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

Systém PKI

OBSAH

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.

Systém PKI

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 http://ca/CMS.

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)

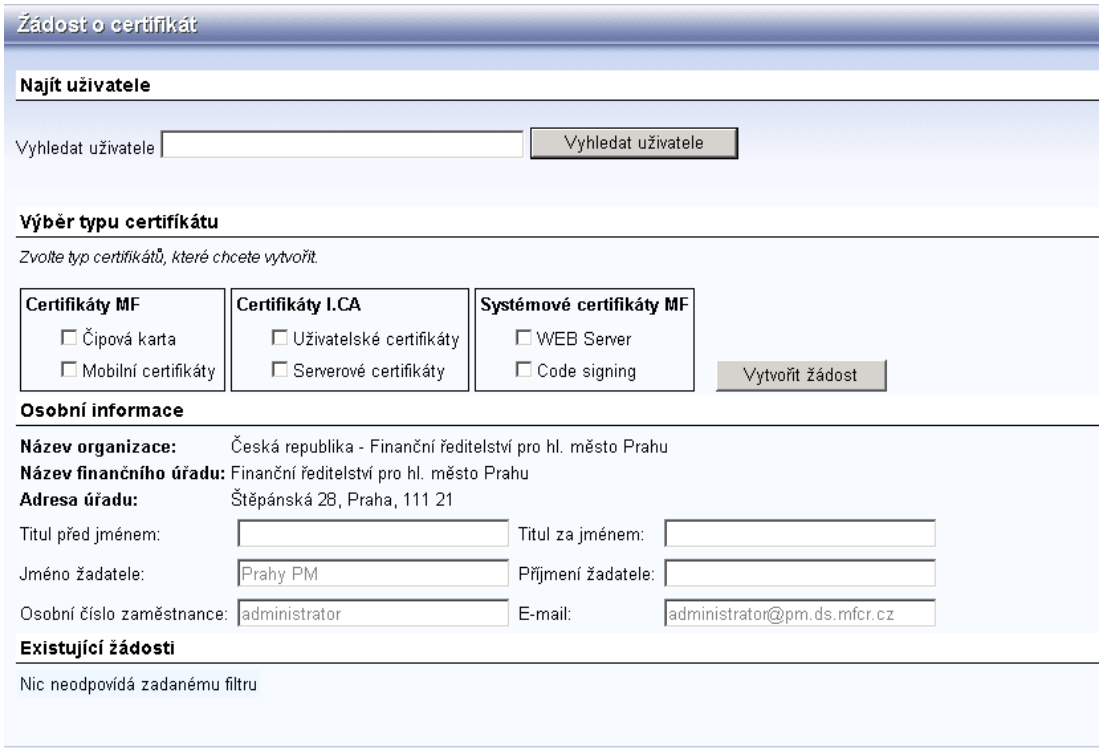
- odblokovat kartu
- změnit PIN na kartě
- zobrazit informace o kartě včetně certifikátů na ní uložených

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



Systém PKI

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

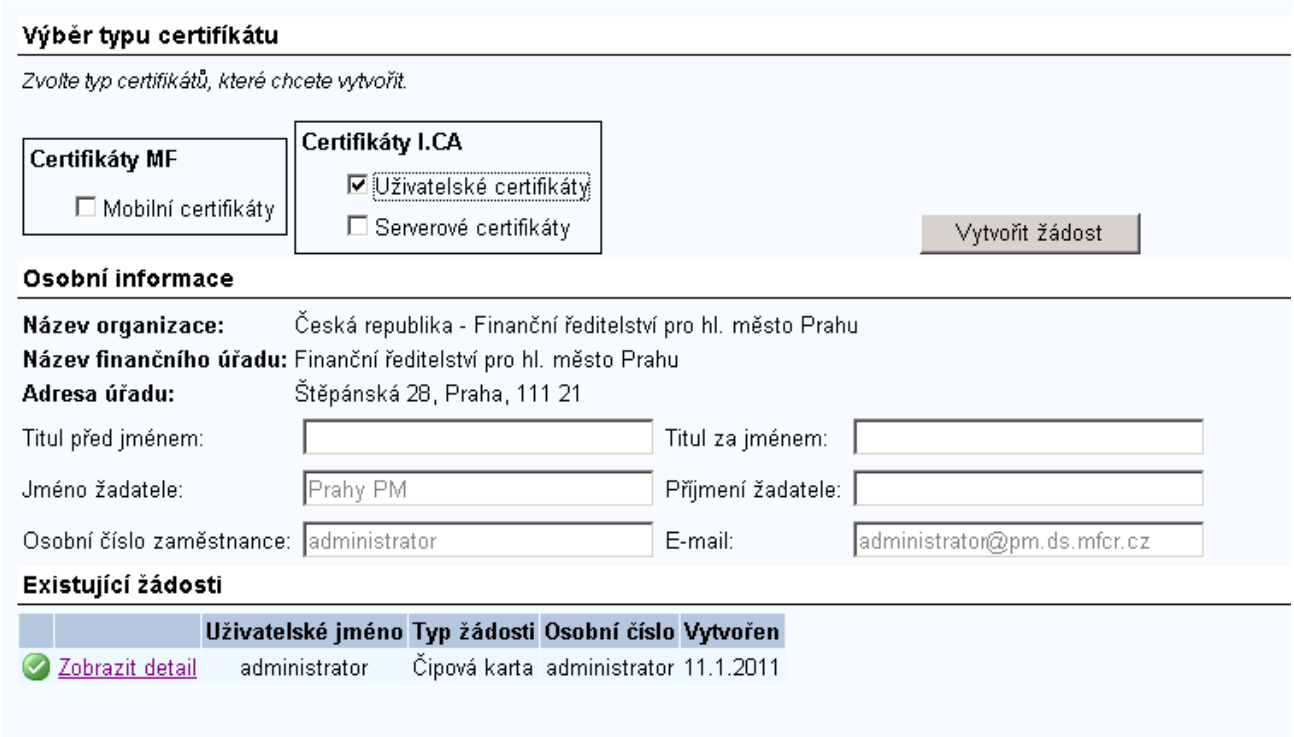
V případě, že uživatel požaduje opětovné vydání čipové karty např. z důvodu ztrát, nefunkčnosti nebo plánované výměny, může uživatel požádat po zneplatnění stávající karty prostřednictvím CMS. Další postup je totožný jako při prvotním vydání karty

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

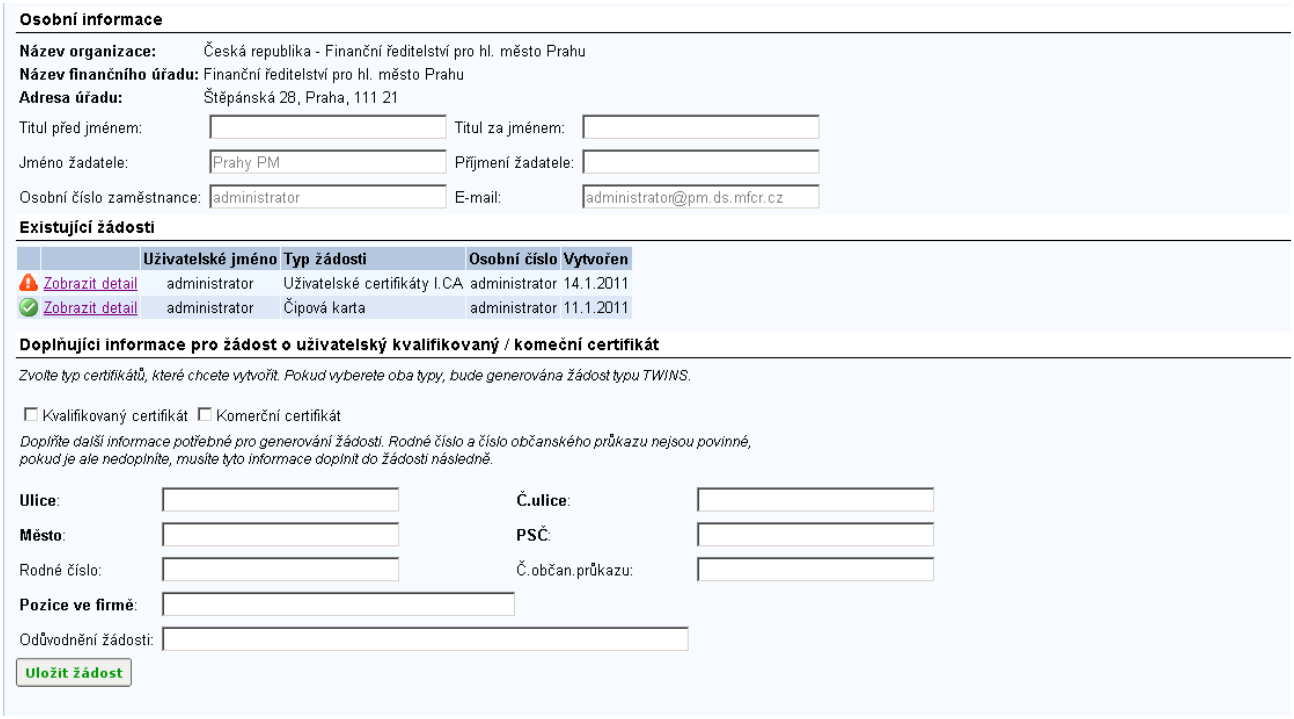
4.4.1. Vytvoření žádosti

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



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.



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.

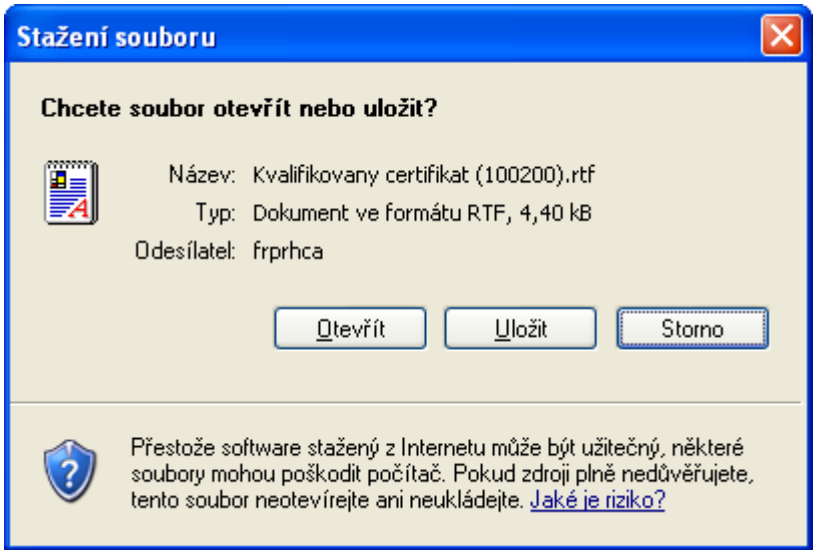
V části Osobní informace doplňte chybějící informace dle skutečnosti podle občanského průkazu. Informace bude kontrolována operátorem registrační autority při výdeji certifikátu na kartu

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.

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:

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:

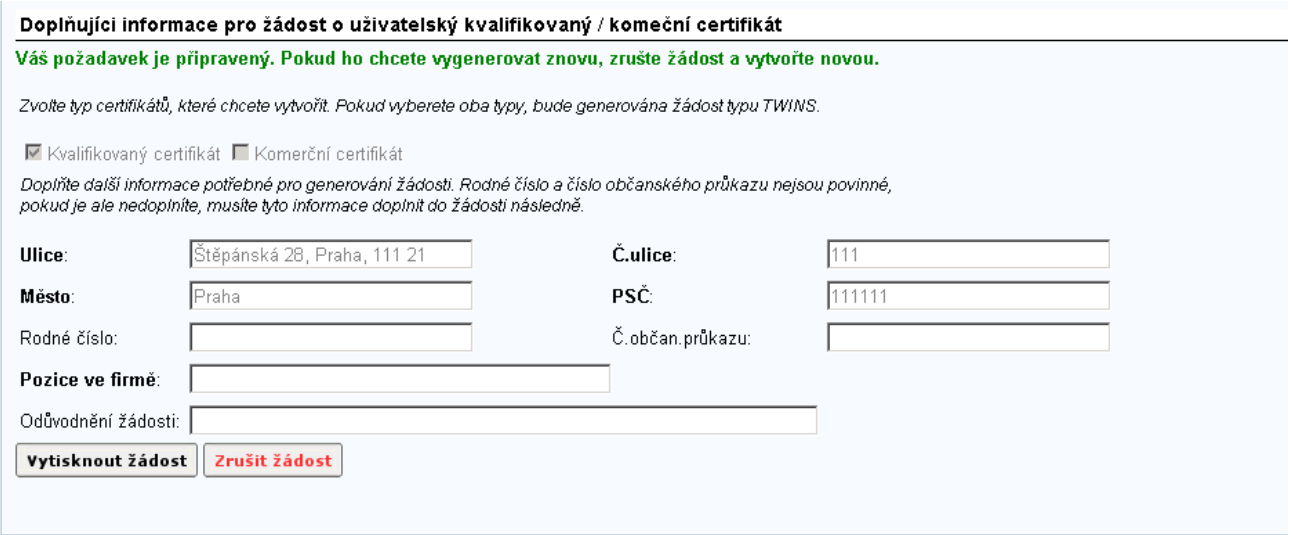
Po kliknutí na tlačítko OK se zobrazí okno na zadání PIN kódu k ČK:

Po zadání PIN, klikněte na tlačítko OK.

O průběhu generování žádosti jste informováni:

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:



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

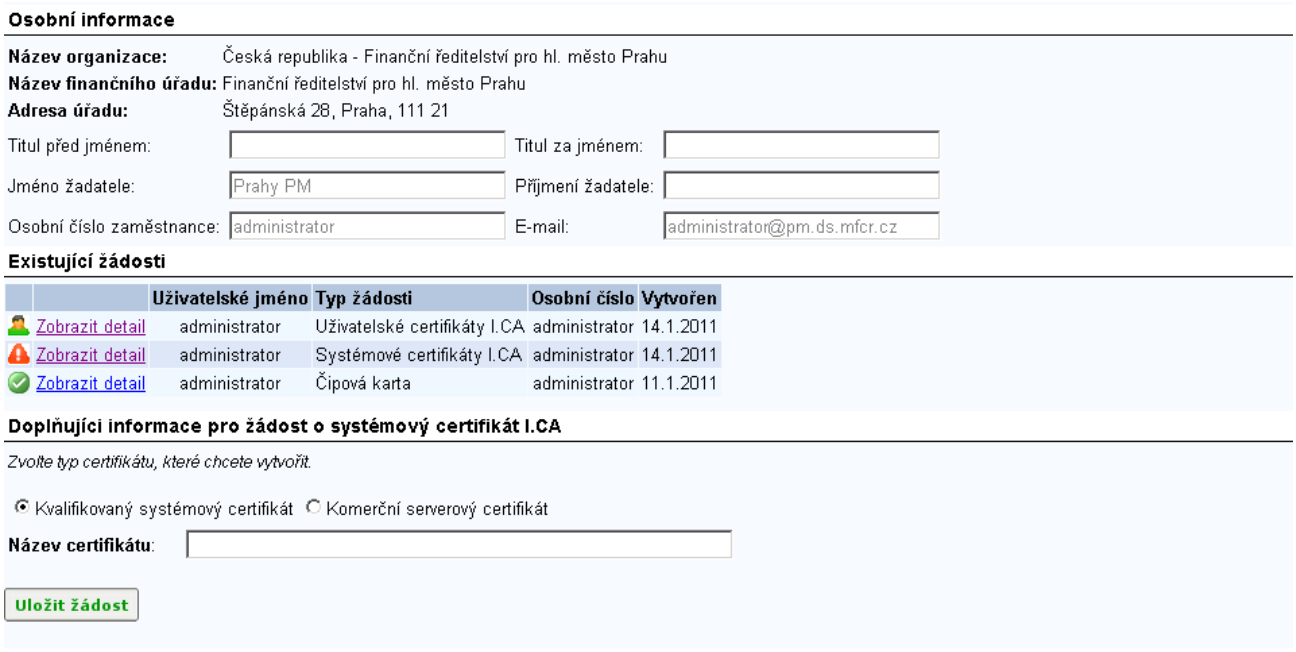
Provedením všech úkonů uvedených v předchozím textu je splněn základní požadavek procesu vydání QC. Nyní vezměte ČK, na kterou byla žádost generována, potvrzený protokol o zaměstnaneckém poměru, občanský průkaz a další průkaz s fotografií (zaměstnanecká ČK karta s potiskem, řidičský průkaz, cestovní 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

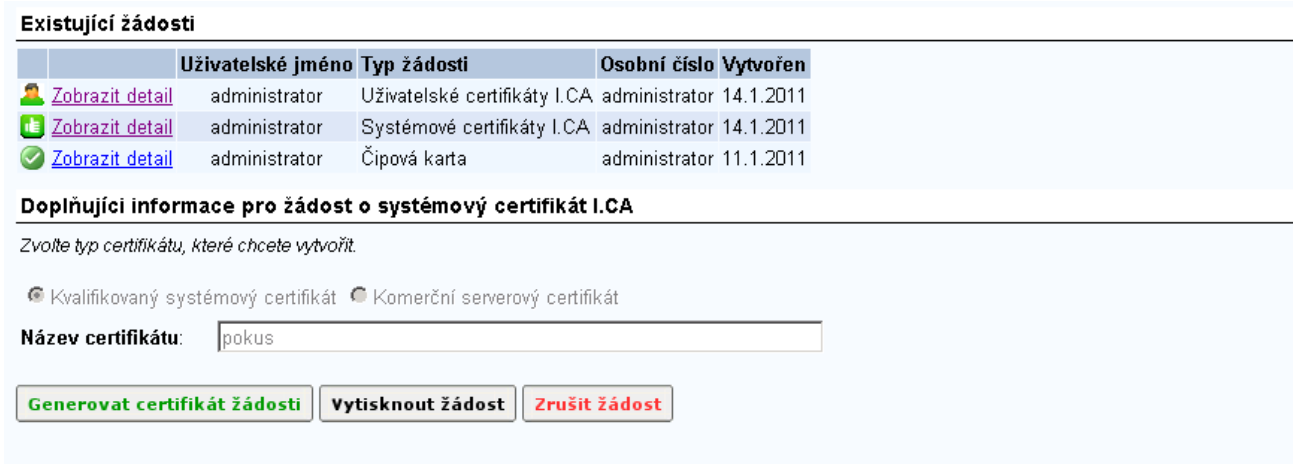
Spusťte Internet Explorer a zadejte adresu http://ca/cms. Zvolte *Žádost o certifikát.* Vyberte **Serverové certifikáty** v sekci *Certifikáty I.CA* a stiskněte tlačítko *Vytvořit žádost.*



Vyberte certifikát o který žádáte

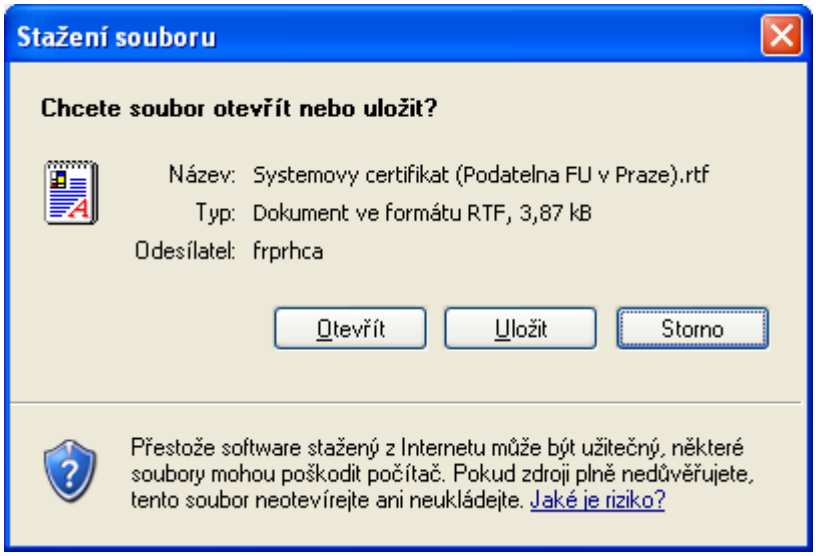
- Kvalifikovaný systémový certifikát
- Komerční serverový certifikát

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.



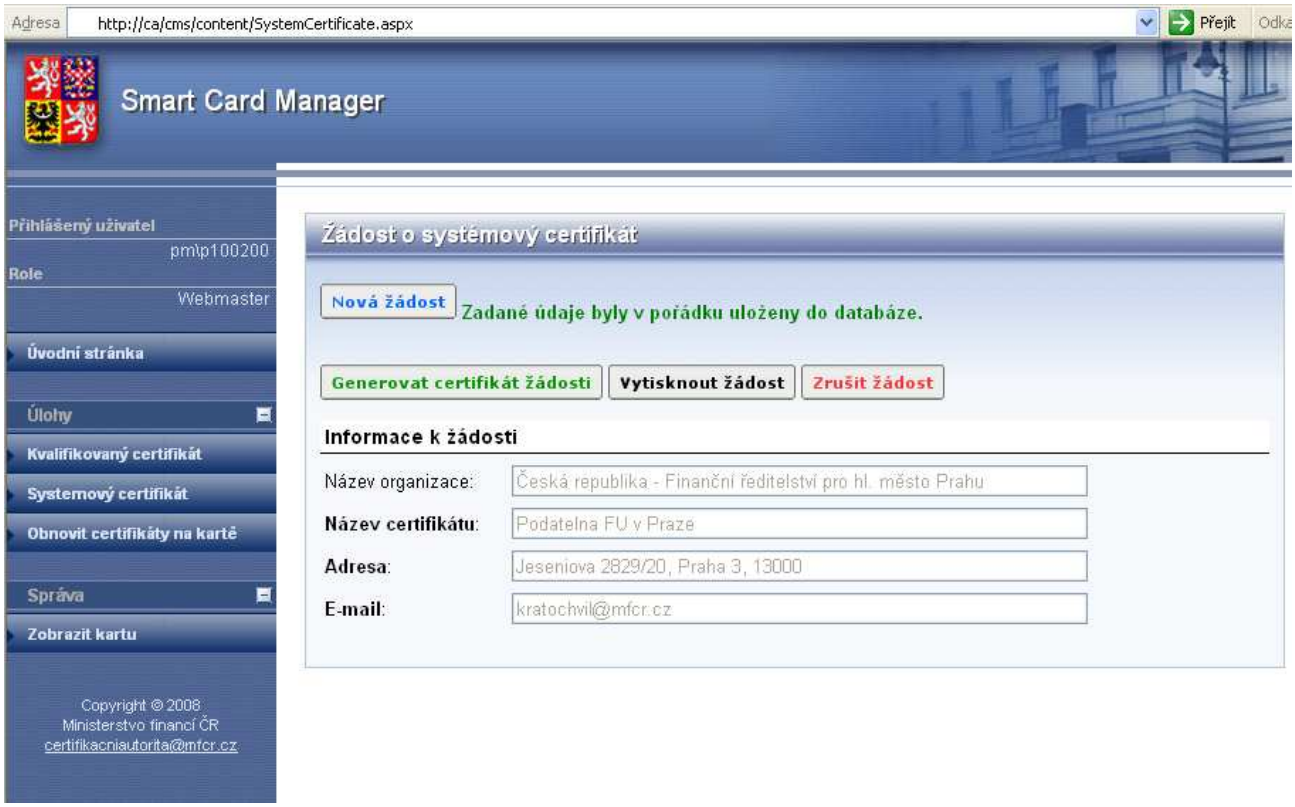
Po provedení kontroly zadaných údajů můžete provést následující akce:

- **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).

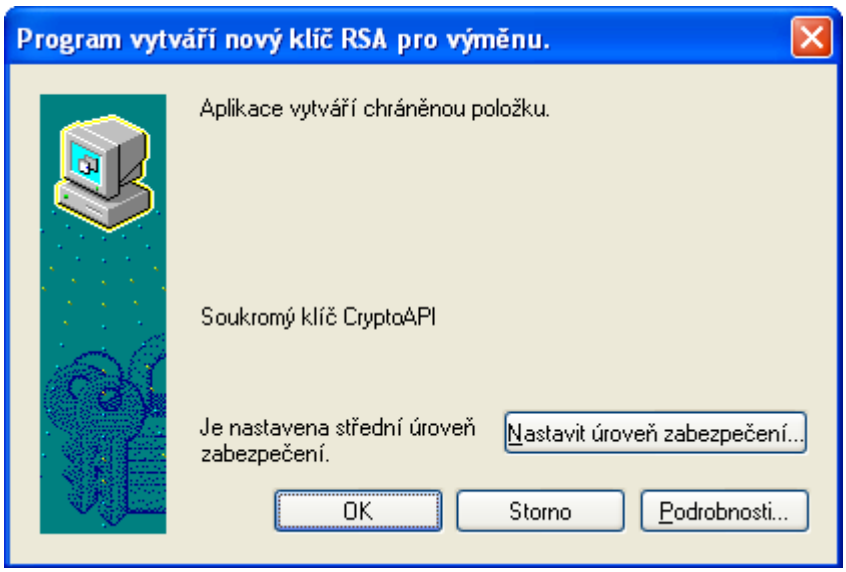
Zároveň přejdete na následující obrazovku:



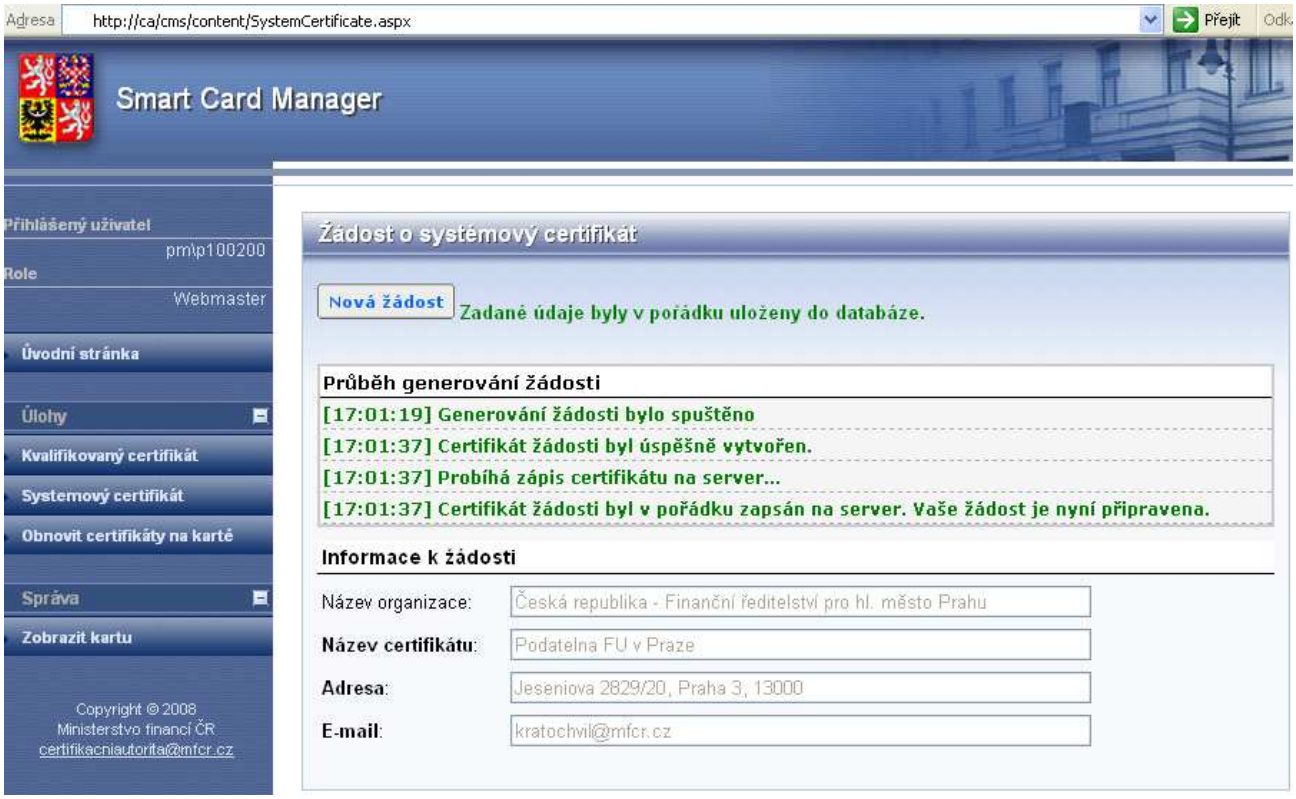
Zde jste v horní části informováni, že máte na serveru uložen aktivní požadavek na QC. I zde ještě máte možnost žádost zrušit kliknutím na tlačítko Zrušit žádost. V případě potřeby můžete znovu vytisknout celou žádost kliknutím na tlačítko Vytisknout žádost. V případě, že jsou zadané informace pořádku, 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**

Systém PKI



O průběhu generování žádosti jste informováni:



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).

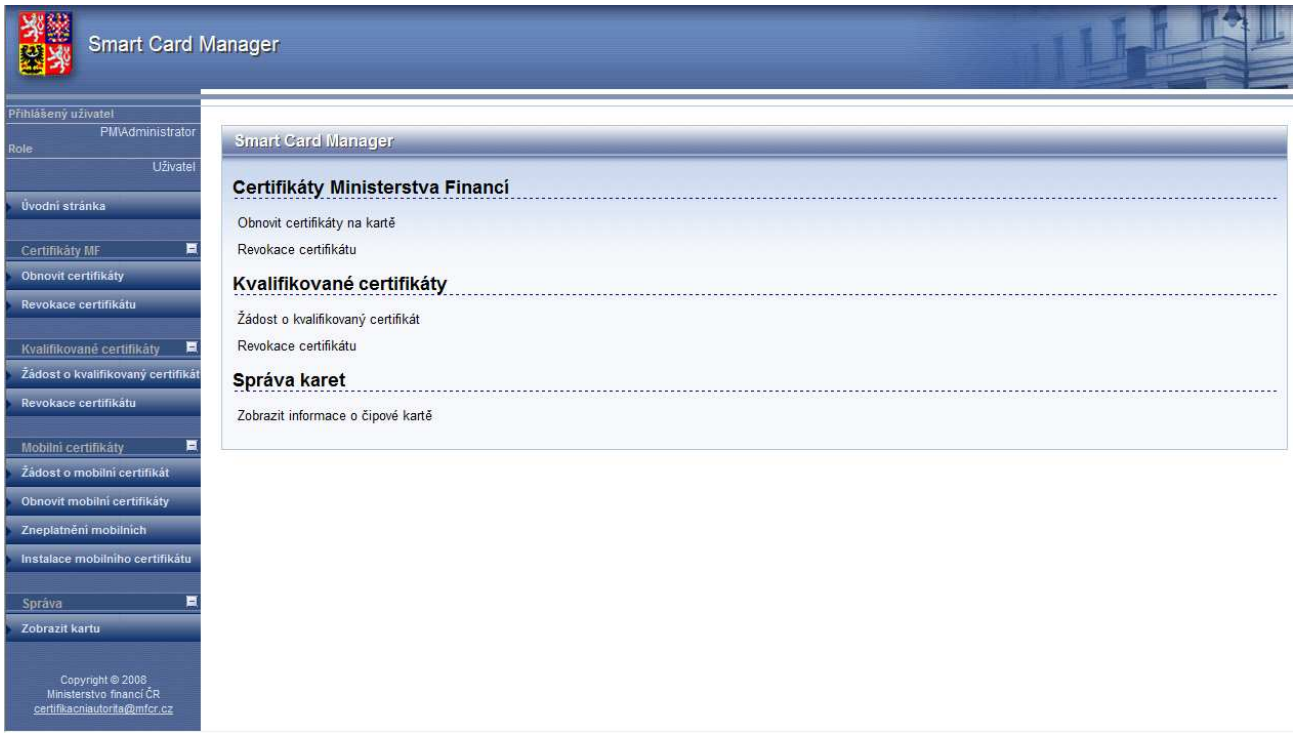
4.5.3. Instalace certifikátu

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)

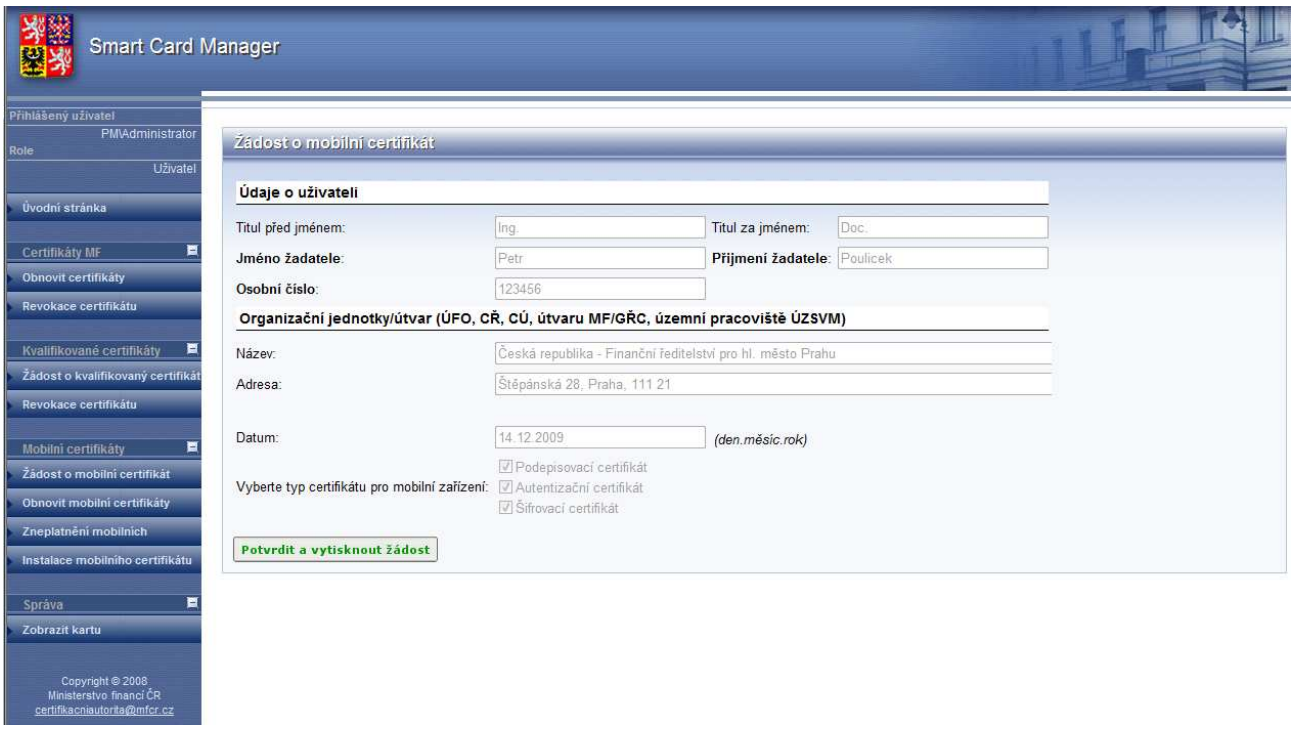
4.6. Vyžádání certifikátů pro mobilní zařízení

4.6.1. Vytvoření žádosti

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

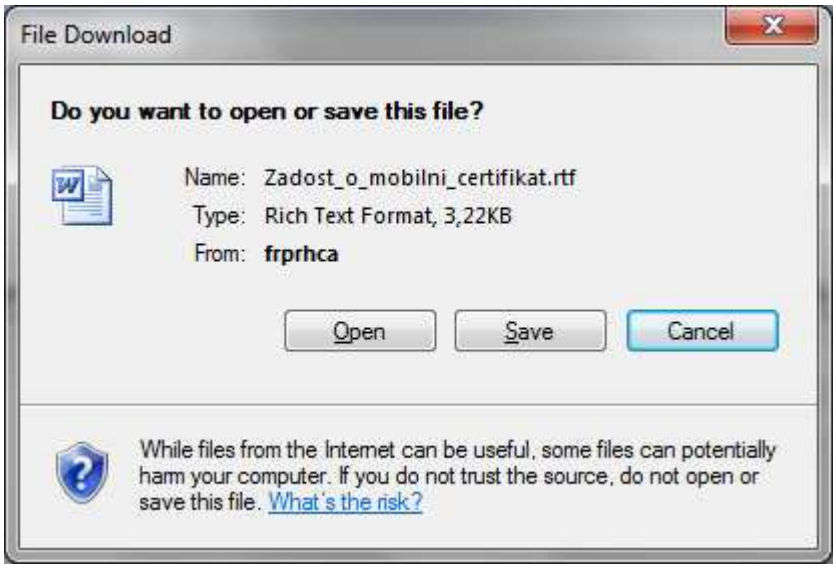


Kliknutím na odkaz Žádost o mobilní certifikát zahájíte proces vytvoření žádosti a zobrazí se vám následující obrazovka:



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.



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*

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

d. **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).

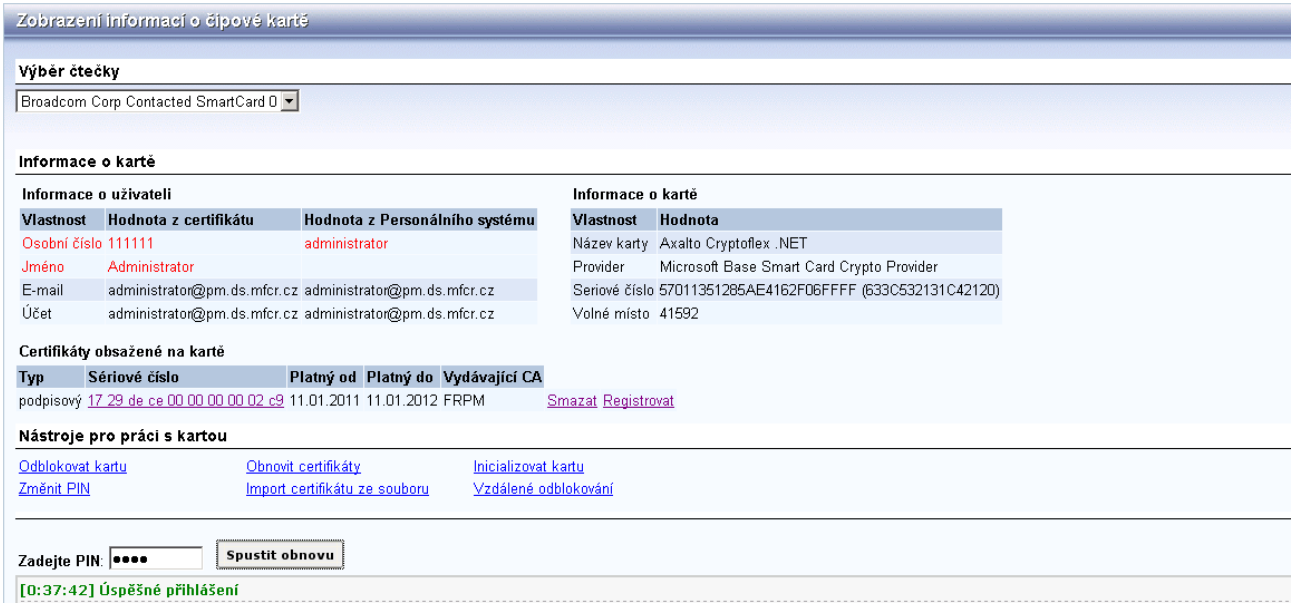
5.3.3. Postup obnovy karty

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)

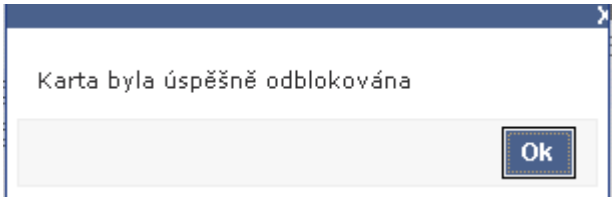
V případě, že uživatel vlastní mobilní certifikáty, uživatel současně obdrží nově vydaný šifrovací certifikát a zároveň jsou vygenerovány ostatní certifikáty urřené pro mobilné zařízení.

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

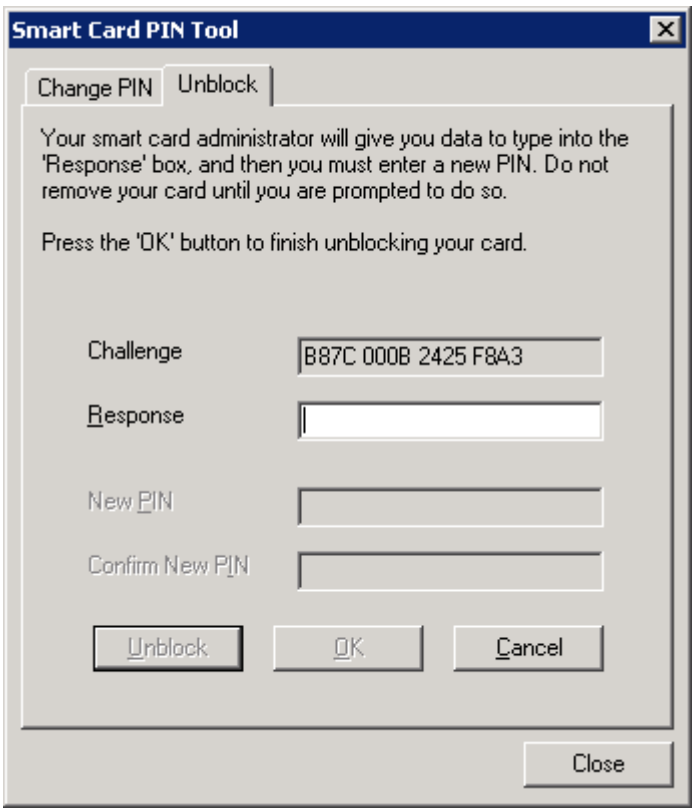


5.5. Vzdálené odblokování karty

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:

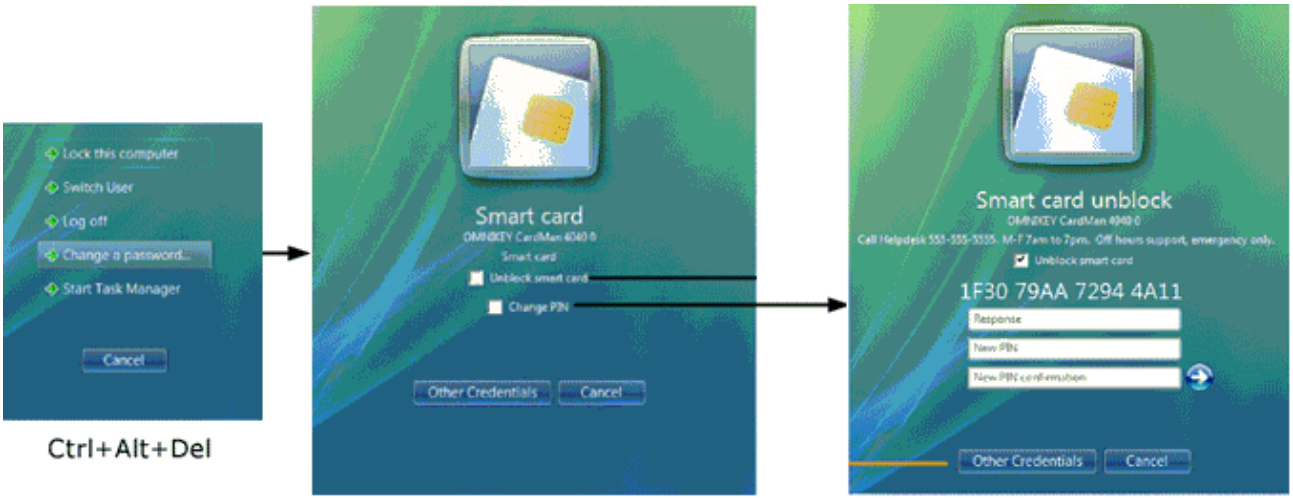
1. Vygenerování request stringu.

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



Po stisknutí tlačítka Unblock je vygenerován request string

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



2. 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.

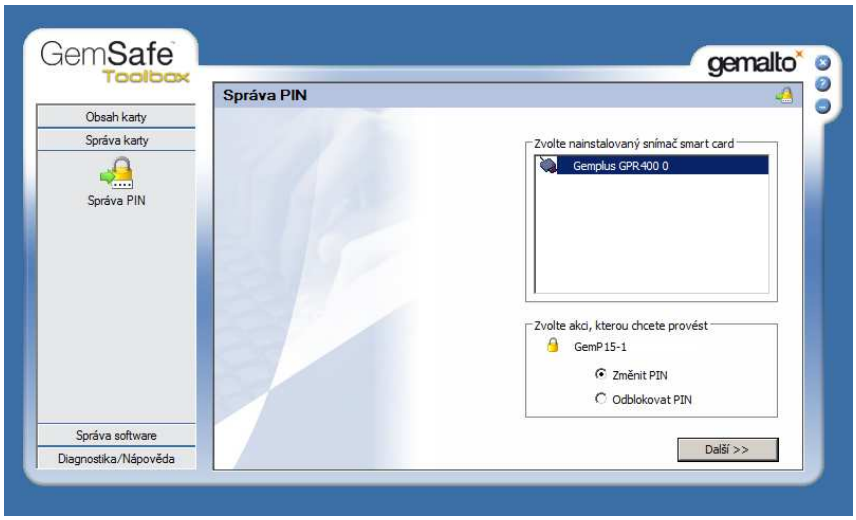
Systém PKI

5.6. Změna PINu

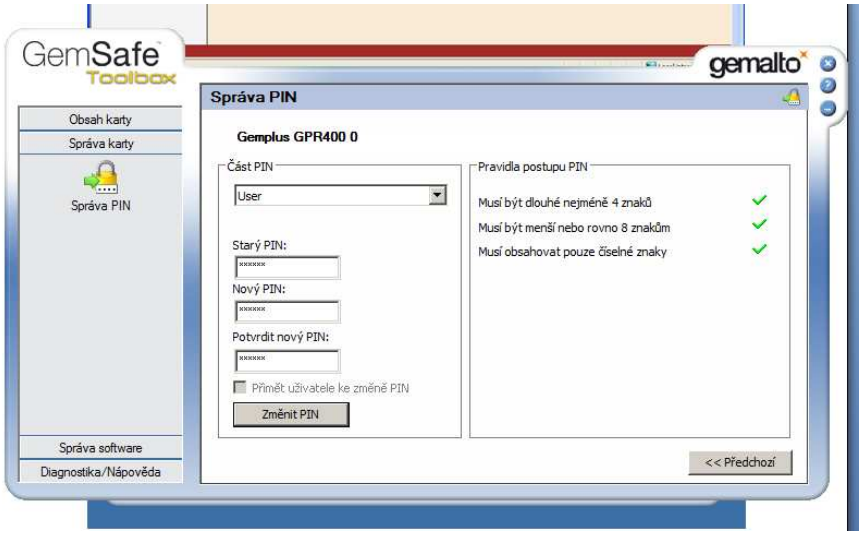
5.6.1. Gemsafe

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**

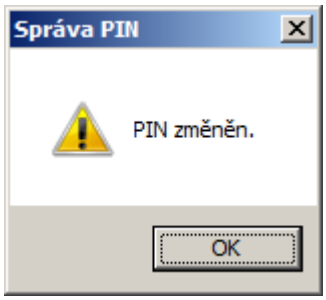


Stiskněte tlačítko **Další**



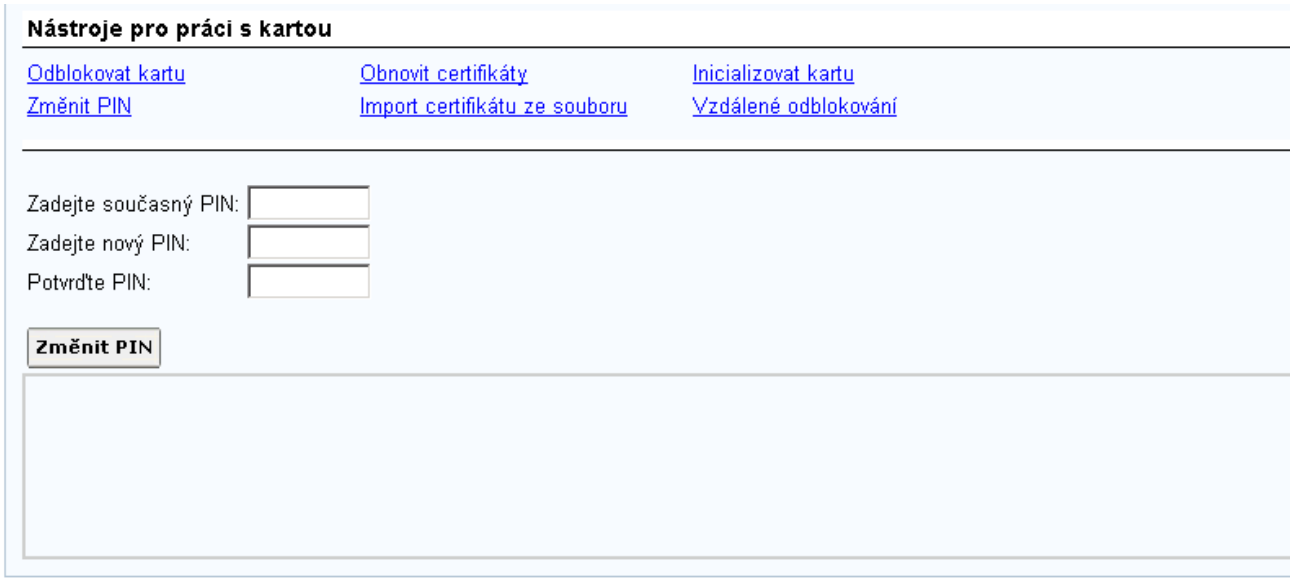
Následující kroky jsou:

- 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.



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**



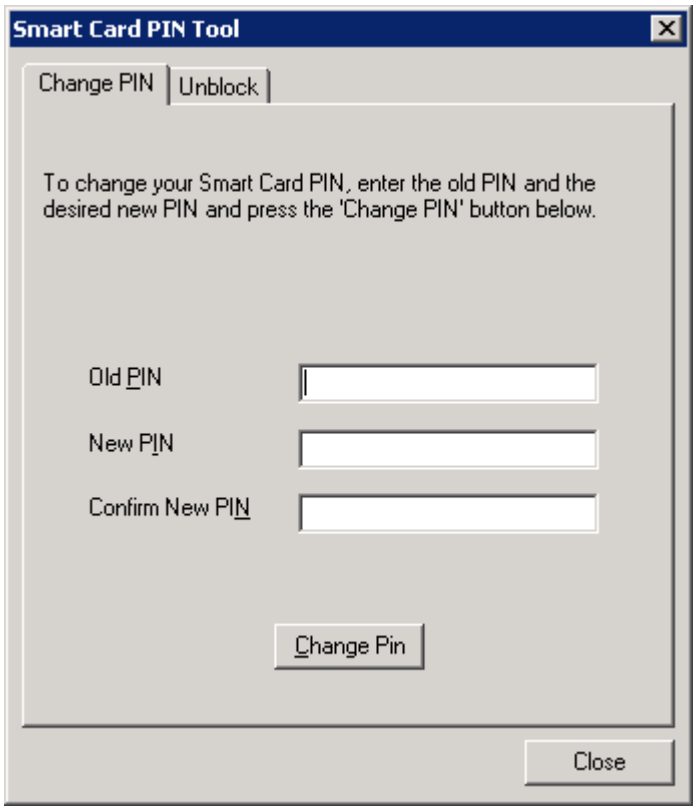
Zadejte stávající PIN a dvakrát nový požadovaný PIN a stiskněte tlačítko **Změnit PIN.**

5.6.3. Odblokování .NET karet

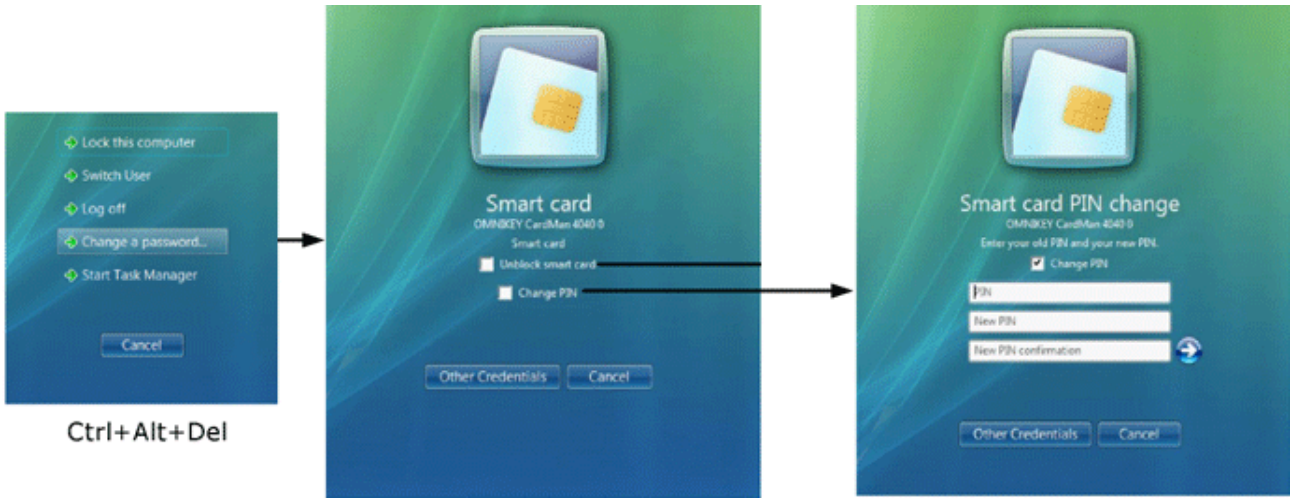
Pro karty podporující minidrivery je možnost podobně jako pro odblokování použít nativní nástroje:

Systém PKI

Pro Windows XP je k dispozici PINTOOL



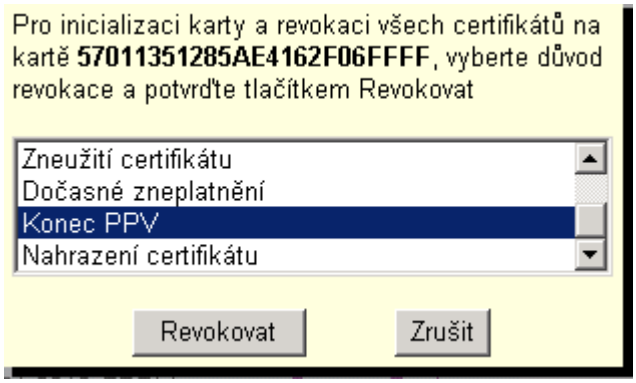
Pro operační systém Windows Vista a Widows 7:



5.7. Inicializace karty

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

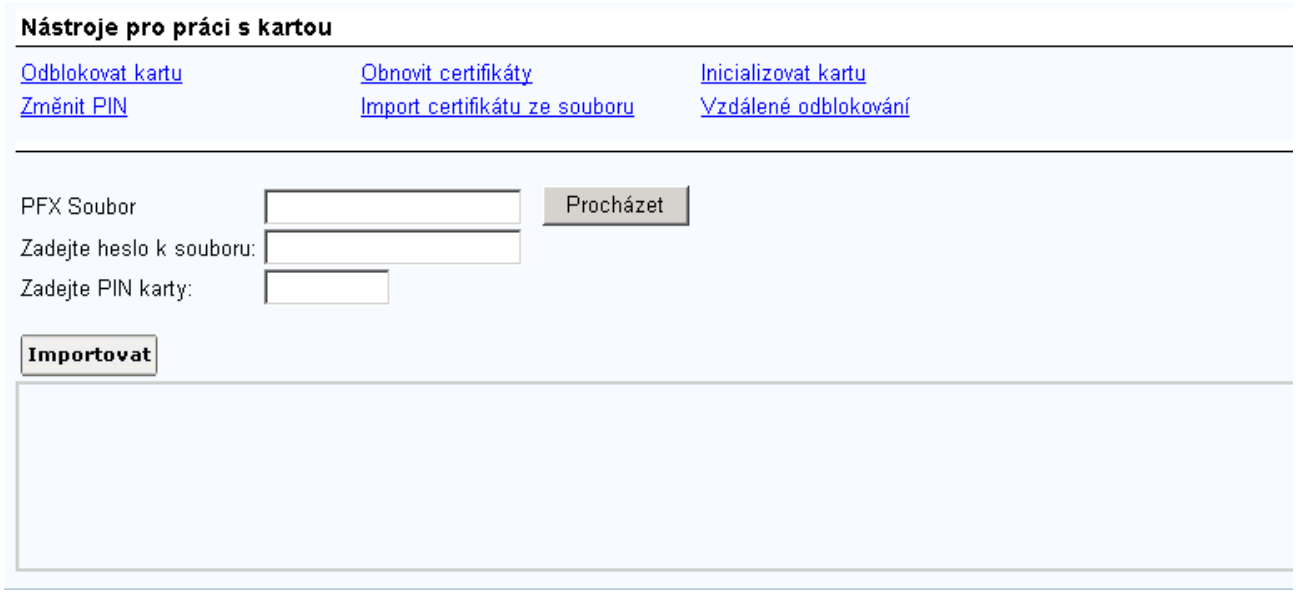
Funkce slouží k uvedení karty do původního stavu: Je vymazán obsah karty a nastaven výchozí uživatelský a administrátorský PIN. Funkce je k dispozici pro roli *doménový operátor, administrátor a enrollment agent.* Po dokončení vymazání karty, systém automaticky požádá o revokaci vymazaných certifikátů.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



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.

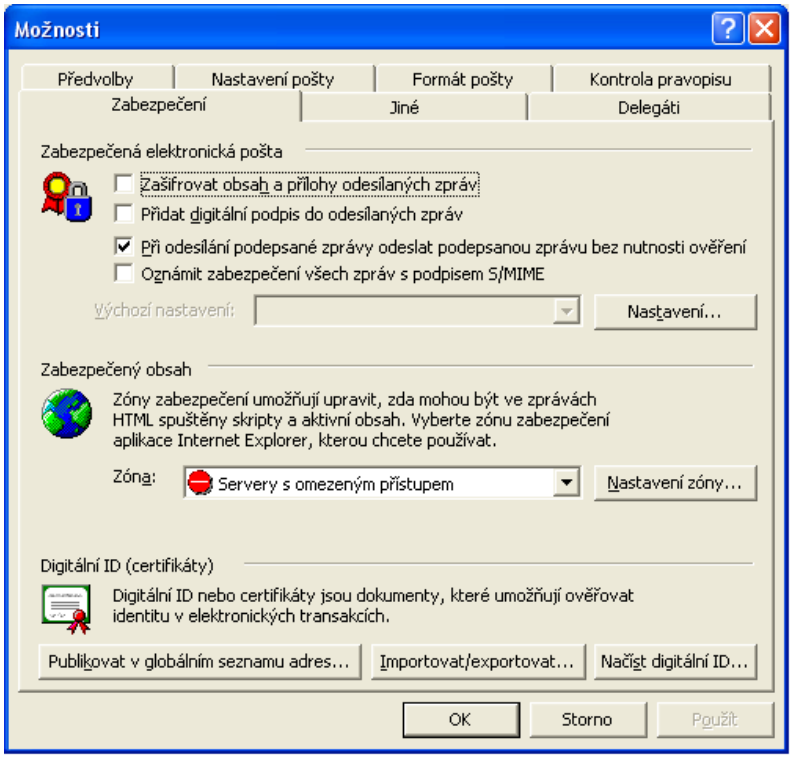


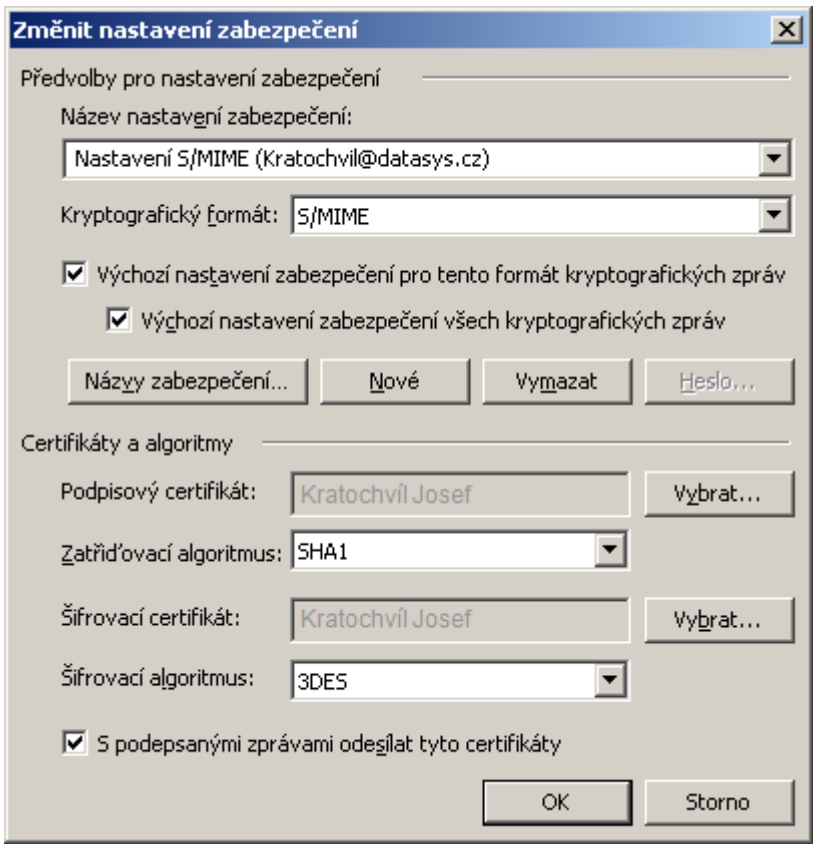
Po zadání požadovaných informací je certifikát uložen na čipovou kartu.

6. KONFIGURACE POŠTOVNÍHO KLIENTA

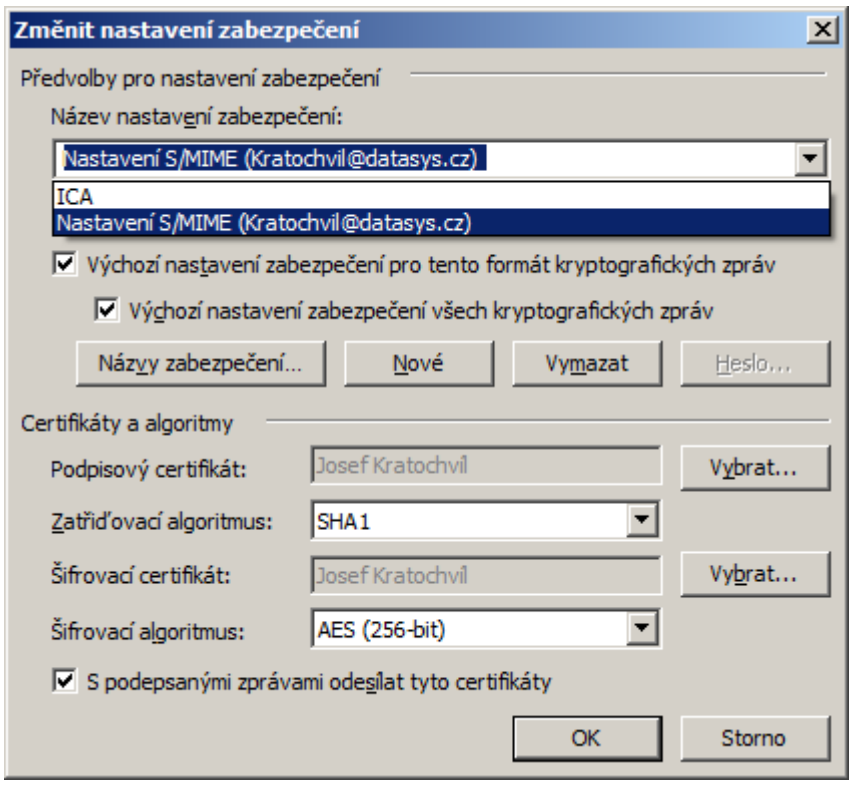
Tato kapitola popisuje nastavení aplikace Outlook pro možnost šifrování a podepisování elektronické pošty - tuto činnost zpravidla provádí pracovník IT

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





- 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



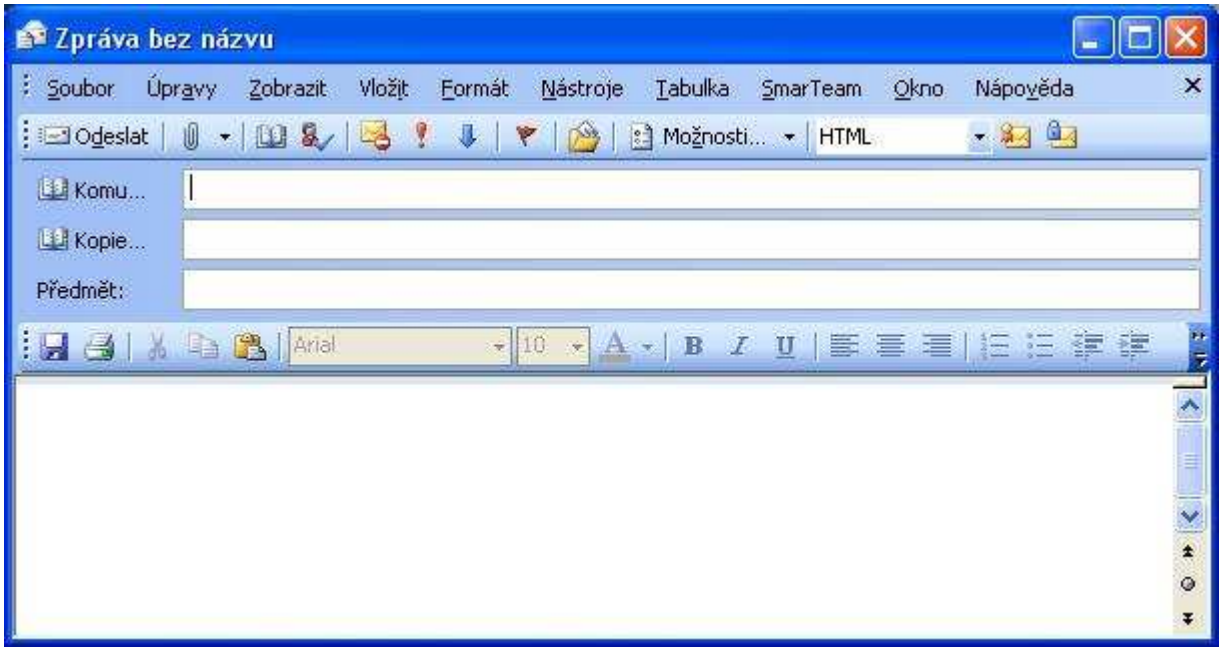
- Stisknutím tlačítka **OK** dokončíte konfiguraci

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:

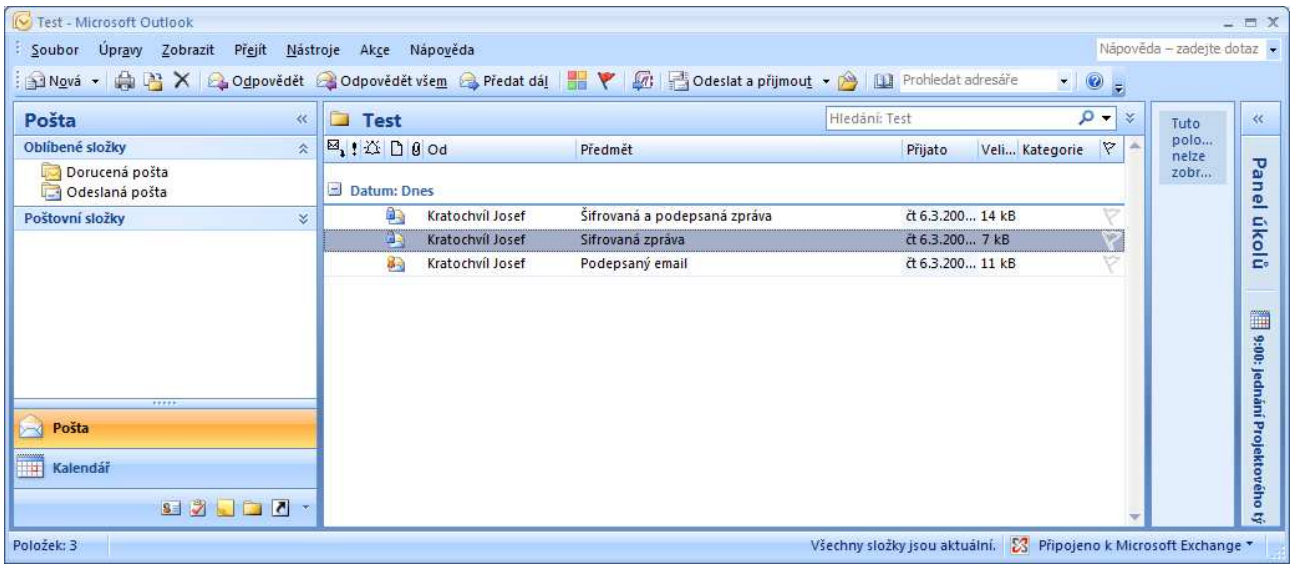
 - Vložení podpisu do zprávy

 - Zašifrování zprávy



Na následujícím obrázku jsou příklady kombinace šifrované a podepsané zprávy

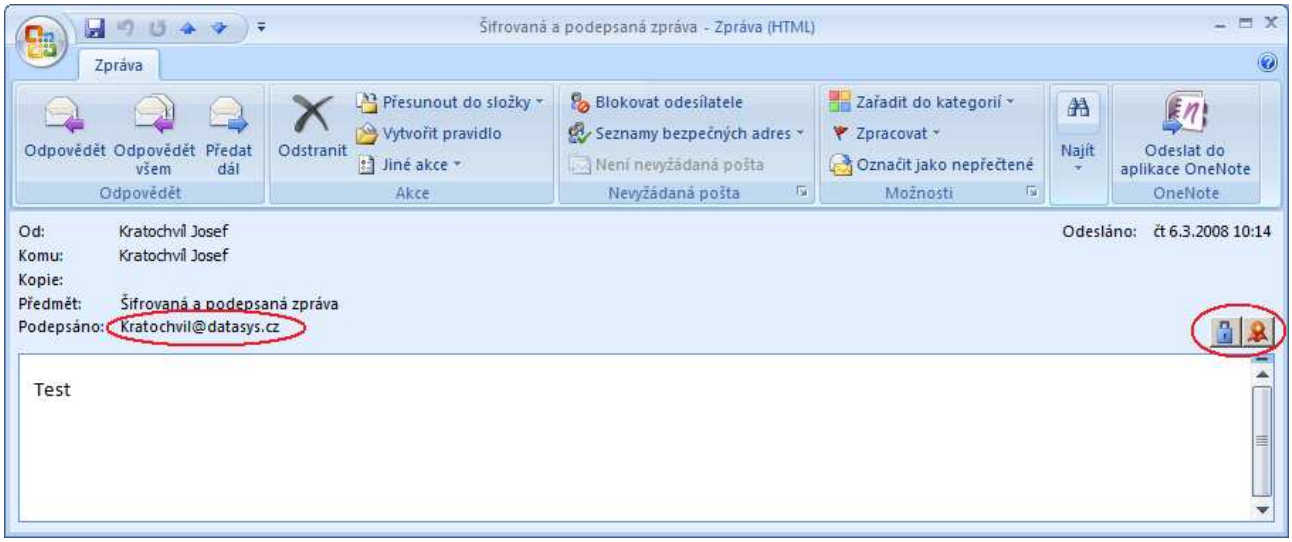
Systém PKI



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

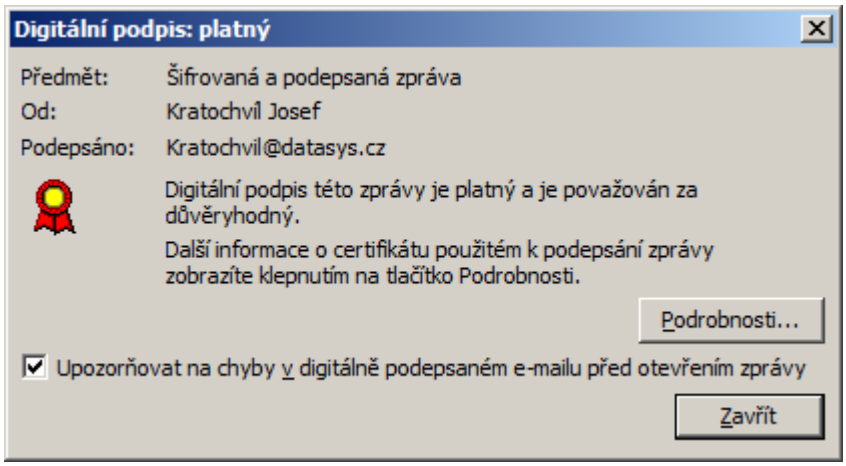
 - Zpráva je podepsaná

 - Zpráva je šifrovaná



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

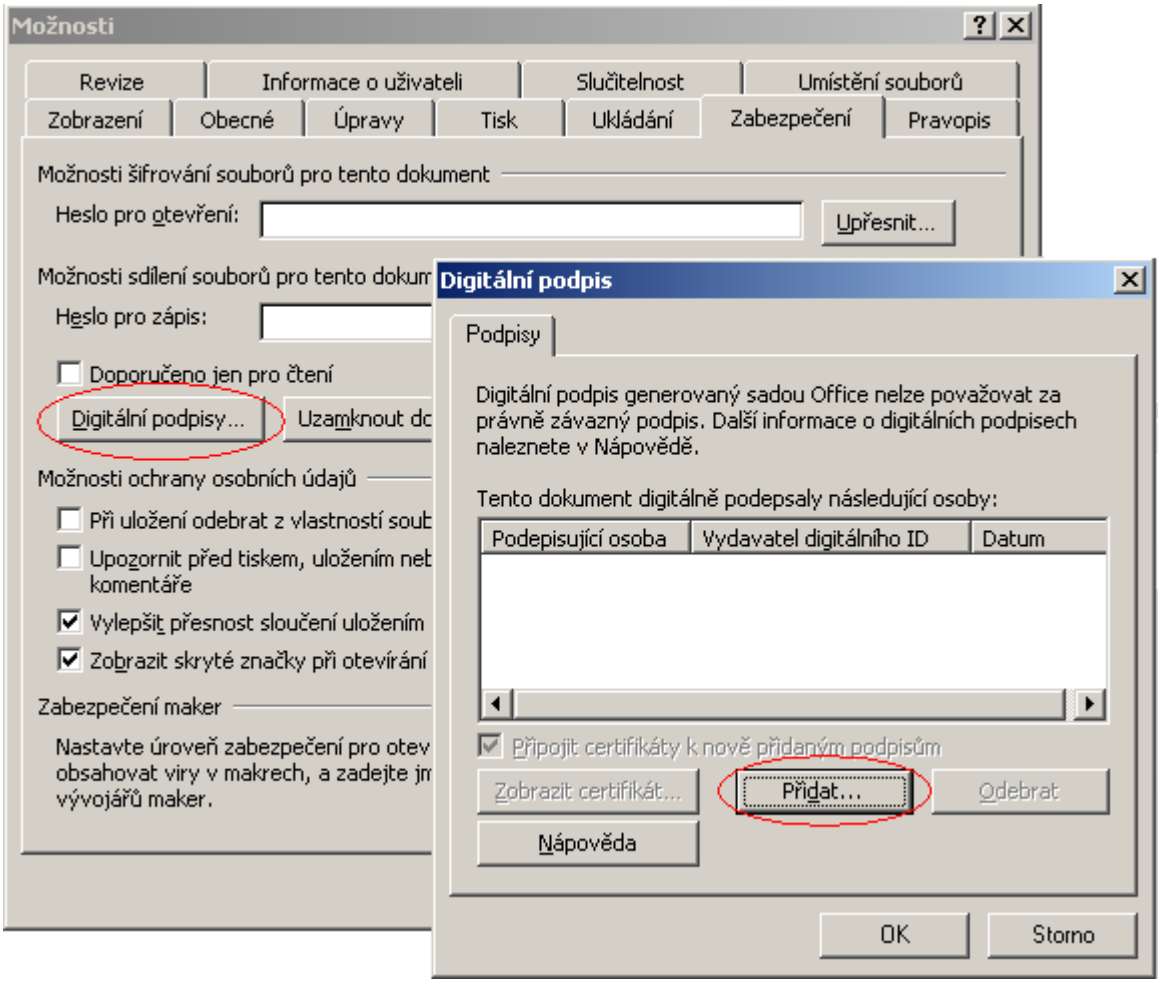
Digitální podpisy lze přidat do dokumentů aplikace Word, sešitů aplikace Excel a prezentací aplikace PowerPoint

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

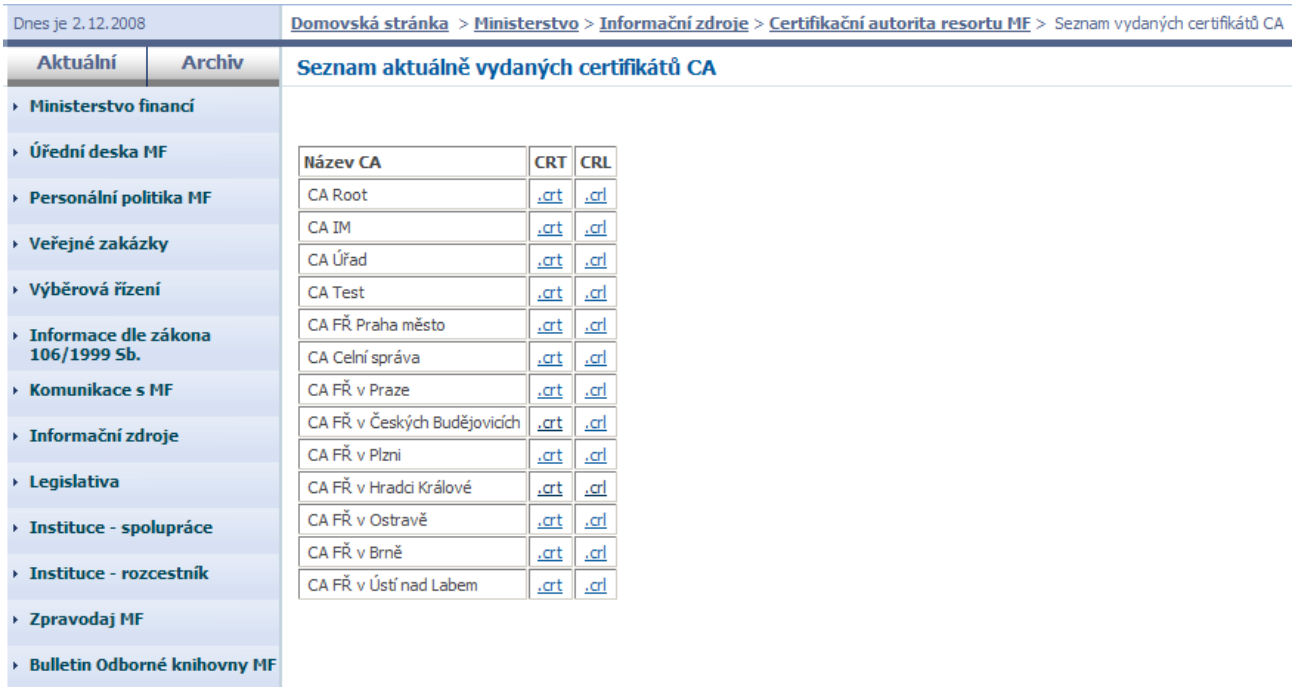


9. WWW ROZHRANÍ CERTIFIKAČNÍ AUTORITY MF ČR

V rámci www stránek MF ČR (www.mfcr.cz) 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

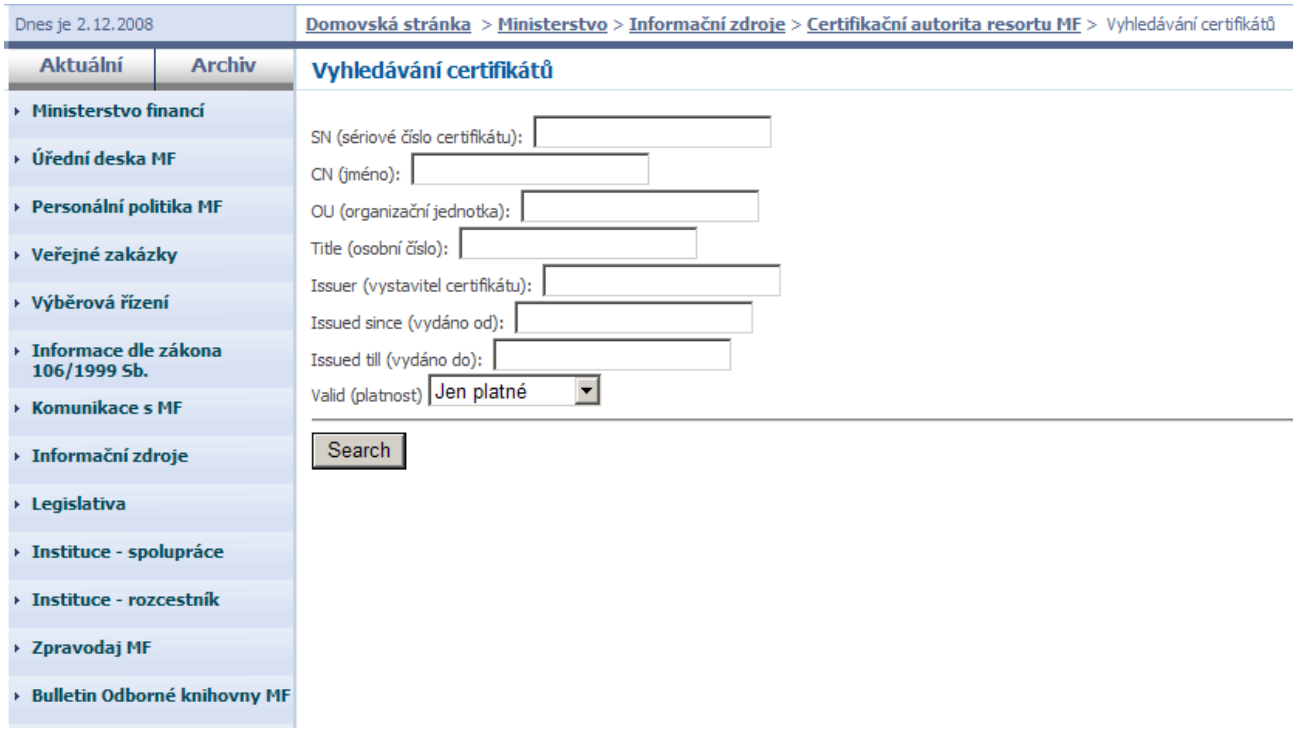
Po kliknutí na odkaz **Seznam aktuálně vydaných certifikátů CA** se objeví následující obrazovka, na níž je seznam certifikátů (sloupec CRT) lokálních certifikačních autorit a aktuálních CRL vydaných těmito autoritami (sloupec CRL):



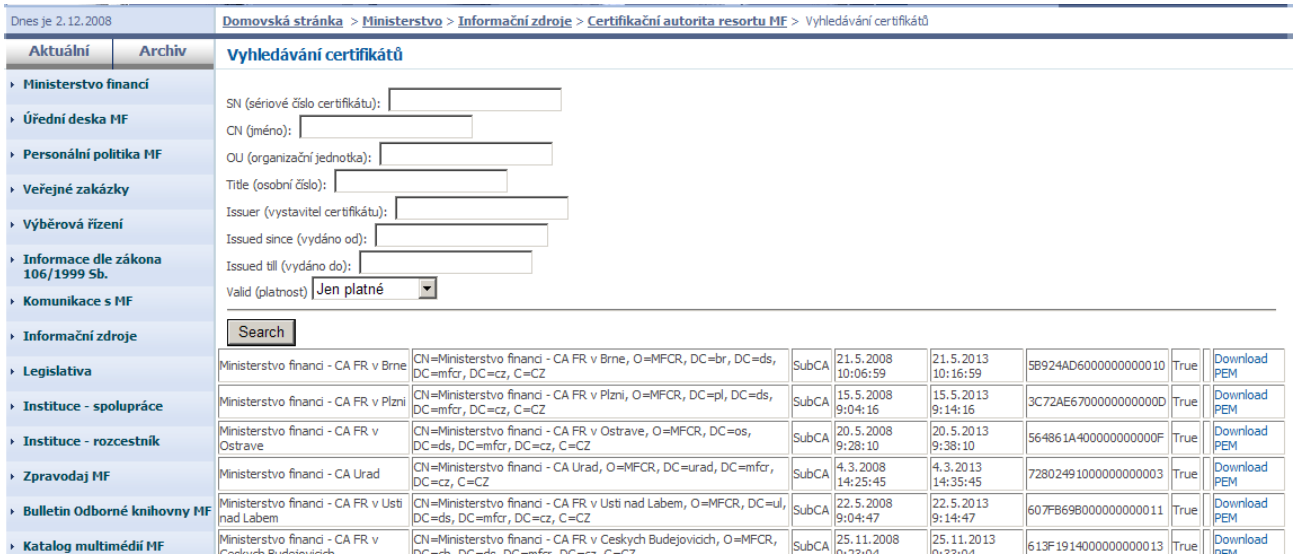
Po kliknutí na příslušný certifikát či CRL si vybrané lze stáhnout nebo zobrazit.

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:



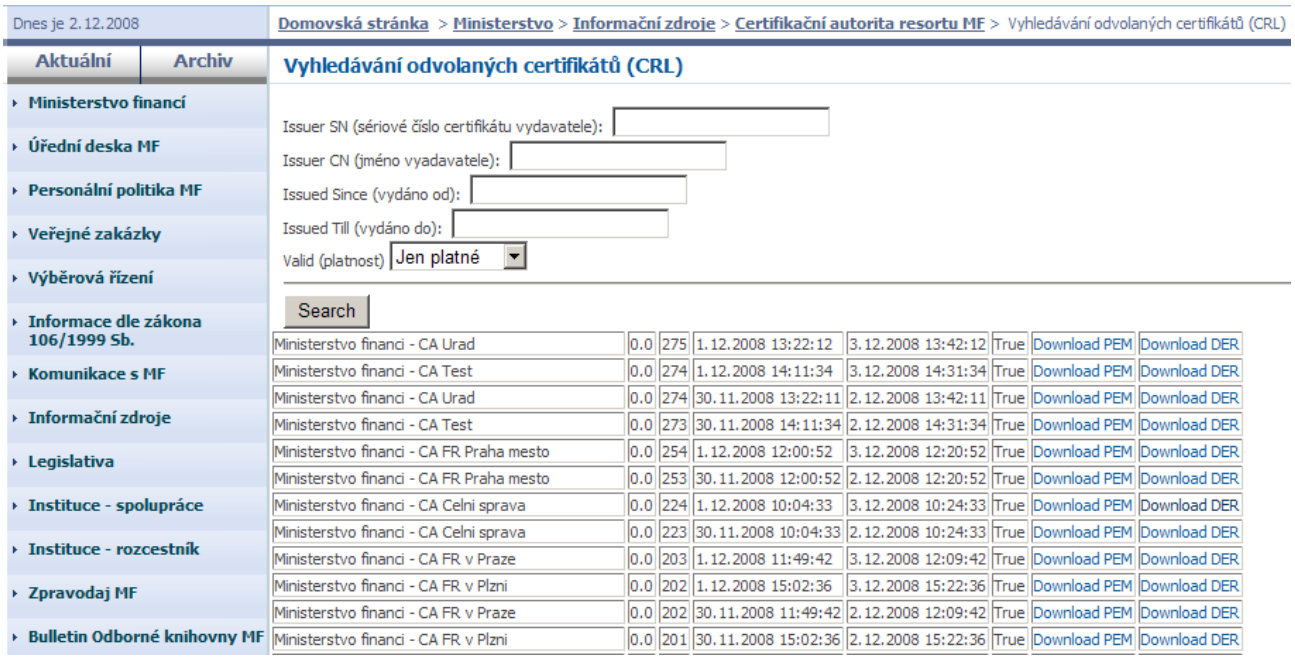
Po zadání parametrů a kliknutí na odkaz **Search** se zobrazí stránka s certifikáty vyhovujícími zadaným kritériím. Při vyplnění více parametrů se vyhledávají certifikáty vyhovující současně všem kritériím (logická spojka).



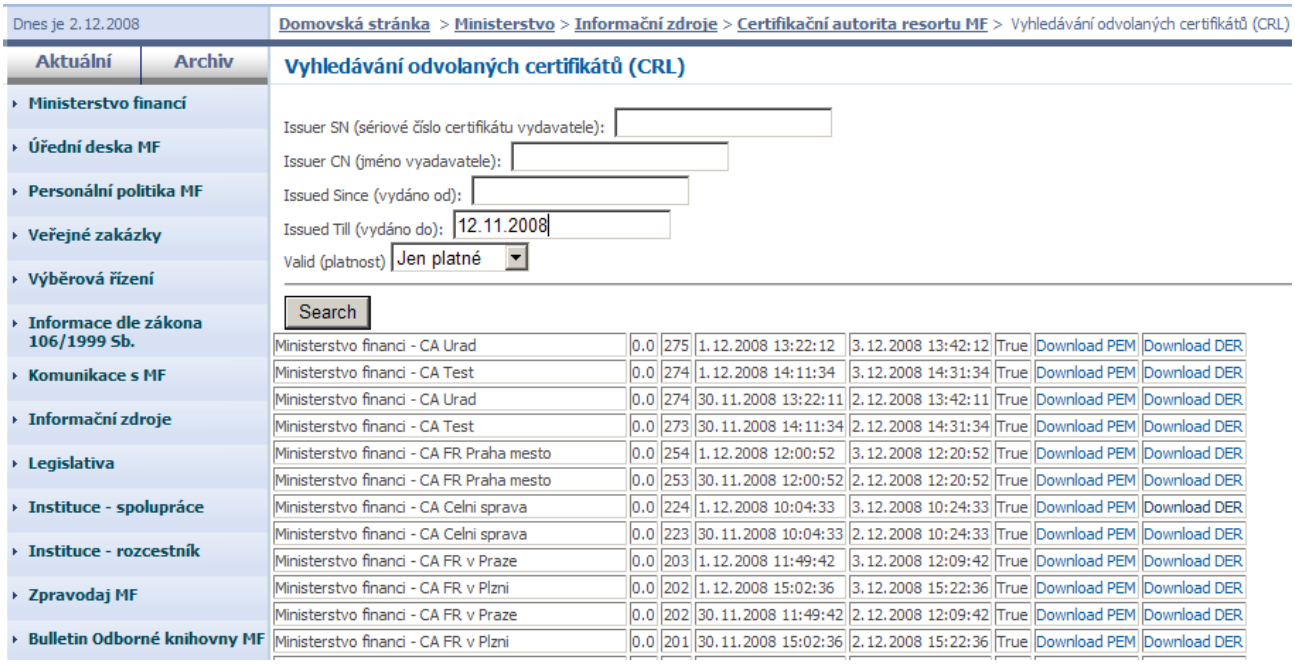
Po kliknutí na příslušný certifikát či CRL si vybrané lze stáhnout nebo zobrazit (sloupec obsahující **Download PEM**).

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).:



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:



Systém PKI

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.

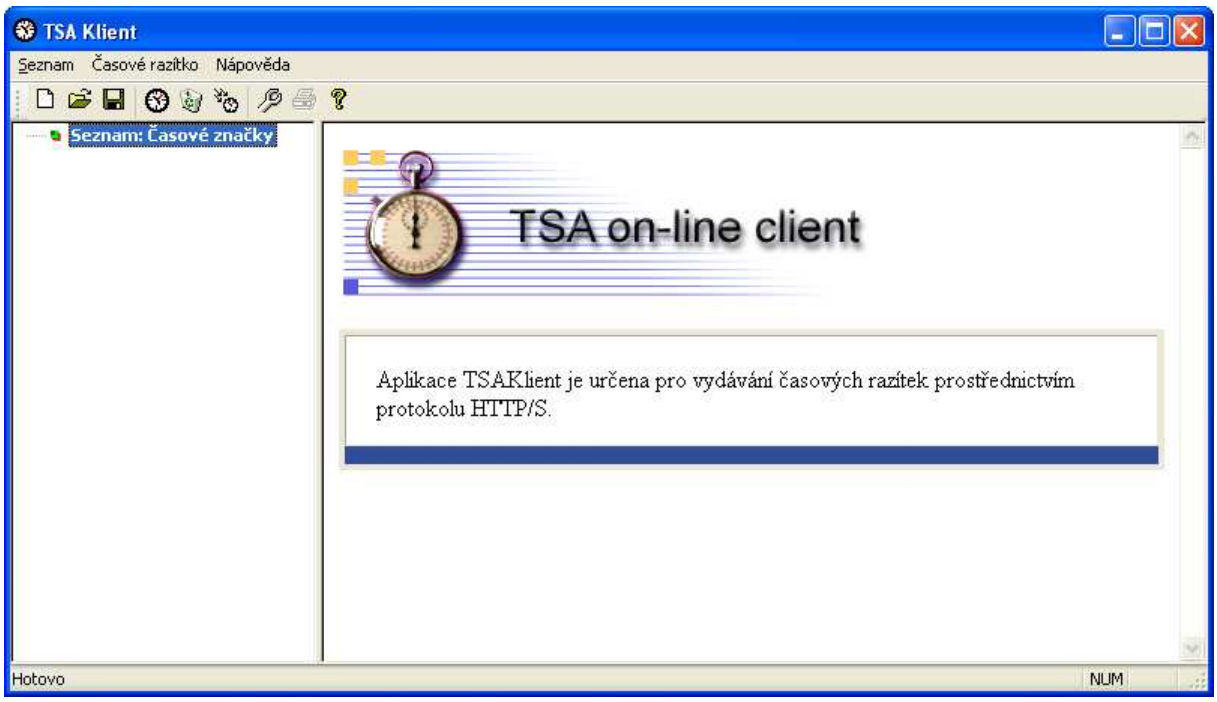
Popisovaná aplikace TSA Klient je určena jednak pro vyžádání časové značky k vybranému souboru prostřednictvím protokolu HTTP nebo HTTPS, jednak pro ověření platnosti časové značky. Časová značka je vydávána k určitému datovému souboru a je zpravidla ukládána do souboru s příponou *.tst. Vymazáním tohoto 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.

Systém PKI

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  je umístěn v horní části hlavního 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 **Další**.

- 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  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).

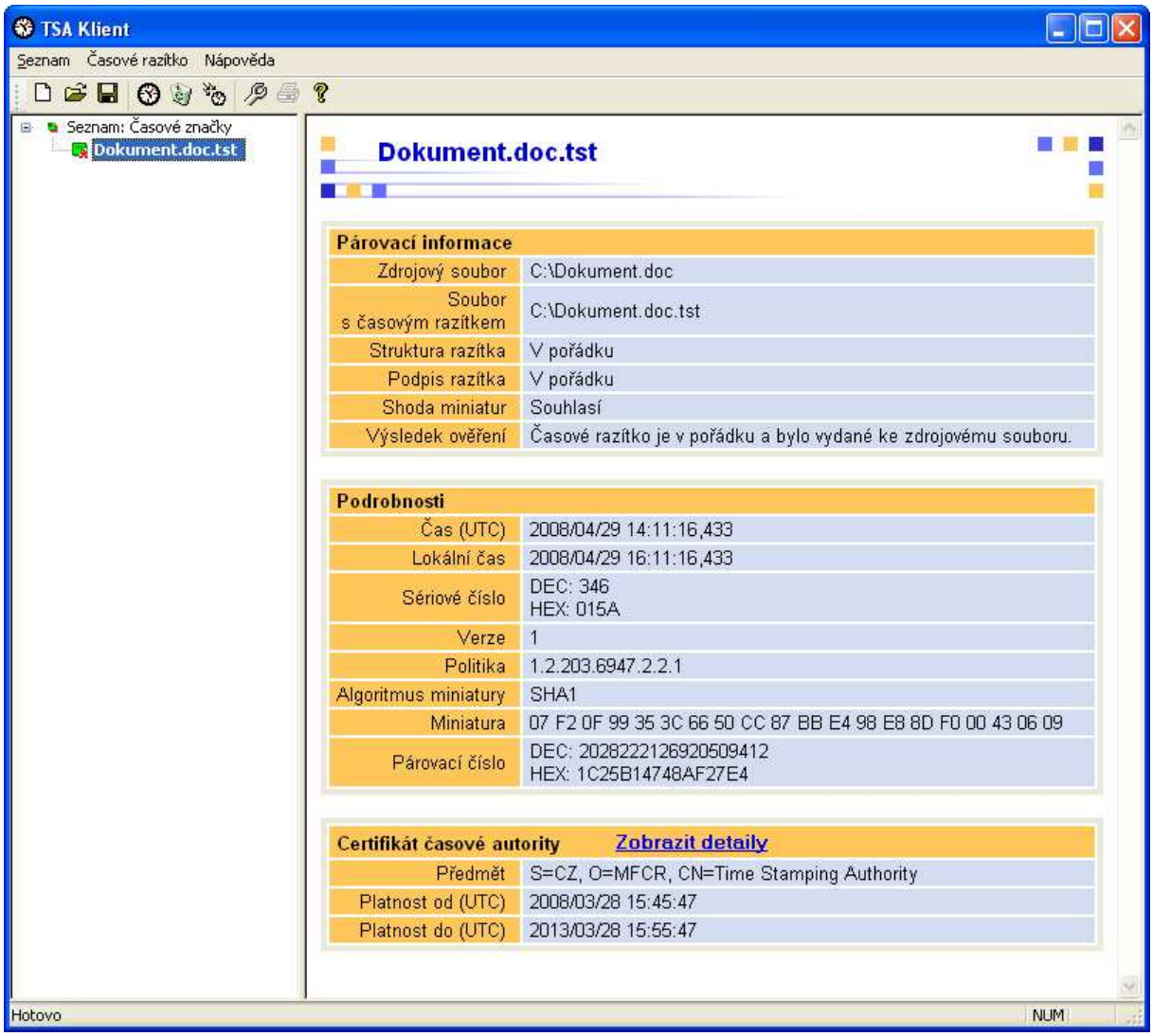
- Jestliže vyberete existující soubor a klepnete na tlačítko **Další**, je provedena kontrola miniatur (HASH hodnot) tohoto souboru a miniatury z časové značky. Pokud jsou tyto miniatury shodné (jedná se o platný pár dokument – časová značka) a je platný i digitální podpis časové autority, dojde k zobrazení 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



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.

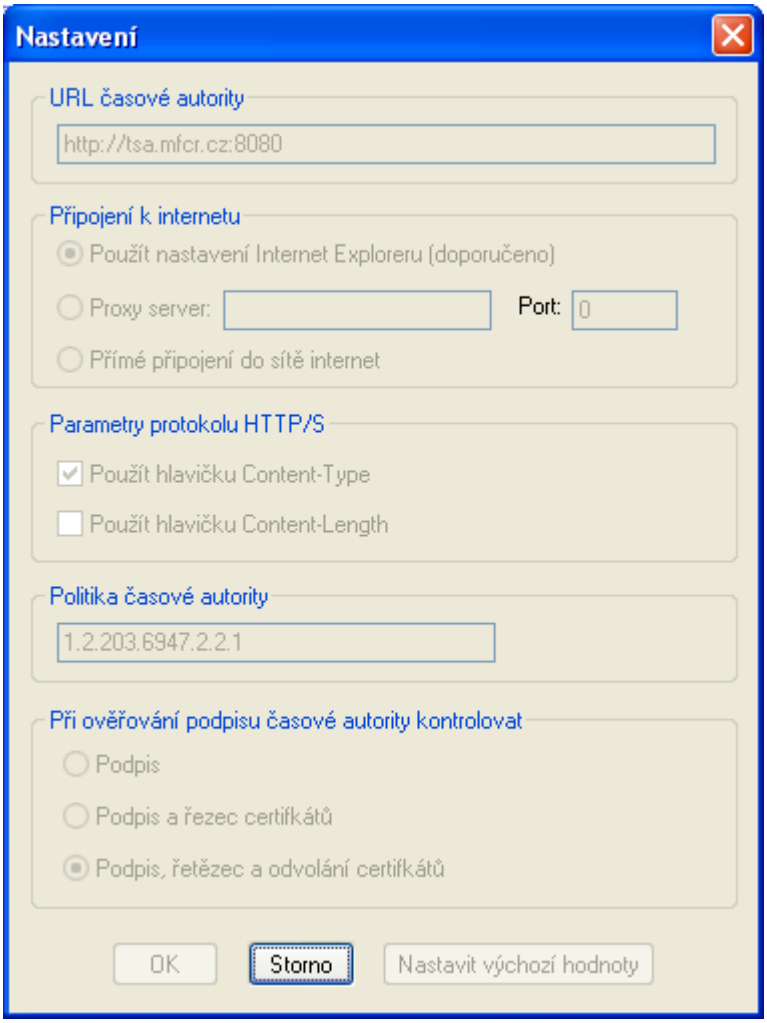
Tabulka **Podrobnosti** obsahuje jednotlivé položky časové značky.

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  v panelu nástrojů nebo příkazem nabídky **Seznam ⇨ Nastavení** lze zobrazit dialogové okno **Nastavení**.

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



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 ⇨ 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  v panelu nástrojů.

11.13. Ukončení aplikace

Aplikaci TSA Klient lze ukončit standardním způsobem klepnutím na tlačítko  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

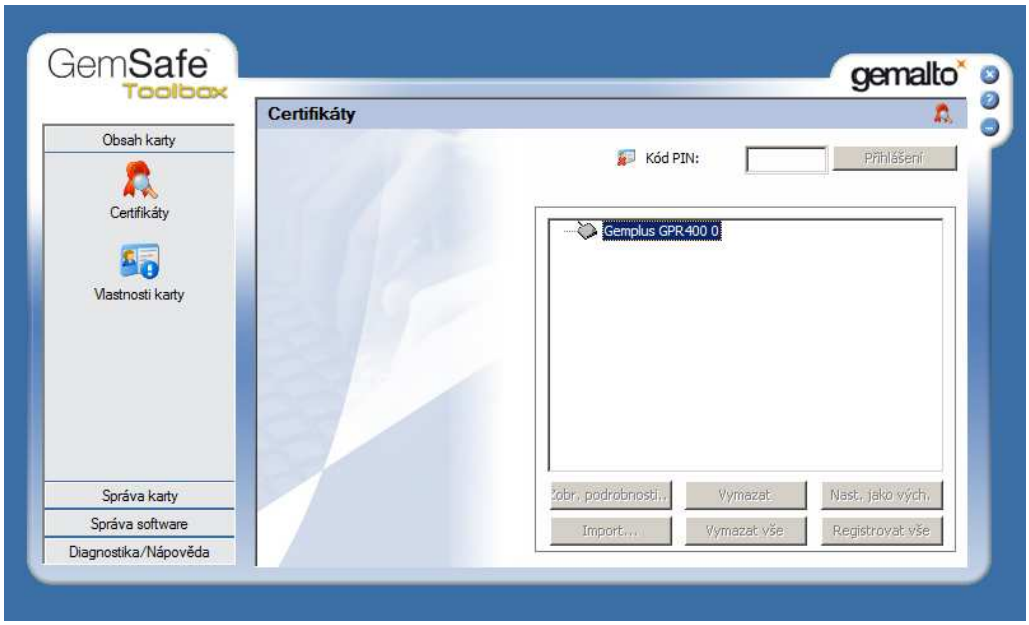
12.2. Problém s použitím certifikátu v Outlooku

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	**helpdesk**	
	MF	Problémy s používáním certifikátů v aplikacích	**helpdesk**	
	FŘ pro hl. m Prahu			
	FŘ v Brně			
	FŘ v Českých Budějovicích			
	FŘ v Hradci Králové			
	FŘ v Ostravě			
	FŘ v Plzni			
	FŘ v Praze			
	FŘ v Ustí n. Labem			
	GŘC			
	CŘ v Ostravě			
	Generální 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

Systém PKI

Žádost o vydání uživatelské čipové karty *)		
Žádost o vydání uživatelského certifikátu *)		
Žádost o vydání testovacího uživatelského certifikátu *)		
***Údaje o uživateli**:*		
Titul:		
Jméno:		
Příjmení:		
Osobní číslo:		
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :		
Název:		
Adresa:		
Byl(a) jsem seznámen(a) s certifikační politikou), příručkou uživatele PKI a povinnostmi uvedenými na této žádosti. Souhlasím s použitím osobních údajů pro fungování systému PKI a žádám o vydání čipové karty / certifikátu*).**		
Datum:		
Podpis uživatele:		
Souhlas vedoucího zaměstnance s vydání čipové karty / certifikátu*) pro výše uvedeného žadatele.		
Jméno Vedoucího zaměstnance organizační jednotky/útvaru		
Datum:		
Podpis Vedoucího zaměstnance		
Potvrzuji, že jsem od správce CA převzal(a) čipovou kartu/certifikát*) s číslem ID:		
Datum:	Podpis uživatele:	Podpis předávajícího:

*) **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 vydání autentizačního tokenu operátora RA *)	
Žádost o vydání certifikátu pro operátora RA *)	
***Údaje o operátorovi**:*	
Titul:	
Jméno:	
Příjmení:	
Osobní číslo:	
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :	
Název	
Adresa	
Byl(a) jsem seznámen(a) s Certifikační politikou).**	
Žádám o vydání autentizačního tokenu operátora registrační autority *)	
Žádám o vydání certifikátu operátora registrační autority*)	
Datum:	
Podpis zaměstnance:	
Souhlas vedoucího zaměstnance s vydáním autentizačního tokenu operátora registrační autority pro výše uvedeného operátora.*)	
Souhlas vedoucího zaměstnance s vydáním certifikátu operátora registrační autority pro výše uvedeného operátora.*)	
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 převzetí autentizačního tokenu operátora RA		
***Údaje o zaměstnanci**:*		
Titul:		
Jméno:		
Příjmení:		
Osobní číslo:		
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :		
Název		
Údaje o přebírané autentizačního tokenu:		
Číslo tokenu:		
Potvrzuji, že jsem od správce CA převzal(a) autentizační token s výše uvedeným číslem.		
Jméno zaměstnance:		
Datum:		
Podpis zaměstnance:		
Datum	jméno správce CA	podpis předávajícího

Žádost o zneplatnění certifikátu	
***Údaje o zaměstnanci**:*	
Titul:	
Jméno:	
Příjmení:	
Osobní číslo:	
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :	
Název	
Číslo certifikátu:	
Žádám o:	
	zneplatnění certifikátu s uvedeným číslem
	zneplatnění všech certifikátů vydaných pro uvedeného zaměstnance
Důvod žádosti:	
	ztráta čipové karty
	prozrazení PIN
	odchod zaměstnance
	změna údajů uvedených v certifikátu
Jméno zaměstnance:	
Datum:	
Podpis zaměstnance:	
Jméno vedoucího zaměstnance:	
Datum:	
Podpis vedoucího zaměstnance:	

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	
***Údaje o operátorovi**:*	
Titul:	
Jméno:	
Příjmení:	
Osobní číslo:	
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :	
Název	
Číslo certifikátu:	
Žádám o:	
	zneplatnění certifikátu s uvedeným číslem
	zneplatnění všech certifikátů vydaných pro uvedeného zaměstnance
Důvod žádosti:	
	ztráta tokenu
	prozrazení PIN
	odchod zaměstnance
	změna údajů uvedených v certifikátu
Jméno zaměstnance:	
Datum:	
Podpis zaměstnance:	
Jméno vedoucího zaměstnance organizační jednotky/útvaru:	
Datum:	
Podpis vedoucího zaměstnance :	

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/serveru:	
DC 2 (*ds* pro Daňovou správu, *urad* pro ministerstvo financí)	
DC.3 (jméno subdomény FŘ, např. ***br*** pro FŘ Brno) :	
OU (číslo ÚFO) :	
CN - jméno aplikace/serveru :	
DNS jméno (*nepovinné*) :	
Byl(a) jsem seznámen(a) s Certifikační politikou. Generování klíčů a digitální žádosti o certifikát pro aplikaci bylo provedeno v souladu s tímto Certifikační politikou. Digitální žádost o certifikát a její textový opis jsou nedílnou součástí této žádosti.	
Organizační jednotky/útvar (ÚFO, 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 certifikátu pro 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 testovacího certifikátu aplikace/serveru)*	
Údaje o aplikaci a certifikátu	
Jméno aplikace tak, jak je uvedeno v certifikátu	
Sériové číslo certifikátu:	
Potvrzuji, že jsem převzal(a) certifikát s výše uvedeným sériovým a tento certifikát instaloval(a) do výše uvedené aplikace.	
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**

Žádost o zneplatnění certifikátu aplikace/serveru	
***Údaje o správci aplikace**:*	
Titul:	
Jméno:	
Příjmení:	
Osobní číslo:	
Organizační jednotky/útvar (ÚFO, CŘ, CÚ, útvaru MF/GŘC, územní pracoviště ÚZSVM) :	
Název	
Údaje o aplikaci:	
Jméno aplikace tak, jak je uvedeno v certifikátu	
Sériové číslo certifikátu	
Žádám o:	
	zneplatnění certifikátu s daným sériovým číslem
	zneplatnění všech certifikátů vydaných pro danou aplikaci
Důvod žádosti:	
	zničení soukromého klíče aplikace
	prozrazení soukromého klíče aplikace
	změna údajů uvedených v certifikátu
Jméno vedoucího zaměstnance organizační jednotky/útvaru	
Datum:	
Podpis vedoucího zaměstnance	
Jméno správce aplikace:	
Datum:	
Podpis 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 seznámen(a) s Certifikační politikou. Generování klíčů a digitální žádosti o certifikát pro aplikaci bylo provedeno v souladu s tímto Certifikační politikou. Digitální žádost o certifikát 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 certifikátu 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:	

Žádost o vydání kvalifikovaného certifikátu - potvrzení o zaměstnaneckém poměru

(platné pro resort MF)

Žadatel

Titul: ..... **Jméno:** ..... **Příjmení:** ..... **Titul za:** .....

R.Č.: ..... bytem: .....

Č.OP.: ....

Osobní číslo: .....

E-mail adresa: .....

Pracovní zařazení (funkce): .....

Žádám o vydání zaměstnaneckého kvalifikovaného certifikátu a souhlasím s elektronickým zpracováním výše uvedených osobních údajů pro potřeby zpracování žádosti u I.CA

Datum ....

(Podpis žadatele)

Potvrzení o zaměstnaneckém poměru

Tímto potvrzujeme, že žadatel pan/paní je k dnešnímu dni zaměstnancem

..... **IČ** .....

Název organizace: .....

Organizační složka: .....

Adresa organizační složky: .....

Vyjádření nadřízeného vedoucího zaměstnance

Zdůvodnění žádosti: .....

.....

.....

Datum ..... Podpis .....

Souhlas oprávněné osoby s vydáním kvalifikovaného certifikátu

Souhlasíme s tím, aby výše uvedenému zaměstnanci byl společností První certifikační autorita, a.s., vydán zaměstnanecký kvalifikovaný certifikát s uvedením názvu naší společnosti .

V ..... dne .....

..... Podpis .....

jméno a funkce oprávněná osoba

oprávněné osoby k jednání za organizaci

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 **zmocněnci**

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 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: .....

V ..... dne ....

podpis zmocněnce

(podle podpisového vzoru)

podpis zmocnitele