech podle bodu d) nemají dokazující účinek.

2.4.6 Formy oznamování zneplatnění

Držitel certifikátu je o zneplatnění svého certifikátu vždy uvědoměn, a to buď telefonem, poštou nebo elektronickou poštou. Konkrétní forma odpovídá příslušné *CP* a volbě žadatele nebo administrátora zaří

2.5 Zajištění důvěrnosti

Informace získané Správou *PKI* od žadatele v souvislosti s jeho žádostí o certifikát budou použity pouze pro účely, pro které byly pořízeny. Použité postupy se řídí zákony České republiky. Pro zajištění odpovídajícího chodu všech prvků infrastruktury veřejných klíčů v *PČS* je zajištěn pravidelný audit činnosti.

2.6 Proces schvalování základních materiálů

Obecná certifikační politika a certifikační prováděcí směrnice jsou schvalovány představenstvem Pojišťovny České spořitelny a.s. Před tímto schválením nelze provádět jakékoliv změny v činnostech, které tato politika popisuje.

K vydávání konkrétních certifikačních politik pro jednotlivé typy certifikátů je zmocněn bezpečnostní manažer pro informační bezpečnost Pojišťovny České spořitelny.

Uplatněné změny v základních materiálech musí být zveřejněny pro ty subjekty, jejichž činnost je těmito materiály upravena nejméně 10 kalendářních dnů před jejich uplatněním.

Tato obecná certifikační politika nabývá platnosti dnem schválení s účinností od 1.2. 2006.

2.7 Zveřejňování a kontaktní informace

Tato Obecná certifikační politika se zveřejňuje na WWW stránkách Pojišťovny České spořitelny <http://www.pojistovnacs.cz/ca>. Veškeré dotazy týkající se její interpretace je nutno směřovat na níže uvedenou elektronickou adresu, která slouží i pro kontakt klienta s *CA*PojCS, zejména pokud se jedná o požadavky na zneplatnění certifikátu.

Kontaktní informace:

Pojišťovna České spořitelny, a.s.
nám. Republiky 115,

530 02 Pardubice**provozní doba v pracovní dny: 8:00 až 17:00 hod**

Tel.: +420 844.164 164 (Call centrum podpory externích uživatelů)

Fax: +420 466 051 380

<mailto:ca@pojistovnacs.cz> veškeré žádosti o zneplatnění a dotazy, změny od interních klientů<mailto:cae@pojistovnacs.cz> nové žádosti externistů o certifikát a hlášení změn externistů<http://www.pojistovnacs.cz/ca>

poznámka: zaměstnanci PČS se mohou v pracovní době obracet též přímo na pověřené pracovnice správy PKI PČS

Kontaktní osoby**Registrační autorita****Pracovnice oddělení správy aplikací pověřené činností Registrační autority**<mailto:ca@pojistovnacs.cz>

Marcela Koryntová

Tel.: +420 466 051 400

Michaela Bečičková

Tel.: +420 466 051 183

Pracovnice úseku podpory prodeje zajišťující registraci externích partnerů a prodejců<mailto:cae@pojistovnacs.cz>

Jana Libánská

Tel.: +420 466 051 291