

Crypta - Program pro zabezpečení souborů

Uživatelská příručka

Aktuální příručky naleznete na webových stránkách PostSignum:

<https://www.postsignum.cz/sifrovani.html>

- **Postup pro zprovoznění programu Crypta**

- **Základní uživatelská příručka**

Copyright © 2010-2024 Česká pošta, s.p. a ICZ a.s.

Žádná část tohoto dokumentu nesmí být kopírována žádným způsobem bez písemného souhlasu majitelů autorských práv.

Autorská a jiná díla odvozená z tohoto díla podléhají ochraně autorských práv vlastníků.

Některé názvy produktů a společností citované v tomto díle mohou být ochranné známky příslušných vlastníků.

Obsah

1. Úvod

Standardy

[Formát souborů](#)

[Certifikáty veřejného klíče](#)

[Úložiště klíčů](#)

[Elektronický podpis](#)

[Šifrování](#)

Profil

2. Systémové požadavky a velikosti souborů

[Systémové požadavky](#)

[Maximální velikost zpracovávaných souborů](#)

3. Instalace

[Průběh instalace s grafickým rozhraním](#)

[Konzolová instalace](#)

4. Funkce programu - bez vybraného profilu

[Spuštění programu](#)

[Nastavení aplikace](#)

[Ukončení programu](#)

[Přidat profil](#)

[Adresář partnerů](#)

[Import certifikátu](#)

[Aktualizovat CRL](#)

[Chybový výstup](#)

[Dešifrovat](#)

[Ověřit podpis](#)

[Přihlášení do profilu](#)

5. Funkce programu - s vybraným profilem

[Editace profilu](#)

[Vytvoření žádosti o certifikát](#)

[Import certifikátu](#)

[Import dvojice klíčů / PKCS#12](#)

[Export certifikátu a certifikátu včetně soukromého klíče/PKCS#12](#)

[Upozornění na skončení platnosti certifikátu](#)

[Obnova certifikátu](#)

[Podpisování souborů](#)

[Podpisování a šifrování souborů](#)

6. Odinstalování

A. Rozhraní příkazové řádky

[Ověřování certifikátů vůči CRL v režimu příkazové řádky](#)

[Stažení CRL](#)

[Kopírování CRL](#)

[Šifrování](#)

[Podpisování](#)

[Dešifrování](#)

[Archivace](#)

[Uložení hesla do souboru](#)

[Výpis obsahu databáze certifikátů](#)

[Aktualizace příjemce](#)

[Zjištění stavu a platnosti certifikátu](#)

B. Aplikační programové rozhraní (API)

Seznam obrázků

- 3.1. [Příprava instalačního programu](#)
- 3.2. [Výběr jazyka pro instalaci](#)
- 3.3. [Úvodní panel](#)
- 3.4. [Úvodní panel - upozornění na předchozí verzi](#)
- 3.5. [Výběr složky pro instalaci](#)
- 3.6. [Výběr pracovního adresáře](#)
- 3.7. [Výběr složky zástupců](#)
- 3.8. [Výběr asociace souborů](#)
- 3.9. [Průběh instalace](#)
- 3.10. [Ukončení instalace](#)
- 4.1. [Úvodní obrazovka](#)
- 4.2. [Nastavení prostředí](#)
- 4.3. [Nový profil](#)
- 4.4. [Adresář partnerů](#)
- 4.5. [Nový partner](#)
- 4.6. [Import certifikátu](#)
- 4.7. [Zadat heslo k profilu](#)
- 4.8. [Dešifrovat](#)
- 4.9. [Ověřit podpis](#)
- 5.1. [Hlavní obrazovka profilu](#)
- 5.2. [Editace profilu](#)
- 5.3. [Uložit žádost](#)
- 5.4. [Import certifikátu v profilu](#)
- 5.5. [Import PKCS#12](#)
- 5.6. [Export certifikátu](#)
- 5.7. [Export PKCS#12](#)
- 5.8. [Upozornění na nutnost obnovy certifikátu](#)
- 5.9. [Uložení a odeslání žádosti při obnově certifikátu](#)
- 5.10. [Uložení a odeslání žádosti při obnově certifikátu](#)
- 5.11. [Podepsat](#)
- 5.12. [Podepsat a šifrovat](#)

Kapitola 1. Úvod

Obsah

[Standardy](#)

- [Formát souborů](#)
- [Certifikáty veřejného klíče](#)
- [Úložiště klíčů](#)
- [Elektronický podpis](#)
- [Šifrování](#)

[Profil](#)

Crypta je speciální program určený pro zákazníky České pošty, s.p., kteří potřebují předávat poště data, např. pro služby SIPO nebo platební styk, zabezpečeným způsobem, tj. opatřená zaručeným elektronickým podpisem a zašifrovaná. Program je novější verzí dříve používané aplikace Crypta, vydané v poslední verzi č. 1.3, a pracuje obdobným způsobem. Vstupní data komprimuje do archivu typu ZIP, který zabezpečuje elektronickým podpisem a zašifrováním pro konkrétní úlohu České pošty. Zákazníci předávají takto vytvořený výstupní soubor běžným způsobem na příslušné pracoviště České pošty. Tuto komunikaci Crypta nezajišťuje. Příjemce zabezpečeného souboru pak může pomocí Crypty přijatý soubor rozšifrovat a ověřit elektronický podpis. Je tak zajištěna

- důvěrnost,
- integrita a
- nepopíratelnost

předávaných dat.

Návrh programu Crypta je v souladu se současnou praxí ve vztahu mezi zákazníky České pošty a Českou poštou. Každá úloha České pošty má pro šifrování souborů svůj vlastní certifikát. Zákazníci jsou identifikováni samostatně v jednotlivých úlohách ČP, mají tedy pro každou úlohu jiný certifikát, certifikát s jiným rozlišovacím jménem. Nejsou ale odděleny certifikáty pro šifrování a podpis.

Crypta používá výhradně certifikáty Veřejné certifikační autority PostSignum VCA České pošty. Nelze tedy již použít certifikáty vydané Interní autoritou ČP. Platnost certifikátů se ověřuje vůči aktuálním seznamu zneplatněných (odvolaných) certifikátů (CRL).

Program Crypta je napsán v programovacím jazyce Java, konkrétně verze 1.8, a může tedy běžet na všech platformách, které podporují běhové prostředí Javy příslušné verze nebo vyšší. Pro zajištění kryptografických funkcí využívá Crypta kryptografické knihovny IAIK.

Program Crypta je možno volat jak ručním způsobem přes grafické rozhraní, tak i z jiných aplikací přes rozhraní příkazové řádky nebo programové aplikační rozhraní (API).

Software je dodáván s komfortním instalačním programem. V případě vydání nové verze bude možné software Crypta aktualizovat přes aktualizací web ČP PowerUpdate.

Crypta neumožňuje zpracovávat soubory vytvořené v předchozí verzi Crypta 1.3 pro OS Windows. Zpětná kompatibilita je zajištěna pouze v rozsahu rozpoznání předchozího formátu.

Standardy

Formát souborů

Crypta používá pro zabezpečené soubory formát dle standardu PKCS#7 (CMS) - SignedData a EnvelopedData. S předchozí verzí Crypta 1.3 je kompatibilní jen do té míry, že rozpozná předchozí formát souborů a uživatele na tuto skutečnost upozorní.

Certifikáty veřejného klíče

V aplikaci jsou podporovány certifikáty dle standardu X.509 v.3 s algoritmem klíče RSA o velikosti modulu 4096 bits.

Úložiště klíčů

Klíče a certifikáty jsou ukládány do souborů dle standardu PKCS#12.

Elektronický podpis

Program vytváří elektronické podpisy dle RSA SHA256.

Šifrování

Pro šifrování je použit algoritmus AES256 nebo volitelně AES128 v modu CBC. Podle zvoleného algoritmu je generován klíč správné délky a náhodný inicializační vektor o délce 128 bitů.

Profil

Program respektuje, jak již bylo uvedeno, současnou praxi v nastavení certifikátů pro jednotlivé úlohy a zákazníky a zavádí v aplikaci tzv. profily, podobně jako Crypta 1.3, kde se toto nastavení nazývá uživatelský profil. Profil představuje specifické nastavení programu, v němž je zvolen jeden určitý podepisovací a šifrovací certifikát zákazníka a v kterém se předpokládá komunikace s jednou vybranou úlohou České pošty. Jak již bylo uvedeno, nejsou odděleny certifikáty a klíče pro šifrování a podpis.

Neveřejné údaje v profilu jsou chráněny heslem, které je společné všem uživatelům. Všichni uživatelé zavedení v příslušném operačním systému mají stejný přístup k danému profilu. Případná omezení nutno provést funkcemi operačního systému.

Kapitola 2. Systémové požadavky a velikosti souborů

Obsah

[Systémové požadavky](#)

[Maximální velikost zpracovávaných souborů](#)

Systémové požadavky

Aplikace je určena pro operační systémy Windows XP, Windows Vista, Windows 7 a Windows 8 a operační systém Linux. Běhové prostředí Java 2 (Java Runtime Environment JRE) verze 1.7 je součástí instalačního balíku pro operační systémy Windows. Doporučujeme použít běhové prostředí z instalačního balíku.

Politiky pro šifrování: Součástí běhového prostředí JRE instalovaného z CD je nastavení neomezených politik pro šifrování (Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files). Pokud pro běh programu Crypta zvolíte jiné JRE, stáhněte si soubory s politikami pro šifrování [ze stránek Javy](#). Upozornění: Bez této úpravy nebude program fungovat.

HW konfigurace pracovní stanice závisí do značné míry na velikosti zpracovávaných souborů.

Doporučená konfigurace: Pentium IV 3 GHz, 1GB RAM, 100 MB diskového prostoru, mechanika CD-ROM, myš nebo jiné polohovací zařízení, rozlišení monitoru alespoň 1024x768.

Maximální velikost zpracovávaných souborů

Maximální velikost zpracovávaných souborů závisí na velikosti paměti alokované pro běhové prostředí Javy. Implicitně je alokovaná paměť nastavena na 256MB, což stačí pro zpracování souborů do velikosti asi 60 MB. (Tento orientační údaj se vztahuje k souboru, jehož velikost se kompresí již znatelně nezmenšuje.) Pro soubory větší velikosti doporučujeme nastavit paměť na větší hodnotu. Nastavení se provádí

- pro grafické prostředí v souboru `Crypta.vmoptions`,
- pro prostředí příkazové řádky v souboru `CryptaCmd.vmoptions`,

v instalačním adresáři aplikace. Nutno nastavit hodnotu parametru spuštění Javy např. na `-Xmx512m`, příp. jinou vhodnou hodnotu, dle HW konfigurace.

Kapitola 3. Instalace

Obsah

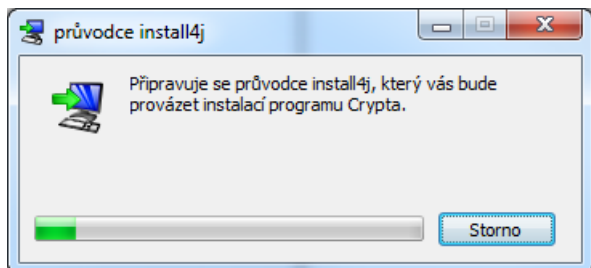
[Průběh instalace s grafickým rozhraním](#)

[Konzolová instalace](#)

Průběh instalace s grafickým rozhraním

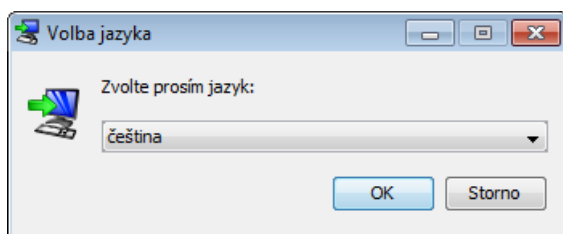
Následující obrázky demonstrují průběh instalace programu.

Obrázek 3.1. Příprava instalačního programu



V prvním okně je uživatel vyzván k výběru jazyka instalace. Lze volit mezi češtinou a angličtinou.

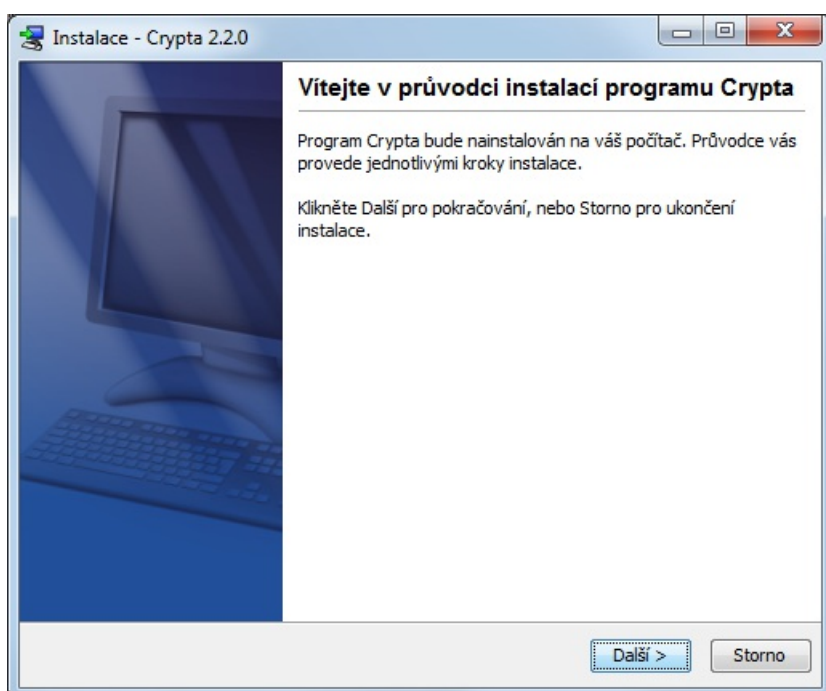
Obrázek 3.2. Výběr jazyka pro instalaci



Instalace programu vyžaduje administrátorské oprávnění. Uživatel je vyzván k zadání hesla administrátora, resp. účtu root.

Následuje úvodní panel. V průběhu instalace je doporučeno vypnout ostatní programy. Tlačítkem Další lze postoupit na další krok instalace, tlačítko Zpět slouží k návratu na předchozí dialogy ke změně nastavení. Tlačítkem Storno lze instalaci předčasně ukončit.

Obrázek 3.3. Úvodní panel



Pokud instalátor zjistí, že v systému je instalovaná dřívější verze programu Crypta, zobrazí se dialog, který nabízí uživateli výběr mezi aktualizací dřívější verze a instalací do jiného adresáře. Při umístění kurzoru na zelený symbol otazníku se zobrazí stávající

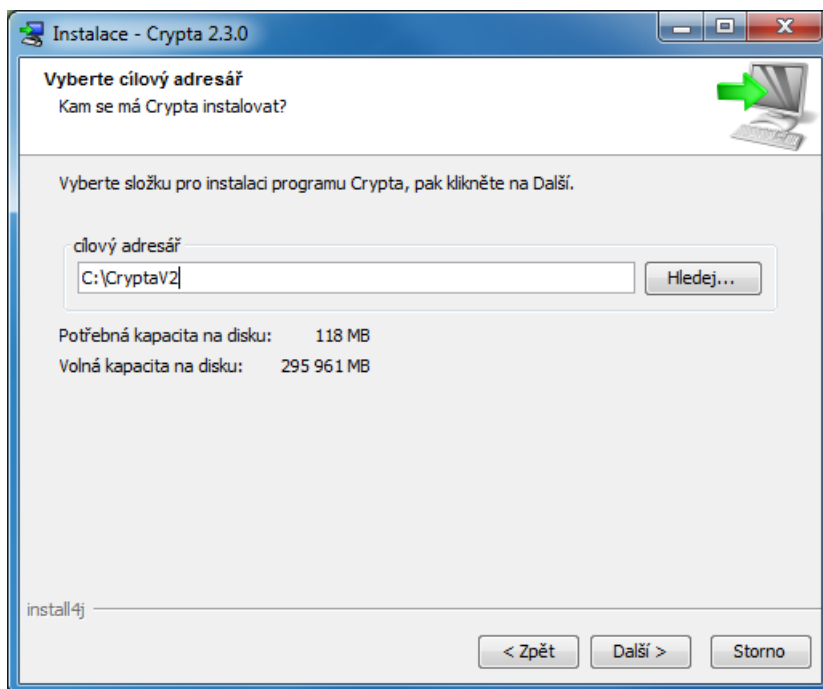
instalační adresář.

Obrázek 3.4. Úvodní panel - upozornění na předchozí verzi

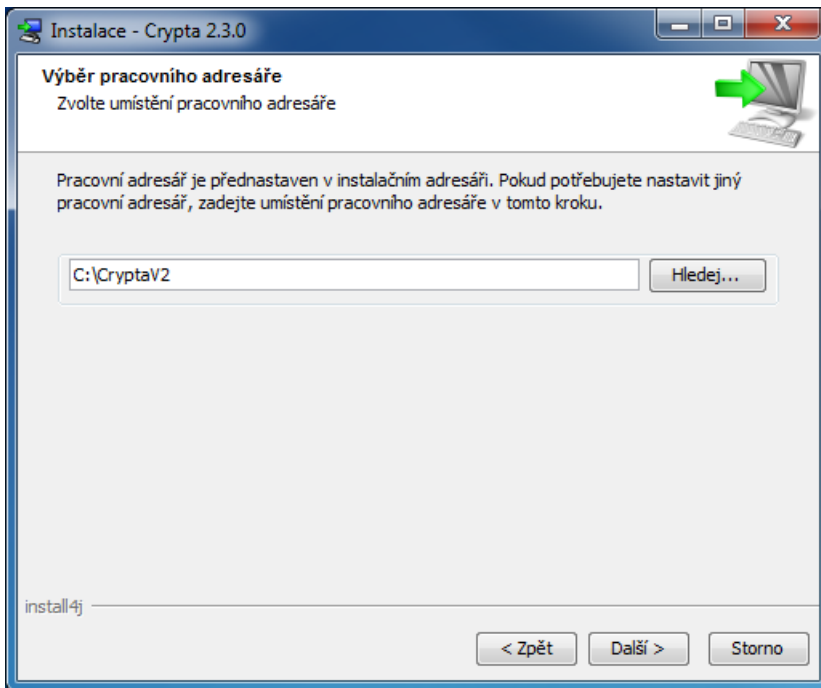


Další dialogy slouží k výběru složky, do níž bude Crypta instalována, výběru pracovního adresáře, k nastavení zástupce aplikace a k nastavení asociace souborů s programem Crypta.

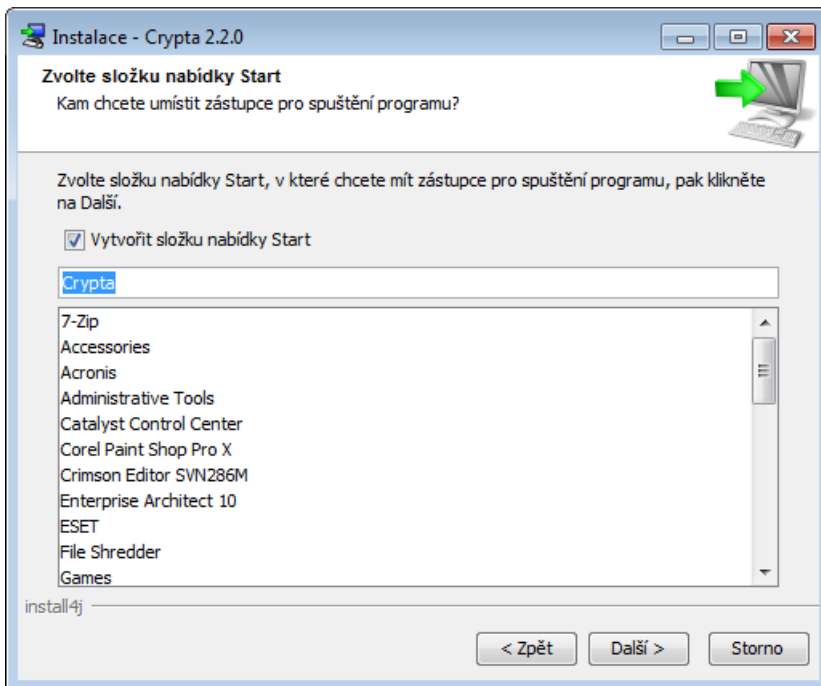
Obrázek 3.5. Výběr složky pro instalaci



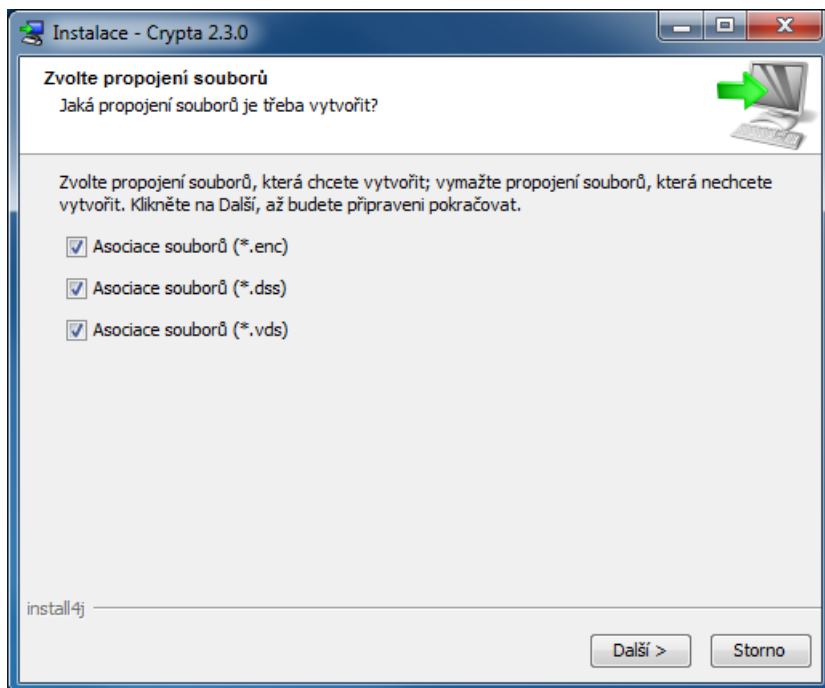
Obrázek 3.6. Výběr pracovního adresáře



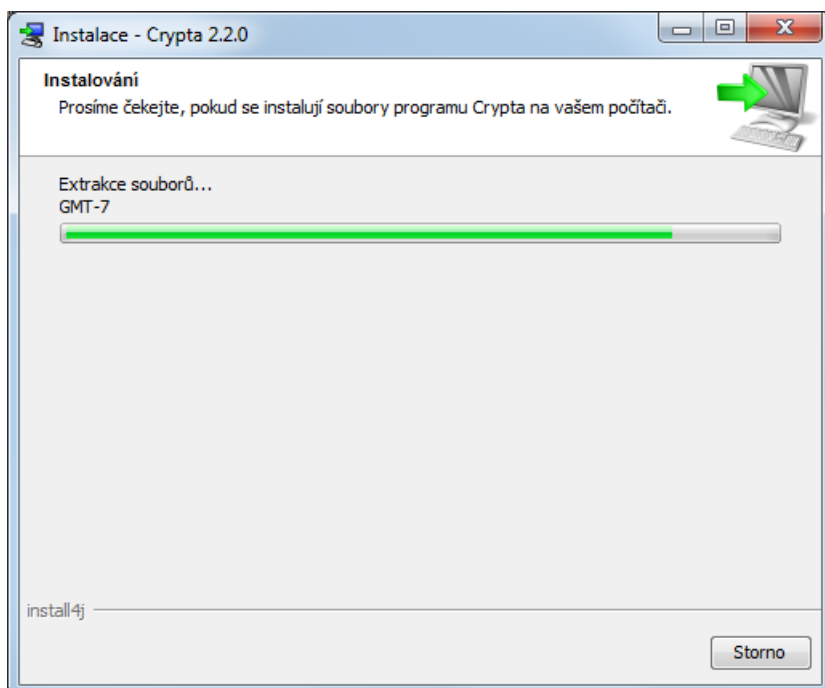
Obrázek 3.7. Výběr složky zástupců



Obrázek 3.8. Výběr asociace souborů

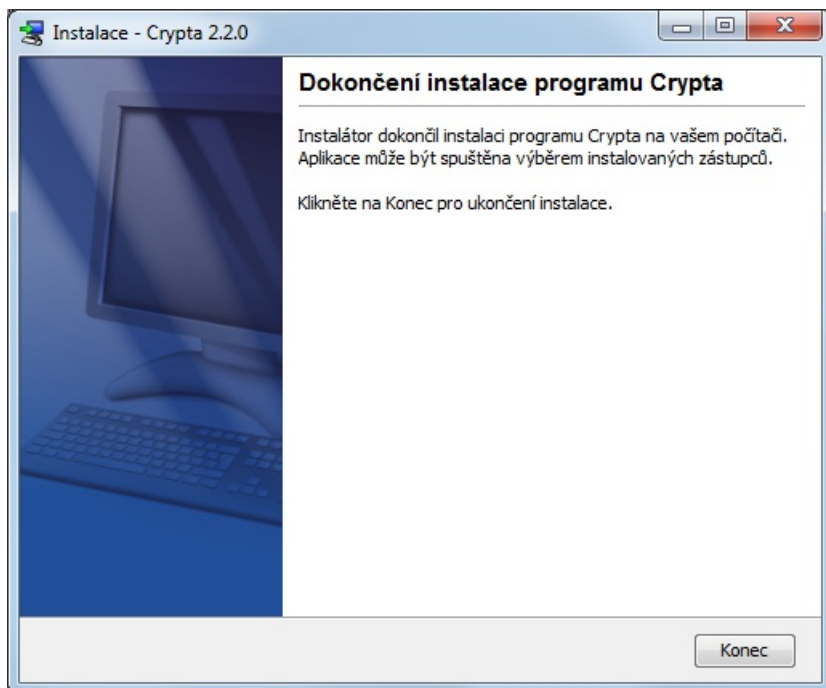


Obrázek 3.9. Průběh instalace



Uživatel je informován o průběhu a úspěšném dokončení instalace, případně o problému, který při instalaci nastal. V průběhu instalace lze ještě použít tlačítko Storno.

Obrázek 3.10. Ukončení instalace



Konzolová instalace

V případě, že v systému není k dispozici grafické uživatelské rozhraní, je možné využít konzolovou instalaci. Konzolová instalace se spouští instalátorem s parametrem -c. Např.

```
installer.exe -c
```

Kapitola 4. Funkce programu - bez vybraného profilu

Obsah

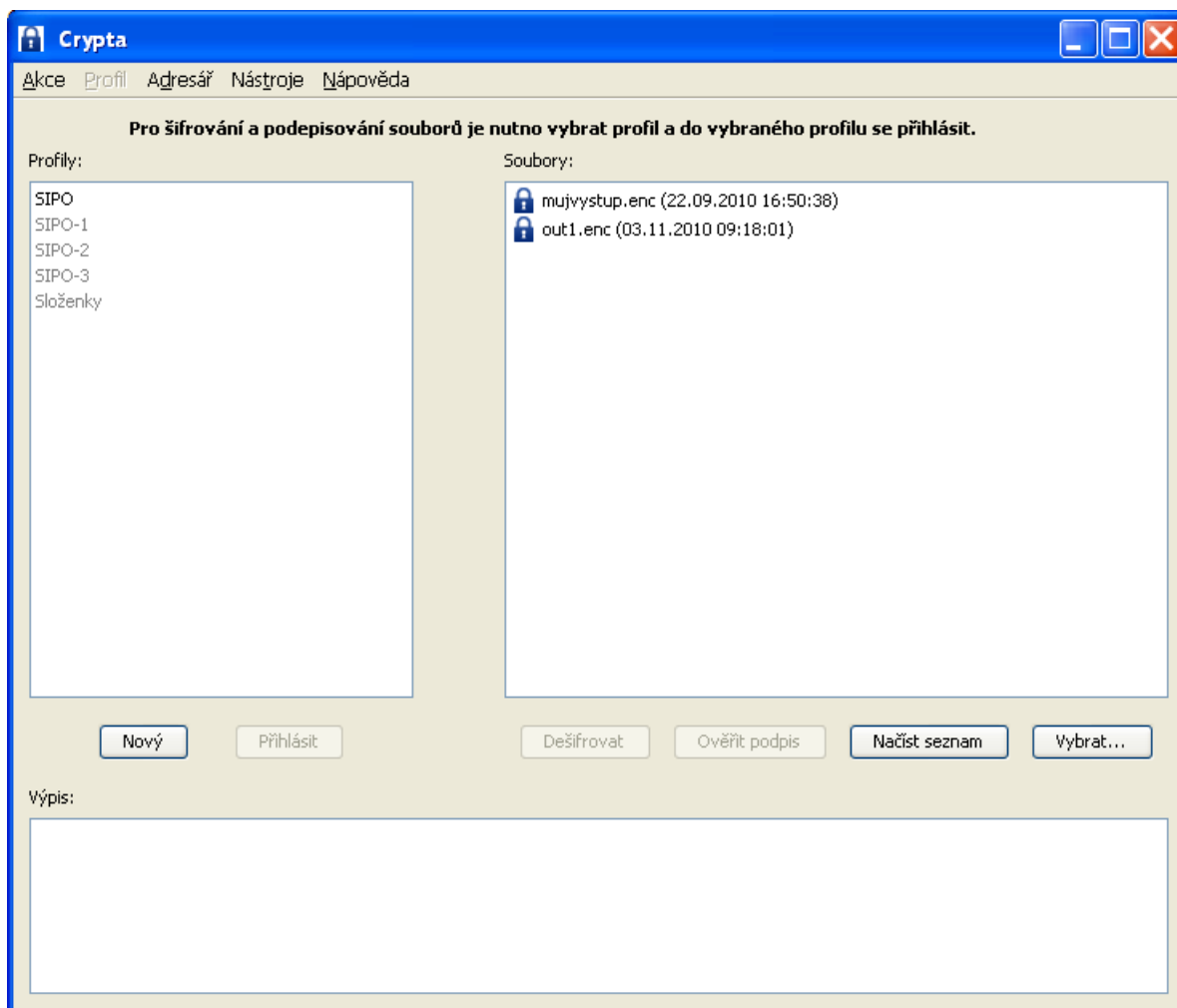
- [Spuštění programu](#)
- [Nastavení aplikace](#)
- [Ukončení programu](#)
- [Přidat profil](#)
- [Adresář partnerů](#)
- [Import certifikátu](#)
- [Aktualizovat CRL](#)
- [Chybový výstup](#)
- [Dešifrovat](#)
- [Ověřit podpis](#)
- [Přihlášení do profilu](#)

Spuštění programu

V grafickém režimu se Crypta spouští buď pomocí spouštěče Crypta.exe pro Windows, resp. Crypta pro Linux, v instalačním adresáři nebo pomocí zástupce Crypta ve zvoleném umístění.

Po spuštění programu v grafickém režimu se zobrazí úvodní obrazovka. Uživatel může zvolit jednu z akcí nabízených v menu nebo vybrat jeden z profilů, příp. založit nový profil, nebo zvolit soubor k dešifrování, příp. ověření podpisu. K dispozici je též nastavení konfigurace aplikace a nápověda. Jednotlivé funkce budou popsány v dalších odstavcích.

Obrázek 4.1. Úvodní obrazovka



Nastavení aplikace

Nastavení aplikace je přístupné z hlavního menu volbou **Nástroje/Nastavit aplikaci**. V dialogu lze zvolit tyto adresáře:

- provozní adresář tj. adresář pro ukládání vstupních i výstupních souborů,
- adresář s klíči tj. adresář pro uložení souborů s klíči profilů,
- adresář s certifikáty partnerů,
- adresář pro ukládání dočasných souborů,
- adresář pro ukládání CRL,
- adresář pro ukládání žádostí o certifikát.

Tlačítko **Vybrat** slouží k výběru adresáře v souborovém systému. Implicitní nastavení odkazuje na adresáře v instalačním adresáři aplikace **Crypta**.

V rámci nastavení aplikace lze zvolit defaultní délku symetrického klíče pro šifrování dle standardu AES, a to buď 128 nebo 256 bitů.

Součástí dialogu jsou volby:

- **Nekontrolovat CRL**. Tato volba není implicitně nastavena, umožňuje ověřit podpis, není-li k dispozici aktuální CRL .
- **Ověřit podpis vůči aktuálnímu času nebo vůči času podpisu**. Implicitně je nastaveno ověření vůči aktuálnímu času. Pokud uživatel nastaví ověření vůči času podpisu, může ověřit podpis, jehož certifikát již není časově platný.

V konfiguraci lze nastavit HTTP proxy. Po stisknutí tlačítka **Nastavit proxy** se zobrazí dialog pro zadání jména příp. IP adresy proxy serveru a čísla portu. V případě, že je potřeba se pro přístup na proxy server autentizovat, lze zadat uživatelské jméno a heslo.

V rámci nastavení aplikace lze změnit jazyk, v kterém se zobrazují texty včetně nápovědy. Přednastaven je jazyk podle národního prostředí operačního systému. V nabídce lze jazyk změnit, např. na angličtinu.

V dialogu **Nastavení aplikace** se zobrazují hodnoty parametrů pro komunikaci s certifikační autoritou **PostSignum VCA**, které jsou zde needitovatelné. Jsou to údaje:

- URL pro odeslání e-mailové žádosti o obnovu certifikátu na Podatelnu PostSignum,
- URL pro uložení žádosti o nový certifikát na webu PostSignum,
- URL pro stahování certifikátů vydaných autoritou PostSignum VCA
- URL pro stahování CRL PostSignum VCA.

Případnou změnu je možno provést na základě doporučení České pošty pouze editací souboru `jcrypta.properties` v instalačním adresáři aplikace.

Obrázek 4.2. Nastavení prostředí

Nastavení aplikace

Provozní adresář

Adresář s klíči

Adresář s certifikáty partnerů

Dočasný adresář

Adresář s CRL

Adresář se žádostmi

Šifrování

AES 128

AES 256

Ověřování podpisu

Nekontrolovat CRL

Ověřovat vůči

aktuálnímu času

času podpisu

Jazyk:

URL upload mail zpráv pro obnovu certifikátu

URL pro uložení žádosti na webu PostSignum

URL PostSignum pro stahování certifikátů

URL PostSignum pro stahování CRL

URL Postsignum pro automatické přijetí certifikátu ze serveru

Nastavené hodnoty se uloží po stisku tlačítka Uložit. Dialog je možno ukončit, aniž by došlo k uložení nastavených hodnot, tlačítkem Storno.

Ukončení programu

Program se ukončí volbou Akce/Konec v nabídce úvodní obrazovky nebo hlavní obrazovky profilu.

Přidat profil

Aby s programem bylo možno začít pracovat, je nutno vytvořit alespoň jeden profil. K vytvoření nového profilu slouží tlačítko Nový na úvodní obrazovce. Po stisknutí tohoto tlačítka se zobrazí dialog Nový profil. V horní části dialogu uživatel zadá povinně název profilu a heslo k profilu a potvrdí heslo k profilu. V sekci Údaje o zákazníkovi zadá údaje, které vstupují do certifikátu:

- Jméno (CN) - common name, běžné jméno do předmětu certifikátu, povinný údaj,
- Organizace - název organizace, povinný údaj,
- IČ - identifikační číslo organizace - nepovinný údaj,
- Organizační jednotka - nepovinný údaj,
- E-mail - nepovinný údaj.

V sekci Příjemci lze vybrat ze seznamu příjemců implicitního příjemce profilu. Implicitního příjemce lze nastavit i později, pro případ, že při založení profilu je seznam příjemců prázdný. Pokud by uživatel změnil seznam příjemců v průběhu vytváření nového profilu, má možnost aktualizovat seznam příjemců pomocí tlačítka Načíst seznam.

K uložení profilu se zadanými hodnotami slouží tlačítko Uložit. Pro opuštění dialogu je k dispozici tlačítko Storno.

Obrázek 4.3. Nový profil

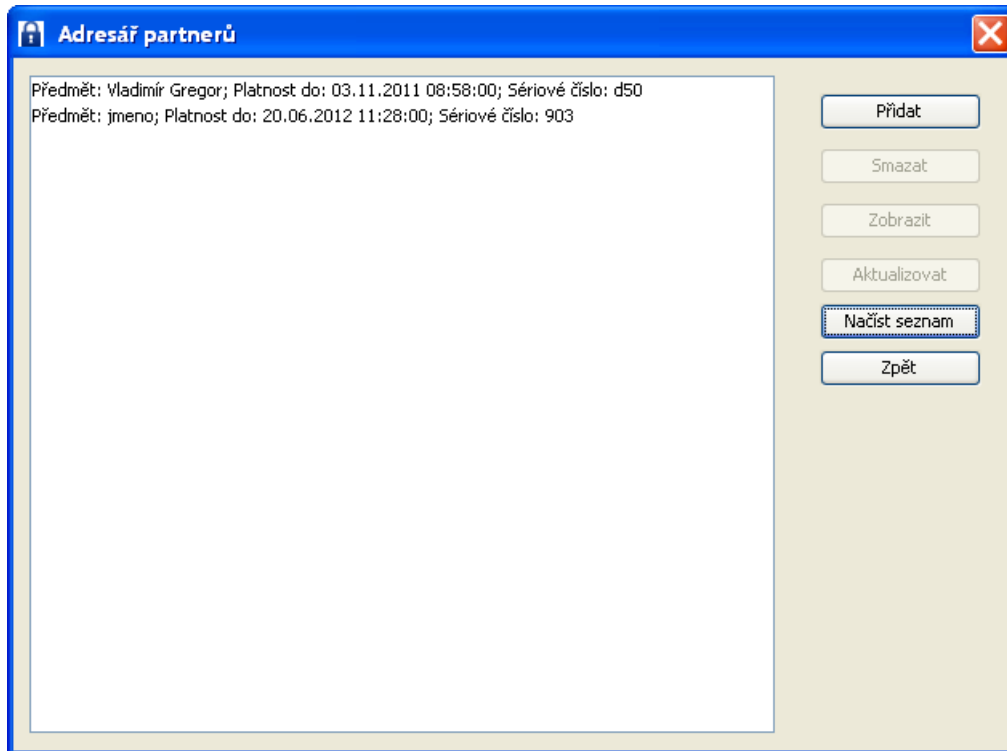
The image shows a dialog box titled "Nový profil" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Profile Information:** Three input fields labeled "Název profilu*", "Heslo*", and "Potvrdit heslo*".
- Údaje o zákazníkovi:** A section with five input fields: "Jméno (CN)*", "Organizace*", "IČ" (split into two boxes), "Org. jednotka", and "E-mail".
- Příjemci:** A list box containing three entries:
 - Předmět: Operátor Centra; Platnost do: 29.01.2016 09:28:00; Sériové číslo: 20db
 - Předmět: Vladimír Gregor Junior; Platnost do: 01.06.2017 08:47:00; Sériové číslo: 21a0
 - Předmět: Vladimír Novák; Platnost do: 31.05.2017 15:06:00; Sériové číslo: 219fA "Načíst seznam" button is located to the right of the list.
- Buttons:** At the bottom, there are two buttons: "Uložit" and "Storno".

Adresář partnerů

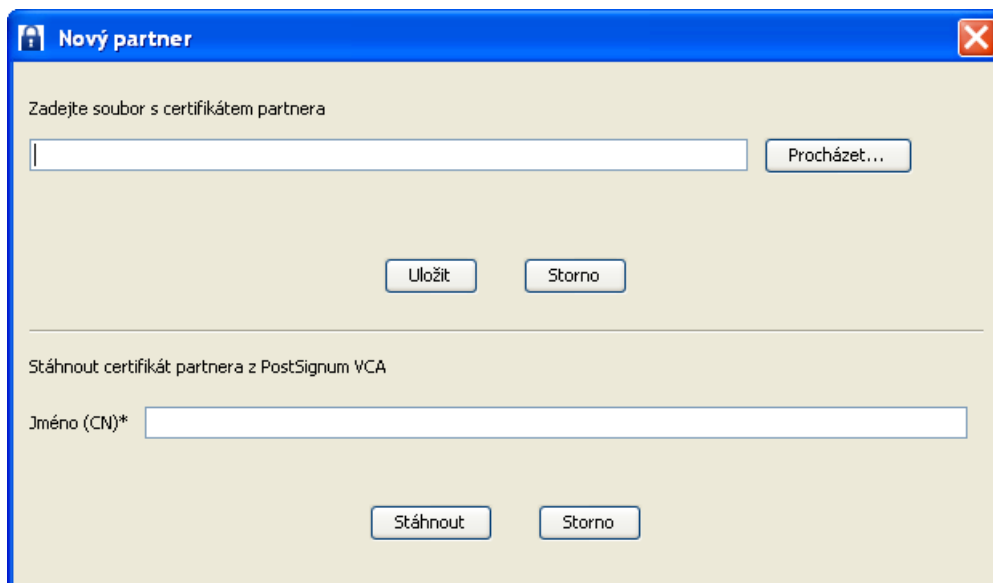
Crypta udržuje seznam partnerů, tj. potenciálních příjemců, pro něž je možno připravovat zašifrované soubory. Formulář pro správu partnerů se zobrazí po volbě Adresář z hlavní nabídky úvodní obrazovky nebo obrazovky profilu. Zobrazuje se seznam CN (common name, běžné jméno) z předmětu certifikátů partnerů uložených v adresáři partnerů, doplněný o časový údaj, kdy certifikát expiruje, a o sériové číslo certifikátu. Uživatel může zvolit jednu z akcí v pravém sloupci formuláře Přidat, Smazat, Zobrazit, Aktualizovat, Načíst seznam nebo opustit formulář přes tlačítko Zpět.

Obrázek 4.4. Adresář partnerů



Tlačítko Přidat - dialog Nový partner: Partnera lze založit buď zadáním souboru s jeho certifikátem nebo zadáním CN jeho certifikátu, který je následně automaticky stažen přes WWW pomocí služeb certifikační autority PostSignum VCA. Tlačítko Smazat slouží ke smazání příjemce ze seznamu.

Obrázek 4.5. Nový partner

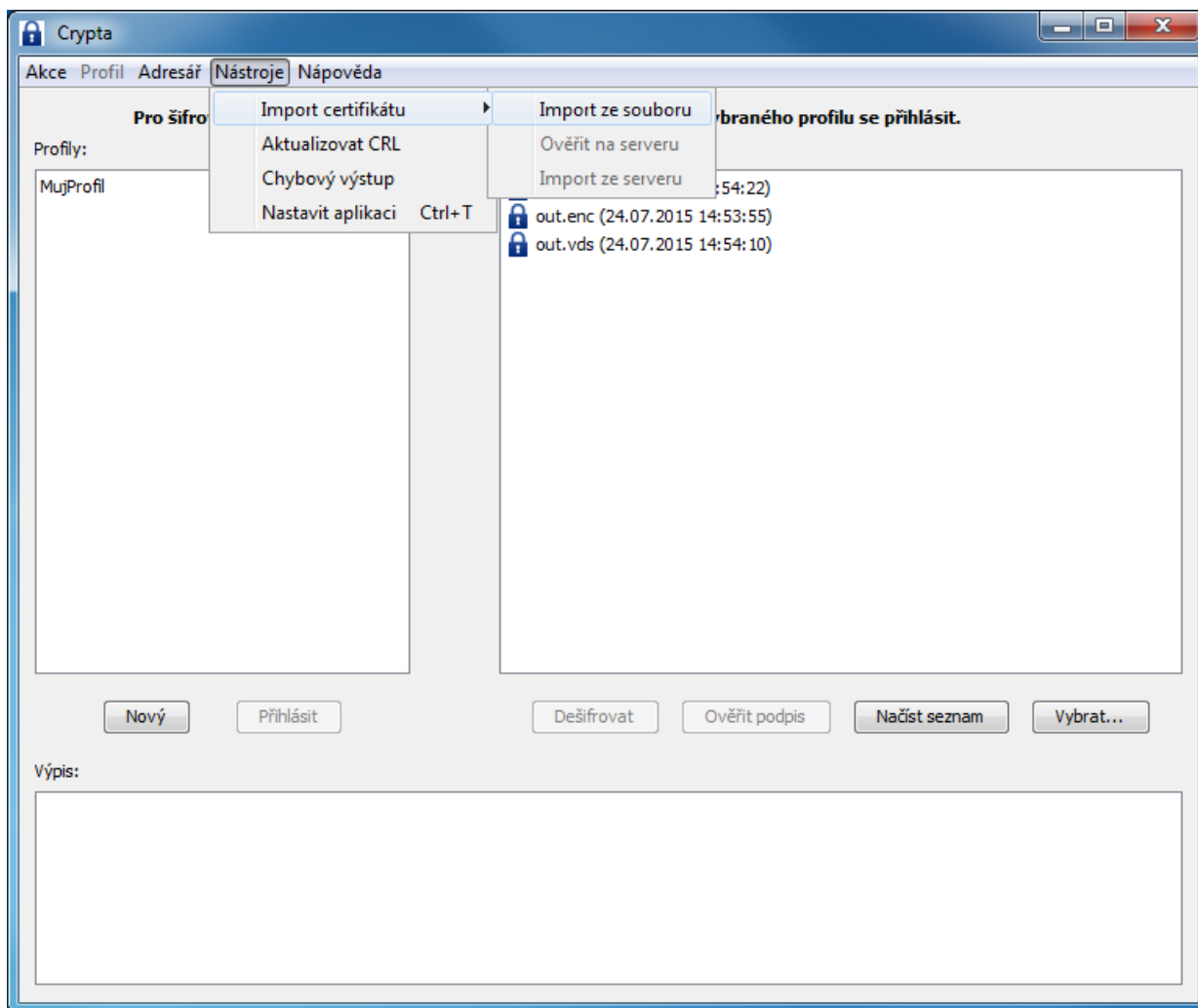


Tlačítko Zobrazit slouží k podrobnému výpisu údajů z certifikátu příjemce. Pomocí tlačítka Aktualizace se automaticky stáhne přes WWW z certifikační autority PostSignum certifikát stejného vydavatele a držitele s nejdelší platností. Po stisknutí tlačítka Načíst seznam se provede nové načtení příjemců z adresáře _data/certs.

Import certifikátu

Na úvodní obrazovce aplikace lze provést import certifikátu pomocí volby v hlavním menu Nástroje/Import certifikátu. Aktivní je nabídka Import ze souboru.

Obrázek 4.6. Import certifikátu



Volba Import ze souboru: Po jejím výběru se zobrazí dialog pro výběr souboru s certifikátem. Program pak porovná veřejný klíč certifikátu s veřejnými klíči profilů a v případě shody zobrazí dialog pro zadání hesla k nalezenému profilu. Dialog obsahuje název nalezeného profilu. Po zadání hesla proběhne import. Při importu certifikátu do profilu dojde ke změně údajů profilu tak, aby se shodovaly s údaji v certifikátu. Následně se zobrazí hlavní obrazovka profilu jako po přihlášení do profilu se zaškrtnutým příznakem Importován certifikát. V případě neúspěchu akce nebo chybného zadání parametrů se zobrazí chybové hlášení.

Aktualizovat CRL

Volba Aktualizovat CRL slouží k uložení aktuálního CRL do adresáře nastaveného v konfiguraci. Implicitně je pro ukládání CRL nastaven adresář `_data/crls` v instalačním adresáři programu. Lze např. stáhnout CRL jiným programem, vložit ho do nastaveného adresáře pomocí volby Aktualizace CRL a pak pracovat s Cryptou bez síťového připojení.

Program Crypta si CRL, které stáhne a s kterým pracuje při ověřování certifikátů, do nastaveného adresáře neukládá. Má-li použít soubory uložené v adresáři CRL, musí tam tyto soubory být již při startu programu nebo mohou být dodatečně načteny funkcí Aktualizovat CRL. Upozornění: Za běhu programu nestačí soubor CRL pouze zkopírovat do nastaveného adresáře prostředky operačního systému. Při každém spuštění Crypta maže z adresáře nepotřebná CRL.

Chybový výstup

V případě komunikace s pracovníky podpory ČP můžete být požádáni o zaslání chybového výstupu. K vytvoření takového souboru slouží volba **Nástroje/Chybový výstup**. V instalačním adresáři programu vznikne soubor `error.zip`, který obsahuje jednak logovací soubor `log.txt`, jednak soubor `dir.txt` - výpis obsahu instalačního adresáře, tj. názvy souborů a adresářů. Chybový výstup je určen k zaslání e-mailem.

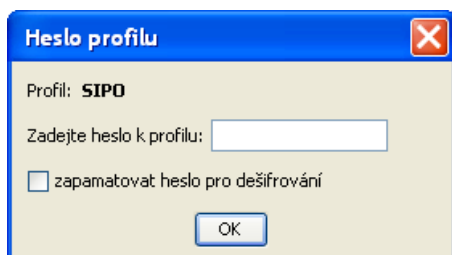
Dešifrovat

Soubor pro dešifrování je třeba umístit do provozního adresáře. Uživatel pak může vybrat soubor v seznamu na úvodní obrazovce a zvolit Dešifrovat. Lze též poklepat na název souboru. Program nalezne vhodný profil, v kterém lze soubor dešifrovat, a zobrazí dialog pro zadání hesla k profilu. V dialogu lze zaškrtnout, zda se má heslo pamatovat pro další operace dešifrování. Následuje vlastní dialog Dešifrovat. Jelikož součástí operace dešifrování je ověření podpisu, jsou součástí dialogu tyto volby:

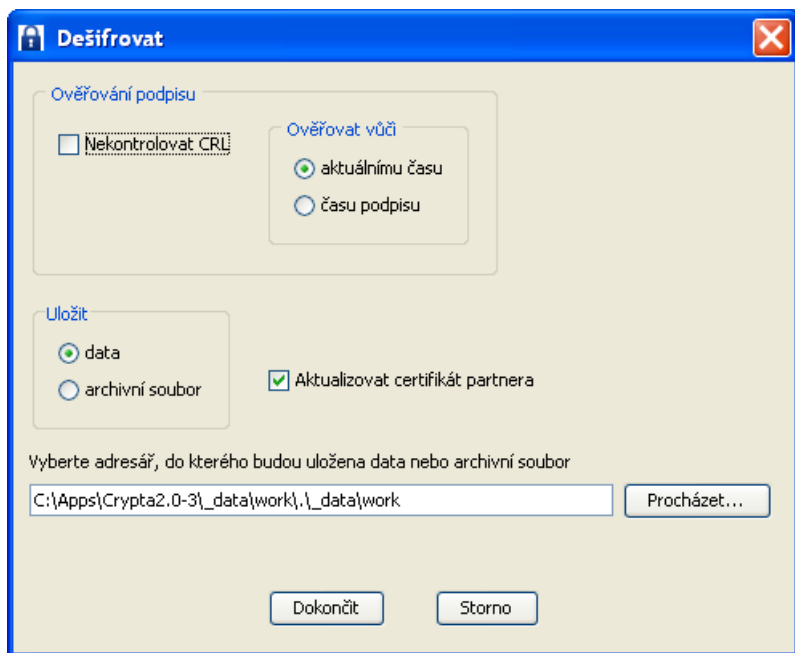
- Nekontrolovat CRL. Tato volba není implicitně nastavena, umožňuje ověřit podpis, není-li k dispozici aktuální CRL.
- Ověřit podpis vůči aktuálnímu času nebo vůči času podpisu. Implicitně je nastaveno ověření vůči aktuálnímu času. Pokud uživatel nastaví ověření vůči času podpisu, může ověřit podpis, jehož certifikát již není časově platný.

V dolní části dialogu je pak možno vybrat typ výstupu, zda má jít o jednotlivé soubory a příp. vybrat adresář, do kterého budou soubory uloženy nebo zda má být výstupem podepsaný zipovaný archiv. Součástí dialogu je zaškrťovací pole pro volbu, zda se má z podpisu v souboru převzít certifikát partnera a nahradit jím původní certifikát v adresáři.

Obrázek 4.7. Zadat heslo k profilu



Obrázek 4.8. Dešifrovat



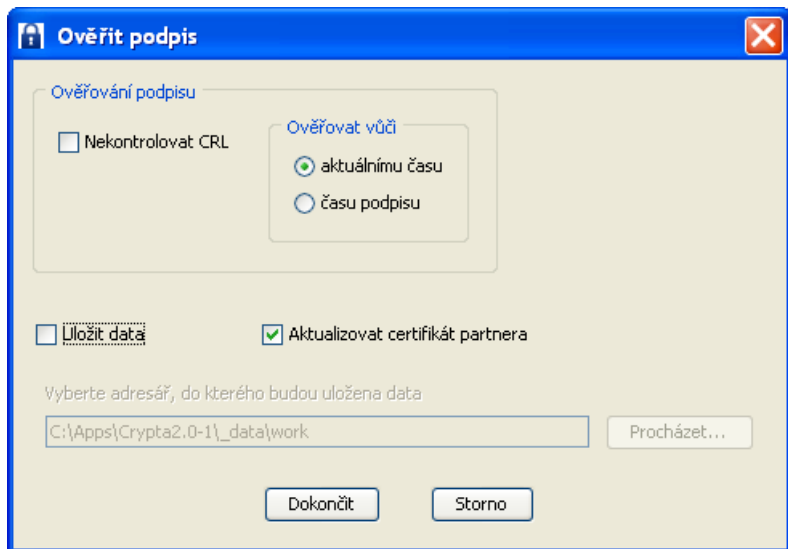
Ověřit podpis

Soubor, jehož podpis se má ověřit, je třeba umístit do provozního adresáře. Uživatel pak může soubor vybrat v seznamu Soubory na úvodní obrazovce a zvolit Ověřit podpis. Lze též poklepat na název souboru. Zobrazí se dialog Ověřit podpis pro nastavení operace. Součástí dialogu jsou opět volby:

- Nekomrolovat CRL. Tato volba není implicitně nastavena, umožňuje ověřit podpis, není-li k dispozici aktuální CRL.
- Ověřit podpis vůči aktuálnímu času nebo vůči času podpisu. Implicitně je nastaveno ověření vůči aktuálnímu času. Pokud uživatel nastaví ověření vůči času podpisu, může ověřit podpis, jehož certifikát již není časově platný.

Lze též zvolit, zda se má jen ověřit podpis na archivním souboru, nebo zda se mají data z archivního souboru uložit do adresáře. Pokud je vybrána volba Uložit data, zobrazí se pole pro výběr nebo zadání adresáře, do kterého se mají uložit data. V případě, že ve vybraném adresáři soubory stejného jména již existují, je uživateli zobrazen dotaz, zda se mají data přepsat.

Obrázek 4.9. Ověřit podpis



Přihlášení do profilu

Přihlášení do profilu probíhá na úvodní obrazovce. Uživatel vybere v okně Profily daný profil a zvolí Přihlásit. Je možné též poklepat na název profilu. Následuje dialog pro zadání hesla a při správně zadaném hesle se zobrazí hlavní obrazovka profilu. Při nesprávně zadaném hesle je uživatel upozorněn a program se vrací na úvodní obrazovku.

Kapitola 5. Funkce programu - s vybraným profilem

Obsah

[Editace profilu](#)

[Vytvoření žádosti o certifikát](#)

[Import certifikátu](#)

[Import dvojice klíčů / PKCS#12](#)

[Export certifikátu a certifikátu včetně soukromého klíče/PKCS#12](#)

[Upozornění na skončení platnosti certifikátu](#)

[Obnova certifikátu](#)

[Podpisování souborů](#)

[Podpisování a šifrování souborů](#)

Po přihlášení do profilu se uživateli zobrazí hlavní obrazovka profilu. V rámci zvoleného profilu se zobrazí údaje o zákazníkovi tak, jak vstupují do certifikátu tj. běžné jméno (CN), organizace (O), IČO, organizační jednotka (OU) a E-mail. Na hlavní obrazovce profilu jsou k dispozici volby pro správu certifikátu profilu: vytvořit žádost, import certifikátu, export certifikátu, export dvojice klíčů a certifikátu (PKCS#12) a import dvojice klíčů a certifikátu (PKCS#12).

Obrázek 5.1. Hlavní obrazovka profilu

Crypta - profil: SIPO

Akce Profil Adresář Nástroje Nápověda

Žádost vytvořena
 Importován certifikát

Údaje o zákazníkovi

Jméno (CN)

Organizace

IČ

Org. jednotka

E-mail

Výpis

Pomocí needitovatelných zaškrtnutých polí je indikováno, zda již v profilu byla vytvořena žádost a zda již byl případně importován certifikát. Pokud byla žádost o certifikát zaslána do úložiště žádostí certifikační autority PostSignum, je zobrazeno i identifikační číslo žádosti.

Z hlavní obrazovky profilu jsou pomocí tlačítek v pravé části obrazovky k dispozici funkce Podpsat a šifrovat a Podpsat. Pomocí těchto tlačítek jsou k dispozici příslušné dialogy popsané dále. Z této obrazovky je v menu k dispozici volba Editace profilu a Nastavení aplikace.

Editace profilu

Uživatel se přihlásí k profilu a zvolí v hlavní nabídce akci Profil/Editace profilu. V rámci editace profilu lze měnit pouze heslo k profilu a nastavení příjemce. Po zadání a potvrzení nového hesla k profilu, je uživatel vyzván, aby se autentizoval vložením původního hesla.

Obrázek 5.2. Editace profilu

Editace profilu - profil: MujProfil_1

Název profilu*

Heslo*

Potvrdit heslo*

Údaje o zákazníkovi

Jméno (CN)*

Organizace*

IČ

Org. jednotka

E-mail

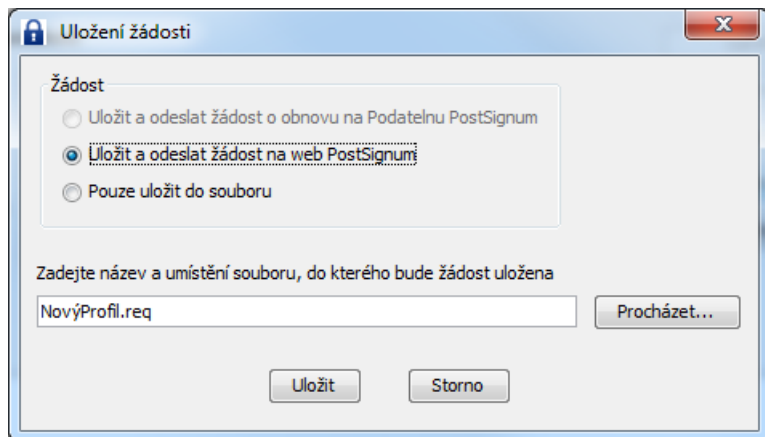
Příjemci

Předmět: Operátor Centra; Platnost do: 29.01.2016 09:28:00; Sériové číslo: 20db
Předmět: Operátor ORA; Platnost do: 28.01.2016 14:26:00; Sériové číslo: 20d6

Vytvoření žádosti o certifikát

Žádost o certifikát lze vytvořit na hlavní obrazovce profilu pomocí volby Vytvořit žádost. Předpokladem je, že do profilu ještě nebyl importován certifikát. Uživateli se zobrazí dialog pro uložení souboru se žádostí a výběr možností odeslání. Lze vybrat volbu Uložit a odeslat žádost na web Postsignum nebo Pouze uložit do souboru a zvolit název a umístění souboru se žádostí v systému uživatele. Přednastaven je název souboru ve tvaru *název_profilu.req*. Do položky OU je vložen text *Crypta2_název_profilu*. Žádost je ukládána ve formátu PKCS#10 PEM. Následně je v profilu vyplněn příznak žádosti. V dolním poli formuláře se vypisuje protokol o provedených akcích. Po vydání certifikátu provede uživatel jeho import pomocí volby Nástroje/Import certifikátu v hlavní nabídce na úvodní obrazovce programu.

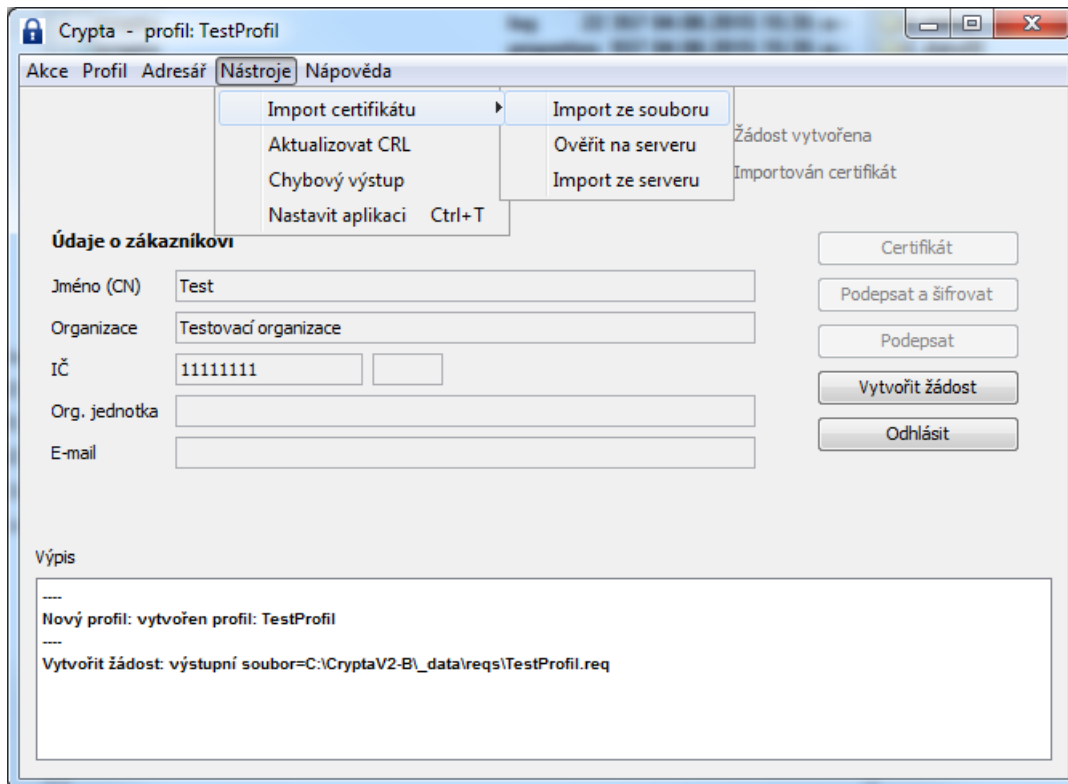
Obrázek 5.3. Uložit žádost



Import certifikátu

Na úvodní obrazovce aplikace lze provést import certifikátu pomocí volby v hlavním menu Nástroje/Import certifikátu. Nabídka se dále větví: Import ze souboru, Ověřit na serveru, Import ze serveru. Tyto volby jsou popsány v následujících odstavcích.

Obrázek 5.4. Import certifikátu v profilu



Volba Import ze souboru: Po jejím výběru se zobrazí dialog pro výběr souboru s certifikátem. Program pak porovná veřejný klíč certifikátu s veřejnými klíči profilů a v případě shody zobrazí dialog pro zadání hesla k nalezenému profilu. Dialog obsahuje název nalezeného profilu. Po zadání hesla proběhne import. Při importu certifikátu do profilu dojde ke změně údajů profilu tak, aby se shodovaly s údaji v certifikátu. Následně se zobrazí hlavní obrazovka profilu jako po přihlášení do profilu se zaškrtnutým příznakem Importován certifikát. V případě neúspěchu akce nebo chybného zadání parametrů se zobrazí chybové hlášení.

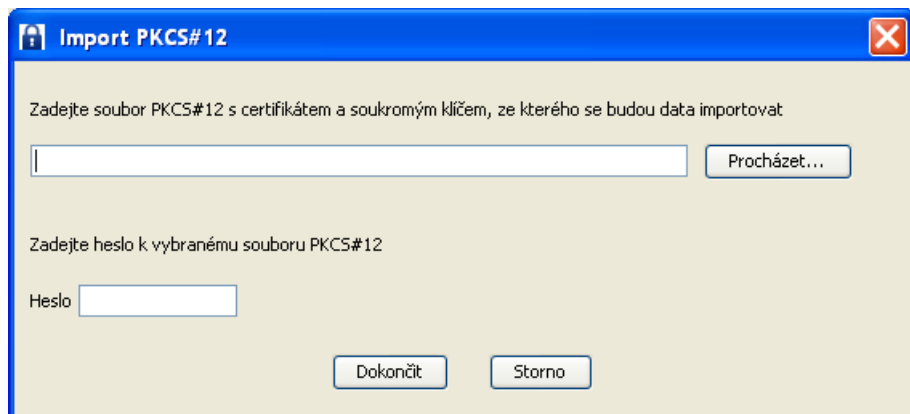
Volba Ověřit na serveru: Crypta zjistí na serveru certifikační autority, zda je k dispozici protokol o vydání certifikátu. Pokud ano, Crypta nabídne protokol ke stažení.

Volba Import ze serveru: Crypta provede import vydaného certifikátu ze serveru certifikační autority a uloží certifikát do profilu.

Import dvojice klíčů / PKCS#12

Pro import dvojice klíčů slouží volba Profil/Import PKCS#12. Po výběru volby se uživateli zobrazí dialog pro nové zadání hesla k profilu. Po kontrole hesla se otevře formulář pro výběr souboru PKCS#12 a zadání jeho hesla. Po vložení údajů je proveden import dvojice klíčů a je změněn identifikátor certifikátu. V dolním poli formuláře se vypisuje protokol o provedených akcích.

Obrázek 5.5. Import PKCS#12



Import PKCS#12

Zadejte soubor PKCS#12 s certifikátem a soukromým klíčem, ze kterého se budou data importovat

Procházet...

Zadejte heslo k vybranému souboru PKCS#12

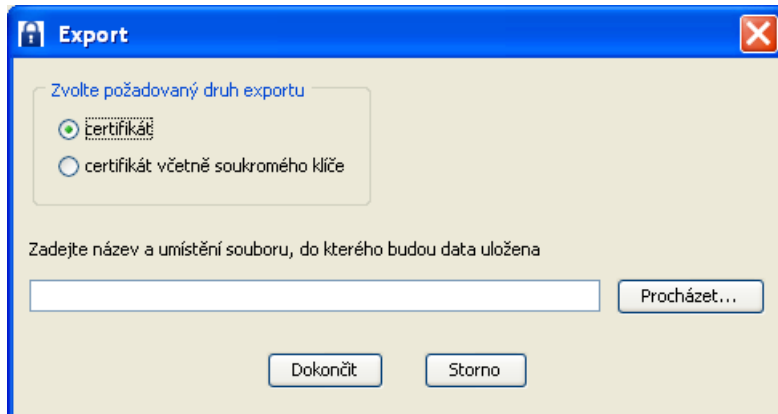
Heslo

Dokončit Storno

Export certifikátu a certifikátu včetně soukromého klíče/PKCS#12

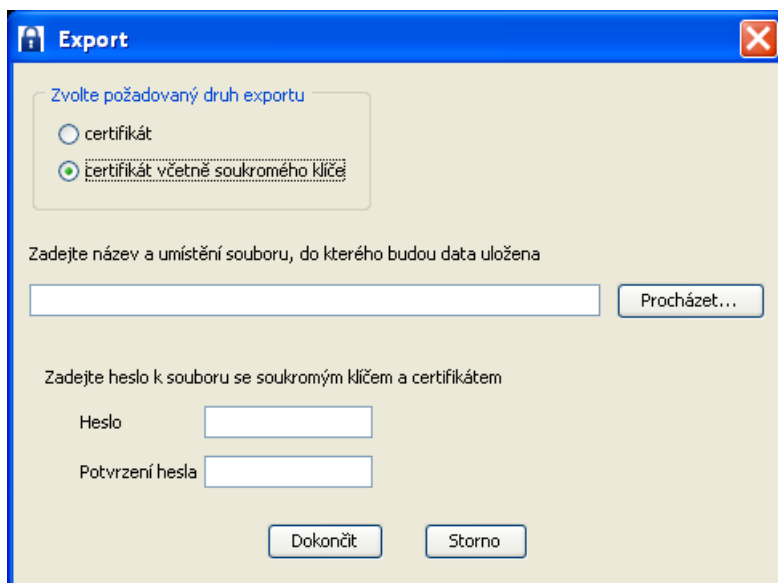
Pro export certifikátu, resp. dvojice klíčů slouží volba Profil/Export certifikátu PKCS#12. Uživateli se zobrazí dialog pro export certifikátu. V horní části je zobrazena volba druhu exportu, zda se má exportovat samotný certifikát profilu nebo zda se má exportovat certifikát včetně soukromého klíče. Podle tohoto nastavení se mění vlastní dialog exportu. V případě exportu samotného certifikátu se zobrazí pole pro zadání exportního souboru. Implicitní koncovka názvu souboru je cer. Po výběru souboru je proveden export certifikátu profilu ve formátu DER. Předpokladem je, že v profilu je importován certifikát.

Obrázek 5.6. Export certifikátu



V případě exportu certifikátu včetně soukromého klíče se uživateli zobrazí dialog pro zadání exportního souboru a hesla k PKCS12. Heslo se zkontroluje na sílu hesla. Následuje dialog pro zadání hesla k profilu. Po správném zadání všech údajů je proveden export.

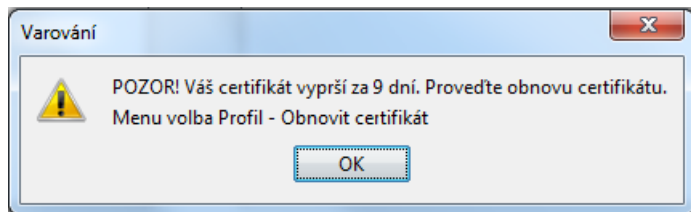
Obrázek 5.7. Export PKCS#12



Upozornění na skončení platnosti certifikátu

Pokud certifikátu skončí platnost za dobu kratší než 20 dnů, upozorňuje program na nutnost jeho obnovy. Upozornění se zobrazuje při přihlášení do profilu a při dešifrování souboru.

Obrázek 5.8. Upozornění na nutnost obnovy certifikátu



Obnova certifikátu

Při obnově certifikátu se vytváří nový profil jako kopie profilu původního a až v novém profilu je možno vytvořit žádost o obnovený certifikát (certifikát nového profilu). Uživatel se přihlásí do profilu a zvolí v hlavní nabídce Profil/Obnovit certifikát. Zobrazí se mu formulář nového profilu s údaji převzatými z původního certifikátu resp. profilu. Pro název nového profilu se nabízí hodnota, která vychází z názvu původního profilu, doplněná pořadovou číslicí. Název nového profilu lze editovat. Nutno vyplnit a potvrdit heslo nového profilu.

Obrázek 5.9. Uložení a odeslání žádosti při obnově certifikátu

Obnova certifikátu - nový profil vytvořený z profilu: MujProfil

Název profilu* MujProfil-2

Heslo*

Potvrdit heslo*

Údaje o zákazníkovi

Jméno (CN)* Operátor ORA

Organizace* ICZ a.s.

IČ 25145444

Org. jednotka 15162

E-mail vladimir.gregor@i.cz

Příjemci

Předmět: Operátor ORA; Platnost do: 28.01.2016 14:26:00; Sériové číslo: 20d6

Načíst seznam

Uložit Storno

Po vytvoření nového profilu vytvoří uživatel žádost, která se pak odešle v na podatelnu certifikační autority PostSignum. K tomu slouží volba "Uložit a odeslat žádost o obnovu na podatelnu PostSignum" v dialogu "Uložení žádosti". Programem vytvořená datová struktura je podepsána klíčem svázaným s původním certifikátem. Certifikační autorita vydá obnovený tzv. následný certifikát a odešle uživateli e-mail s touto informací a pokyny pro stažení certifikátu.

Obrázek 5.10. Uložení a odeslání žádosti při obnově certifikátu

Uložení žádosti

Žádost

Uložit a odeslat žádost o obnovu na Podatelnu PostSignum

Uložit a odeslat žádost na web PostSignum

Pouze uložit do souboru

Zadejte název a umístění souboru, do kterého bude žádost uložena

TestProfil-1.req

Procházet...

Uložit Storno

Pokud se vám volba "Uložit a odeslat žádost o obnovu na podatelnu PostSignum" nenabízí, znamená to, že certifikát, který se snažíte obnovit, již není platný nebo je odvolán. V takovém případě můžete použít volby "Uložit a odeslat žádost na web PostSignum" nebo "Pouze uložit do souboru".

Pokud zvolíte volbu "Uložit a odeslat žádost na web PostSignum", je žádost odeslána na web certifikační autority PostSignum, kde je uložena pod identifikačním číslem, které se vám zobrazí. Toto číslo je nutno sdělit na pobočce České pošty se službou

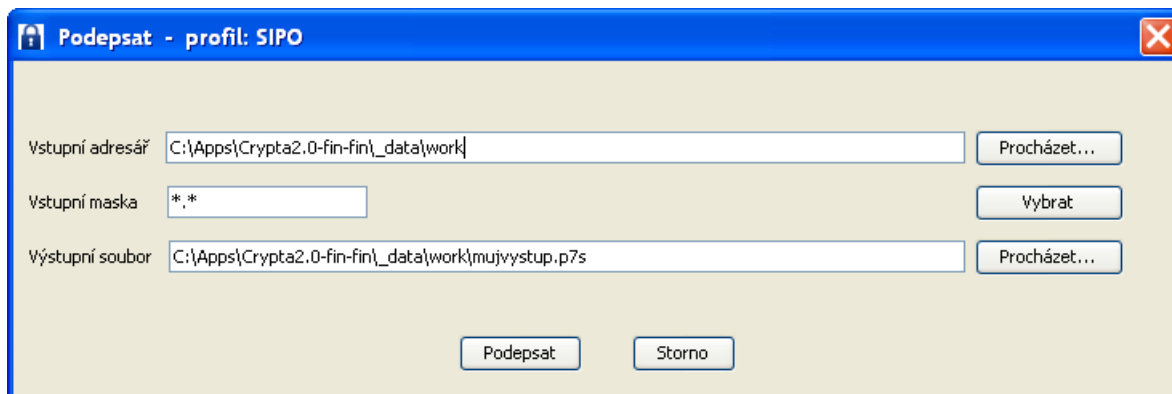
CzechPoint při vyzvednutí certifikátu. Pokud zvolíte "Pouze uložit do souboru", žádost se uloží do vámi zvoleného souboru. Soubor se žádostí je nutno předat na pobočce České pošty se službou CzechPoint.

Po vytvoření a odeslání, příp. uložení žádosti se v novém profilu vyznačí příznak existence žádosti v profilu. V dolním poli obrazovky se vypisuje protokol o provedených akcích. Po vydání certifikátu provede uživatel jeho import pomocí volby Nástroje/Import certifikátu v hlavní nabídce na úvodní obrazovce programu.

Podpisování souborů

Uživatel se přihlásil k profilu a zvolil tlačítkem v pravé části hlavní obrazovky profilu akci Podepsat. Na následující obrazovce zvolí vstupní soubory s daty, konkrétně vstupní adresář a masku pro výběr vstupních souborů, název výstupního souboru a jeho umístění. Následně potvrdí akci tlačítkem Podepsat. Výsledný soubor má koncovku p7s. V dolním poli hlavní obrazovky profilu se vypisuje protokol o provedených akcích.

Obrázek 5.11. Podepsat



The screenshot shows a dialog box titled "Podepsat - profil: SIPO". It contains three input fields for file selection and two buttons at the bottom.

| | | |
|-----------------|---|---|
| Vstupní adresář | <input type="text" value="C:\Apps\Crypta2.0-fin-fin_data\work"/> | <input type="button" value="Procházet..."/> |
| Vstupní maska | <input type="text" value="*.*"/> | <input type="button" value="Vybrat"/> |
| Výstupní soubor | <input type="text" value="C:\Apps\Crypta2.0-fin-fin_data\work\mujvystup.p7s"/> | <input type="button" value="Procházet..."/> |

Buttons at the bottom: and

Podepisování a šifrování souborů

Uživatel se přihlásí do profilu a zvolí tlačítkem v pravé části hlavní obrazovky profilu akci Podepsat a šifrovat. Na následující obrazovce pak nastaví vstupní soubory s daty, konkrétně vstupní adresář a masku pro výběr vstupních souborů, výstupní soubor a jeho umístění, vybere adresáty. Pro název výsledného souboru se nabízejí koncovky vds a enc. Následně uživatel potvrdí akci tlačítkem Podepsat a šifrovat. Vybrané soubory se zkomprimují, vytvoří se elektronický podpis komprimovaného souboru a celek se zašifruje. V dolním poli hlavní obrazovky profilu se vypisuje protokol o provedených akcích.

Obrázek 5.12. Podepsat a šifrovat

The screenshot shows a dialog box titled "Podpisat a šifrovat - profil: SIPO". It contains several input fields and buttons:

- Vstupní adresář:** C:\Apps\Crypta2.0-fin-fin_data\work (with a "Procházet..." button)
- Vstupní maska:** *.* (with a "Vybrat" button)
- Výstupní soubor:** C:\Apps\Crypta2.0-fin-fin_data\work\mujvystup.enc (with a "Procházet..." button)
- Adresáti:** A list box containing two entries:
 - Předmět: Vladimír Gregor; Platnost do: 03.11.2011 08:58:00; Sériové číslo: d50
 - Předmět: jmeno; Platnost do: 20.06.2012 11:28:00; Sériové číslo: 903(with a "Načíst seznam" button)

At the bottom of the dialog are two buttons: "Podpisat a šifrovat" and "Storno".

Kapitola 6. Odinstalování

Program Crypta lze pomocí instalačního programu též odinstalovat.

Postup odinstalování:

- Spustit "Crypta deinstalace" ze složky zástupců, nebo v adresáři, v němž je program nainstalován spustit ve Windows soubor "uninstall.exe", v ostatních systémech "uninstall".
- Odsouhlasit v následujícím okně tlačítkem "Další".
- Po skončení odinstalování se objeví okno se seznamem souborů, které nebyly (záměrně) odinstalovány.
- Ukončit odinstalování tlačítkem Konec.
- Neodinstalované soubory dle potřeby zálohovat v jiném adresáři.
- Původní adresář, v němž byl klient instalován, lze nyní smazat.

Nedoporučujeme používat pro odinstalování programu nástrojů operačního systému např. ve Windows nepoužívejte volbu: Nastavení/Ovládací panely/"Přidat nebo odebrat programy".

Příloha A. Rozhraní příkazové řádky

Obsah

[Ověřování certifikátů vůči CRL v režimu příkazové řádky](#)

[Stážení CRL](#)

[Kopírování CRL](#)

[Šifrování](#)

[Podepisování](#)

[Dešifrování](#)

[Archivace](#)

[Uložení hesla do souboru](#)

[Výpis obsahu databáze certifikátů](#)

[Aktualizace příjemce](#)

[Zjištění stavu a platnosti certifikátu](#)

V režimu příkazové řádky se program spouští příkazem CryptaCmd.exe, resp. CryptaCmd.sh z instalačního adresáře.

Návrh rozhraní příkazové řádky vychází z požadavku na zpětnou kompatibilitu s Cryptou 1.3. Z tohoto důvodu jsou povoleny všechny stávající přepínače (2, d, 7, +, -), které ovšem aplikace ignoruje. Lze zadat i samotné parametry "e" a "s", bez přepínačů.

Pokud se vstupní soubory zadávají maskou, je nutno cestu uzavřít do uvozovek. Při zadání souboru s heslem předchází heslo znak "?", při přímém zadání hesla předchází heslo znak "!". Jsou-li součástí hesla speciální znaky, zadejte heslo do uvozovek.

Upozornění pro OS MS Windows: jako oddělovač položek v údaji cesty používejte i ve Windows normální, nikoliv zpětné lomítko - viz příklady u jednotlivých příkazů.

Upozornění pro OS Linux: pokud uzavíráte heslo do uvozovek, použijte jednoduché uvozovky. Pokud uzavíráte cestu k adresářům nebo souborům do uvozovek, uzavřete do uvozovek i heslo. Např. '!Qq.1234'

Ověřování certifikátů vůči CRL v režimu příkazové řádky

Způsob práce s CRL v grafickém režimu a režimu příkazové řádky se liší. V režimu příkazové řádky je nutno před začátkem práce vložit platné CRL do příslušného adresáře dle nastavení. K tomu slouží příkazy pro stažení CRL, příp. kopírování CRL popsané v následujících odstavcích. (V grafickém režimu uživatel tuto činnost nemusí provádět, program stahuje CRL automaticky.)

Stažení CRL

Stažení aktuálního CRL ze serveru certifikační autority PostSignum VCA a jeho uložení v adresáři nastaveném pro ukládání CRL, implicitně je to adresář `_data/crls` v instalačním adresáři programu.

```
CryptaCmd ln crl
```

Kopírování CRL

Kopírování souboru CRL z lokálního umístění do adresáře nastaveného pro ukládání CRL, implicitně je to adresář `_data/crls` v instalačním adresáři programu. Příkaz má obdobnou funkci jako volba [Aktualizovat CRL](#) v grafickém režimu.

```
CryptaCmd cc jmeno_souboru
```

Příklad:

```
CryptaCmd cc c:/import/vca2_crl.crl
```


Šifrování

```
CryptaCmd e{2|d|7}{+|-} nazev_profilu vstupni_soubory vystupni_soubor adresat {adresat} {?soubor_s_heslem|!heslo} {rwr}
```

Volba rwr nastavuje přepsání souboru zadaného jména, pokud už existuje.

Příklad:

```
CryptaCmd e MujProfil "./in/*.pdf" ./out/vystup.enc prijemce1 prijemce2 ?mojeHeslo
```

Příklad:

```
CryptaCmd e MujProfil "./in/*.pdf" ./out/vystup.enc prijemce1 prijemce2 !Qq.1234
```

Podpisování

```
CryptaCmd s{2|d|7}{+|-} navez_profilu vstupni_soubory vystupni_soubor {?soubor_s_heslem|!heslo}
```

Příklad:

```
CryptaCmd s MujProfil "./in/*.pdf" ./out/vystup.p7s ?mojeHeslo
```

Dešifrování

V režimu příkazové řádky je nutné zadat pro dešifrování profil (jméno, případně heslo).

```
CryptaCmd d nazev_profilu vstupni_soubor vystupni_adresar {?soubor_s_heslem|!heslo} {rwr}
```

Volba rwr nastavuje přepsání souboru zadaného jména, pokud už existuje

Příklad:

```
CryptaCmd d MujProfil ./prijem.enc ./open ?mojeHeslo
```

Poznámka: Při dešifrování se v provozním adresáři vytváří textový soubor result.txt s informací o výsledku dešifrování. Při úspěšném dešifrování: "OK: CN_certifikátu_odesilatele". Při neúspěšném dešifrování: "Chyba: CN_příjemce".

Archivace

CryptaCmd a nazev_profilu vstupni_soubor vystupni_adresar {?soubor_s_heslem|!heslo}

Příklad:

CryptaCmd a MujProfil ./prijem.enc ./archiv ?mojeHeslo

Uložení hesla do souboru

CryptaCmd sp soubor_s_heslem

Výpis obsahu databáze certifikátů

CryptaCmd lcdb nazev_profilu

Aktualizace příjemce

Stážení certifikátu s danou hodnotou běžného jména (CommonName), který má nejdelší platnost, ze serveru certifikační autority PostSignum VCA.

```
CryptaCmd ln CN_certifikatu
```

Příklad:

```
CryptaCmd ln "SIPO CENTRUM"
```

Zjištění stavu a platnosti certifikátu

V případě, že certifikát existuje a je dostupný ke stažení, tak výsledkem jsou údaje: CN certifikátu, datum začátku platnosti a datum konce platnosti. Pokud není certifikát k dispozici ke stažení, tak výsledkem bude návratový kód 1, který se vypíše na obrazovku

```
CryptaCmd st CN_certifikatu
```

Příklad:

```
CryptaCmd st "SIPO CENTRUM"
```


Příloha B. Aplikační programové rozhraní (API)

API Crypta je popsán v samostatné dokumentaci jako javadoc.