PŘÍRUČKA UŽIVATELE

verze: 1.5

Ministerstvo financí České republiky

Historie dokumentu

Verze	Datum	Provedená změna	Provedl	Platnost od
0.98	06.06. 2008	První verze dokumentu	RNDr. Miroslav Šedivý, TO2	
1.0	16. 6. 2008	Zapracování připomínek	RNDr. Miroslav Šedivý, TO2	
1.1	17.06.2008	Úprava problematiky testovací RA	RNDr. Miroslav Šedivý, TO2	
1.2	02.12.2008	Popis www rozhraní	RNDr. Miroslav Šedivý, TO2	7.12.2008
1.3	1.4.2008	Aktualizace aplikace, kvalifikovaný certifikát, vložena kap. 13	Josef Kratochvíl, Datasys	15.4.2009
1.4	12.12.2009	Mobilní certifikáty	Josef Kratochvíl, Datasys	
1.5	20.12.2010	Podpora .NET karet, interaktivní formuláře	Josef Kratochvíl, Datasys	15. 4. 2011

OBSAH

 Část 1: POUŽÍVANÍ SYSTÉMU SPRÁVY ČIPOVÝCH KARET	6 6 7 8 8 8 9
 Úvod	6 7 8 8 9 10 11 11
 Uživatelské možnosti a obsluha CMS	6 8 8 9
 4. Vyžádání certifikátu	7 8 8 9
 4.1. Popis funčnosti 4.1.1. Najít uživatele 4.1.2. Osobní informace 4.1.3. Existující žádosti 4.2. Nastavení systému pro jednotlivé typy certifikátů 4.2.1. Čipová karta 4.2.2. Mobilní certifikáty. 4.2.3. Uživatelské kvalifikované a komerční certifikáty 4.2.4. Serverové certifikáty I.CA 4.2.5. Interní serverové certifikáty 4.2.6. Code signing 4.3.1 Prvotní vydání čipové karty. 4.3.2. Opětovné vydání dipové karty. 4.3.2. Návštěva registrační autority s vydáním certifikátu 4.4.2. Návštěva registrační autority s vydání certifikátu 4.5.1. Vytvoření žádosti 4.5.2. Návštěva registrační autority s vydání certifikátu 4.5.3. Instalace certifikátu 4.5.4.5.1. Vytvoření žádosti 4.5.2. Návštěva registrační autority s vydání certifikátu 4.5.1. Vytoření žádosti 4.5.2. Návštěva registrační autority s vydání certifikátu 4.5.1. Vytoření žádosti 4.5.2. Návštěva registrační autority s vydání certifikátu 4.5.1. Vytoření žádosti 4.5.2. Návštěva registrační autority s vydání certifikátu 4.6. Vyžádání certifikátů pro mobilní zařízení 4.6.1. Vytoření žádosti 4.7.1. Prvotní vytoření žádosti 4.7.2. Obnova certifikátu 4.8.1. Prvotní vytoření žádosti 4.7.2. Obnova certifikátu 4.8.1. Prvotní vytoření žádosti 4.8.2. Obnova certifikátu 5. Práce s čipovou kartou 5.1. Nastavení klientského počítače 5.2. Zobrazení obsahu karty	8 8 9
 4.1. Popis funcnosti. 4.1.1. Najít uživatele. 4.1.2. Osobní informace. 4.1.3. Existující žádosti. 4.2. Nastavení systému pro jednotlivé typy certifikátů 4.2.1. Čipová karta. 4.2.2. Mobilní certifikáty. 4.2.3. Uživatelské kvalifikované a komerční certifikáty. 4.2.4. Serverové certifikáty I.CA. 4.2.5. Interní serverové certifikáty 4.2.6. Code signing. 4.3. Žádost o čipovou kartu. 4.3.1. Prvotní vydání čipové karty. 4.3.2. Opětovné vydání čipové karty. 4.3.2. Opětovné vydání čipové karty. 4.3.2. Opětovné vydání čipové karty. 4.3.2. Návštěva registrační autority s vydáním certifikátu 4.4.1. Vytoření žádosti 4.5.1. Vytoření žádosti 4.5.2. Návštěva registrační autority s vydání certifikátu 4.5.3. Instalace certifikátu 4.5.3. Instalace certifikátu 4.6.1. Vytvoření žádosti. 4.7.1. Prvotní vytoření žádosti. 4.7.1. Prvotní vytoření žádosti. 4.7.1. Prvotní vytoření žádosti. 4.7.2. Obnova certifikátu 4.7.3. Prvotní vytoření žádosti. 4.7.4.5.3. Instalace certifikátu 4.6.1. Vytvoření žádosti. 4.7.1. Prvotní vytoření žádosti. 4.7.2. Obnova certifikátu 4.8.1. Prvotní vytoření žádosti. 4.8.2. Obnova certifikátu 5.2. Práce s čipovou kartou 5.1. Nastavení klientského počítače. 5.2. Zobrazení obsahu karty 	8 8 9
 4.1.2. Osobní informace. 4.1.3. Existující žádosti 4.2. Nastavení systému pro jednotlivé typy certifikátů 4.2.1. Čipová karta	8 9 9 9 9 9 9 9 9 10 10 11 11
 4.1.3. Existující žádosti 4.2. Nastavení systému pro jednotlivé typy certifikátů 4.2.1. Čipová karta 4.2.2. Mobilní certifikáty 4.2.3. Uživatelské kvalířikované a komerční certifikáty 4.2.4. Serverové certifikáty I.CA 4.2.5. Interní serverové certifikáty 4.2.6. Code signing 4.3. Žádost o čipovou kartu 4.3.1. Prvotní vydání čipové karty 4.3.2. Opětovné vydání čipové karty 4.3.2. Opětovné vydání čipové karty 4.3.2. Opětovné vydání čipové karty 4.4.1. Vytoření žádosti 4.4.2. Návštěva registrační autority s vydáním certifikátu 4.5. Vyžádání kvalifikovaného systémového certifikátu 4.5.1. Vytorění žádosti 4.5.2. Návštěva registrační autority s vydáním certifikátu 4.5.3. Instalace certifikátu 4.5.4.1. Vytorění žádosti 4.6.1. Vytorění žádosti 4.7.1. Prvotní vytoření žádosti 4.7.2. Obnova certifikátu 4.7.3. Vyžádání interního aplikačního certifikátu 4.7.4.3.1. Prvotní vytoření žádosti 4.7.4.5.4.4.3.1. Prvotní vytoření žádosti 4.7.5.2. Donova certifikátu 4.8.1. Prvotní vytoření žádosti 4.8.2. Obnova certifikátu 5.1. Nastavení klientského počítače 5.2. Zobrazení obsahu karty 	8 9 9 9 9 9 9 9 9 10 10 11 11
 4.2. Nastavení syštému pro jednotlivé typy certifikátů 4.2.1. Čipová karta. 4.2.2. Mobilní certifikáty. 4.2.3. Uživatelské kvalifikované a komerční certifikáty. 4.2.4. Serverové certifikáty I.CA. 4.2.5. Interní serverové certifikáty 4.2.6. Code signing 4.3. Žádost o čipovou kartu. 4.3.1. Prvotní vydání čipové karty. 4.3.2. Opětovné vydání čipové karty. 4.3.2. Opětovné vydání čipové karty. 4.4.1. Vytoření žádosti. 4.4.2. Návštěva registrační autority s vydáním certifikátu 4.5.1. Vytoření žádosti. 4.5.2. Návštěva registrační autority s vydáním certifikátu 4.5.3. Instalace certifikátu. 4.6.1. Vytoření žádosti. 4.6.1. Vytoření žádosti. 4.7.1. Prvotní vytoření žádosti. 4.7.2. Obnova certifikátu. 4.7.1. Prvotní vytoření žádosti. 4.7.2. Obnova certifikátu. 4.8.1. Prvotní vytoření žádosti. 4.7.2. Obnova certifikátu. 4.8.1. Prvotní vytoření žádosti. 4.7.2. Obnova certifikátu. 5.1. Nastavení klientského počítače. 5.2. Zobrazení obsahu karty. 	9 9 9 9 9 9 9 10 10 10 11 11
 4.2.1. Čipová karta	9 9 9 9 10 10 10 11 11
 4.2.2. Mobilní certifikáty	9 9 9 10 10 10 11 11
 4.2.3. Uživatelské kvalifikované a komerční certifikáty	9 9 10 10 10 10 11 11
 4.2.4. Serverové certifikáty I.CA. 4.2.5. Interní serverové certifikáty	9 9 10 10 10 11 11 11
 4.2.5. Interni serverove certifikáty	9 9 10 10 11 11 11
 4.2.6. Code signing. 4.3. Žádost o čipovou kartu	10 10 10 11 11 16
 4.3. Prvotní vydání čipové karty	10 10 11 11
 4.3.2. Opětovné vydání čipové karty 4.4. Vyžádání kvalifikovaného/komerčního zaměstnaneckého certifikátu	10
 4.4. Vyžádání kvalifikovaného/komerčního zaměstnaneckého certifikátu	11
 4.4.1. Vytvoření žádosti	11
 4.4.2. Návštěva registrační autority s vydáním certifikátu	16
 4.5. Vyžádání kvalifikovaného systémového certifikátu	
 4.5.1. Vytvoření žádosti	16
 4.5.2. Návštěva registrační autority s vydání certifikátu	16
 4.5.3. Instalace certifikátu. 4.6. Vyžádání certifikátů pro mobilní zařízení	21
 4.6. Vyzadaní certifikatu pro mobilni zarizení	22
 4.6.1. Vytvoreni zadosti 4.7. Vyžádání interního aplikačního certifikátu 4.7.1. Prvotní vytvoření žádosti 4.7.2. Obnova certifikátu 4.8. Vyžádání certifikátu Code Signing 4.8.1. Prvotní vytvoření žádosti 4.8.2. Obnova certifikátu 5. Práce s čipovou kartou 5.1. Nastavení klientského počítače 5.2. Zobrazení obsahu karty	22
 4.7. Vyzadaní interního aplikacního čertifikátu	22
 4.7.1. Prvotní vytvoření zadosti	24
 4.7.2. Obnova certifikátu 4.8. Vyžádání certifikátu Code Signing	24
 4.8.1. Prvotní vytvoření žádosti	25
 4.8.2. Obnova certifikátu 5. Práce s čipovou kartou 5.1. Nastavení klientského počítače 5.2. Zobrazení obsahu karty 	25
 Práce s čipovou kartou 5.1. Nastavení klientského počítače 5.2. Zobrazení obsahu karty 	25
5. Prace s cipovou kartou5.1.5.1.Nastavení klientského počítače5.2.Zobrazení obsahu karty	26
5.1.Nastavení klientského počítače5.2.Zobrazení obsahu karty	20
5.2. Zobrazení obsahu karty	26
	26
5.3. Obnova interních certifikátů	27
5.3.1. Notifikace	28
5.3.2. Obnova karty	28
5.3.3. Postup obnovy karty	29
5.5 Vzdálopá odblokování karty	21
5.5. vzudielle uublukuvalli kaity	JT
5.0. Zillella Fillu	22
5.6.2. Anlikace CMS	
5.6.3. Uadiokovani .NET karet	34

	5.1.	Import certifikátů na kartu	36		
6.	Konfigurace poštovního klienta37				
7.	Odesílání podepsané a šifrované pošty 40				
8.	Podpis	v Microsoft Office dokumentech	43		
	8.1. Vložení podpisu do dokumentu				
9.	WWW I	rozhraní Certifikační autority MF ČR	45		
	9.1. 9.2. 9.3.	Seznam aktuálně vydaných certifikátů CA Vyhledávání certifikátů Vyhledávání certifikátů	45 45 47		
Čás	st 2: PR/	ÁCE S AUTORITOU ČASOVÉ ZNAČKY	49		
10.	Úvod		49		
11.	Práce s	aplikací TSA Klient	49		
	$11.1.\\11.2.\\11.3.\\11.4.\\11.5.\\11.6.\\11.7.\\11.8.\\11.9.\\11.10.\\11.11.\\11.12.\\11.13.$	Spuštění aplikace Panel nástrojů Vyžádání nové časové značky ke zdrojovému souboru Ověření již existující časové značky Smazání časové značky ze seznamu Obsah detailního pohledu Nastavení Otevření seznamu časových značek Uložení seznamu časových značek Vytvoření nového seznamu časových značek Tisk Nápověda Ukončení aplikace	50 50 51 52 53 55 55 55 55 55 56 56		
12.	Řešení	problémů	57		
	12.1. 12.2. 12.3. 12.4.	Problém s generováním karty Problém s použitím certifikátu v Outlooku Problém s šifrováním pošty Problém se změnou PINu	57 57 58 58		
13.	Závěre	čné ustanovení	59		
14.	Příloha	č.1 - Seznam kontaktů na Spolupracující subjekty a jejich dosažitelnost .	60		
15.	Příloha	č. 2 - Formuláře žádostí	61		

1. SHRNUTÍ

Tento dokument popisuje základní postupy pro operaci s čipovou kartou (dále jen "kartou"), certifikáty a časovými razítky

Dokument popisuje tyto činnosti:

- Práci s čipovou kartou (získání, základní operace)
- Práce s certifikáty (požádání o vystavení, instalace, obnova a zneplatnění certifikátu)
- Používání certifikátu v aplikacích (podepisování, šifrování, ověřování)
- Práce s časovými razítky.

Část 1: POUŽÍVANÍ SYSTÉMU SPRÁVY ČIPOVÝCH KARET

2. ÚVOD

Tato část příručky je zaměřena na popis základních činností spojených s užíváním čipových karet nesoucích certifikáty a na práci s certifikáty.

Nově budovaná infrastruktura PKI je postavena na poněkud odlišné filozofii než tomu je v případě certifikační autority Daňové správy a jejích služeb. Základní odlišnosti jsou následující:

- CA DS je budovaná jako centralizovaná služba s jedním autorizačním střediskem naproti tomu nová infrastruktura je postavena ve shodě se strukturou resortu: nyní úřad, každé finanční ředitelství a celní správa disponují vlastní certifikační autoritou,
- byly zavedeny kroky směřující k urychlení procesu získání certifikátu a čipové karty tím, že jejich distribuce byla přenesena na jednotlivé celky uvedené v předchozím odstavci
- byly rozšířeny možnosti potisku čipových karet
- byly zavedeny nové funkčnosti infrastruktury PKI, které mají za cíl zvýšit jednak bezpečnost PKI, jednak uživatelský komfort – všechny funkce z pohledu uživatele jsou nyní přístupné přes jednotící rozhraní aplikace CMS.

V následujících kapitolách jsou popsány jednotlivé kroky kompletního životního cyklu certifikátů a čipových karet včetně aplikačního využití.

3. UŽIVATELSKÉ MOŽNOSTI A OBSLUHA CMS

Za účelem vyššího komfortu byla zavedena aplikace CMS (Card Management System – systém managementu čipových karet). Tuto aplikaci spustíme voláním www stránky s adresou <u>http://ca/CMS</u>.

Prostřednictvím této aplikace lze:

- inicializovat čipovou kartu před přidělením uživateli a vystavit na ni první certifikát (tato činnost je přístupna pouze tzv. operátorovi RA – viz dále)
- obnovit si certifikát před vypršením platnosti starého certifikátu
- zneplatnit certifikát (rovněž tato činnost je přístupna pouze operátorovi RA)

- odblokovat kartu
- změnit PIN na kartě
- zobrazit informace o kartě včetně certifikátů na ní uložených

Uvedená adresa je základním vstupním bodem pro práci s novými čipovými kartami a certifikáty, pro práci s čipovými kartami a certifikáty vydanými původní certifikační autoritou DS je nutno použít původní postupy.

4. VYŽÁDÁNÍ CERTIFIKÁTU

Prostřednictvím aplikace CMS může uživatel požádat o tyto typy certifikátů:

- 1. Certifikát pro vnitřní použití
 - a. Čipová karta podpisový a šifrovací certifikát
 - b. Mobilní certifikáty
 - c. Certifikát pro WEB server
 - d. Certifikát code signing
- 2. Certifikáty I.CA
 - a. Uživatelská kvalifikovaný s komerční certifikát
 - b. Kvalifikovaný systémový certifikát
 - c. Komerční serverový certifikát

Žádost o certifikát					
Najít uživatele					
√yhledat uživatele					
Výběr typu certifíkátu					
Zvolte typ certifikátů, které cl	hcete vytvořit.				
Certifikáty MF Certifikáty I.CA Sys		Systémové certifikáty MF			
🗖 Čipová karta	🗖 Uživatelské certifikáty	UVEB Server			
🗖 Mobilní certifikáty	🗖 Serverové certifikáty	🗖 Code signing	∨ytvořit žádost		
Osobní informace					
Název organizace: Česká republika - Finanční ředitelství pro hl. město Prahu Název finančního úřadu: Finanční ředitelství pro hl. město Prahu Adresa úřadu: Štěpánská 28, Praha, 111 21					
Titul před jménem:		Titul za jménem:			
Jméno žadatele: Prahy PM		Příjmení žadatele:			
Osobní číslo zaměstnance	administrator	E-mail: adr	ninistrator@pm.ds.mfcr.cz		
Existující žádosti					
Nic neodpovídá zadanému filtru					

4.1. Popis funčnosti

Obrazovka je rozdělena do 4 částí:

4.1.1. Najít uživatele

Tato sekce je určena pouze pro roli enrollment agent. Operátor zde má možnost zadat osobní číslo uživatele a požádat v jeho zastoupení o daný typ certifikátu. V případě, že uživatel není nalezen v personálním systému, může doplnit informace ručně a vytisknout pro uživatele žádost. Tato žádost je uložena v systému, k vydání certifikátu ale dojde až když je uživatel dostupný z personálního systému.

Volba je vhodná pro prvotní vydání čipové karty, kdy uživatel nemá vytvořen účet v doméně, nebo v případě kvalifikovaného certifikátu uživatel nepožádal, nebo došlo k nějakému pochybení.

Výběr typu certifikátu

V této části formuláře může uživatel vybrat certifikát(y), na které má oprávnění. V případě, že uživatel nemá oprávnění na daný typ certifikátu, volba není zobrazena. Uživatel může vybrat více typů současně

4.1.2. Osobní informace

V této části jsou zobrazeny informace o vybraném uživateli. Jednotlivé položky nelze měnit, vše je načteno přímo z personálního systému. V případě špatně vyplněných hodnot je nutno iniciovat změnu v personálním systému.

4.1.3. Existující žádosti

Zde je uveden přehled všech vydaných certifikátů i připravených žádostí. U vydaných certifikátů je možno vyžádat jejich zneplatnění, u žádostí uživatel doplňuje požadované informace pro vydání certifikátu. Na tomto místě je možno stáhnout vydané certifikáty.

4.2. Nastavení systému pro jednotlivé typy certifikátů

4.2.1. Čipová karta

Oprávnění mají všichni uživatelé. V případě, že uživatel vlastní aktivní čipovou kartu, nemá tuto volbu aktivní. V případě, že uživatel kartu ztratí, může na tomto místě požádat o revokaci karty a poté i bez schválení operátora může okamžitě požádat o novou čipovou kartu.

Revokace karty v tomto případě znamená vytvoření požadavku na revokaci, kterou musí schválit operátor. V případě, že operátor ve lhůtě 30ti dnů revokaci neschválí, dojde k automatickému zneplatnění.

4.2.2. Mobilní certifikáty

Oprávnění mají všichni uživatelé, kteří mají roli *Mobile User*. Do role může být přiřazen uživatel přímo nebo prostřednictvím skupiny Active Directory.

Uživatel může pořádat pouze jednou o tento typ certifikátu. Pokud z nějakého důvodu žádá opakovaně, musí nejdříve požádat o zneplatnění stávajícího podpisového certifikátu. Pokud uživatel vyžaduje zneplatnění šifrovacího certifikátu, musí požádat o revokaci čipové karty.

4.2.3. Uživatelské kvalifikované a komerční certifikáty

Podobně jako u čipové karty, musí uživatel požádat nejprve o zneplatnění stávajícího certifikátu. Uživatel musí být v roli *ICA user* přidělené přímo nebo prostřednictvím skupiny v AD. Prozatím bylo dohodnuto, že oprávnění budou mít všichni uživatelé.

4.2.4. Serverové certifikáty I.CA

Uživatel může mít současně více takových certifikátů, uživatel musí být v roli ICA application.

4.2.5. Interní serverové certifikáty

Uživatel může mít současně více takových certifikátů., uživatel musí být v roli WEB Admin

4.2.6. Code signing

Uživatel může mít pouze jeden takový certifikát, musí být v roli CodeSigning user

4.3. Žádost o čipovou kartu

4.3.1. Prvotní vydání čipové karty

Vydání čipové karty a/nebo prvního osobního certifikátu v rámci nové infrastruktury probíhá podle následujících kroků:

- Uživatel vyplní formulář Žádost o vydání uživatelské čipové karty / Žádost o vydání uživatelského certifikátu (vzor je uveden v příloze této příručky) a nechá si jej schválit nadřízeným. Žádost může vytvořit personalista v zastoupení uživatele a předat mu vytištěnou doplněnou žádost. V případě, že jsou dostupné informace z personálního systému, je formulář automaticky doplněn.
- S vyplněným a podepsaným formulářem (a čipovou kartou, pokud ji již vlastní) se dostaví na pracoviště RA
- Operátor RA zkontroluje údaje na žádosti, porovná je s údaji v personálním systému a vystaví uživateli na kartu příslušné certifikáty (jeden pro přihlašování, který slouží zároveň jako podepisovací a pokud má uživatel příslušná oprávnění, tak i pro přístup do aplikace ADIS, a druhý sloužící pro šifrování e-mailových zpráv či souborů). Pokud uživatel kartu nevlastní, potom operátor RA vydá certifikát na novou kartu, kterou předtím ještě personalizuje
- Uživatel převezme kartu s certifikáty oproti podpisu na žádosti.

Tímto je základní postup vydání karty a/nebo certifikátu u konce a uživatel může od této chvíle kartu používat pro přístup do své domény, podepisování zpráv a dokumentů a jejich šifrování.

4.3.2. Opětovné vydání čipové karty

V případě, že uživatel požaduje opětovné vydání čipové karty např. z důvodu ztrát, nefunkčnosti nebo plánované výměny, může uživatel požádat po zneplatnění stávající karty prostřednictvím CMS. Další postup je totožný jako při prvotním vydání karty

V případě že se jedná o ztrátu karty, je tato skutečnost ohlášena na personální oddělení prostřednictvím e-mailové zprávy. Uživatel pak může být požádán o úhradu ztracené karty.

4.4. Vyžádání kvalifikovaného/komerčního zaměstnaneckého certifikátu

4.4.1. Vytvoření žádosti

Spusťte Internet Explorer a zadejte adresu http://ca/cms, zvolte možnost žádost o certifikát

Výběr typu certifíkátu				
Zvolte typ certifikátů, které chcete vytvořit.				
Certifikáty MF Image: Certifikáty I.CA Image: Mobilní certifikáty Image: Certifikáty Image: Certifikáty Image: Certifikáty				
Osobní informace				
Název organizace: Ceská republika - Finanční ředitelství pro hl. město Prahu Název finančního úřadu: Finanční ředitelství pro hl. město Prahu Adresa úřadu: Štěpánská 28, Praha, 111 21				
Titul před jménem:		Titul za jménem:		
Jméno žadatele:	Prahy PM	Příjmení žadatele:		
Osobní číslo zaměstnance: administrator E-mail: administrator@pm.ds.mfcr.cz				
Existující žádosti				
Uživatelské jméno Typ žádosti Osobní číslo Vytvořen Zobrazit detail administrator Čipová karta administrator 11.1.2011				

Zaškrtněte volby Uživatelské certifikáty v sekci Certifikáty I.CA a stiskněte tlačítko Vytvořit žádost.

V dolní části obrazovky je zobrazen nový odkaz *Uživatelské certifikáty I.CA* se symbolem červeného trojúhelníku, který znamená, že uživatel musí doplnit další požadované informace.

Osobní informace	
Název organizace: Česká republika - Finanční ředitels Název finančního úřadu: Finanční ředitelství pro hl. město F Adresa úřadu: Štěpánská 28, Praha, 111 21	ství pro hl. město Prahu ^J rahu
Titul před jménem:	Titul za jménem:
Jméno žadatele: Prahy PM	Příjmení žadatele:
Osobní číslo zaměstnance: administrator	E-mail: administrator@pm.ds.mfcr.cz
Existující žádosti	
Užívatelské jméno Typ žádosti Zobrazit detail administrator Uživatelské certifikáty Zobrazit detail administrator Čipová karta Doplňujíci informace pro žádost o uživatelský kvali Zvote typ certifikátů, které chcete vytvořit. Pokud vyberete oba typ Kvalifikovaný certifikát Komerční certifikát Doplňujíle další informace potřebné pro generování žádosti. Rodné pokud je ale nedoplnite, musite tyto informace doplnit do žádosti Ulice:	Osobní číslo Vytvořen LCA administrator 14.1.2011 administrator 11.1.2011 fikovaný / komeční certifikát yv, bude generována žádost typu TWINS. *číslo a číslo občanského průkazu nejsou povinné, následně. Č.ulice: PSČ: Č.občan.průkazu:

Obrazovka je rozdělena do několika částí.

V záhlaví formuláře musí uživatel vybrat typ certifikátu o který žádá:

- Kvalifikovaný certifikát
- Komerční certifikát
- TWINS pokud uživatel zaškrtne obě volby

V horní části – *Základní informace* jsou informace automaticky doplněné z personálního systému, přičemž lze změnit pouze položku pozice ve firmě. Pokud některý z údajů nesouhlasí, kontaktujte správce systému.

V části Osobní informace doplňte chybějící informace dle skutečnosti podle občanského průkazu. Informace bude kontrolována operátorem registrační autority při výdeji certifikátu na kartu

V poslední části okna Informace pro tisk žádosti doplňte rodné číslo a číslo občanského průkazu. Tyto informace nejsou nikde uloženy, slouží pouze pro automatické doplnění do formuláře žádosti. Pokud tyto informace nevyplníte je možné je zapsat až při tisku žádosti.

Po doplnění požadovaných informací stiskněte tlačítko **Uložit žádost.** Zobrazí se následující okno, kde provedete konečnou kontrolu doplněných informací.

Doplňujíci inform	Doplňujíci informace pro žádost o uživatelský kvalifikovaný / komeční certifikát					
Kontrola	žádosti					
Zkontrolujte vyplněné	údaje a vytiskněte žádost					
Zvolte typ certifikátů, l	teré chcete vytvořit. Pokud vyberete oba typy, bude ge	nerována žádost typu TWINS	5.			
🗹 Kvalifikovaný certifikát 🔲 Komerční certifikát Doplňte další informace potřebné pro generování žádosti. Rodné číslo a číslo občanského průkazu nejsou povinné, pokud je ale nedoplníte, musíte tyto informace doplnit do žádosti následně.						
Ulice:	Masarykova	Č.ulice:	111			
Město: Praha		PSČ:	111111			
Rodné číslo: 681828/2299		Č.občan.průkazu:	sk00303003			
Pozice ve firmě: referent						
Odůvodnění žádosti: Příhlášení do aplikace						
Zrušit žádost Opravit žádost Potvrdit a vytisknout žádost						

Po provedení kontroly zadaných údajů můžete provést následující akce:

- Zrušit žádost žádost bude zrušena a zadané údaje budou odstraněny. V případě nové žádosti musíte opět doplnit všechny potřebné údaje.
- Opravit žádost tuto volbu použijete v případě, že jste při kontrole zjistili chyby a chcete je opravit
- Potvrdit a vytisknout žádost Pokud všechny údaje souhlasí, je žádost odeslána ke zpracování, je zobrazena výzva ke stažení nebo otevření souboru, který obsahuje doplněný formulář žádosti o zaměstnanecký certifikát. Otevřete formulář a ještě jednou zkontrolujte zapsané údaje, případně doplňte chybějící údaje. Žádost pak vytiskněte.



Vytištěný formulář je nutné schválit vaším nadřízeným a oprávněnou osobou s pověřením schvalovat vydání kvalifikovaného certifikátu za danou organizační složku (personální odbor).

Zároveň přejdete na následující obrazovku:

Doplňujíci inform	Doplňujíci informace pro žádost o uživatelský kvalifikovaný / komeční certifikát					
Zadané údaje byly	Zadané údaje byly v pořádku uloženy do databáze.					
Zvolte typ certifikátů, i	Zvolte typ certifikátů, které chcete vytvořit. Pokud vyberete oba typy, bude generována žádost typu TWINS.					
🗹 Kvalifikovaný cer	ifikát 📕 Komerční certifikát					
Doplňte další informace potřebné pro generování žádosti. Rodné číslo a číslo občanského průkazu nejsou povinné, pokud je ale nedoplníte, musíte tyto informace doplnit do žádosti následně.						
Ulice: Štěpánská 28, Praha, 111 21 Č.ulice:			111			
Město:	Praha	PSČ:	111111			
Rodné číslo: 681828/2299 Č. občan. průkazu:			sk00303003			
Pozice ve firmě:						
Odůvodnění žádosti: Příhlášení do aplikace						
Generovat certifikát žádosti Vytisknout žádost Zrušit žádost						

Zde jste v horní části informováni, že máte na serveru uložen aktivní požadavek na QC. I zde ještě máte možnost žádost zrušit kliknutím na tlačítko Zrušit žádost. V případě potřeby můžete znovu vytisknout celou žádost kliknutím na tlačítko Vytisknout žádost, ale musíte opět ručně doplnit RČ a OP, protože nejsou nikde uložená. Pokud máte zasunutou čipovou kartu (dále jen ČK) do čtečky ČK, stiskněte tlačítko Generovat certifikát žádosti. Tím spustíte proces vytvoření elektronické žádosti s následným vygenerování klíčů na ČK.

Nejdříve se zobrazí výzva na kontrolu vložení karty do čtečky ČK:



Po kliknutí na tlačítko OK se zobrazí okno na zadání PIN kódu k ČK:

5		
V	Zadejte prosím svůj PIN	
	.[1	
010	-1	Council 1

Po zadání PIN, klikněte na tlačítko OK.

O průběhu generování žádosti jste informováni:

dost o kvalifikovaný certifikát	
te aktivní požadavek na kvalifikovaný certifikát.	
ůběh generování žádosti	
:43:54] Generování žádosti bylo spuštěno	
:45:31] Certifikát žádosti byl úspěšně vytvořen.	
:45:31] Probíhá zápis certifikátu na server	
:45:34] Certifikát žádosti byl v pořádku zapsán na server. Vaše žádost je nyní připravena.	

Pokud vše proběhne v pořádku, jsou všechny řádky zelené. V případě chyby je daný řádek červený. Pokud tato situace nastane, kontaktujte svého IT administrátora.

Tím je proces žádosti o kvalifikovaný certifikát ukončen. Kliknutím v levé části okna na odkaz Kvalifikovaný certifikát se zobrazí následující obrazovka:

Doplňujíci informace pro žádost o uživatelský kvalifikovaný / komeční certifikát				
Váš požadavek je připravený. Pokud ho chcete vygenerovat zn	ovu, zrušte žádost a vytvo	řte novou.		
Zvolte typ certifikátů, které chcete vytvořit. Pokud vyberete oba typy, bude generována žádost typu TWINS.				
🗹 Kvalifikovaný certifikát 📕 Komerční certifikát				
Doplňte další informace potřebné pro generování žádosti. Rodné číslo a číslo občanského průkazu nejsou povinné, pokud je ale nedoplníte, musíte tyto informace doplnit do žádosti následně.				
Ulice: Štěpánská 28, Praha, 111 21	Č.ulice:	111		
Město: Praha	PSČ:	111111		
Rodné číslo:	Č.občan.průkazu:			
Pozice ve firmě:				
Odůvodnění žádosti:				
Vytisknout žádost Zrušit žádost				

Zde již nemáte možnost generovat žádost, ale pouze opětovně vytisknout papírovou část žádosti a případně žádost zrušit.

4.4.2. Návštěva registrační autority s vydáním certifikátu

Provedením všech úkonů uvedených v předchozím textu je splněn základní požadavek procesu vydání QC. Nyní vezměte ČK, na kterou byla žádost generována, potvrzený protokol o zaměstnaneckém poměru, občanský průkaz a další průkaz s fotografií (zaměstnanecká ČK karta s potiskem, řidičský průkaz, cestovní pas apod.) a dostavte se na registrační autoritu I.CA vydávající QC (personální odbor).

4.5. Vyžádání kvalifikovaného systémového certifikátu

4.5.1. Vytvoření žádosti

Žádat o kvalifikovaný systémový certifikát má možnost pouze uživatel, který má v aplikaci přiřazenou roli *ICA applicaton*. Certifikáty jsou určeny pro aplikace jako jsou WEB servery případně obecné účty typu podatelna

Spusťte Internet Explorer a zadejte adresu http://ca/cms. Zvolte Žádost o certifikát. Vyberte Serverové certifikáty v sekci Certifikáty I.CA a stiskněte tlačítko Vytvořit žádost.

Osobní informace					
Název organizace:	ázev organizace: Česká republika - Finanční ředitelství pro hl. město Prahu				
Název finančního úř	ʻ adu: Finanční ře	ditelství pro hl. město Pra	ahu		
Adresa úřadu:	Štěpánská	28, Praha, 111 21			
Titul před jménem:			Titul za jménem:		
Jméno žadatele:	Prahy PN	1	Příjmení žadatele:		
Osobní číslo zaměstna	ance: administra	ator	E-mail:	administrator@pm.ds.mfcr.cz	
Existující žádosti					
Uži	Uživatelské jméno Typ žádosti Osobní číslo Vytvořen				
💄 <u>Zobrazit detail</u> administrator Uživatelské certifikáty I.CA administrator 14.1.2011					
🔒 Zobrazit detail	<u> Zobrazit detail</u> administrator Systémové certifikáty I.CA administrator 14.1.2011				
Zobrazit detail administrator Čipová karta administrator 11.1.2011					
Doplňujíci informace pro žádost o systémový certifikát I.CA					
Zvolte typ certifikátu, které chcete vytvořit.					
Kvalifikovaný systémový certifikát C Komerční serverový certifikát					
Název certifikátu:					
Uložit žádost	Uložit žádost				

Vyberte certifikát o který žádáte

- Kvalifikovaný systémový certifikát
- Komerční serverový certifikát

Zkontrolujte předvyplněné informace doplňte Název certifikátu. Pokud se jedná o certifikát pro WEB server, zadejte jméno serveru (jméno serveru včetně domény), případně název popisující účel certifikátu. Po doplnění požadovaných informací stiskněte tlačítko **Uložit žádost.** Zobrazí se následující okno, kde provedete konečnou kontrolu doplněných informací.

Existující žádosti							
		Uživatelské jméno	Typ žádosti	Osobní číslo	Vytvořen		
2	<u>Zobrazit detail</u>	administrator	Uživatelské certifikáty I.CA	administrator	14.1.2011		
🛅 2	<u>Zobrazit detail</u>	administrator	Systémové certifikáty I.CA	administrator	14.1.2011		
0	<u>Zobrazit detail</u>	administrator	Čipová karta	administrator	11.1.2011		
Doplňujíci informace pro žádost o systémový certifikát I.CA							
Zvolte typ certifikátu, které chcete vytvořit.							
👁 Kvalifikovaný systémový certifikát 🔎 Komerční serverový certifikát							
Název certifikátu: pokus							
Generovat certifikát žádosti Vytisknout žádost Zrušit žádost							

Po provedení kontroly zadaných údajů můžete provést následující akce:

- Zrušit žádost žádost bude zrušena a zadané údaje budou odstraněny. V případě nové žádosti musíte opět doplnit všechny potřebné údaje.
- Opravit žádost tuto volbu použijete v případě, že jste při kontrole zjistili chyby a chcete je opravit
- Potvrdit a vytisknout žádost Pokud všechny údaje souhlasí, je žádost odeslána ke zpracování, je zobrazena výzva ke stažení nebo otevření souboru, který obsahuje doplněný formulář žádosti o zaměstnanecký certifikát. Otevřete formulář a ještě jednou zkontrolujte zapsané údaje, případně doplňte chybějící údaje. Žádost pak vytiskněte.

Stažení	souboru 🔀						
Chcete soubor otevřít nebo uložit?							
	Název: Systemovy certifikat (Podatelna FU v Praze).rtf Typ: Dokument ve formátu RTF, 3,87 kB Odesílatel: frprhca						
	<u>O</u> tevřít <u>U</u> ložit Storno						
1	Přestože software stažený z Internetu může být užitečný, některé soubory mohou poškodit počítač. Pokud zdroji plně nedůvěřujete, tento soubor neotevírejte ani neukládejte. <u>Jaké je riziko?</u>						

Vytištěný formulář je nutné schválit vaším nadřízeným a oprávněnou osobou s pověřením schvalovat vydání kvalifikovaného certifikátu za danou organizační složku (personální odbor).

Zároveň přejdete na následující obrazovku:

Adresa http://ca/cms/content/SystemCertificate.aspx	V Dodka
Smart Card Manager	
Přihlášený uživatel Žádosť o systěr pm\p100200 Role Webmaster Nová žádost –	nový certifikát
Úvodní stránka Úlohy E Informace k žádo	dane udaje byly v poradku ulozeny do databaze. ikát žádosti Vytisknout žádost <mark>Zrušít žádost</mark> osti
Kvalifikovaný certifikát Systemový certifikát Název organizace: Název certifikátu:	Česká republika - Finanční ředitelství pro hl. město Prahu Podatelna FU v Praze
Správa E-mail:	Jeseniova 2829/20, Praha 3, 13000 kratochvil@mfcr.cz
Zobrazit kartu Copyright © 2008 Ministerstvo financí ČR <u>-sertifikacniautorita@mfcr.cz</u>	

Zde jste v horní části informováni, že máte na serveru uložen aktivní požadavek na QC. I zde ještě máte možnost žádost zrušit kliknutím na tlačítko Zrušit žádost. V případě potřeby můžete znovu vytisknout celou žádost kliknutím na tlačítko Vytisknout žádost. V případě, že jsou zadané informace pořádku, můžete stisknout tlačítko Generovat certifikát žádosti. Generování žádosti na rozdíl od kvalifikovaného certifikátu musíte provést na počítači, pro který je certifikát určen. V případě, že není možno vytvořit certifikát na cílovém počítači, můžete vygenerovat certifikát žádosti na jiném počítači, kde provedete i následnou instalaci po vygenerování žádosti a certifikát pak můžete exportovat ve formátu pfx na cílový počítač.

Při generování žádosti certifikátu je zobrazeno okno, kde můžete nastavit úroveň zabezpečení, stiskněte tlačítko **OK**

Program vytv	áří nový klíč RSA pro výměnu.	×
	Aplikace vytváří chráněnou položku.	
	Soukromý klíč CryptoAPI	
	Je nastavena střední úroveň Nastavit úroveň zabezpečení zabezpečení.	

O průběhu generování žádosti jste informováni:

Adresa http://ca/cms/content/SystemCer	Přejit Odk.	
Smart Card Man	ager	
Přihlášený uživatel pm\p100200 Role Webmaster	Žádost o systém Nová žádost Zad	iový certifikát ané údaje byly v pořádku uloženy do databáze.
Úvodní stránka		
	Průběh generová	iní žádosti
Úlohy 💻	[17:01:19] Gener	ování žádosti bylo spuštěno
Kvalifikovaný certifikát	[17:01:37] Certifi	kát žádosti byl úspěšně vytvořen.
Systemový certifikát	[17:01:37] Probíh	á zápis certifikátu na server
	[17:01:37] Certifi	kát žádosti byl v pořádku zapsán na server. Vaše žádost je nyní připravena.
Obnovit certifikäty na karté	Informace k žádo:	sti
Správa 📕	Název organizace:	Česká republika - Finanční ředitelství pro hl. město Prahu
Zobrazit kartu	Název certifikátu:	Podatelna FU v Praze
	Adresa:	Jeseniova 2829/20, Praha 3, 13000
Copyright © 2008 Ministerstvo financí ČR <u>certifikacniautorita@mfcr.cz</u>	E-mail:	kratochvil@mfcr.cz

Pokud vše proběhne v pořádku, jsou všechny řádky zelené. V případě chyby je daný řádek červený. Pokud tato situace nastane, kontaktujte svého IT administrátora.

Tím je proces žádosti o systémový certifikát ukončen. Kliknutím v levé části okna na odkaz Systémový certifikát se zobrazí následující obrazovka:



Na rozdíl od kvalifikovaného certifikátu je zde možnost generovat další žádosti, případně stávající zrušit. Aktuální certifikát je možné změnit kliknutím a odkaz *Zobrazit detail*. V seznamu je možno rozlišit dvě úrovně připravenosti certifikátu.

Certifikát s ikonou 🧐 je připravený včetně vygenerovaného privátního klíče na cílovém počítači.

Certifikát s ikonou 📧 nemá vygenerovaný privátní klíč.

4.5.2. Návštěva registrační autority s vydání certifikátu

Provedením všech úkonů uvedených v předchozím textu je splněn základní požadavek procesu vydání QC. Nyní vezměte potvrzený formulář, občanský průkaz a další průkaz s fotografií (zaměstnanecká ČK karta s potiskem, řidičský průkaz, cestovní pas apod.) a dostavte se na registrační autoritu I.CA vydávající QC (personální odbor).

4.5.3. Instalace certifikátu

Po vydání certifikátu, obdrží uživatel poštovní zprávu s vydaným certifikátem a informací jak nainstalovat vydaný certifikát. Instalaci je nutné dokončit na serveru, kde byla vytvořena žádost (vygenerován privátní klíč)

4.6. Vyžádání certifikátů pro mobilní zařízení

4.6.1. Vytvoření žádosti

Spusťte Internet Explorer a zadejte adresu http://ca/cms. Po automatickém přihlášení se zobrazí následující obrazovka:

Smart Card	Manager
Přihlášený uživatel PMAdministrator Role Uživatel Úvodní stránka Certifikáty MF E Obnovit certifikáty Revokace certifikátu Kvalifikované certifikátu Zádost o kvalifikovaný certifikát Revokace certifikátu	Smart Card Manager Certifikáty Ministerstva Financí Obnovit certifikáty na katě Revokace certifikátu Kvalifikované certifikáty Žádost o kvalifikovaný certifikát Revokace certifikátu Správa karet Zobrazit informace o čipové kartě
Žádost o mobilní certifikát Obnovit mobilní certifikáty Zneplatnění mobilních Instalace mobilního certifikátu Správa Zobrazit kartu Copyright © 2008 Ministerstvo financi ČR certifikacniautorta@mfcr.cz	

Kliknutím na odkaz Žádost o mobilní certifikát zahájíte proces vytvoření žádosti a zobrazí se vám následující obrazovka:

Smart Card Manager				
Přihlášený uživatel PMAdministrator Role Uživatel				
Údaje o uživateli				
Titul před jménem:	Ing.	Titul za jménem: Doc.		
Certifikáty MF Jméno žadatele:	Petr	Přijmení žadatele: Poulicek		
Obnovit certifikāty Osobní číslo:	123456			
Revokace certifikátu Organizační jednotky/útvar (ÚFO, C	Ř <mark>, C</mark> Ú, útvaru MF/GŘC, úzer	nní pracoviště ÚZSVM)		
Kvalifikované certifikáty 📕 Název:	Česká republika - Finanční ředit	elstvi pro hl. město Prahu		
Žádost o kvalifikovaný certifikát Adresa:	Štěpánská 28. Praha. 111 21			
Revokace certifikátu	Na - 54			
Datum:	14.12.2009	(den.měsic.rok)		
Žádost o mobilní certifikát Vyberte typ certifikátu pro mobilní zařízení Obnovit mobilní certifikáty	 Podepisovací certifikát Autentizační certifikát Šifrovací certifikát 			
Zneplatnění mobilních Instalace mobilního certifikátu				
Správa 📕				
Zobrazit kartu				
Capyright © 2008 Ministerstvo financi ČR				

Formulář obsahuje informace automaticky doplněné z personálního systému, přičemž žádnou z položek nelze změnit. Pokud některý z údajů nesouhlasí, kontaktujte správce systému.

Pokud všechny údaje souhlasí, je žádost odeslána ke zpracování, je zobrazena výzva ke stažení nebo otevření souboru, který obsahuje doplněný formulář žádosti o zaměstnanecký certifikát. Otevřete formulář a ještě jednou zkontrolujte zapsané údaje, případně doplňte chybějící údaje. Žádost pak vytiskněte.

Do you want i	to open or save this file?
Ni T F	ame: Zadost_o_mobilni_certifikat.rtf [ype: Rich Text Format, 3,22KB From: frprhca Qpen <u>S</u> ave Cancel

Vytištěný formulář je nutné schválit vaším nadřízeným a oprávněnou osobou s pověřením schvalovat vydání kvalifikovaného certifikátu za danou organizační složku (personální odbor). Po schválení žádosti uživatel obdrží e-mail s nově vygenerovanými certifikáty a s obnoveným

šifrovacím certifikátem. Uživatel pak synchronizuje poštovní přihrádku do mobilního zařízení a poklepáním na certifikát provede instalaci na mobilní zařízení. Soubor s certifikátem je chráněn heslem, heslo k certifikátům uživatel obdrží na mobilní zařízení. Číslo musí být zadáno v personálním systému.

4.7. Vyžádání interního aplikačního certifikátu

4.7.1. Prvotní vytvoření žádosti

Žádost o certifikát probíhá podobně jako žádost o kvalifikovaný systémový certifikát.

Postup žádosti:

- Uživatel, který je v roli WEBAdmin požádá v systému o certifikát podobně jako o kvalifikovaný
- Systém připraví žádost ve formátu RTF, který uživatel vytiskne a nechá podepsat příslušným nadřízeným
- Uživatel vygeneruje privátní klíče může zvolit, zda klíče jsou exportovatelné, nebo vloží již vygenerovanou žádost do formuláře
- Operátorovi se zobrazí žádost o certifikát, kterou může vydat pouze na registrační autoritě, kde je k dispozici certifkát enrollment agenta, kterým žádost podepíše a odešle na server.
- CA vydá certifikát bez nutnosti schvalování managerem CA
- Vydaný certifikát se nabídne ke stažení v seznamu žádostí
- Uživatel si certifikát stáhne a nainstaluje.

4.7.2. Obnova certifikátu

Pokud uživatel žádá o obnovu certifikátu je uplatněn následující postup:

- Uživatel požádá o nový certifikát
- Uživatel vygeneruje privátní klíče může zvolit, zda klíče jsou exportovatelné, nebo vloží již vygenerovanou žádost do formuláře
- Pokud systém najde v databázi již vydaný certifikát stejného jména a shoduje se i žadatel o certifikát, považuje ho za obnovu

- Uživatel podepíše žádost vlastním podpisovým certifikátem (volitelně)
- Žádost je pak zobrazena operátorovi RA, který po ověření podpisu uživatele vydá certifikát
- Uživatel si vydaný certifikát stáhne a nainstaluje

4.8. Vyžádání certifikátu Code Signing

4.8.1. Prvotní vytvoření žádosti

Postup žádosti:

- Uživatel, který je v roli CODESigning User požádá v systému o certifikát podobně jako o kvalifikovaný
- Systém připraví žádost ve formátu RTF, který uživatel vytiskne a nechá podepsat příslušným nadřízeným
- Uživatel vygeneruje privátní klíče může zvolit, zda klíče jsou exportovatelné
- Operátorovi se zobrazí žádost o certifikát, kterou může vydat pouze na registrační autoritě, kde je k dispozici certifkát enrollment agenta, kterým žádost podepíše a odešle na server.
- CA vydá certifikát bez nutnosti schvalování managerem CA
- Vydaný certifikát se nabídne ke stažení v seznamu žádostí
- Uživatel si certifikát stáhne a nainstaluje.

4.8.2. Obnova certifikátu

Pokud uživatel žádá o obnovu certifikátu je uplatněn následující postup:

- Uživatel požádá o nový certifikát
- Uživatel vygeneruje privátní klíče může zvolit, zda klíče jsou exportovatelné, nebo vloží již vygenerovanou žádost do formuláře
- Pokud systém najde v databázi již vydaný certifikát stejného jména a shoduje se i žadatel o certifikát, považuje ho za obnovu
- Uživatel podepíše žádost vlastním podpisovým certifikátem (volitelně)
- Žádost je pak zobrazena operátorovi RA, který po ověření podpisu uživatele vydá certifikát

• Uživatel si vydaný certifikát stáhne a nainstaluje

5. PRÁCE S ČIPOVOU KARTOU

5.1. Nastavení klientského počítače

Předpokladem pro využití CMS a práci s certifikátem je použití určitého vybavení klientského PC. Předpokládá se proto, že PC je vybaveno:

- Operačním systémem fy Microsoft, a to Windows XP, Windows Vista, Windows 7
- Internet Explorer verze 6.0 a vyšší

Na počítači uživatele musí být instalován ActiveX prvek MFPKI.DLL pro manipulaci s kartou. Instalace je prováděna automaticky prostřednictvím Group Policy nebo manuální registrací knihovny do systému.

5.2. Zobrazení obsahu karty

Všechny operace jsou prováděny na jediné stránce – Zobrazit kartu

Zobrazení informací o čipové kartě						
Pyper clecky						
[Dioadcoin]	corp contacted officiate of					
Informace o kartě						
Informace	o uživateli			Informace o) kartě	
Vlastnost	Hodnota z certifikátu	Hodnota z Personálního	systému	Vlastnost	Hodnota	
Osobní čísl	o 111111	administrator		Název karty	Axalto Cryptoflex .NET	
Jméno	Administrator			Provider	Microsoft Base Smart Card Crypto Provider	
E-mail	administrator@pm.ds.mfcr.	cz administrator@pm.ds.mfcr	r.cz	Seriové číslo	57011351285AE4162F06FFFF (633C532131C42120)	
Účet administrator@pm.ds.mfcr.cz administrator@pm.ds.mfcr.cz		r.cz	Volné místo	41592		
Certifikáty obsažené na kartě						
Тур 9	šériové číslo	Platný od Platný do Vydá	ávající CA			
podpisový <u>1</u>	<u>7 29 de ce 00 00 00 00 02 c9</u>	11.01.2011 11.01.2012 FRP	M <u>S</u>	<u>Smazat</u> <u>Registro</u>	ovat	
Nástroje pro práci s kartou						
Odblokovat	Odblokovat kartu Obnovit certifikátv Inicializovat kartu					
Změnit PIN Import certifikátu ze souboru Vzdálené odblo						

Stránka je rozdělena na 3 oddíly:

- 1. Výběr čtečky k dispozici je rozbalovací menu, kde je možnost vybrat libovolnou čtečku, ve které je vložena čipová karta
- 2. Detailní informace o vložené kartě. Tento oddíl obsahuje další až 4 tabulky:

- a. Informace o uživateli k dispozici jsou základní informace o uživateli: Osobní číslo uživatele, jméno, příjmení a titul, e.mailová adresa a atribut userprincipalname. Tabulka obsahuje informace získané z certifikátu a informace získané z personálního systému. Pokud se jednotlivé atributy liší, může uživatel požádat o obnovu.
- b. Informace o kartě k dispozici jsou základní informace o vložené čipové kartě -Název karty, Provider karty, volné místo na kartě a sériové číslo karty uvedené ve 2 formátech. U karet podporující minidrivery (.NET karty) mají uvedená odlišná čísla z důvodu kompatibility dřívějšího PKCS11 formátu.
- c. Certifikáty obsažené na kartě v této tabulce je zobrazen seznam certifikátů, přičemž uživatel má podle konfigurace možnost uvedené certifikáty z karty odstranit, případně zaregistrovat do store lokálního počítače. Tato možnost není ve výchozím nastavení uživatelům dovolena. Kliknutím na odkaz sérového čísla certifikátu je zobrazen certifikátv grafickém rozhraní Windows se všemi jeho detaily. Typ certifikátu je rozlišován následovně:
 - i. Podpisový vytvořen podle šablony MFCR_Authisgn
 - ii. Šifrovací vytvořen podle šablony MFCR_Encryption
 - iii. ICA kvalifikovaný nebo komerční certifikát vydaný I.CA
 - iv. Neznámý ostatní typy certifikátů
- Úložiště bez certifikátů v této tabulce je zobrazen seznam prázdných kontejnerů určených ke smazání
- e. Nástroje v tomto oddílu jsou k dispozici jednotlivé nástroje pro práci s kartou jako je Odblokováním Obnova, Změna PINU, Import Certifikátu, Inicializace. Jednotlivé volby je možno skrýt nebo zobrazit podle role v systému.

5.3. Obnova interních certifikátů

Tato kapitola popisuje proces obnovy interních certifikátů uložených na čipové kartě a certifikátů určených pro mobilní zařízení

5.3.1. Notifikace

Certfikační autorita je nastavena tak, že před vypršením platnosti certifikátu obdrží uživatel informaci o jeho expiraci prostřednictvím e-mailové zprávy. Notifikace proběhne ve třech intervalech

- 1 měsíc informaci obdrží uživatel
- 3 týdny informaci obdrží uživatel
- 1 týden informaci obdrží uživatel a administrátor domény

V těle zprávy je informace o expirujících certifikátech a krátký postup s odkazem jak certifikát obnovit.

V případě, že uživatel neobnoví certifikát v době jeho platnosti, dojde automaticky k jeho zneplatnění. Zneplatněným certifikátem již nelze vzdáleně požádat o obnovu a proto uživatel musí navštívit pracoviště registrační autority, kde požádá o vygenerování nové karty (viz kap. 4).

5.3.2. Obnova karty

Čipová karta uživatele obsahuje, jak vyplývá z kapitoly 4 minimálně 2 certifikáty s následujícími šablonami:

- MFCR_Encyption tento certifikát je určen pro šifrování elektronické pošty. Certifikát je platný po dobu dvou let.
- MFCR_AuthSign tento certifikát slouží jednak pro přihlašování do systému pomocí čipové karty, jednak pro podepisování elektronické pošty případně jiných dokumentů (Workd, Excel, Acrobat) a především pro přihlašování do aplikace ADIS.

Certifikáty pro mobilní zařízení jsou vydávány podle následující šablon:

- MFCR_Encyption tento certifikát je určen pro šifrování elektronické pošty a je shodný s certifikátem uloženým na čipové kartě. V případě, že je provedena obnova certifikátů na čipové kartě, mu sí být provedena i obnova mobilních certifikátů
- MFCR_AuthSign_Mobile tento certifikát slouží pro podepisování elektronické pošty na mobilním zařízení
- MFCR_Auth_Mobile tento certifikát slouží pro autentizaci uživatele

Vzhledem k tomu, že platnost všech zmíněných typů certifikátů je omezena na 2 roky (s výjimkou testovacích certifikátů, u nichž je platnost zkrácena na 3 měsíce), je nezbytné si po této době požádat o certifikáty nové. Tato situace se řeší tzv. obnovou certifikátu. Tuto obnovu (popsanou dále) je nezbytné provést ještě před vypršením platnosti certifikátu.

Obnova mobilních certifikátů je provedena automaticky - tzn. pokud uživatel obnoví certifikáty na čipové kartě, automaticky je provedena obnova mobilních certifikátů. Ty jsou pak zaslány uživateli jako příloha elektronické pošty. Uživatel pak obnovu musí dokončit na mobilním zařízení instalací těchto certifikátů. Instalace je prováděna po synchronizace zprávy na mobilní zařízení poklepá ním na přiložený PFX soubor

Aplikace CMS je nastavena tak, že po úspěšném provedení obnovy autentizačního certifikátu, kdy je vygenerován a do karty uložen nový autentizační certifikát, původní certifikát smaže (i se soukromým klíčem uloženým na kartě). To je dáno tím, že dále je tento certifikát používán pouze pro ověřování (není potřebný soukromý klíč) – pokud je potřebné cokoliv podepsané tímto certifikátem ověřit, lze jej získat z centrálního úložiště.

Naproti tomu v případě šifrovacího certifikátu je situace jiná, zde je potřebné původní certifikáty i po jejich obnovení a získání nových ponechat pro potřeby dešifrace starších e-mailových zpráv. Zde je aplikace nastavena tak, že po obnovení zůstává určitý počet starších šifrovacích certifikátů stále na kartě (jejich počet je dán kapacitou čipové karty, vždy zůstávají alespoň dva certifikáty).

5.3.3. Postup obnovy karty

Do adresy Internet exploreru zadejte http://ca/CMS.

Zobrazí se úvodní stránka

Pro úspěšné provedení obnovy musí na kartě existovat alespoň podepisovací certifikát vydaný lokální certifikační autoritou. Obnoví se vždy podepisovací i šifrovací certifikát.

V sekci úlohy klikněte na odkaz **Zobrazit kartu** a v dolní části obrazovky klikněte na odkaz *Obnovit* certifikáty

Zadejte PIN a stiskněte tlačítko **Spustit Obnovu.** Po úspěšné obnově můžete zkontrolovat obsah karty buď kliknutím na odkaz **Zobrazit kartu.** Po správné obnově by na kartě měl být jedíný podepisovací certifikát a jeden nebo více šifrovacích certifikátů (podle kapacity karty)

V případě, že uživatel vlastní mobilní certifikáty, uživatel současně obdrží nově vydaný šifrovací certifikát a zároveň jsou vygenerovány ostatní certifikáty urřené pro mobilné zařízení.

5.4. Odblokování karty

Odblokování karty je k dispozici pro případ kdy uživatel zapomene svůj PIN ke kartě, nebo dojde k jejímu zablokování.

Odblokování karty může provést pouze oprávněná osoba (administrátor domény), která má delegována příslušná oprávnění v aplikaci. Uživatel navštíví administrátora domény, Administrátor ověří totožnost uživatele a pomocí Aplikace kartu odblokuje. V tomto případě si uživatel musí zadat nový PIN na stanici administrátora.

Odblokování karty je možné provádět pouze v případě, že uživatel má v roli **Doménový operátor.** V případě Enrollment agenta lze použít pouze funkci Inicializace karty, která smaže obsah karty a nastaví výchozí uživatelský a administrátorský PIN

Nástroje pro práci s kartou					
<u>Odblokovat kartu</u>	<u>Obnovit certifikáty</u>	Inicializovat kartu			
Změnit PIN	Import certifikátu ze souboru	<u>Vzdálené odblokování</u>			
Zadejte nový PIN: •••• Potvrďte PIN: ••••					
Odblokovat kartu					
Detailní průběh					
[0:44:52] Zjišťování a	dmin PINu z databáze				
[0:44:52] Úspěšné nad	čtení admin PINu				
[0:44:54] Úspěšné odl	olokování karty				
T.					

Karta byla úspěšně odblokována	>
	Ok

5.5. Vzdálené odblokování karty

Funkce vzdáleného odblokování karty je k dispozici pouze pro karty podporující minidrivery (.NET karty). Tato funkce je vhodná pro uživatele, kteří nemají přístup k aplikaci. Postup odblokování probíhá následujícím způsobem:

1. Vygenerování request stringu.

Tato část je odlišná podle verze operačního systému. **Windows XP** má k dispozici nástroj PINTOOL

Smart Card PIN Tool 🛛 🗙		
Change PIN Unblock		
Your smart card administrator will give you data to type into the 'Response' box, and then you must enter a new PIN. Do not remove your card until you are prompted to do so.		
Press the 'OK' button to finish unblocking your card.		
Challenge	B87C 000B 2425 F8A3	
<u>R</u> esponse		
New <u>P</u> IN		
Confirm New PIN		
<u>U</u> nblock	<u>OK</u> <u>C</u> ancel	
	Close	

Po stisknutí tlačítka Unblock je vygenerován request string

Operační systém Windows Vista a Windows 7 nativně obsahuje nástroj pro vzdálené odblokování:



 Uživatel se identifikuje operátorovi příslušné domény a ten vygeneruje příslušnou odpověď (Response), který uživatel zadá do formuláře, dále zadá nový požadovaný PIN a může odblokovat kartu.

5.6. Změna PINu

5.6.1. Gemsafe

Změna uživatelského PINu pro karty Gemsafe Classic TPC je prováděna přímo v aplikaci **GemSafe**, která je k dispozici na všech klientských stanicích.

Spusťte aplikace GemSafe Toolbox a zvolte Správa karty, klikněte na ikonu Správa PIN

Joalbar		gemalt
100100	Správa PIN	
Obsah karty		
Správa karty		Zvolte nainstalovaný snímač smart card
Správa PIN		Gemplus GPR400 0
		Civalte akd, kterou chcete provést GemP15-1 © Změnit PIN Č Odblokovat PIN
Správa software		
agnostika /Nánověda		Další >>

Stiskněte tlačítko Další

C A COMPANY CONTRACTOR	Správa PIN		13
Obsah karty Správa karty	Gemplus GPR400 0		
Språva PIN	Cast PIN User	Pravidla postupu PIN Musí být dlouhé nejméně 4 znaků Musí být menší nebo rovno 8 znakům Musí obsahovat pouze číselné znaky	>>>
práva software			

Následující kroky jsou:

- V horní části zvolte User v žádném případě neměňte jiný než USER PIN, v opačném případě může dojít k nevratnému zablokování karty
- Zadejte Starý PIN a dvakrát zapište PIN nový
- Po úspěšné změně PINu se zobrazí následující okno.

Správa PIN 🔀	
PIN změněn.	
(OK	

5.6.2. Aplikace CMS

Pomocí aplikace CMS je možné měnit PIN na všech podporovaných typech karet. Zvolte možnost Zobrazit kartu a v dolní části obrazovky vyberte **Změnit PIN**

Nástroje pro práci s kartou		
Odblokovat kartu	<u>Obnovit certifikáty</u>	Inicializovat kartu
Změnit PIN	Import certifikátu ze souboru	Vzdálené odblokování
Zadejte současný PIN:		
Zadejte nový PIN:		
Potvrďte PIN:		
Změnit PIN		

Zadejte stávající PIN a dvakrát nový požadovaný PIN a stiskněte tlačítko Změnit PIN.

5.6.3. Odblokování .NET karet

Pro karty podporující minidrivery je možnost podobně jako pro odblokování použít nativní nástroje:

Pro Windows XP je k dispozici PINTOOL

Smart Card PIN Tool		×
Change PIN Unblock		
To change your Smart C desired new PIN and pre	ard PIN, enter the old PIN and th sss the 'Change PIN' button below	ie N.
Old <u>P</u> IN New P <u>I</u> N Confirm New PI <u>N</u>		
	<u>C</u> hange Pin	
		Close

Pro operační systém Windows Vista a Widows 7:



5.7. Inicializace karty

Inicializace se provádí opět ve WEB rozhraní aplikace CMS – Zobrazení karty - Inicializace

Funkce slouží k uvedení karty do původního stavu: Je vymazán obsah karty a nastaven výchozí uživatelský a administrátorský PIN. Funkce je k dispozici pro roli *doménový operátor, administrátor a enrollment agent*. Po dokončení vymazání karty, systém automaticky požádá o revokaci vymazaných certifikátů. Příslušný operátor pak potvrdí nebo zamítne revokaci. Pokud operátor nereaguje během 30 dnů (možno konfigurovat), dojde k automatickému zneplatnění těchto certifikátů.

Pro inicializaci karty a revokaci všech certifikátů na kartě 57011351285AE4162F06FFFF , vyberte důvod revokace a potvrďte tlačítkem Revokovat		
Zneužití certifikátu 🔺		
Dočasné zneplatnění		
Konec PPV		
Nahrazení certifikátu 🗾		
Revokovat Zrušit		

Při inicializaci je operátor dotázán na důvod revokace karty.

5.1. Import certifikátů na kartu

Pro uživatele je k dispozici možnost importu libovolného certifikátu včetně privátního klíče ve formátu PFX.

Nástroje pro práci s kartou		
<u>Odblokovat kartu</u> <u>Změnit PIN</u>	<u>Obnovit certifikáty</u> Import certifikátu ze souboru	<u>Inicializovat kartu</u> <u>Vzdálené odblokování</u>
PFX Soubor Zadejte heslo k souboru: Zadejte PIN karty: Importovat	Procházet	

Po zadání požadovaných informací je certifikát uložen na čipovou kartu.
6. KONFIGURACE POŠTOVNÍHO KLIENTA

Tato kapitola popisuje nastavení aplikace Outlook pro možnost šifrování a podepisování elektronické pošty - tuto činnost zpravidla provádí pracovník IT

- Spusťte aplikaci Outlook
- Z menu Nástroje Možnosti –záložka zabezpečení, stiskněte tlačítko Nastavení

Možnosti			? 🛛							
Předvolby	Nastavení pošty	Formát pošty	Kontrola pravopisu							
Zabezpe	Zabezpečení Jiné Delegáti									
Zabezpečená elel	ktronická pošta									
🔽 🗆 🖸 🖸	On 🔽 Zašifrovat obsah a přílohy odesílaných zpráv									
🔫 🗾 🔲 Přid	at <u>d</u> igitální podpis do odesík	aných zpráv								
Prìo	desílání podepsané zprávy ázik zakoze žesí užech zm	odeslat podepsanou	zprávu bez nutnosti ověření							
j O <u>z</u> n	amic zabezpeceni vsech zpi	av s poopisem s/imim								
<u>v</u> ychozi na	iscaveni;									
Zabezpečený obs	ah									
Zóny za HTML sp aplikace	bezpečení umožňují upravil puštěny skripty a aktivní ob Internet Explorer, kterou	:, zda mohou být ve z sah. Vyberte zónu za chcete používat.	právách bezpečení							
Zón <u>a</u> :	😑 Servery s omezeným	přístupem	▼ <u>N</u> astavení zóny…							
Digitální ID (certif	ikáty)									
Digitálni identitu	ID nebo certifikáty jsou do v elektronických transakcío	kumenty, které umož h.	ňují ovéřovat							
Publikovat v glot	bálním seznamu adres	Importovat/exportov	vat Načí <u>s</u> t digitální ID							
		ОК	Storno P <u>o</u> užít							

Změnit nastavení zabezpečení 🛛 🔀							
Předvolby pro nastavení zabezpečení							
Název nastav <u>e</u> ní zabezpečení:							
Nastavení S/MIME (Kratochvil@datasys.cz)							
Kryptografický <u>f</u> ormát: S/MIME							
Výchozí nastavení zabezpečení pro tento formát kryptografických zpráv							
Výchozí nastavení zabezpečení všech kryptografických zpráv							
Náz <u>v</u> y zabezpečení <u>N</u> ové Vy <u>m</u> azat <u>H</u> eslo,							
Certifikáty a algoritmy							
Podpisový certifikát: Kratochvíl Josef Vybrat							
Zatřid'ovací algoritmus: SHA1							
Šifrovací certifikát: Kratochvíl Josef Vy <u>b</u> rat							
Šifrovací algoritmus: 3DES 💌							
S podepsanými zprávami ode <u>s</u> ílat tyto certifikáty							
OK Storno							

V sekci Certifikáty vyberte správný Podpisový a Šifrovací certifikát. V případě, že vlastníte zároveň kvalifikovaný certifikát, musíte v nastavení poštovního klienta vytvořit nový profil s kvalifikovaným podepisovacím certifikátem a před odesláním podepsané pošty vždy zkontrolovat, který profil (interní, nebo ICA) je vybrán

Změnit nastavení zabezp	ečení	X					
Předvolby pro nastavení zabezpečení							
Název nastav <u>e</u> ní zabezpe	čení:						
Nastavení S/MIME (Krato	ochvil@datasys.cz)	•					
ICA Nastavení S/MIME (Krato	chvil@datasvs.cz)						
Výchozí nastavení zab	ezpečení pro tento formát kryptogra	fických zpráv					
Výchozí nastaven	í zabezpečení všech kryptografických	zpráv					
Názvy zabezpečení	. <u>N</u> ové Vy <u>m</u> azat	<u>H</u> eslo					
Certifikáty a algoritmy							
Podpisový certifikát:	Josef Kratochvíl	V <u>v</u> brat					
Zatřiďovací algoritmus:	SHA1]					
Šifrovací certifikát:	Josef Kratochvíl	Vy <u>b</u> rat					
Šifrovací algoritmus:	AES (256-bit)]					
S podepsanými zpráva	ami ode <u>s</u> ílat tyto certifikáty						
	OK	Storno					

• Stisknutím tlačítka OK dokončíte konfiguraci

7. ODESÍLÁNÍ PODEPSANÉ A ŠIFROVANÉ POŠTY

V případě, že je aplikace Outlook nakonfigurována dle předchozího postupu, můžete začít digitálně podepisovat a šifrovat poštovní zprávy. Na ovládací liště jsou zobrazeny ikony pro vložení podpisu, nebo zašifrování zprávy:



- Vložení podpisu do zprávy
- Zašifrování zprávy

😰 Zpráva bez názvu 💽 💽	
Soubor Úpravy Zobrazit Vložit Formát Nástroje Tabulka SmarTeam Okno Nápověda	×
🗄 ⊡ Ogeslat 🔘 🔹 🛄 🌡 / 😼 📍 💺 🌾 🏠 😢 Možnosti 🔹 HTML 🛛 🛃 🌬	
🔛 Komu 📗]
LE Kopie	
Předmět:	
: 🕞 🛃 X 🖙 🏝 Arial 🔹 🔹 10 🔹 🗛 → B Z U 副 副 国 日 日 日 印 日	* 5
	~
	-
	*
	0 ¥

Na následujícím obrázku jsou příklady kombinace šifrované a podepsané zprávy

🕑 Test - Microsoft Outlook							_	ΞX
Soubor Úpr <u>avy Z</u> obrazit Př <u>ejít N</u> ás	stroje Ak <u>c</u> e	Nápo <u>v</u> ěda				Nápověd	la – zadejte do	otaz 👻
🗄 🔂 Nová 🔹 🦣 隆 🗙 🙈 Odpovědět	🕞 Odpovědě	it všem 🛛 🙈 Předat dá <u>l</u>	🛛 🏭 🥐 🛛 🕼 📑 Odeslat a přijmou <u>t</u>	🝷 🖄 🔛 Prohledat a	dresáře 👻 🦉			
Pošta «	📮 Test			Hledání: Test	Q	• *	Tuto	~~
Oblíbené složky	⊠,!∆D	Ø Od	Předmět	Přijato	Veli Kategorie	8	polo nelze	
🤯 Dorucená pošta 📑 Odeslaná pošta	🗄 Datum: I	Dnes					zobr	Pane
Poštovní složky 🛛 🖇	<u>e</u>	Kratochvíl Josef	Šifrovaná a podepsaná zpráva	čt 6.3.200	. 14 kB	7		5
		Kratochvíl Josef	Sifrovaná zpráva	čt 6.3.200	. 7 kB	Y		6
	83	Kratochvíl Josef	Podepsaný email	čt 6.3.200	. 11 kB	Ŷ		E •
Pošta								9:00: Jednání Pro
📰 Kalendář 🖭 🖉 🔔 🍙 7						Ŧ		jektového tý
Položek: 3				/šechny složky jsou aktua	ální. 🔀 Připojeno	o k Micro	soft Exchang	e •

Pokud je zpráva zašifrována nebo podepsána, je zobrazen příslušný symbol v pravé části okna:

- 2 Zpráva je podepsaná
- Zpráva je šifrovaná

Zpráva	⊽ Šifrovanā	a podepsaná zpráva – Zpráva (HTML)	1		- = ×
Odpovědět Odpovědět Předat všem dál Odpovědět	Odstranit 🗳 Přesunout do složky *	 Blokovat odesílatele Seznamy bezpečných adres * Není nevyžádaná pošta Nevyžádaná pošta 	 Zařadit do kategorií * Zpracovat * Označit jako nepřečtené Možnosti 	AA Najit	Odeslat do aplikace OneNote OneNote
Od: Kratochvil Josef Komu: Kratochvil Josef Kopie: Předmět: Šifrovaná a podeps Podepsáno: Kratochvil@datasys	ianá zpráva ;.cz			Odesl	àno: čt 6.3.2008 10:14
Test					

Pokud je podpis v pořádku, zobrazí se text: Podepsáno: emailová_adresa

Stisknutím symbolu šifrované 🛅 nebo podepsané 🔎 pošty jsou zobrazeny detailní informace (viz obr.):



8. PODPIS V MICROSOFT OFFICE DOKUMENTECH

Dokument můžete digitálně podepsat z mnoha stejných důvodů, ze kterých podepisujete papírové dokumenty. Digitální podpis se používá k ověření (Ověřování: Proces, při němž je zjišťováno, zda jsou uživatelé a produkty opravdu tím, za koho nebo za co se vydávají. Například při potvrzení zdroje a integrity kódu vydavatele softwaru je ověřován digitální podpis použitý k podepsání kódu.) digitálních informací (například dokumentů, e-mailových zpráv a maker) pomocí počítačové kryptografie. Digitální podpisy pomáhají poskytnout následující záruky:

- **Pravost** Digitální podpis pomáhá zaručit, že podepsaný je tím, za koho se vydává.
- Integrita Digitální podpis pomáhá zaručit, že obsah nebyl poté, co byl digitálně podepsán, změněn ani zfalšován.
- Nepopiratelnost odpovědnosti Digitální podpis pomáhá dokázat všem stranám původ podepsaného obsahu.

8.1. Vložení podpisu do dokumentu

Digitální podpisy lze přidat do dokumentů aplikace Word, sešitů aplikace Excel a prezentací aplikace PowerPoint

Digitální podpis na rozdíl od klasického papírového dokumentu není viditelný v obsahu samotného dokumentu, ale příjemci dokumentu mohou zjistit, zda byl dokument digitálně podepsán, zobrazením digitálního podpisu dokumentu nebo vyhledáním tlačítka Podpisy na stavovém řádku v dolní části obrazovky.



Digitálně podepsaný dokument je určen pouze pro čtení, v případě jakéhokoliv zásahu do podepsaného dokumentu způsobí vymazání všech předchozích podpisů.

Pokud chcete zobrazit seznam uživatelů, kteří dokument podepsali, klikněte na ikonu elektronického podpisu.

- V nabídce Nástroje Možnosti, záložka Zabezpečení stiskněte tlačítko Elektronický podpis
- Stiskněte tlačítko Přidat a vyberte podpisový certifikát
- Takto podepsaný dokument můžete například odeslat dalšímu uživateli k podepsání. Počet podpisů v dokumentu není omezen

Možnosti	<u>? ×</u>
Revize Informace o užival Zobrazení Obecné Úpravy Možnosti šifrování souborů pro tento doku Heslo pro <u>o</u> tevření:	teli Slučitelnost Umístění souborů Tisk Ukládání Zabezpečení Pravopis ument <u>U</u> přesnit
Možnosti sdílení souborů pro tento dokum H <u>e</u> slo pro zápis: Doporučeno jen pro čtení Digitální podpisy Uza <u>m</u> knout dc Možnosti ochrany osobních údajů Při uložení odebrat z vlastností sout	Digitální podpis Podpisy Digitální podpis generovaný sadou Office nelze považovat za právně závazný podpis. Další informace o digitálních podpisech naleznete v Nápovědě. Tento dokument digitálně podepsaly následující osoby:
 Upozornit před tiskem, uložením net komentáře Vylepšit přesnost sloučení uložením Zobrazit skryté značky při otevírání Zabezpečení maker 	Podepisující osoba Vydavatel digitálního ID Datum
Nastavte úroveň zabezpečení pro otev obsahovat viry v makrech, a zadejte jm vývojářů maker.	Připojit certifikáty k nově přidaným podpisům Zobrazit certifikát Nápověda OK

9. WWW ROZHRANÍ CERTIFIKAČNÍ AUTORITY MF ČR

V rámci www stránek MF ČR (<u>www.mfcr.cz</u>) je v sekci **Ministerstvo** pod odkazem **Informační** zdroje nově zřízena stránka **Certifikační autorita resortu MF**. Na této stránce jsou kromě aktuálních informací jednak umístěny odkazy na platnou dokumentaci, jednak odkazy umožňující vyhledání certifikátů a CRL.

9.1. Seznam aktuálně vydaných certifikátů CA

Po kliknutí na odkaz **Seznam aktuálně vydaných certifikátů CA** se objeví následující obrazovka, na níž je seznam certifikátů (sloupec CRT) lokálních certifikačních autorit a aktuálních CRL vydaných těmito autoritami (sloupec CRL):

Dnes je 2.12.2008	Domovská stránka > Ministerstvo > Informační zdroje > Certifikační autorita resortu MF > Seznam vydaných certifikátů				
Aktuální Archiv	Seznam aktuálně vyda	ných	cert	ifikátů CA	
 Ministerstvo financí 					
 Úřední deska MF 	Název CA	CRT	CRL		
 Personální politika MF 	CA Root	<u>.crt</u>	<u>.crl</u>		
Veřejné zakázky	CA IM	<u>.crt</u>	<u>.crl</u>		
Verejne zakazky	CA Úřad	<u>.crt</u>	<u>.crl</u>		
 Výběrová řízení 	CA Test	<u>.crt</u>	<u>.crl</u>		
 Informace dle zákona 	CA FŘ Praha město	<u>.crt</u>	<u>.crl</u>		
106/1999 Sb.	CA Celní správa	<u>.crt</u>	<u>.crl</u>		
 Komunikace s MF 	CA FŘ v Praze	<u>.crt</u>	<u>.crl</u>		
Informační zdroje	CA FŘ v Českých Budějovicích	<u>.crt</u>	<u>.crl</u>		
	CA FŘ v Plzni	<u>.crt</u>	<u>.crl</u>		
 Legislativa 	CA FŘ v Hradci Králové	<u>.crt</u>	<u>.crl</u>		
Instituce - spolupráce	CA FŘ v Ostravě	<u>.crt</u>	<u>.crl</u>		
	CA FŘ v Brně	<u>.crt</u>	<u>.crl</u>		
Instituce - rozcestnik	CA FŘ v Ústí nad Labem	<u>.crt</u>	<u>.crl</u>		
 Zpravodaj MF 					
 Bulletin Odborné knihovny MF 					

Po kliknutí na příslušný certifikát či CRL si vybrané lze stáhnout nebo zobrazit.

9.2. Vyhledávání certifikátů

Po kliknutí na odkaz **Vyhledávání certifikátů** se objeví následující obrazovka, na níž lze zadat parametry specifikující rozsah hledání a následně lze provést vyhledání:

Dnes je 2.12.2008		Domovská stránka > Ministerstvo > Informační zdroje > Certifikační autorita resortu ME > Vyhledávání certifikátů
Aktuální Ar	rchiv	Vyhledávání certifikátů
 Ministerstvo financí 		
 Úřední deska MF 		SN (seriove cislo certifikatu): CN (jméno):
 Personální politika M 	1F	OU (organizační jednotka):
Veřejné zakázky		Title (osobní číslo):
 Výběrová řízení 		Issuer (vystavitel certifikátu): Issued since (vydáno od):
 Informace dle zákona 106/1999 Sb. 	ia	Issued till (vydáno do):
 Komunikace s MF 		Valid (platnost) Jen platne
 Informační zdroje 		Search
 Legislativa 		
 Instituce - spoluprác 	ce	
 Instituce - rozcestník 	ik	
 Zpravodaj MF 		
 Bulletin Odborné knih 	hovny MF	

Po zadání parametrů a kliknutí na odkaz **Search** se zobrazí stránka s certifikáty vyhovujícími zadaným kritériím. Při vyplnění více parametrů se vyhledávají certifikáty vyhovující současně všem kritériím (logická spojka).

Dnes je 2.12.2008	Domovská stránka > Ministerstvo > Informační zdroje > Certifikační autorita resortu MF > Vyhledávání certifikátů									
Aktuální Archiv	Vyhledávání certifikátů	Vyhledávání certifikátů								
 Ministerstvo financí 										
 Úřední deska MF 	SN (senove aslo certifikatu): CN (iméno):									
 Personální politika MF 	OU (organizační jednotka):	OU (organizační jednotka):								
Veřejné zakázky	Title (osobní číslo):									
 Výběrová řízení 	Issuer (vystavitel certifikátu):	Issued since (vydáno od):								
 Informace dle zákona 106/1999 Sb. 	Issued till (vydáno do):	Issued till (vydáno do):								
 Komunikace s MF 	Valid (platnost) Jen platné	Valid (platnost) Jen platné								
 Informační zdroje 	Search									
Legislativa	Ministerstvo financi - CA FR v Brne	CN=Ministerstvo financi - CA FR v Brne, O=MFCR, DC=br, DC=ds, DC=mfcr, DC=cz, C=CZ	SubCA	21.5.2008 10:06:59	21.5.2013 10:16:59	5B924AD6000000000000000000000000000000000000	True	Download PEM		
 Instituce - spolupráce 	Ministerstvo financi - CA FR v Plzni	Ministerstvo financi - CA FR v Pizni CN=Ministerstvo financi - CA FR v Pizni, O=MFCR, DC=pl, DC=ds,						Download PEM		
Instituce - rozcestník	Ministerstvo financi - CA FR v OCN=Ministerstvo financi - CA FR v Ostrave, O=MFCR, DC=os, Ostrave Octave Oc						Download PEM			
 Zpravodaj MF 	Ministerstvo financi - CA Urad	CN=Ministerstvo financi - CA Urad, O=MFCR, DC=urad, DC=mfcr, DC=cz, C=CZ	SubCA	4.3.2008 14:25:45	4.3.2013 14:35:45	7280249100000000003	True	Download PEM		
 Bulletin Odborné knihovny MF 	Ministerstvo financi - CA FR v Usti nad Labem	CN=Ministerstvo financi - CA FR v Usti nad Labem, O=MFCR, DC=ul, DC=ds, DC=mfcr, DC=cz, C=CZ	SubCA	22.5.2008 9:04:47	22.5.2013 9:14:47	607FB69B00000000011	True	Download PEM		
 Katalog multimédií MF 	Ministerstvo financi - CA FR v	CN=Ministerstvo financi - CA FR v Ceskych Budejovicich, O=MFCR,	SubCA	25.11.2008	25.11.2013	613F1914000000000013	True	Download		

Po kliknutí na příslušný certifikát či CRL si vybrané lze stáhnout nebo zobrazit (sloupec obsahující **Download PEM**).

9.3. Vyhledávání certifikátů

Po kliknutí na odkaz **Vyhledávání odvolaných certifikátů (CRL)** se objeví následující obrazovka, na níž lze zadat parametry specifikující rozsah hledání a následně lze provést vyhledání (automaticky se na obrazovce objeví aktuální CRL).:

Dnes je 2.12.2008	Domovská stránka > Ministerstvo > Informační zdroje > Certifikační autorita resortu MF > Vyhledávání odvolaných certifikátů				
Aktuální Archiv	Vyhledávání odvolaných certifikátů (CRL)				
 Ministerstvo financí 					
 Úřední deska MF 	Issuer SN (seriove cisio cerbitikatu vydavatele): Issuer CN (jméno vyadavatele):				
 Personální politika MF 	Issued Since (vydáno od):				
Veřejné zakázky	Issued Till (vydáno do):				
 Výběrová řízení 	Valid (platnost) Jen platne				
 Informace dle zákona 106/1999 Sb 					
 Komunikace s MF 	Inistensivo innario - CA Urad IO.01 [275] 1.12.2008 13:22:12 IS.12.2008 13:22:12 ITUE [Download PEM] Download DER 4inistersivo innario - CA Test Io.0 274 1.12.2008 14:11:34 3.12.2008 14:31:34 True [Download PEM] Download DER				
 Informační zdroje 	Inisterstvo financi - CA Urad 0.0 274 30.11.2008 13:22:11 2.12.2008 13:42:11 True Download PEM Download DER Inisterstvo financi - CA Test 0.0 273 30.11.2008 14:31:34 2.12.2008 14:31:34 True Download PEM Download DER				
▶ Legislativa	Inisterstvo financi - CA FR Praha mesto 0.0 254 1.12.2008 12:20:52 3.12.2008 12:20:52 True Download PEM Download DER Inisterstvo financi - CA FR Praha mesto 0.0 253 30.11.2008 12:20:52 2.12.2008 12:20:52 True Download PEM Download DER				
Instituce - spolupráce	inisterstvo financi - CA Celni sprava 0.0 224 1.12.2008 10:04:33 3.12.2008 10:24:33 True Download PEM Download DER				
 Instituce - rozcestník 	Inisterstvo financi - CA Celni sprava 0.0 223 30.11.2008 10:04:33 2.12.2008 10:24:33 True Download PEM Download DER 4inisterstvo financi - CA FR v Praze 0.0 203 1.12.2008 11:49:42 3.12.2008 12:09:42 True Download PEM Download DER				
 Zpravodaj MF 	inisterstvo financi - CA FR v Plzni 0.0 202 1.12.2008 15:02:36 3.12.2008 15:22:36 True Download PEM Download DER				
 Bulletin Odborné knihovny MF 	Inisterstvo financi - CA FR v Praze 0.0 202 30.11.2008 11:49:42 2.12.2008 12:09:42 True Download PEM Download DER Inisterstvo financi - CA FR v Plzni 0.0 201 30.11.2008 15:02:36 2.12.2008 15:22:36 True Download PEM Download DER				

Po zadání parametrů a kliknutí na odkaz **Search** se zobrazí stránka s CRL vyhovujícími zadaným kritériím. Při vyplnění více parametrů se vyhledávají certifikáty vyhovující současně všem kritériím (logická spojka). Příklad: hledání všech CRL vydaných do 12.11.2008:

Aktuální Archiv Vyhledáv	ní odvolaných certifikátů (CRL)
 Ministerstvo financí 	
 Úřední deska MF Issuer CN (ja 	ino vyadavatele):
Personální politika MF Issued Since	vydáno od):
 Veřejné zakázky Issued Till (v 	Jáno do): 12.11.2008
Výběrová řízení	Jen platné 🔽
Informace dle zákona Search Misisteratura 6	
Komunikace s MF Ministerstvo fi	and - CA Orad 0.0 [279] 1.12.2008 15:22:12 [5.12.2008 15:42:12 [True Download PEN Download DER and - CA Test 0.0 [274] 1.12.2008 14:11:34 [3.12.2008 14:31:34 [True Download PEM Download DER
Informační zdroje Ministerstvo fi Ministerstvo fi	anci - CA Urad 0.0 274 30.11.2008 13:22:11 2.12.2008 13:42:11 True Download PEM Download DER anci - CA Test 0.0 273 30.11.2008 14:11:34 2.12.2008 14:31:34 True Download PEM Download DER
Legislativa	anci - CA FR Praha mesto 0.0 254 1.12.2008 12:00:52 3.12.2008 12:20:52 True Download PEM Download DER
Instituce - spolupráce Ministerstvo fi	and - CA PR Prana mesto 0.0 [253 [30, 11,2008 12:0052 [2, 12, 2008 12:2052] [The [Download PEN] Download DER anci - CA Celni sprava 0.0 [224 1.12,2008 10:04:33 [3, 12,2008 10:24:33] True [Download PEN] Download DER
Instituce - rozcestník	anci - CA Celni sprava 0.0 223 30.11.2008 10:04:33 2.12.2008 10:24:33 True Download PEM Download DER
Zpravodaj MF Ministerstvo fi	and - CA FR v Plzni 0.0 [202] 1.12.2008 15:02:36 [3.12.2008 15:22:36 [True Download PEM Download DER
Bulletin Odborné knihovny MF Ministerstvo fi	anci - CA FR v Praze 0.0 202 30.11.2008 11:49:42 2.12.2008 12:09:42 True Download PEM Download DER anci - CA FR v Plzni 0.0 201 30.11.2008 15:02:36 2.12.2008 15:22:36 True Download PEM Download DER

Po kliknutí na příslušný certifikát či CRL si vybrané lze stáhnout nebo zobrazit (sloupec obsahující **Download PEM** nebo **Download DER**).

Systém PKI Část 2: PRÁCE S AUTORITOU ČASOVÉ ZNAČKY

10. ÚVOD

Jedním z rozšíření služeb poskytovaných novou infrastrukturou PKI, je možnost používání tzv, časových značek. Časová značka je speciální elektronický (digitální) podpis, který v sobě zahrnuje údaj o přesném čase přidělení časové značky (tedy vystavení podpisu). Podpis sám je zajišťován důvěryhodnou aplikací, tzv. autoritou časových značek (časovou autoritou označovanou často jako TSA). Tím je důvěryhodným způsobem stanoven časový okamžik existence dat, ke kterým byla daná časová značka vystavena – data musela existovat před časovým okamžikem uvedeným ve značce, tedy nejpozději v udávaném čase. Tohoto faktu se nejčastěji využívá v případech, kdy je např. nutné zajistit dokument tak, aby později bylo možné prokázat jeho existenci v určité době. Jelikož TSA nezkoumá totožnost žadatele, časová značka nemůže obsahovat identifikaci žadatele. Tudíž časová značka není důkazem o tom, že nějaký dokument měla v okamžiku před vydáním časové značky v držení konkrétní osoba.

Pro účely využití časových značek v rámci resortu Ministerstva financí ČR byla vybudována časová autorita (služba běžící samostatně bez možnosti ovlivnění uživateli) a instalován tzv. klient TSA, který umožňuje práci s časovými značkami.

11. PRÁCE S APLIKACÍ TSA KLIENT

Následující kapitola je určena především pro běžné uživatele a popisuje způsob práce s Autoritou časové značky (dále též TSA) MF ČR z hlediska obsluhy klientské aplikace TSA Klient. Uživatel zde nalezne podrobně popsaný postup vyžádání a ověření časové značky, což jsou dvě operace, které bude provádět nečastěji, a další užitečné informace.

Popisovaná aplikace TSA Klient je určena jednak pro vyžádání časové značky k vybranému souboru prostřednictvím protokolu HTTP nebo HTTPS, jednak pro ověření platnosti časové značky. Časová značka je vydávána k určitému datovému souboru a je zpravidla ukládána do souboru s příponou *.tst. Vymazáním tohoto souboru ztratí uživatel možnost podávat důkaz o existenci souboru s nezměněnými daty v čase.

Poznámka: Zatímco k vyžádání časové značky k vybranému souboru je nutné připojení k telekomunikační síti s dostupnou Autoritou časové značky, při ověřování časové značky je připojení k síti nutné pouze pro stažení seznamu odvolaných certifikátů.

11.1. Spuštění aplikace

Po spuštění aplikace poklepáním na ikonu **TSA Klient** [™]umístěnou na ploše nebo klepnutím na příkaz **TSA Klient** v nabídce **Start** ⇒ **Programy** ⇒ **TSAKlient** se zobrazí hlavní okno aplikace, které obsahuje seznam časových značek a detailní pohled na jednotlivé položky tohoto seznamu. Položkou seznamu je časová značka.



Obrázek 1 – Hlavní okno aplikace TSA Klient

11.2. Panel nástrojů

Panel nástrojů aplikace TSA Klient Panel nástrojů aplikace TSA Klient Navního okna aplikace pod nabídkou. Tlačítka panelu nástrojů umožňují zrychlené vyvolání požadovaných příkazů bez nutnosti otevírat pro zadání příkazu nabídku aplikace. Funkce jednotlivých tlačítek panelu nástrojů jsou popsány v následujících podkapitolách.

11.3. Vyžádání nové časové značky ke zdrojovému souboru

Novou časovou značku pro zvolený zdrojový soubor získáte dle následujícího postupu:

Klepnutím na tlačítko [™] v panelu nástrojů nebo příkazem nabídky Časové razítko ⇒
 Nové zobrazte průvodce vyžádáním časové značky.

V prvním okně zadejte zdrojový soubor (tj. soubor, ke kterému chcete vydat časovou značku). Zdrojový soubor můžete zadat tak, že do odpovídajícího textového pole vepíšete název zdrojového souboru s příponou a celou cestou, nebo klepnutím na tlačítko s ikonou

složky zobrazíte standardní dialogové okno **Otevřít** operačního systému a zdrojový soubor vyberete v něm. Po zadání zdrojového souboru klepněte na tlačítko **Dalš**í.

- Stejným způsobem jako v předchozím kroku zadejte název souboru časové značky a klepněte na tlačítko **Další**. Aplikace přednastaví původní název souboru s příponou ".tst", který můžete libovolně měnit.
- Pokud je vše v pořádku, dalším klepnutím na tlačítko Další odešlete žádost o vydání časové značky na server TSA.
- Po obdržení odpovědi serveru TSA je přijatá časová značka ověřena a zobrazena potvrzující informace. Klepnutím na tlačítko dokončit provedete dokončení celé operace a vložení právě přijaté a zkontrolované časové značky do seznamu. Podrobné údaje o časové značce jsou zobrazeny v pravém panelu.

11.4. Ověření již existující časové značky

Již existující časovou značku můžete kdykoliv ověřit vzhledem k vybranému zdrojovému souboru dle následujícího postupu:

- Klepnutím na tlačítko [™] v panelu nástrojů nebo příkazem nabídky Časové razítko ⇒
 Ověření zobrazte průvodce ověřením existující časové značky a odpovídajícího zdrojového souboru.
- Ve zobrazeném dialogovém okně zadejte soubor s časovou značkou. Také tento soubor můžete zadat tak, že do příslušného textového pole vepíšete název souboru časové značky

s příponou a celou cestou, nebo klepnutím na tlačítko s ikonou složky i zobrazíte standardní dialogové okno **Otevřít** operačního systému a soubor časové značky vyberete v něm. Po zadání souboru časové značky klepněte na tlačítko **Další**.

- Po provedení kontroly struktury časové značky vyberte stejným způsobem jako v předchozím kroku odpovídající zdrojový soubor (tj. soubor, k němuž byla zvolená časová značka vydána).
- Pokud ponecháte vstupní pole prázdné a klepnete na tlačítko Další, nebude ke značce přiřazen žádný zdrojový soubor (tato možnost slouží k prohlížení časových značek).

- Jestliže vyberete existující soubor a klepnete na tlačítko Další, je provedena kontrola miniatur (HASH hodnot) tohoto souboru a miniatury z časové značky. Pokud jsou tyto miniatury shodné (jedná se o platný pár dokument časová značka) a je platný i digitální podpis časové autority, dojde k zobrazení zprávy o úspěšném ověření časové značky.
- Ověřenou časovou značku lze vložit do aktuálně otevřeného seznamu a jednotlivé položky časové značky jsou zobrazeny v detailním pohledu vpravo.

11.5. Smazání časové značky ze seznamu

Aktuálně vybranou časovou značku lze odstranit ze seznamu časových značek klepnutím na tlačítko v panelu nástrojů nebo příkazem nabídky Časové razítko ⇒ Smazat. Tato akce maže pouze záznam o umístění zdrojového souboru a souboru s časovou značkou ze seznamu časových značek, vlastní soubory zůstanou uloženy a lze je kdykoliv do seznamu vložit prostřednictvím ověření již existující časové značky popsané v kapitole 2.4.

11.6. Obsah detailního pohledu

S TSA Klient	
Seznam Časové razítko Nápověda	
D 🛎 🖬 🕲 🥹 🗞 🤌 🚔 የ	
Dokument.doc.tst	t.doc.tst
Párovací informa	Ce
Zdrojový soubo	pr C:\Dokument.doc
Soub s časovým razítke	n C:\Dokument.doc.tst
Struktura razítk	a V pořádku
Podpis razitk	a V pořádku
Shoda miniate	ir Souhlasí
Výsledek ověře	ní Časové razítko je v pořádku a bylo vydané ke zdrojovému souboru.
Podrobnosti	
Čas (UTC) 2008/04/29 14:11:16,433
Lokální ča	s 2008/04/29 16:11:16,433
Sériové čís	OEC: 346 HEX: 015A
Verz	e 1
Politik	a 1.2.203.6947.2.2.1
Algoritmus miniatur	y SHA1
Miniatu	a 07 F2 0F 99 35 3C 66 50 CC 87 BB E4 98 E8 8D F0 00 43 06 09
Párovací čísl	DEC: 2028222126920509412 HEX: 1C25B14748AF27E4
Certifikát časové	autority <u>Zobrazit detaily</u>
Předmo	et S=CZ, O=MFCR, CN=Time Stamping Authority
Platnost od (UTC) 2008/03/28 15:45:47
Platnost do (UTC) 2013/03/28 15:55:47
	M
HOLOVO	NUM

Obrázek 2 – Detailní pohled aplikace TSA Klient

Tabulka **Párovací informace** zobrazuje souhrnný přehled o dvojici časová značka – zdrojový soubor (dokument). Dále obsahuje informace o výsledku kontroly struktury časové značky, digitálního podpisu časové autority TSA uvedeného na časové značce, shody miniatury zdrojového souboru a miniatury obsažené v časové značce a souhrnnou informaci o výsledku kontrol.

Tabulka **Podrobnosti** obsahuje jednotlivé položky časové značky.

V tabulce **Certifikát časové autority** naleznete vybrané informace o certifikátu časové autority a tlačítkem **Zobrazit detaily** můžete vyvolat standardní dialogové okno operačního systému s podrobnými informacemi o certifikátu časové autority.

11.7. Nastavení

Klepnutím na tlačítko ¹∕2² v panelu nástrojů nebo příkazem nabídky **Seznam ⇒ Nastaven**í lze zobrazit dialogové okno **Nastaven**í.

Měnit nastavení aplikace mohou pouze uživatelé, kteří mají tuto činnost povolenou administrátorem, ostatním uživatelům slouží dialogové okno **Nastavení** pouze k prohlížení nastavených hodnot!

Nastavení 🛛
URL časové autority
http://tsa.mfcr.cz:8080
Připojení k internetu
Použít nastavení Internet Exploreru (doporučeno)
O Proxy server: Port: 0
O Přímé připojení do sítě internet
Parametry protokolu HTTP/S
Použít hlavičku Content-Type
Použít hlavičku Content-Length
Politika časové autority
1.2.203.6947.2.2.1
Při ověřování podpisu časové autority kontrolovat
O Podpis a řezec certifkátů
Podpis, řetězec a odvolání certifkátů
OK Storno Nastavit výchozí hodnoty

Obrázek 3 – Dialogové okno Nastavení aplikace TSA Klient

Jednotlivé skupiny dialogového okna Nastavení mají následující význam:

- URL časové autority internetová adresa serveru časové autority.
- Připojení k internetu určuje nastavení připojení k internetu.

- Parametry protokolu HTTP/S nastavení hlaviček posílaných při komunikaci se serverem časové autority.
- Politika časové autority identifikátor OID politiky časové autority.
- Při ověřování podpisu časové autority kontrolovat nastavení ověření podpisu časové autority.

11.8. Otevření seznamu časových značek

Seznam časových značek lze otevřít ze souboru s příponou *.tsp (TSA project). Tento soubor obsahuje pouze názvy souborů jednotlivých párů časová značka – zdrojový soubor. Po spuštění aplikace automaticky otevírá naposledy otevřený seznam časových značek.

Uživatel navíc může otevřít kterýkoliv již existující seznam časových značek klepnutím na tlačítko ✓ v panelu nástrojů nebo příkazem nabídky **Seznam ⇔ Otevřít**. Čtyři naposledy otevřené seznamy časových značek lze také otevřít klepnutím na odpovídající název souboru v nabídce **Seznam**.

11.9. Uložení seznamu časových značek

Aktuální stav seznamu časových značek lze uložit do právě otevřeného souboru *.tsp (TSA project) klepnutím na tlačítko
v panelu nástrojů nebo příkazem nabídky Seznam
v Uložit. Při ukončení aplikace je aktuální stav seznamu časových značek ukládán automaticky.

Příkazem nabídky **Seznam ⇔ Uložit jako** je možné uložit aktuální stav seznamu časových značek do jiného souboru.

11.10. Vytvoření nového seznamu časových značek

Nový seznam časových značek lze vytvořit klepnutím na tlačítko [□] v panelu nástrojů nebo příkazem nabídky **Seznam ⇒ Nový**. Nově vytvořený seznam je prázdný a má přiřazeno implicitní jméno souboru **Bez názvu.tsp**, které lze změnit příkazem **Uložit jako**.

11.11.Tisk

Obsah detailního pohledu lze vytisknout klepnutím na tlačítko 🎒 v panelu nástrojů

11.12.Nápověda

Integrovanou nápovědu aplikace TSA Klient lze zobrazit klepnutím na tlačítko ¹ v panelu nástrojů.

11.13. Ukončení aplikace

Aplikaci TSA Klient lze ukončit standardním způsobem klepnutím na tlačítko i ve tvaru křížku umístěné v záhlaví okna aplikace nebo příkazem nabídky Seznam ⇔ Konec.

12. ŘEŠENÍ PROBLÉMŮ

12.1. Problém s generováním karty

Popis problému

• Při obnově karty se zobrazí chybová zpráva

Řešení

- Zkontrolujte obsah kapacitu karty problém s nedostatkem místa pro další certifikát
- Kontaktujte pracovníka IT

12.2. Problém s použitím certifikátu v Outlooku

Popis problému

• Při pokusu o podepisování zprávy se nezobrazují tlačítka pro podpis

Řešení

Zkontrolujte, zda je certifikát zaregistrován v systému, případně proveďte registraci (možno i opakovaně)



Spusťte GemSafe Toolbox, v sekci certifikáty zadejte PIN a tlačítko Přihlášení, Stiskněte tlačítko Registrovat vše

• Kontaktujte pracovníka IT

12.3. Problém s šifrováním pošty

Popis problému

• Při pokusu o šifrování pošty je zobrazena informace – Nelze šifrovat poštu tomuto příjemci

Řešení

- Příjemce nemá vygenerovaný certifikát nelze zprávu šifrovat
- Příjemce má k dispozici kartu, certifikát není zaregistrovaný v doméně kontaktujte pracovníka IT

12.4. Problém se změnou PINu

Popis problému

 Při pokusu o změnu PINu, nebo odblokování karty je zobrazena informace Není možné změnit PIN

Řešení

 Zkontrolujte politiku, zda heslo odpovídá lokální politice PINů (minimální délka – 6 číslic, maximální délka – 8 číslic, PIN se nesmí opakovat)

13. ZÁVĚREČNÉ USTANOVENÍ

Tato Příručka uživatele, vydaná pro resortní Certifikační autoritu Ministerstva financí České republiky, nabývá účinnosti dnem stanoveným v tabulce Historie dokumentu v úvodu této Příručky.

14. PŘÍLOHA Č.1 - SEZNAM KONTAKTŮ NA SPOLUPRACUJÍCÍ SUBJEKTY A JEJICH DOSAŽITELNOST

Jméno	Organizace	Problém	E-mail, helpdesk	Telefon
	MF	Problém s obnovou karty	helpdesk	
	MF	Problém se změnou PINu	<mark>helpdesk</mark>	
	MF	Problémy s používáním certifikátů v aplikacích	helpdesk	
	FŘ pro hl. m Prahu			
	<mark>FŘ v Brně</mark>			
	FŘ v Českých Budějovicích			
	FŘ v Hradci Králové			
	FŘ v Ostravě			
	<mark>FŘ v Plzni</mark>			
	<mark>FŘ v Praze</mark>			
	FŘ v Ustí n. Labem			
	GŘC			
	CŘ v Ostravě			
	<mark>Generální</mark> finanční ředitelství			

Na úrovni finanční úřadů a celních úřadů je kontaktním subjektem pracoviště IT podpory

15. PŘÍLOHA Č. 2 - FORMULÁŘE ŽÁDOSTÍ

Na následujících stránkách jsou uvedeny formuláře dokumentů používaných v provozu systému PKI. Jedná se o následující dokumenty:

- Žádost o vydání uživatelské čipové karty / uživatelského certifikátu
- Žádost o vydání autentizačního tokenu operátora registrační autority / certifikátu operátora RA
- Protokol o převzetí autentizačního tokenu operátora RA
- Žádost o zneplatnění certifikátu
- Žádost o zneplatnění certifikátu operátora RA
- Žádost o vydání certifikátu aplikace/serveru
- Protokol o převzetí certifikátu aplikace/serveru
- Žádost o zneplatnění certifikátu aplikace/serveru
- Žádost o vydání certifikátu doménového řadiče
- Protokol o vrácení čipové karty
- Protokol o vrácení autentizačního tokenu RA

Žádost o vydár	ní uživate	elské čipové karty *)	
Žádost o vydání uživatelského certifikátu *)			
st o vydání testo	ovacího u	uživatelského certifikátu *)	
:			
otky/útvar (ÚFO, CŘ,	CÚ, útvaru	MF/GŘC, územní pracoviště ÚZSVM) :	
ámen(a) s certifikačr to žádosti. Souhlasíı /dání čipové karty / c	ní politikou m s použití certifikátu*)	u**), příručkou uživatele PKI a povinnostmi ím osobních údajů pro fungování systému *).	
ho zaměstnance s v	ydání čipov	ové karty / certifikátu [*]) pro výše uvedeného	
zaměstnance tky/útvaru			
Podpis Vedoucího zaměstnance			
n od správce CA pře	vzal(a) čipo	oovou kartu/certifikát [*])	
Podpis uživatele:		Podpis předávajícího:	
	Žádost o vydár Žádost o vydár st o vydání testo st o vydání testo tky/útvar (ÚFO, CŘ, ámen(a) s certifikačn o žádosti. Souhlasín vdání čipové karty / o ho zaměstnance s v zaměstnance ky/útvaru	Žádost o vydání uživat Žádost o vydání uživat st o vydání testovacího tky/útvar (ÚFO, CŘ, CÚ, útvaru ámen(a) s certifikační politikou o žádosti. Souhlasím s použit rdání čipové karty / certifikátu ho zaměstnance s vydání čipo zaměstnance ky/útvaru o zaměstnance ho d správce CA převzal(a) čip	

*) Nehodící se škrtněte

**) Text Certifikační politiky je uveden na webové adrese:

Poučení:

Uživatelská čipová karta se soukromým klíčem a certifikátem je digitálním průkazem, pomocí kterého se držitel karty identifikuje při přístupu do PC a stanovených aplikací. Držitel karty je povinen se chovat tak, aby nemohlo dojít k jejímu zneužití. Pro zajištění objektové bezpečnosti je ČK využívána též jako vstupní identifikační průkaz. Z tohoto důvodu musí být i vizuálně personifikována. Obsah vizuální personifikace: označení rezortní organizační složky, která ČK vydala; osobní číslo; jméno a příjmení, popřípadě titul; datum vystavení; fotografie.

Povinnosti při užívání autentizační čipová karta

- Čipová karta se nesmí půjčovat jiným osobám.
- Hodnoty uživatelského PIN nesmí být prozrazeny jiným osobám.
- Čipová karta nesmí být ponechána ve čtečce čipových karet, pokud držitel karty odchází od počítače, ke kterému je čtečka připojena.
- Ztráta čipové karty nebo podezření z její zneužití musí být okamžitě hlášeno příslušné registrační autoritě, která zajistí revokaci uživatelského certifikátu podle postupu uvedeném v provozní dokumentaci.
- Pokud se změní údaje uvedené v certifikátu, který je v kartě uložen, je třeba vzdáleně žádat o vydání nového certifikátu.
- Před vypršením platnosti certifikátu uloženého v kartě, nebo po jeho revokaci, je třeba žádat na RA o vygenerování nového certifikátu vystavení, nebo o novou kartu.
- Uživatel je povinen čipovou kartu odevzdat zpět příslušné registrační autoritě po ukončení pracovně právního nebo smluvního vztahu, nebo se ČK stane nefunkční.

Žádost o v	ydání autentizačního tokenu operátora RA *)
Žádost	o vydání certifikátu pro operátora RA *)
Údaje o operátorovi:	
Titul:	
Jméno:	
Příjmení:	
Osobní číslo:	
Organizační jednotky/út	var (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :
Název	
Adresa	
Byl(a) jsem seznámen	(a) s Certifikační politikou**).
Žádám o vydání auten	tizačního tokenu operátora registrační autority *)
Žádám o vydání certifi	kátu operátora registrační autority*)
Datum:	
Podpis zaměstnance:	
Souhlas vedoucího registrační autority pro	zaměstnance s vydáním autentizačního tokenu operátora o výše uvedeného operátora.*)
Souhlas vedoucího za pro výše uvedeného o	městnance s vydáním certifikátu operátora registrační autority perátora.*)
Jméno vedoucího zaměstnance organizační jednotky/útvaru:	
Datum:	
Podpis vedoucího zaměstnance :	

- *) **Nehodící se škrtněte** (operátor registrační autority, kterému již byla vydána čipová karta s uživatelským certifikátem, může požádat o vydání a nahrání certifikátu pro operátora registrační autority na tento token)
- **) Text Certifikační politiky je uveden na adrese

Protokol o př	ŕevze	etí autentizačního to	okenu o	operátora RA	
Údaje o zaměstn	anci:				
Titul:					
Jméno:					
Příjmení:					
Osobní číslo:					
Organizační jedno	otky/ú	tvar (ÚFO, CŘ, CÚ, útvaru	u MF/GŘ(C, územní pracoviště ÚZSVM) :	
Název					
Údaje o přebíran	Údaje o přebírané autentizačního tokenu:				
Číslo tokenu:					
Potvrzuji, že jse číslem.	em o	d správce CA převzal(a	i) autent	izační token s výše uvedeným	
Jméno zaměstna	nce:				
Datum:					
Podpis zaměstnance:					
Datum		jméno správce CA		podpis předávajícího	

Žádost o zneplatnění certifikátu				
Údaje o	o zaměstn	anci:		
Titul:				
Jméno:				
Příjmen	ıí:			
Osobní	číslo:			
Organiz	ační jedno	otky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :		
Název				
Číslo ce	ertifikátu:			
Žádám	0:			
zne	zneplatnění certifikátu s uvedeným číslem			
zne	eplatnění	všech certifikátů vydaných pro uvedeného zaměstnance		
Důvod 2	Důvod žádosti:			
ztr	ztráta čipové karty			
pro	prozrazení PIN			
od	odchod zaměstnance			
zm	změna údajů uvedených v certifikátu			
Jméno z	zaměstnar	nce:		
Datum:				
Podpis zaměstnance:				
Jméno vedoucího zaměstnance:				
Datum:				
Podpis v zaměstr	vedoucího nance:			

Pokud je důvodem revokace certifikátu odchod zaměstnance nebo změna údajů uvedených v certifikátu, stačí podpis vedoucího zaměstnance. V ostatních případech stačí podpis zaměstnance.

Žádost o zneplatnění certifikátu operátora RA				
Úda	je o operáto	rovi:		
Titul	:			
Jmé	no:			
Příjn	není:			
Oso	bní číslo:			
Orga	anizační jedno	otky/útvar (ÚFC	D, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :	
Náze	ev			
Číslo	o certifikátu:			
Žáda	ám o:			
	zneplatnění	neplatnění certifikátu s uvedeným číslem		
	zneplatnění všech certifikátů vydaných pro uvedeného zaměstnance			
Dův	od žádosti:			
	ztráta token	áta tokenu		
	prozrazení	rozrazení PIN		
	odchod zan	něstnance		
	změna údaj	na údajů uvedených v certifikátu		
Jmé	méno zaměstnance:			
Datum:				
Podpis zaměstnance:		nce:		
Jméno vedoucího zaměstnance organizační jednotky/útvaru:) anizační		
Datum:				
Pod zam	ois vedoucího ěstnance :)		

Pokud je důvodem revokace certifikátu odchod zaměstnance nebo změna údajů uvedených v kartě, stačí podpis vedoucího zaměstnance organizační jednotky/útvaru. V ostatních případech stačí podpis zaměstnance.

Žádost o vydání certifikátu aplikace/serveru)*		
Žádost o vydání testovacího certifikátu aplikace/serveru)*		
Údaje o aplikaci/serv	/eru:	
DC 2		
(<i>ds</i> pro Daňovou <i>urad</i> pro ministerstvo	správu, financí)	
DC.3		
(jméno subdomény Fl br pro FŘ Brno) :	Ř, např.	
OU (číslo ÚFO) :		
CN - jméno aplikace/s	erveru :	
DNS jméno (nepovinn	né) :	
Byl(a) jsem seznámo o certifikát pro ap Digitální žádost o ce	en(a) s (likaci by rtifikát a	Certifikační politikou. Generování klíčů a digitální žádosti ylo provedeno v souladu s tímto Certifikační politikou. její textový opis jsou nedílnou součástí této žádosti.
Organizační jednotky/	útvar (ÚF	FO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :
Název		
Jméno správce:		
Osobní číslo:		
Druh a číslo dokladu:		
Kontaktní e-mail:		
Kontaktní telefon:		
Datum:		
Podpis správce:		
Žádám o vydání cert	ifikátu p	ro výše uvedenou aplikaci/server.
Jméno vedoucího zaměstnance organizační jednotky/útvaru		
Datum:		
Podpis vedoucího zaměstnance		

*) Nehodící se škrtněte

Protokol o převzetí certifikátu aplikace/serveru)*			
Protokol o převzetí	testov	/acího certifikátu aplikace/serveru)*	
Údaje o aplikaci a certifi	kátu		
Jméno aplikace tak, jak je uvedeno v certifikátu			
Sériové číslo certifikátu:			
Potvruji, že jsem převz instaloval(a) do výše uve	al(a) ce edené ap	rtifikát s výše uvedeným sériovým a tento certifikát olikace.	
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :			
Název			
Jméno správce aplikace:			
Datum:			
Podpis správce aplikace:			
Jméno správce CA			
Datum:			
Podpis správce CA			

*) Nehodící se škrtněte

Г

Žác	lost o zneplatně	ní cert	ifikátu aplikace/serveru
Úda	je o správci aplikace	:	
Titul	:		
Jmé	no:		
Příjn	není:		
Oso	bní číslo:		
Orga	anizační jednotky/útva	r (ÚFO, (CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :
Náz	ev		
Úda	je o aplikaci:		
Jmé uvec	no aplikace tak, jak je Jeno v certifikátu		
Séri	ové číslo certifikátu		
Žáda	ám o:		
	zneplatnění certifiká	itu s dar	ným sériovým číslem
	zneplatnění všech o	ertifikát	ů vydaných pro danou aplikaci
Dův	od žádosti:		
	zničení soukromého	o klíče a	plikace
	prozrazení soukrom	ého klíč	e aplikace
	změna údajů uvede	ných v c	ertifikátu
Jmé zam jedn	no vedoucího ěstnance organizační otky/útvaru		
Datu	ım:		
Pod zam	pis vedoucího ěstnance		
Jmé	no správce aplikace:		
Datu	ım:		
Pod	pis správce aplikace:		

Žádost o vydání certifikátu doménového řadiče			
Údaje doménového	řadiče:		
DC.0 :	CZ		
DC.1 :	mfcr		
DC.2 :			
DC.3 :			
DC.4 :			
OU :	Domain Controllers		
CN :			
DNS jméno :			
GUID :			
Byl(a) jsem seznám o certifikát pro ap Digitální žádost o ce	en(a) s Certifikační politikou. Generování klíčů a digitální žádosti likaci bylo provedeno v souladu s tímto Certifikační politikou. rtifikát a její textový opis jsou nedílnou součástí této žádosti.		
Jméno správce:			
Osobní číslo:			
Organizační jednotky/	útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :		
Název:			
Druh a číslo dokladu:			
Kontaktní e-mail:			
Kontaktní telefon:			
Datum:			
Podpis správce:			
Žádám o vydání cert	ifikátu pro výše uvedený doménový řadič.		
Jméno vedoucího zaměstnance organizační jednotky/útvaru			
Datum:			

Podpis vedoucího	
zaměstnance	

Protokol o vrácení čipové karty

Údaje o zaměstnanci:			
Titul:			
Jméno:			
Příjmení:			
Osobní číslo:			
E-mail adresa:			
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, pracoviště ÚZSVM) :			
Údaje o čipové kartě:			
Číslo karty:			
Stav vrácené čipové karty :			
Datum:			
Podpis zaměstnance :			
Jméno operátora RA:			
Podpis operátora RA:			


Protokol o vrácení autentizačního tokenu operátora RA

Údaje o operátorovi RA:			
Titul:			
Jméno:			
Příjmení:			
Osobní číslo:			
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, pracoviště ÚZSVM) :			
Název			
Údaje o autentizačním tokenu:			
Číslo tokenu:			
Stav vráceného autentizačního tokenu:			
Datum:			
Podpis zaměstnance:			
Jméno správce CA:			
Podpis správce CA:			

Systém PKI

Žádost o vydání kvalifikovaného certifikátu potvrzení o zaměstnaneckém poměru (platné pro resort MF)

Žadatel

Titul:	Jméno:	Přijmení:	Titul za:
R.Č.:		bytem:	
Č.OP.:		·····	
Osobní číslo:			
E-mail adresa:			
Pracovní zařazení (funkce):			
Žádám o vydání zaměstnano osobních údajů pro potřeby z	eckého kvalifikované zpracování žádosti u	ho certifikátu a souhlasím I.CA	s elektronickým zpracováním výše uvedenýc
Datum			
			(Podpis žadatele)
Potvrzení o zaměstnanecké	n poměru		
Tímto potvrzujeme, že žadat	el pan/paní je k dneš	śnímu dni zaměstnancem	IČ
Název organizace:			
Organizační složka:			
Adresa organizační složky:			
Vyjádření nadřízeného vedo	ucího zaměstnance		
Zdůvodnění žádosti:			
Datum		Podpis	
Souhlas oprávněné osoby s Souhlasíme s tím, aby výs zaměstnanecký kvalifikovan	vydáním kvalifikovar še uvedenému zai ý certifikát s uvedení	ného certifikátu městnanci byl společnos m názvu naší společnosti .	stí První certifikační autorita, a.s., vydá
V	dne	 Po	dpis
jméno a fu	nkce		oprávněná osoba
oprávněné osoby k jednár	ní za organizaci		

Systém PKI

Žádost o vydání systémového kvalifikovaného certifikátu plná moc (platné pro resort MF)

Tímto žádám o vydání kvalifikovaného systémového certifikátu s následujícím vyplnění položek

Jméno certifikátu:	
Název organizace:	IČ:
Adresa:	
E-mail adresa:	
Účel použití systémového certifikátu:	
	Datum:
	Podpis
Jméno a funkce a organizační útvar,	

žadatele o systémový kvalifikovaný certifikát

Plná moc

Níže podepsaný zmocnitel dává tímto plnou moc zmocr	iěnci
Jméno, přijmení:	Titul
Adresa trvalého bydliště:	
Datum narození:	Rodné číslo:
Číslo OP:	Osobní číslo:
k těmto úkolům souvisejícím s poskytnutí služeb I.CA, a	.s.:
 podat žádost o výše uvedený certifikát a tento o 	certifikát převzít
 podat žádost o následný certifikát 	
 podat žádost zneplatnění certifikátu 	
Zmocnitel:	
Název organizace:	IČ:
Sídlo organizace:	
Osoba oprávněná jednat za organizaci:	
Funkce:	
Jméno, přijmení:	Titul
Adresa trvalého bydliště:	
Datum narození:	Rodné číslo:
Číslo OP:	Osobní číslo:
Tato plná moc má účinnost do:	
Vdne	
	podpis zmocněnce
	(podle podpisového vzoru)
	podpis zmocnitele