Programový balík Crypta

verze 1.3

Uživatelská dokumentace

---

1. Úvod

Programový balík (software) Crypta je jednoduchým šifrovacím softwarem pro operační systém Windows95/98 či Windows NT 4.0. Tento software je určen pro

1. zajištění utajení přenášených dat - šifrování a dešifrování souborů a pro
2. zajištění integrity dat a jejich nepopiratelnosti - vytváření elektronického podpisu a jeho následného ověřování.

Software Crypta je možné ovládat jak prostřednictvím grafického rozhraní, tak i pomocí příkazové řádky, což je vhodné zejména pro dávkové úlohy.

Tento software podporuje algoritmy se silnou délkou klíče – pro vlastní šifrování dat používá symetrický algoritmus Triple DES o síle 112 bitů nebo RC2 o síle 128 bitů a pro výměnu klíčů a podepisování dat používá asymetrický algoritmus RSA od síle 1024 či 2048 bitů.

Vlastní výměna klíčů je postavena na principu centrální certifikační autority, která musí zaregistrovat každý klíč vytvořený tímto programem (musí vydat certifikát).

Podrobnější popis vlastností je popsán v příloze č. 1

2. Instalace

Po podepsání smlouvy s odštěpným závodem České pošty, státní podnik (dále ČP) dostanete 2 diskety s instalací programu. Po příchodu na pracoviště, kde budete program Crypta používat, vložíte první disketu do počítače a spustíte instalaci programem **`setup.exe`**. Dále instalace probíhá dle scénáře typického pro program **`InstallShield`**, nicméně pro neznalé zde uvedeme krátký popis:

1. Tlačítkem “Další” (tímto tlačítkem se vždy potvrzuje aktuální obrazovka – proto jej dále nebudeme uvádět) potvrdíte úvodní “Vítejte” obrazovku programu.
2. V obrazovce “Zvolte cílové umístění” ponecháte předvolený cílový adresář.
3. V obrazovce “Zvolte typ instalace” ponecháte typický typ instalace.
4. V obrazovce “Zvolte programovou složku” ponecháte předvolenou programovou skupinu, do které bude umístěno spouštění programů ze software Crypta.
5. Spustí se kopírování. V jeho průběhu budete vyzváni ke vložení nové diskety.
6. Konečnou obrazovku instalace potvrdíte tlačítkem “Skončit”.

Při instalaci byl ve vámi zvoleném kořenovém adresáři [*)] vytvořen podadresář **`bin`**, kam byly nakopírovány tři hlavní programové soubory (+ 2 DLL knihovny). V případě, kdy při instalaci ponecháte přednastavené hodnoty, se bude jednat o adresář **`c:\crypta\bin`** a o následující soubory:

1. program **`CryptaCmd.exe`** určený pro šifrování z příkazové řádky a vhodný zejména pro dávkové zpracování dat;
2. program **`CryptaGui.exe`** – program určený pro šifrování a dešifrování z grafického prostředí Windows

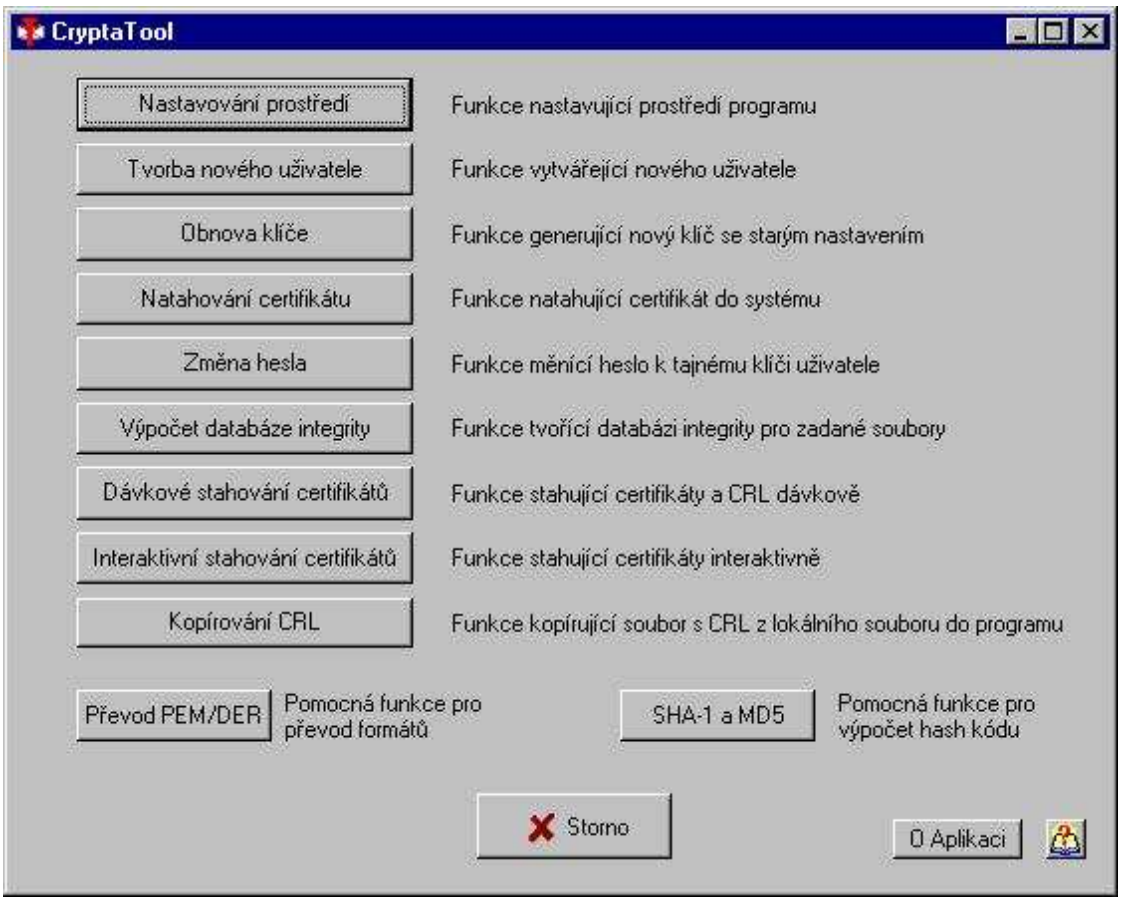
a nakonec

3. program **`CryptaTool.exe`** – program určený pro podpůrné operace, jako například pro generování klíčů, pro jejich natahování do systému, pro nastavování prostředí a pro stahování certifikátů z centrálního serveru (tato možnost je v současné době dostupná pouze pro pracoviště ČP).

Dále se v tomto adresáři nachází ještě dvě dynamické knihovny **`CryptaLib.dll`** (podpůrná dynamická knihovna pro šifrovací programy) a **`nsldapssl32v30.dll`** (knihovna firmy Netscape pro komunikaci s LDAP serverem za účelem stahování certifikátů a seznamu zneplatněných certifikátů - CRL).

3. První spuštění

Spustíte program **`CryptaTool`** (*Start/Programy/Aplikace Crypta v1.3/CryptaTool*) a objeví se vám hlavní okno programu **`CryptaTool`** s nabídkou jednotlivých operací, které jsou vám k dispozici.



Operace **nastavování prostředí** zabezpečuje, jak již název vypovídá, nastavování prostředí programu, speciálně tedy cest k programovým souborům, úrovně kontrol, typu použité symetrické šifry a případně parametrů LDAP serverů.

Následné dvě operace (**tvorba nového uživatele a obnova klíče**) se zabývají generováním RSA klíčů a následným vytvářením žádostí o certifikát. Zatímco však při operaci tvorba nového uživatele musíte ručně zadat veškeré údaje potřebné k identifikaci klíče, u operace obnova klíče se tyto identifikační údaje překopírují ze starého uživatele.

Operace **natahování certifikátu** zajišťuje fázi vkládání certifikátu, vydaného na základě žádosti vytvořené jednou z výše uvedených operací do programového prostředí, jakož i kopírování certifikátů certifikačních autorit a seznamů zneplatněných certifikátů (CRL) k těmto autoritám a kopírování certifikátů ČP z adresáře *Certs* do stejnojmenného adresáře v Cryptě. Všechny tyto soubory budou nakopírovány na disketu na kontaktním místě ČP.

Operaci **změna hesla** snad není nutné podrobněji vysvětlovat – mění přístupové heslo k tajnému klíči

uloženému na disku.

Operaci **výpočet databáze integrity** je možné provádět až po vytvoření uživatele a natažení certifikátu. Tato operace vytváří elektronický podpis všech důležitých souborů tohoto programového balíku. Jedná se o konfigurační soubor, soubor s certifikáty certifikační autority, dynamickou knihovnu, program pro šifrování v dávkovém režimu a program pro šifrování v grafickém režimu. Tato databáze se poté kontroluje před každým šifrováním, či dešifrováním dat. Díky tomu není možné, aby vám někdo nepozorovaně pozměnil soubory.

Operace **dávkové stahování certifikátů** umožňuje stáhnout ze zadaných LDAP serverů (na kterých jsou uloženy všechny vydané certifikáty) certifikáty dle zadaných kritérií a uložit je do adresáře určeného pro ukládání dočasných souborů*) (např. `c:\crypta\temp`). Dále nabízí stahování aktuálních CRL, které ukládá do jim vyhrazeného adresáře*) (např. `c:\crypta\crls`).

Operace **interaktivní stahování certifikátů** zajišťuje stejnou činnost jako předchozí operace s tím rozdílem, že se uživatel poté může rozhodnout, které ze stažených certifikátů chce skutečně uložit na disk.

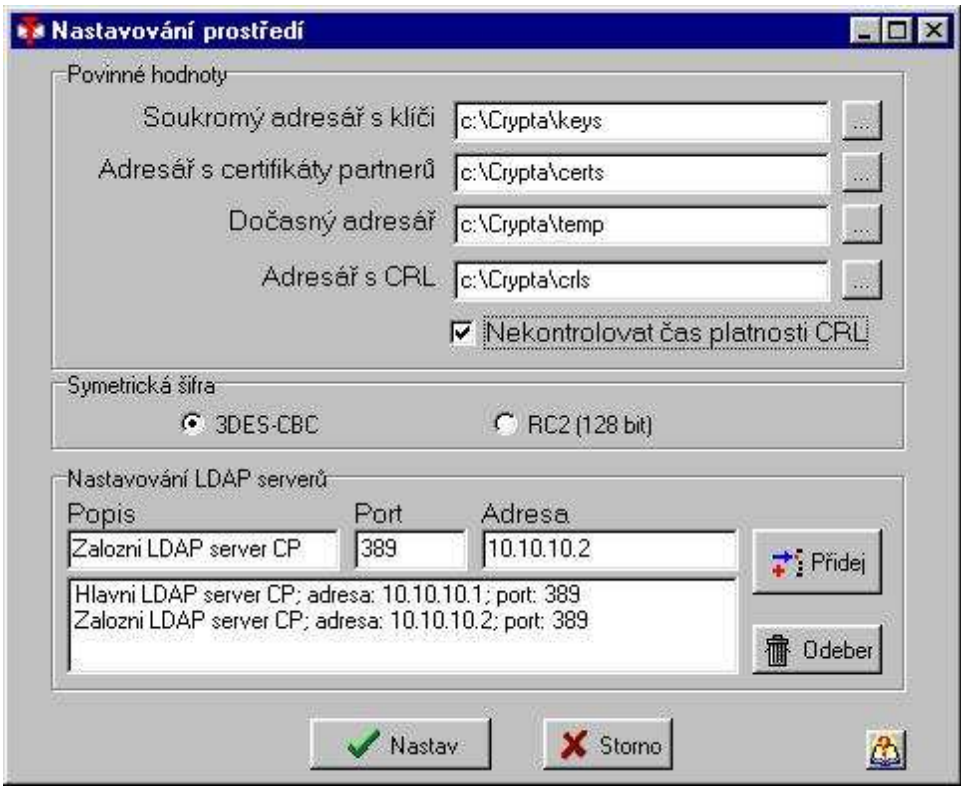
Operace **kopírování CRL** umožní zkopírování CRL souborů, které vám např. přijdou e-mailem, do programu Crypta. Oproti ručnímu zkopírování tato funkce kopírovaný soubor přejmenuje do interního formátu, takže v adresáři s CRL*) nebude uloženo víc stejných CRL souborů pod různými názvy.

Další operaci nazvanou **převod PEM/DER** nebudete za normálních okolností potřebovat – je určena pro speciální případy, kdy je nutné převést certifikáty či žádosti o certifikát z PEM formátu do DER či naopak.

Poslední operace **SHA-1 a MD5** je určena pro výpočet hash kódu ze zadaných souborů či zadaného textu. Je určena pro uvěřování pravosti různých souborů, speciálně certifikátu certifikační autority.

3.1 Nastavování prostředí

Zvolíte operaci Nastavování prostředí a objeví se vám stejnojmenné okno s předvyplněnými údaji. V oblasti "Povinné hodnoty" doporučujeme ponechat tato nastavení (za předpokladu, že je Crypta nainstalována v adresáři **c:\Crypta**).



V případě, že nemáte možnost stahovat aktuální seznamy zneplatněných certifikátů (CRL) a nechcete být neustále upozorňováni, že vaše CRL již není platné, potom zatrhněte volbu "Nekontrolovat čas platnosti

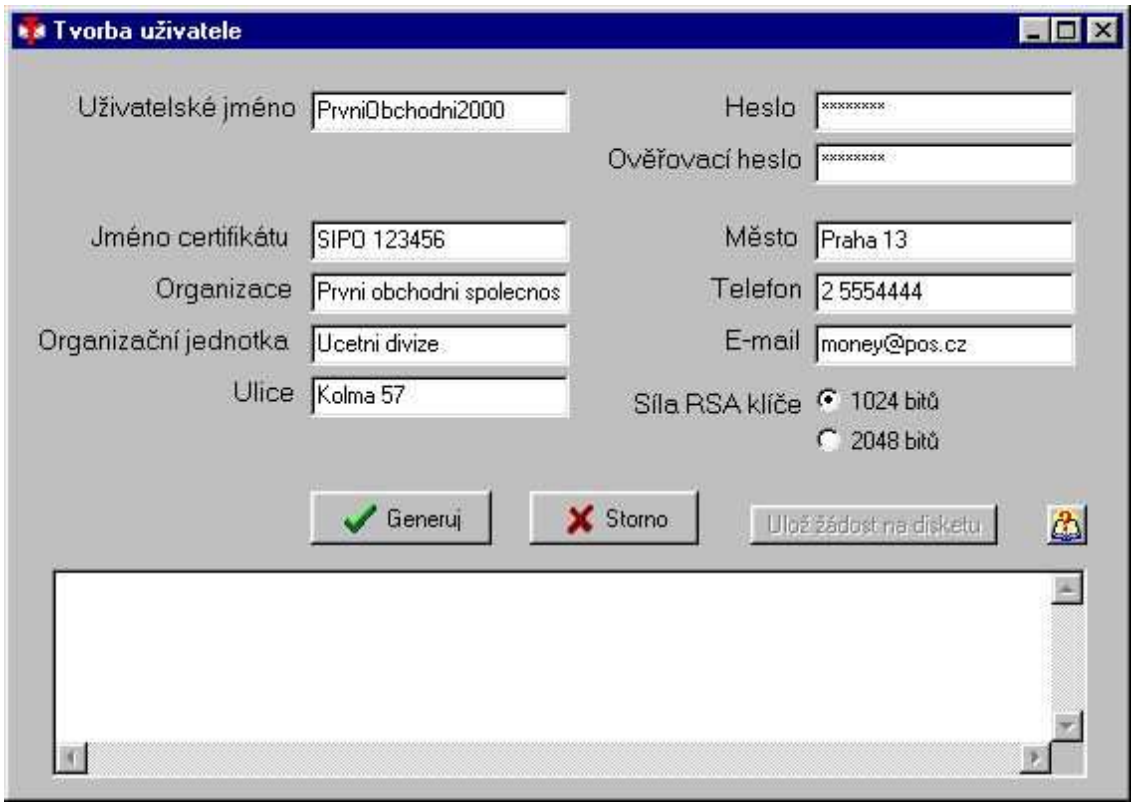
CRL".

V oblasti nazvané "Nastavování LDAP serverů" můžete zadávat LDAP servery, ze kterých chcete stahovat nové certifikáty a seznamy zneplatněných certifikátů. Při zadávání nového serveru nejprve vyplníte položku "Popis", potom položku "Port" (standardně se jedná o port 389), dále položku "Adresa" (kam uvedete adresu LDAP serveru) a vše ukončíte stiskem tlačítka "Přidej". Naopak, pokud budete chtít již existující server odebrat, potom na něj klikněte a stiskněte tlačítko "Odeber".

Nakonec vše uložíte tlačítkem “Nastav”. Potvrdíte hlášku, že nastavení proběhlo v pořádku (pokud ne, tak jste pravděpodobně zadali na počátku špatnou cestu k adresáři s programy) a doporučení, abyste přepočítali databázi integrity. Protože však nemáte zatím založeného žádného uživatele, tak toto doporučení ignorujte.

3.2 Tvorba nového uživatele

Po spuštění této operace se vám objeví okno, kde budete zadávat údaje o novém uživateli (a o jeho klíči - certifikátu).



Nejprve zadáte uživatelské jméno, které od této chvíle budete zadávat při každé kryptografické operaci. Toto uživatelské jméno identifikuje dvojici klíčů použitou pro šifrování/dešifrování nebo podpepsání/ověření elektronického podpisu. Protože toto jméno je použito pro pojmenování vašich uživatelských souborů na disku, doporučujeme je výstižné, bez mezer, diakritiky a jiných speciálních znaků.

Dále zadáte heslo a jeho kopii (pro ověření správnosti zápisu). Toto heslo musí být delší než 8 znaků a musí obsahovat alespoň jeden znak malého písmena a alespoň jeden znak velkého písmena či číslo. Tato omezení jsou podmíněna skutečností, že toto heslo je jediným prostředkem pro zabezpečení tajného klíče, na jehož utajení je postaveno šifrování. Proto bychom zde rádi uvedli několik poznámek na téma hesla:

1. Hesla nemají obsahovat žádné součásti vašeho jména, jmen vašich blízkých, vašeho psa, rodného čísla či telefonu.
2. Heslem nesmí být jméno standardně se vyskytující ve slovníku (např. jablko).
3. Heslem dále nesmí být jméno z vašeho okolí (např. uctarna).
4. Doporučují se hesla delší 8 znaků, kde se vyskytují jak malá písmena, tak i velká spolu s jinými znaky (např. !?.,).

V případě, kdy ke klíči má přístup větší počet lidí, je nutné tento přístup omezit pomocí vlastního operačního systému (tedy použít mechanismů Windows NT).

Dále zadáte jméno vašeho certifikátu, které se skládá z identifikace úlohy a čísla přiděleného vám v rámci této úlohy (např. při podpisu smlouvy). Pro ilustraci uvádíme příklady jmen certifikátů pro úlohy ČP v současné době spolupracující s programem Crypta:

Úloha	**Jméno certifikátu zákazníka ČP**	**Jméno certifikátu pracoviště ČP**
SIPO	`SIPO 123456` nebo `SIPO 1234`	`SIPO-VT StC-100`
Platební styk - poukázky AV	`PKA 12345`	`PKA-VT StC-100`
Platební styk - emitace poukázek AV	`PKAE 123456`	`PKAE-VT StC-100`
Platební styk - poukázky H	`PKB 123456`	`PKB-VT StC-100`
Hybridní pošta	`POSTSERVIS HP123456`	`POSTSERVIS-VT JC-001`
Tracing and Tracking	`TT 12345678`	`TT-OZ VAKUS-0001`

Název organizace je uveden ve vaší smlouvě s ČP, pouze vypusťte diakritiku a speciální oddělovače typu čárka, středník či znak @. Toto pravidlo platí i pro ostatní položky (kromě znaku @ v položce e-mailu). Dále se na konci textu jakékoliv položky nesmí nacházet prázdný znak (tedy znak " " - mezerník).

Vyplnění položky organizační jednotka záleží na vás. Pouze v případě, že vaše organizace má více pracovišť používajících program Crypta (např. geograficky oddělených) by bylo dobré, aby tato položka pomohla identifikaci tohoto pracoviště. Tedy pro ČP bude tato položka obsahovat názvy odštěpných závodů, například **OZ Stredni Cechy**.

Ulice a Město budou shodné s adresou uvedenou na smlouvě mezi ČP a vaší organizací (v případě zákazníka) či adresou pracoviště ČP.

Zadaný telefon a e-mail by měl vést na pracoviště, kde se bude tento program používat, aby v případě problému měla protější komunikující strana k dispozici kontaktní údaje.

Sílu klíče doporučujeme nastavit na 1024 bitů (generování delšího klíče trvá dlouho a zatím není potřeba).

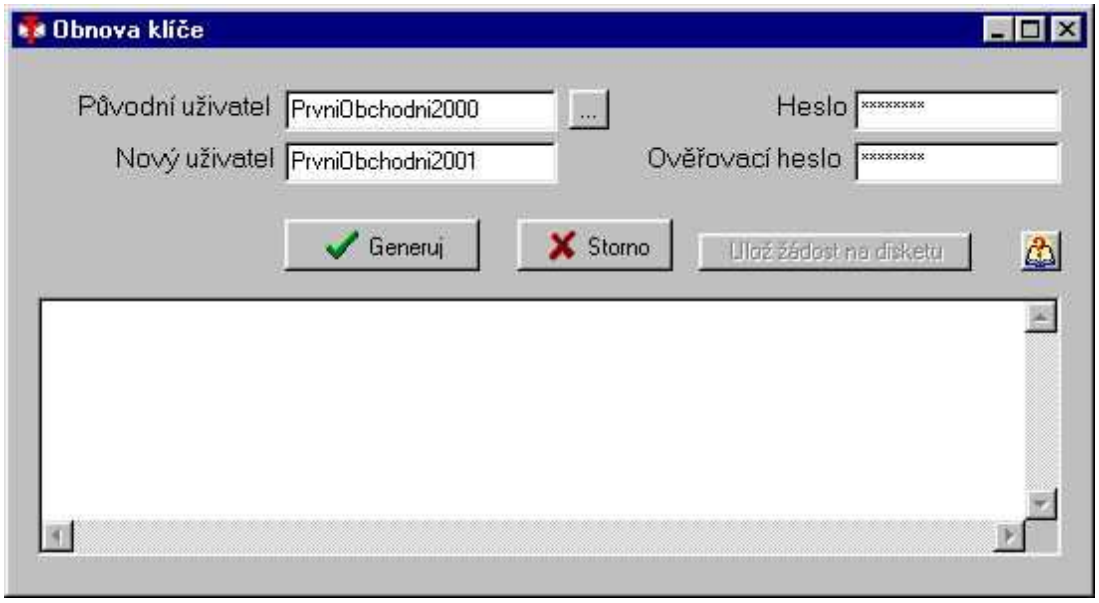
Nakonec pomocí tlačítka “Generuj” spustíte generování dvojice RSA klíčů a tvorbu žádosti o certifikát. Nyní se vám objeví okno s emblémem České pošty, kde budete tak hlouho tisknout různé klávesy nebo hýbat myší, než program nasbírá dostatek náhodných údajů potřebných pro generování klíče. Čas potřebný pro generování klíče je závislý na výkonnosti počítače (např. klíč o délce 1024 bitů trvá na 333 MHz Pentiu II do 30 sekund a klíč o délce 2048 bitů do 5 minut), proto se obrňte trpělivostí.

Po ukončení generování potvrdíte okno s hlášením o průběhu generování a ve spodním okně pod tlačítkem “Generuj” si můžete prohlédnout celou historii generování klíče. Zároveň se vám zpřístupnilo tlačítko “Ulož žádost na disketu”, které vygenerovanou žádost nakopíruje na disketu (doporučujeme ponechat pro kopírování jméno shodné se jménem uživatele). Pokud tuto možnost nevyužijete, je možné vytvořenou žádost později nalézt v adresáři s klíči[*)] (např. **`c:\crypta\keys`**), v souboru s názvem shodným se zadaným jménem uživatele a příponou **`*.req`**. S disketou (a v případě zákazníka ČP ještě s originálem smlouvy podepsané mezi ČP a vámi) se poté dostavíte na kontaktní pracoviště ČP (s operátorem certifikační autority), kde vám na základě této žádosti operátor vydá certifikát (viz. materiál "Poučení pro zákazníky České pošty" nebo materiál "Poučení pro uživatele České pošty").

Obrazovku opustíte pomocí tlačítka “Storno”.

3.3 Obnova klíče

Pokud právě provádíte první nastavení tohoto programového balíku, tak tento odstavec můžete přeskočit.



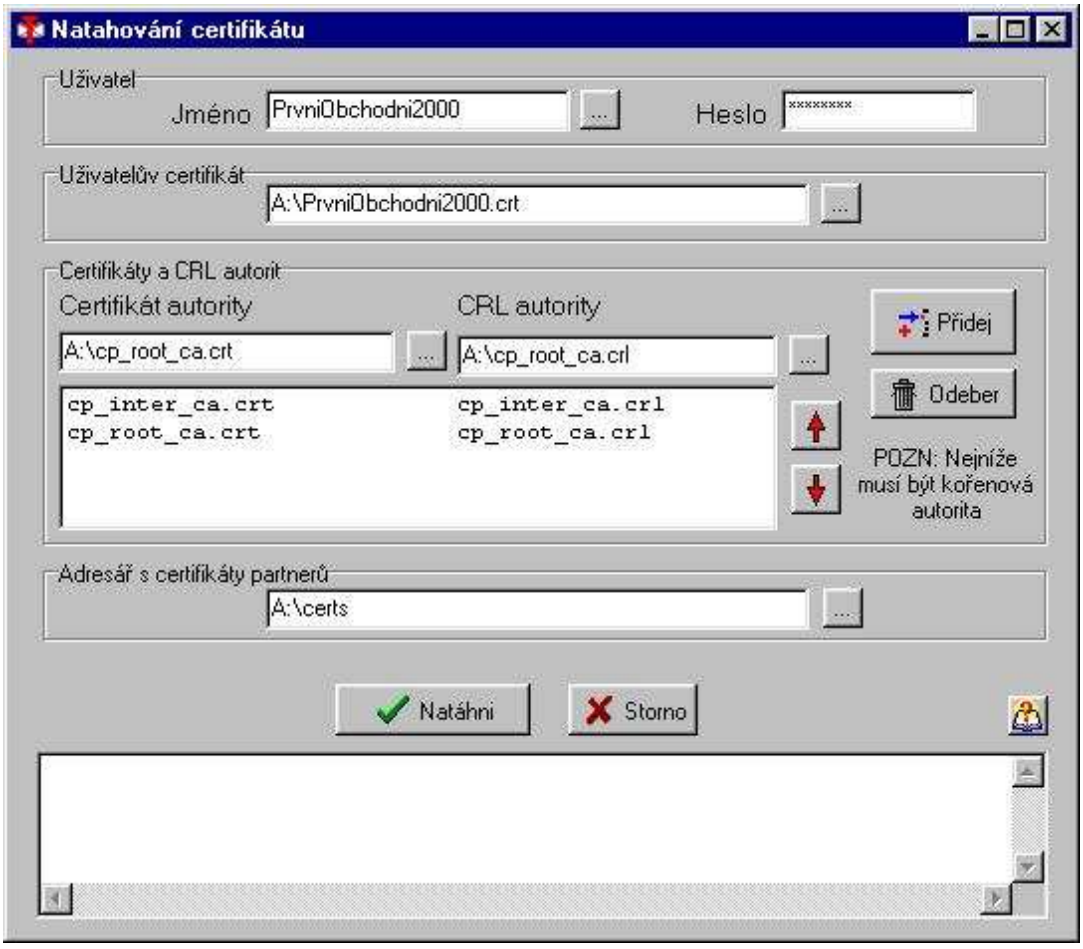
Obnova klíče starého uživatele se provádí stejně jako předchozí operace **Tvorba nového uživatele** a stejně jako ona generuje novou dvojici klíčů a žádost o certifikát, ale s tím rozdílem, že se všechny potřebné údaje přejímají ze starého uživatele. Tuto funkci použijete v okamžiku, kdy bude platnost právě používané dvojice klíčů končit a budete muset zažádat o nový certifikát.

Zde zadáte (nebo si vyberete) jméno původního uživatele, potom zadáte jméno nového uživatele (lišící se od starého uživatele) a zadáte dvakrát heslo nového uživatele. Generování spustíte stiskem tlačítka “Generuj”. Dále je už vše stejné jako v předchozím případě.

Poznámka: Rozdíl mezi touto a předchozí akcí je jediný - nemusíte znovu vyplňovat již dříve uvedené údaje. Nic však nebrání tomu nahradit tuto akci výše uvedenou.

3.4 Natahování certifikátu

Stiskem tohoto tlačítka se vám otevře stejnojmenné okno, kde zadáte soubory přinesené od operátora certifikační autority (dále CA), které je pro další funkčnost programu nutné do něj "natáhnout".



Postup zadávání údajů je následující:

1. nejprve zadáte (vyberete) své uživatelské jméno s heslem;
2. zadáte soubor se svým certifikátem, který jste donesli na disketě (např. **`vase_jmeno.crt`**);
3. zadáte tzv. "řetěz certifikátů", tedy posloupnost certifikátů a CRL autorit od autority, která vydala váš certifikát, až po hlavní kořenovou autoritu. K tomuto řetězu je nutné poznamenat:
   - Každá zadávaná autorita je reprezentována souborem s certifikátem a souborem s CRL. Je nutné zadat (vybrat) oba dva soubory. Přidávání do řetězu autorit se poté provádí stiskem tlačítka "Přidej".
   - Ve vytvořeném řetězu certifikačních autorit je možné jednotlivé autority mazat (kliknutím vyberete autoritu a stisknete tlačítko "Odeber") nebo měnit pořadí jednotlivých autorit (kliknutím vyberete vhodnou autoritu a poté pomocí šipek změníte její pořadí v řetězu.
   - **Pořadí zadaných autorit je velmi důležité** - nejvýše by měla být umístěna autorita, která vydala váš certifikát (např. **`cp_inter_ca.crt/crl`**) a nejníže kořenová (anglicky *root*) autorita (např. **`cp_root_ca.crt/crl`**). Tato část obrazovky by se měla shodovat s výše uvedeným příkladem obrazovky.

   (V tomto případě tedy nejprve zvolíte jako certifikát autority soubor **`cp_inter_ca.crt`** a jako CRL autority soubor **`cp_inter_ca.crl`**, kliknete na tlačítko "Přidej", zvolíte jako certifikát autority soubor **`cp_root_ca.crt`** a jako CRL autority soubor **`cp_root_ca.crl`** a opět kliknete na tlačítko "Přidej".)
4. Zkontrolujte nebo doplňte adresář s certifikáty partnerů. Pokud zvolíte uživatelův certifikát přes tlačítko [...], doplní se tento adresář automaticky, jinak jej musíte doplnit ručně - zvolte takový adresář, do nějž vám operátor nakopíroval certifikáty pracovišť ČP. Program z něj nakopíruje všechny nalezené certifikáty do svého adresáře s certifikáty partnerů[*)].

   (Tuto položku je možné nechat prázdnou, pak se žádné certifikáty kopírovat nebudou. Program kopíruje všechny certifikáty, takže pokud jsou v adresáři s certifikáty partnerů i certifikáty autorit, budou také zkopírovány.)

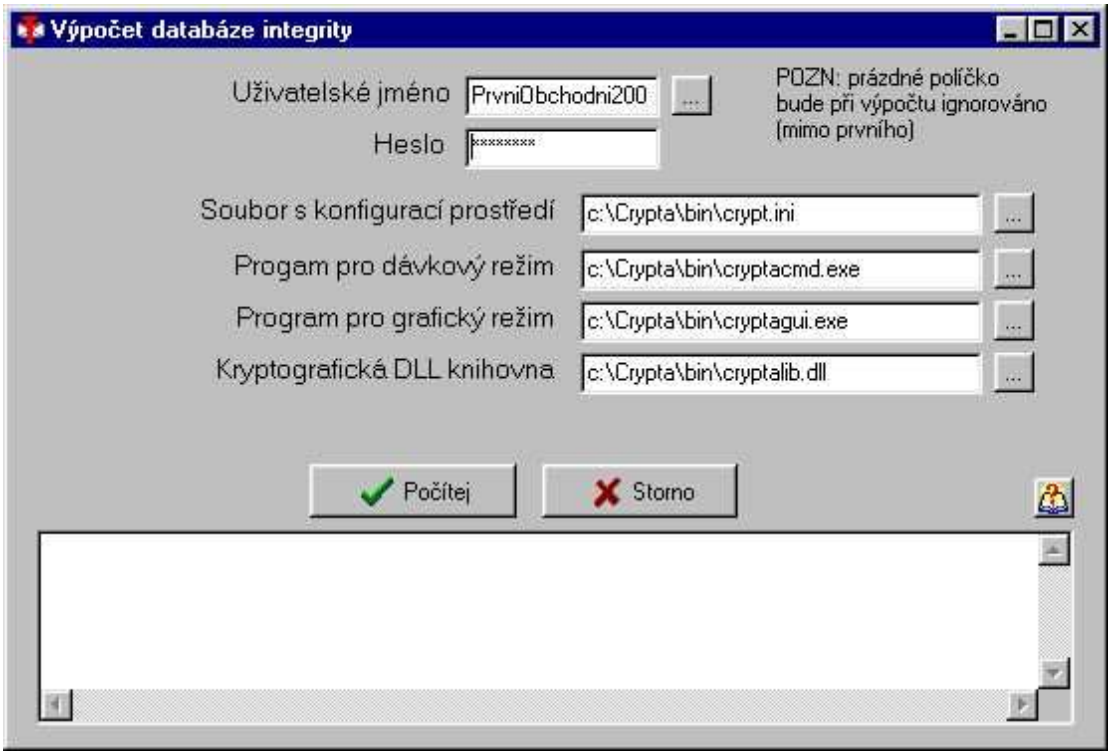
V případě, že by se některé jméno souboru lišilo, budete na toto operátorem CA upozorněni.

Natahování spustíte tlačítkem "Natáhni", kdy se zadané soubory načtou do programu, ověří se jejich správnost a nakonec se uloží do adresáře se soukromými klíči. Pokud se vám v této fázi objeví chyba, potom je nutné překontrolovat zadané hodnoty (jak heslo, tak i vybrané soubory). V případě, že vše proběhlo v pořádku, se vám ještě objeví upozornění na nutnost vypočítat databázi integrity (viz. další bod).

Nakonec **ZAZÁLOHUJTE KLÍČE** (viz. bod 5.1)!!!

3.5 Výpočet databáze integrity

Po stisku tohoto tlačítka se vám objeví okno, kde zadáte jméno uživatele, pro kterého je prováděn vypočet databáze integrity, a jeho heslo.



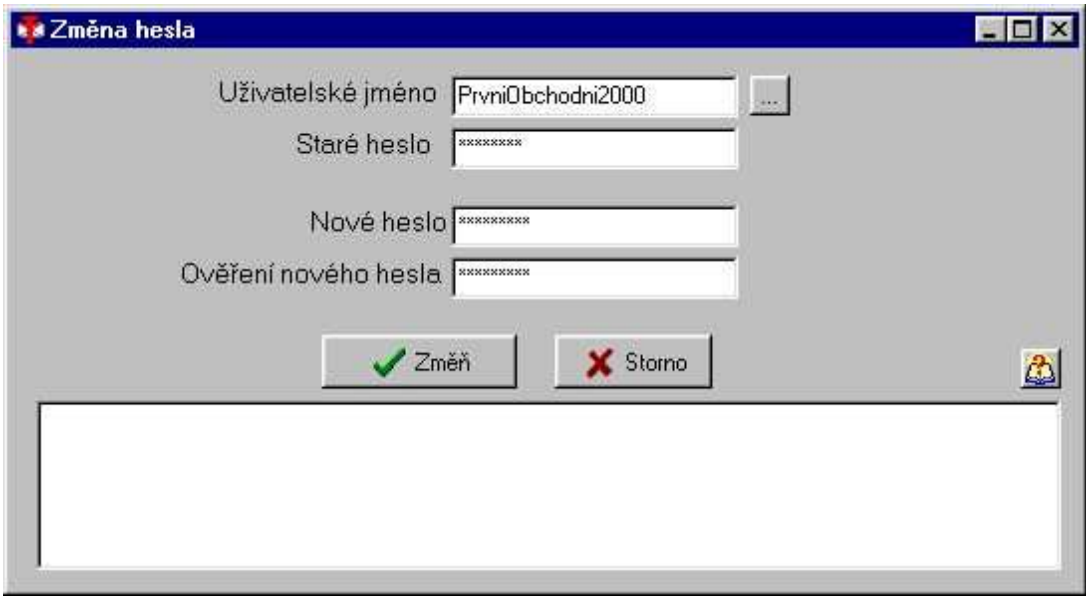
Dále v tomto okně zadáte soubory, které mají být do databáze zahrnuty. První možnost (soubor s konfigurací prostředí) je povinná, neboť jeho modifikací by se potenciálně dalo dosáhnout nebezpečné práce programu. Výpočet integrity pro další tři soubory (jedná se o dva programy na šifrování a hlavní dynamickou knihovnu) sice není povinný, ale taktéž jej silně doporučujeme.

Pokud jste při nastavování prostředí ponechali přednastavené hodnoty, je možné ponechat tyto i zde – takže stačí zadat uživatele a jeho heslo. Poté spustíte výpočet databáze integrity tlačítkem “Počítej”.

Nyní jste už připraveni k šifrování.

3.6 Změna hesla

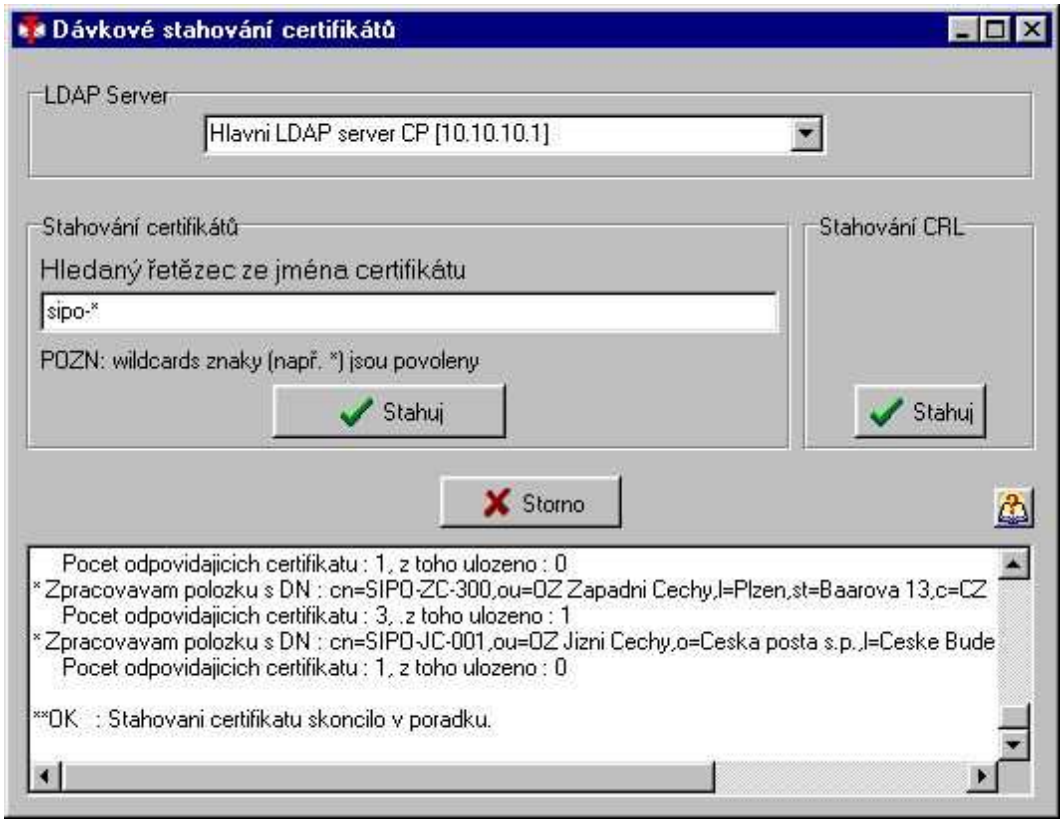
Význam této operace snad ani nemá smysl vysvětlovat – provádí změnu hesla k tajnému klíči uloženému na disku. Zde zadáte jméno uživatele, jehož heslo chcete měnit, jeho současné heslo (položka Staré heslo) a dvakrát nové heslo (jednou pro ověření správnosti zápisu).



Po stisku tlačítka "Změň" se provede požadovaná změna. Opět je možné sledovat průběh změn ve spodním okně obrazovky. Tlačítkem "Storno" opustíme okno.

3.7 Dávkové stahování certifikátů

Tato (stejně jako následující operace) je určená pouze pro pracoviště s přístupem k LDAP serveru.



Po stisku tlačítka se vám objeví okno "Dávkové stahování certifikátů". Toto okno nabízí dvě operace – stahování certifikátů a stahování aktuálního CRL.

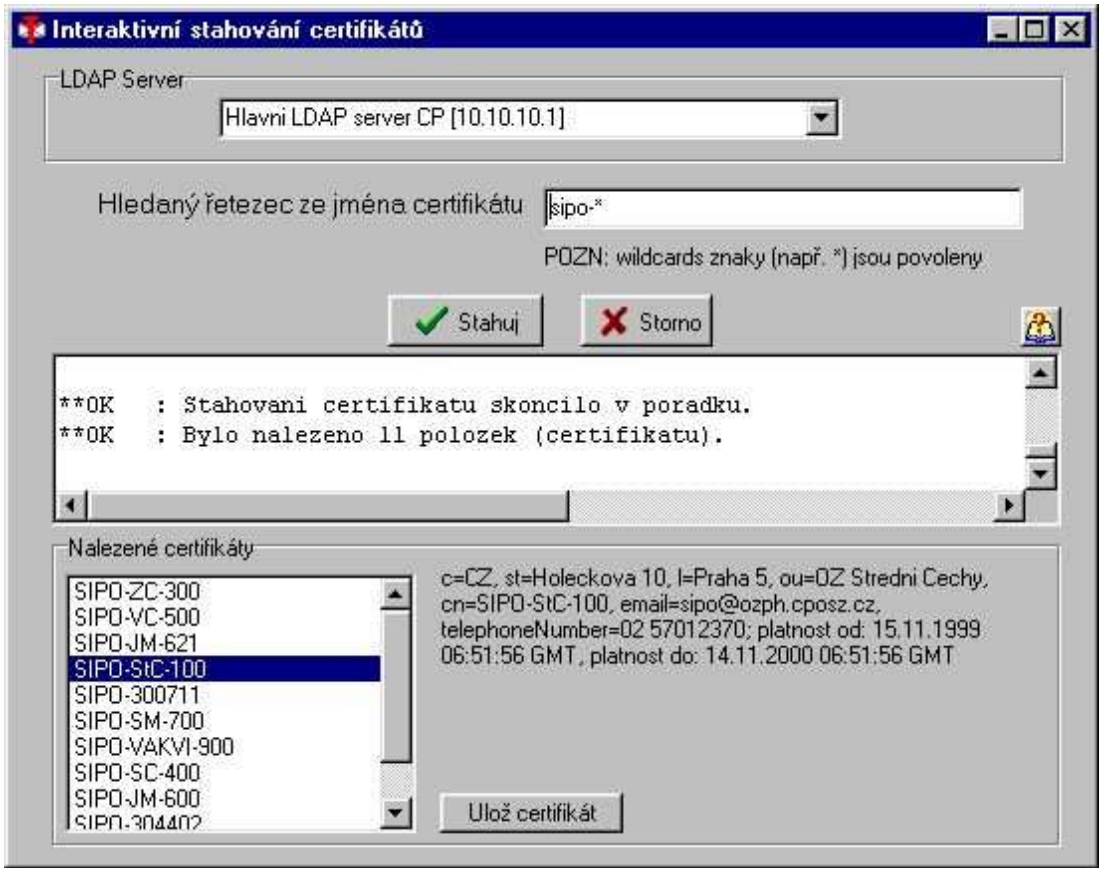
V případě, že chcete stahovat certifikáty, musíte vybrat LDAP server, ze kterého chcete certifikáty stahovat, a zadat část řetězce ze jména certifikátu (pokud tedy např. hledáte všechny certifikáty pracovišť SIPO na Severní Moravě, potom zadáte řetězec **SIPO-SM-***). Stahování poté spustíte tlačítkem "Stahuj" v části okna věnované stahování certifikátů. Platné certifikáty jsou ukládány pod jménem **`jmeno_certifikatu.crt`** do adresáře určeného pro ukládání dočasných souborů[*)] (např. **`c:\crypta\temp`**). Odtud potom musíte potřebné certifikáty ručně překopírovat do adresáře určeného pro ukládání certifikátů partnerů (např. **`c:\crypta`**

`\certs`). Průběh stahování je opět možné sledovat ve spodní části okna.

Stahování CRL je podobné s tím rozdílem, že se stahují pouze soubory obsahující CRL autorit používaných programem. Jejich jména vychází z celých jmen autorit s tím rozdílem, že tyto jsou zapsány pouze pomocí písmen a čísel oddělených pomlčkami (např. `cCZ-oCeskapostasp-cnRootCA.crl` a ukládají se do adresáře vyhrazeného pro CRL[*)] (např. `c:\crypta\crls`).

3.8 Interaktivní stahování certifikátů

Tato operace zabezpečuje stejnou funkci jako předchozí s tím rozdílem, že je určena pro menší množství certifikátů, kdy si chcete vybrat, který je opravdu ten pravý.



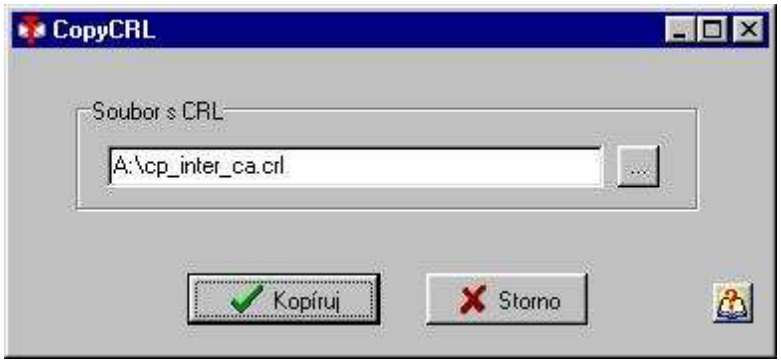
Po spuštění této operace se vám objeví okno podobné oknu z předchozí operace. Pouze chybí možnost stahování CRL a ve spodní části okna přibyly prvky určené pro práci s nalezenými certifikáty.

Opět vyberete LDAP server, zadáte hledaný řetězec jako v předchozím případě a spustíte stahování tlačítkem "Stahuj". V případě, že vámi hledaný certifikát byl nalezen, se jméno tohoto certifikátu objeví v levé části podokna "Nalezené certifikáty". Potom stačí na tento certifikát kliknout a v pravé části podokna se vám objeví celé jeho jméno. Potom pomocí tlačítka "Ulož certifikát" můžete tento certifikát uložit.

Zde se ukládání provádí přímo do adresáře určeného pro certifikáty komunikačních partnerů, neboť vše je plně pod kontrolou uživatele, a můžete se tedy rozhodnout, zda-li chcete některý certifikát přepsat či nikoliv. V případě, že vybraný certifikát se v tomto adresáři nenachází, se tento bez dalšího uloží. V opačném případě, kdy v tomto adresáři už existuje certifikát se stejným jménem (například certifikát od stejného uživatele, kterému však končí platnost) budete dotázáni na jméno, pod kterým se má tento nový certifikát uložit.

3.9 Kopírování CRL

Tato operace je podobná stahování CRL v **Dávkovém stahování certifikátů**. Nestahuje se však z LDAP serveru, ale probíhá kopírování souboru CRL, který vám přijde např. e-mailem.



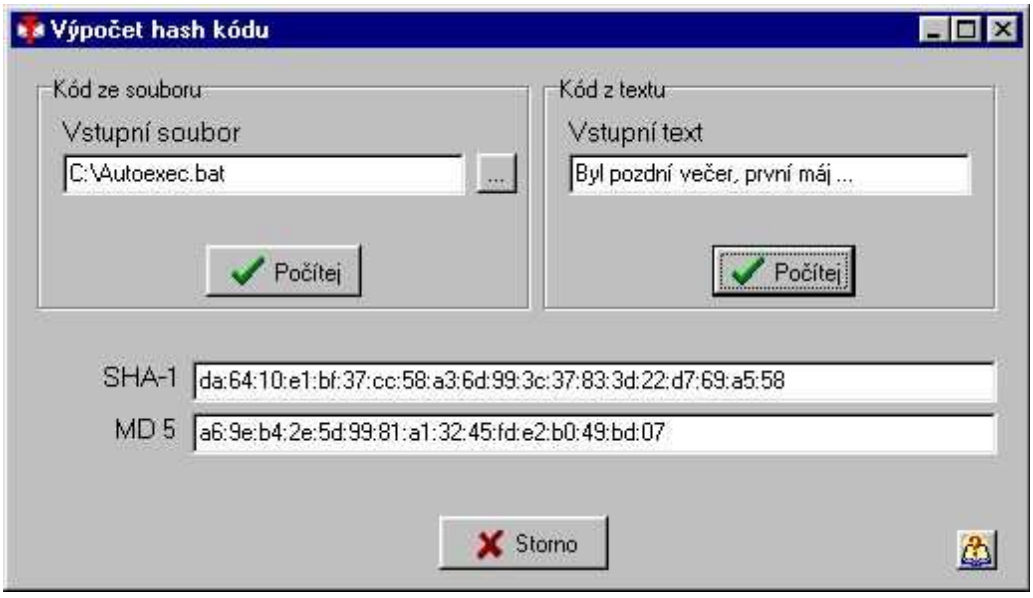
V okně pouze vyhledáte nebo ručně zadáte cestu k souboru, v němž je CRL uloženo a kliknete na tlačítko "Kopíruj". Úspěšné zkopírování potvrdí informační okno. Pokud nechcete kopírovat žádný CRL soubor, klikněte na tlačítko "Storno".

Program umí najednou zkopírovat pouze jeden soubor, který je nakopírován do adresáře s CRL[*)] (např. **c:\crypta\crls**). Jméno souboru je upraveno stejně, jako tomu je v případě stahování z LDAP serveru.

3.10 SHA-1 a MD 5

Stiskem tohoto tlačítka se vám otevře okno, ve kterém můžete vypočítat *hash kód* pro soubory i pro textové řetězce.

Okno je rozděleno do dvou částí: v jedné zadáváte vstupní soubor, ze kterého poté vypočítáte hash kód, a v druhé text, ze kterého vypočítáte hash kód.



Program nabízí dva typy hash kódů:

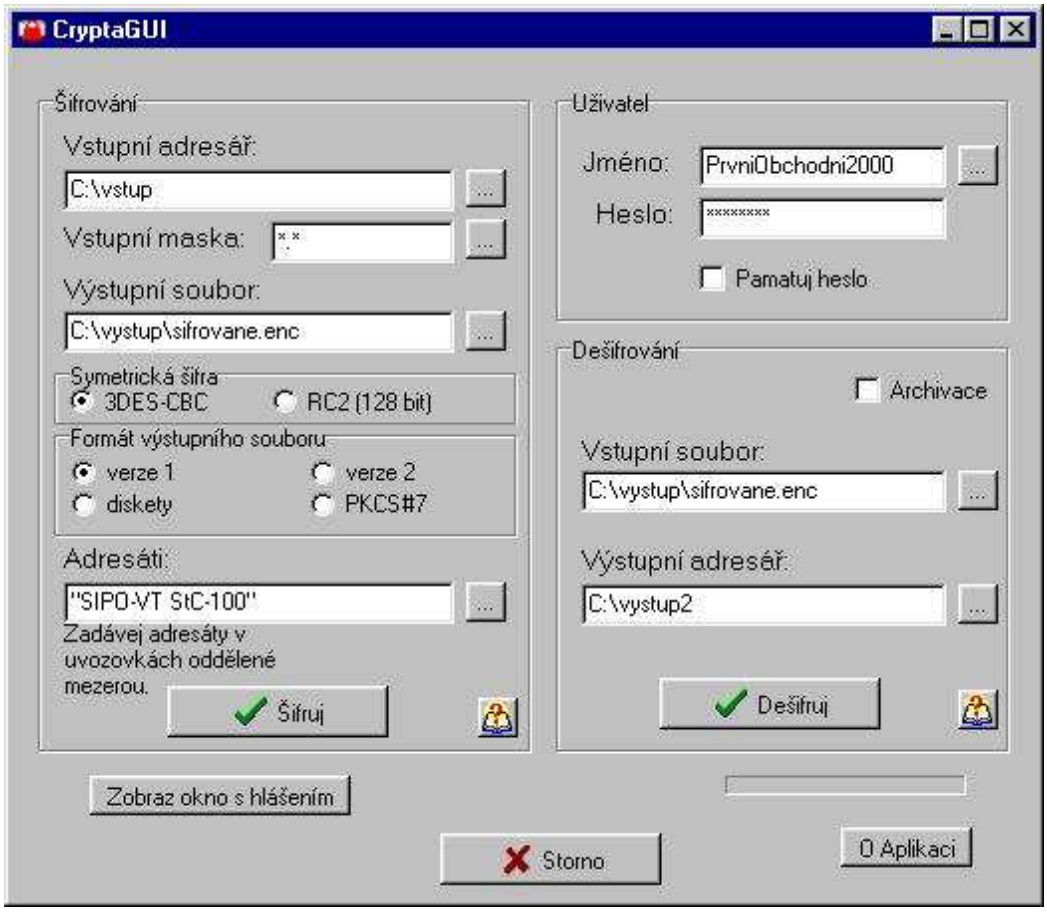
1. starší a kratší (128 bitů dlouhý) **MD 5 a**
2. novější, spolehlivější a delší (160 bitů) **SHA-1.**

Tyto dva typy hash kódů patří k nejrozšířenějším na světě. Viditelný zápis těchto kódů v textové formě vyjadřuje jednotlivé byty zapsané hexadecimálně oddělené dvojtečkou.

4. Šifrování a dešifrování souborů

Soubory je možné šifrovat a dešifrovat jak v grafickém, tak i v příkazovém režimu. Popisu šifrování v příkazovém režimu je věnována příloha 2.

Pro šifrování v grafickém režimu spustíte program **`CryptaGui.exe`** (*Start/Programy/Aplikace Crypta v1.3/CryptaGui*) a objeví se vám hlavní a jediné okno.



Toto okno je rozděleno do tří oblastí:

1. oblasti věnované uživateli, kde se zadává uživatel a jeho heslo. Položky v této oblasti musí být vždy vyplněné.
2. oblasti věnované šifrování souborů a
3. oblasti věnované dešifrování souborů,

kdy z posledních dvou oblastí stačí vyplnit pouze položky v jedné, tj. pokud chcete pouze šifrovat, nemusíte vyplňovat oblast pro dešifrování.

4.1 Šifrování souborů

Pro šifrování souborů je nutné zadat následující hodnoty:

1. Vstupní adresář a vstupní masku – tyto parametry dohromady určují počet a typ vstupních souborů;
2. Výstupní soubor – typicky se jedná o soubory s příponou **enc** (*encrypted*), ale zvolit si můžete jakýkoliv;
3. Symetrická šifra - zde můžete ponechat předvolený typ 3DES-CBC;
4. Formát výstupního souboru - můžete zvolit prakticky jakýkoliv, verze 1.2 a nižší však podporují jen "verzi 1", formát "diskety" automaticky rozděluje zašifrované soubory do částí o velikosti 1,44 MB;
5. Množinu adresátů, kterým je určen vytvářený soubor (max. 32). Tyto adresáty lze, stejně jako ostatní hodnoty, vybrat pomocí dialogu či přímo zadat. Jednotliví adresáti musí být v uvozovkách a oddělení mezerou.

Po zadání výše uvedených hodnot můžete spustit šifrování tlačítkem “Šifruj”. Průběh šifrování lze sledovat v nově se objevivším okně, kam se vypisují hlášky o průběhu šifrování. Dále je v pravém dolním rohu umístěn ukazatel postupu, který však pouze indikuje práci programu a nikoliv přesné procentuální hodnoty.

Po potvrzení ukončení šifrování máte k dispozici dvě možnosti – uložit si obsah viditelného okna do souboru (např. v případě chyby, aby ji bylo možné lépe dohledat) tlačítkem "Ulož okno s hlášením", či toto okno zrušit tlačítkem "Zruš okno s hlášením". Tím se toto tlačítko změní na "Zobraz okno s hlášením", takže funguje jako přepínač mezi oknem na zadávání hodnot a oknem na sledování průběhu šifrování.

Při šifrování program testuje jak platnost vašeho certifikátu, tak i platnost certifikátů vašich partnerů a 14 dní před ukončením jejich platnosti vás program začne upozorňovat. Dále je nutné si pamatovat ještě jednu věc - pokud odešlete zprávu podepsanou klíčem těsně před koncem jeho platnosti, potom se může stát, že zpráva dojde adresátovi v době, kdy váš klíč už nebude platný. Proto doporučujeme provádět výměny klíčů včas a ne na poslední chvíli.

Poznámky:

1. Tlačítko výběru umístěné vedle položky Vstupní maska umožňuje vybrat pouze jeden soubor.
2. Pokud zapnete volbu Pamatuj heslo, bude si program toto heslo pamatovat po celou dobu svého běhu.

4.2 Dešifrování souborů

V případě, že chcete dešifrovat vstupní soubor a ověřit jeho podpis musíte (kromě zadání informací o uživateli) zadat ještě potřebné údaje do oblasti určené pro dešifrování souborů, tedy jméno vstupního souboru a výstupní adresář, do kterého se soubory obsažené v zašifrovaném souboru uloží. Opět je možné (stejně jako při šifrování) sledovat průběh dešifrování v okně, jehož obsah je možné uložit. Po ukončení akce se vám objeví hláška o průběhu dešifrování, která v případě bezchybného průběhu v sobě obsahuje i jméno certifikátu odesilatele dat.

V části okna určeného pro dešifrování je ještě možné nalézt přepínač označený jako "Archivace". Tento přepínač je možné použít v případě, kdy je potřeba zašifrovaný a podepsaný soubor dešifrovat, ale nechat podepsaný (takže po čase je možné jej opět použít, a to i v případě, kdy byl původní klíč adresáta ztracen či zapomenut). Nyní se však v cílovém adresáři nevytvoří jeden či více souborů obsažených v zašifrovaném a podepsaném archivu, ale jeden soubor, jehož název bude vycházet ze zdrojového souboru prodlouženého o předponu **`arch-`**, tedy například ze souboru **`kd010199.enc`** vznikne soubor **`arch-kd010199.enc`**

Poznámky:

1. Při dešifrování je prováděno testování, zda-li je certifikát odesilatele zprávy v pořádku. V případě, že jeho platnost skončila, budete na toto upozorněni a program se vás zeptá, zda-li stále chcete provést dešifrování.
2. Při dešifrovací nebo archivační operaci se každý ověřený certifikát uložený v příchozím souboru uloží do adresáře určeného pro certifikáty, diky čemuž máte možnost komunikovat s kýmkoliv, kdo vám již poslal soubor.

5. Pár rad pro správce

5.1 Zálohování klíčů

Vzhledem k tomu, že každý klient má v jednu dobu jednu dvojici klíčů, jejíž ztráta by způsobila nemalé problémy (to samé platí například pro zapomenutí hesla), je nutné tento klíč zálohovat. Vlastní způsob zálohování závisí samozřejmě na vás, nicméně doporučujeme následující postup:

Po vygenerování nové dvojice klíčů (operace Tvorba nového uživatele nebo operace Obnova klíče) a po

následném natažení certifikátu do systému doporučujeme změnit heslo na náhodnou změť znaků, toto zapsat na kus papíru v jedné kopii (nebo zapsat do souboru), potom zkopírovat na záložní disketu následující soubory (symbol **<root_crypta>** označuje kořenový adresář programu Crypta, např. **c:\crypta**):

1. důležité soubory spojené se zálohovaným uživatelem ze soukromého adresáře **<crypta_root>\keys** (např. z adresáře **c:\crypta\keys** soubory ***.pol**, ***.p12**);
2. databáze certifikátů (***.cdb**) z adresáře **<crypta_root>\keys**;
3. seznamy zneplatněných certifikátů (***.crl**) z adresáře **<crypta_root>\crls** a
4. vlastní certifikát a certifikát certifikační autority (jsou na disketě přinesené od pracoviště ČP).

Tato disketa by dále měla být uložena spolu s heslem u vedoucího daného útvaru, aby ji bylo v případě nutnosti možné použít.

Po této akci je ještě potřeba obnovit původní heslo.

5.2 Obměna klíčů

Platnost každé vygenerované dvojice klíčů je shodná s platností certifikátu vydaného k této dvojici klíčů (konkrétně k veřejnému klíči z této dvojice), která je jeden rok. Proto je nutné před uplynutím doby platnosti vygenerovat novou dvojici klíčů spolu s žádostí o certifikát a následně i požádat o vydání nového certifikátu. Program sám vás začne 14 dní před vypršením platnosti vašeho certifikátu na tuto skutečnost upozorňovat.

To samé však platí i pro certifikát komunikujícího partnera – když začne program hlásit, že do 14 dnů jeho platnost vyprší, je čas si obstarat nový. Tento je možné získat několika způsoby:

1. z LDAP serveru,
2. na kontaktním místě České pošty, kde se vydávají certifikáty,
3. na veřejně přístupném WWW/FTP serveru (e-mailem) a nebo
4. přímo od vašeho komunikačního partnera

To samé platí i pro seznam zneplatněných certifikátů – pro CRL, který je aktualizován každý den. Protože zatím není toto CRL na Internetu volně přístupné, nabízí ČP možnost denního rozesílání toto CRL e-mailem. Pokud máte o tento typ distribuce zájem, potom o něj požádejte operátora CA (např. při vydávání vašeho certifikátu). Potom budete denně dostávat zásilky s připojeným souborem ***.crl** o velikosti několika málo KB (do 10 KB)

Poznámka: Ještě si musíte uvědomit, že v přechodném období, kdy vám bude platit jak nový, tak i starý certifikát, můžete dostávat soubory zašifrované pro kterýkoliv z nich. Proto, pokud vás program v tomto období překvapí hláškou *"ERROR: nejsi příjemce"*, není nutné propadat panice - nejprve vyzkoušejte druhého platného uživatele.

5.3 Registry

Programový balík Crypta si do registrů systému Windows zaznamenává cestu k programu (normálně je tato hodnota zadána již při instalaci) a poslední nastavení programu **CryptaGui.exe**. Z těchto hodnot je provozně důležitá pouze cesta k programu (a to natolik, že pokud program dále uvedenou hodnotu nenajde, vyzve vás k jejímu zadání), která se nachází v

[HKEY_LOCAL_MACHINE\Software\CzechPost\Crypta]
"PrgDir"="c:\crypta\bin"

Poznámka: V případě nasazení programu Crypta na systému Windows NT/2000 je nutné zajistit, aby k výše uvedenému klíči registru měli přístup (čtení i zápis) všichni uživatelé pracující s programem Crypta. Změnu přístupových práv může provést jen administrátor za použití nástroje REGEDT32.EXE

5.4 Adresářová struktura

Vlastní program má doporučenou následující adresářovou strukturu:

1. **<root_crypta>**- zde je uloženo několik souborů instalačního programu **InstallShield**;
2. **<root_crypta>\bin** – zde jsou uloženy všechny 3 programy a obě používané DLL knihovny spolu s konfiguračním souborem;
3. **<root_crypta>\keys** – adresář, kde jsou uloženy soubory všech lokálních uživatelů;
4. **<root_crypta>\certs** – adresář, kde jsou uloženy všechny certifikáty komunikujících partnerů;
5. **<root_crypta>\crls** – adresář, kde jsou uloženy všechny seznamy zneplatněných certifikátů autorit používaných programem;
6. **<root_crypta>\temp** – adresář určený pro dočasné soubory vznikající při práci programu a nebo používaný pro dávkové stahování certifikátů z LDAP serveru;
7. **<root_crypta>\doc** – adresář s touto dokumentací v HTML formátu.

5.5.a Nastavení přístupových práv pro adresář Crypta na operačním systému Windows NT

Je výhodné omezit činnosti uživatelů v adresáři Crypta, aby například nemohlo dojít k neúmyslnému smazání důležitých souborů. Pro maximální omezení použijte následující postup (kromě skupiny *Users* přidávejte vždy skupiny *Administrators* a *SYSTEM* s právem *Full Control*; odstraňujte skupinu *Everyone*):

1. Adresáři **<root_crypta>** nastavte právo *Read* pro skupinu *Users* a zaškrtněte položky "Replace permissions on files" a "Replace permissions on directories".
2. Adresářům **<root_crypta>\bin** a **<root_crypta>\crls** nastavte právo *Add & Read (RWX)(RX)* pro skupinu *Users*.
3. Adresáři **<root_crypta>\temp** nastavte právo *Change (RWXD)(RWXD)* pro skupinu *Users*.
4. Souborům **<root_crypta>\bin*.exe** nastavte právo *Read (RX)* pro skupinu *Users*. Lze použít také pouze právo *(X)*, na testovacím stroji se však uživatelům poté nezobrazovaly ikony programů.
5. Souborům **<root_crypta>\bin*.dll** nastavte právo *(X)* pro skupinu *Users*

   (Podle místních podmínek můžete u všech bodů nahradit skupinu *Users* jinou uživatelskou skupinou)

Po tomto nastavení mohou uživatelé pouze šifrovat/dešifrovat a používat funkce **Dávkové stahování certifikátů** a ***Kopírování CRL***). Ostatní činnosti (nastavování prostředí, generování uživatelů, obnova klíčů, natahování certifikátů, výpočet databáze integrity) mohou provádět pouze administrátoři.
Povolení měnit nastavení prostředí uživateli se provede přístupovým právem *(RW)* pro skupinu *Users* souboru **<root_crypta>\bin\crypt.ini**.
Ostatní činnosti (všechny najednou!!) se povolí přístupovým právem *(RWX)(RWX)* pro adresář **<root_crypta>\keys** a přístupovým právem *(RW)(RW)* pro adresář **<root_crypta>\certs** skupině Users.
(V obou případech však uživatelé nebudou mít stále právo mazání souborů).

Poznámka:
Pokud potřebujete monitorovat práci uživatelů s programem Crypta, doporučujeme aktivování auditu souborů **<root_crypta>\keys*.p12** (Při vytvoření nového uživatele je pak potřeba přidat audit i nově vzniklému souboru P12).

5.5.b Nastavení přístupových práv pro adresář Crypta na operačním systému Windows 2000

Postup nastavování přístupových práv je na tomto operačním systému poměrně odlišný, proto se nachází v samostatné podkapitole. Níže uvedená práva se zadávají do sloupce "Allow", sloupec "Deny" ponechte prázdný. Zadávají se v okně, které se objeví po kliknutí na tlačítko "Advanced", zvolení skupiny uživatelů a

kliknutí na tlačítko "View/Edit..."
Pro maximální omezení použijte následující postup (kromě skupiny *Users* přidávejte vždy skupiny *Administrators* a *SYSTEM* s právem *Full Control*; odstraňujte skupinu *Everyone*):

1. Adresáři **<root_crypta>** nastavte následující právo, zaškrtněte položku "Reset permissions on all child objects and enable propagation of inheritable permissions."

Name:	Users
Aply onto:	This folder, subfolders and files
Permissions:	Traverse Folder/Execute File List Folder/Read Data Read Attributes Read Extended Attributes Read Permissions

2. Adresářům **<root_crypta>\bin** a **<root_crypta>\crls** nastavte **tato práva**:
(Abyste mohli provést změnu, musíte odškrtnout "Allow inheritable permissions from parent to propagate to this object")

Name:	Users
Aply onto:	Files only
Permissions:	Traverse Folder/Execute File List Folder/Read Data Read Attributes Read Extended Attributes Read Permissions

Name:	Users
Aply onto:	This Folder and subfolders
Permissions:	Traverse Folder/Execute File List Folder/Read data Read Attributes Read Extended Attributes Create Files/Write Data Read Permissions

3. Adresáři **<root_crypta>\temp** nastavte právo:

Name:	Users
Aply onto:	This folder, subfolders and files
Permissions:	Traverse Folder/Execute File List Folder/Read Data Read Attributes Read Extended Attributes Create Files/Write Data Create Folders/Append Data Delete Read Permissions

4. Souborům **<root_crypta>\bin*.exe** a **<root_crypta>\bin*.dll** nastavte právo:

Name:	Users
Aply onto:	This object only
Permissions:	Traverse Folder/Execute File Read Attributes Read Permissions

(Podle místních podmínek můžete u všech bodů nahradit skupinu *Users* jinou uživatelskou skupinou)

Po tomto nastavení mohou uživatelé pouze šifrovat/dešifrovat a používat funkce **Dávkové stahování certifikátů** a ***Kopírování CRL***). Ostatní činnosti (nastavování prostředí, generování uživatelů, obnova klíčů, natahování certifikátů, výpočet databáze integrity) mohou provádět pouze administrátoři.
Povolení měnit nastavení prostředí uživateli se provede následujícím přístupovým právem pro soubor **<root_crypta>\bin\crypt.ini**:

Name:	Users
Aply onto:	This object only

Permissions:	Traverse Folder/Execute File List Folder/Read Data Read Attributes Read Extended Attributes Create Files/Write Data Create Folders/Append Data Write Attributes Write Extended Attributes Read Permissions

Ostatní činnosti (všechny najednou!!) se povolí těmito přístupovými právy:

pro adresář **<root_crypta>\certs**

Name:	Users
Aply onto:	This folder, subfolders and files
Permissions:	List Folder/Read Data Read Attributes Read Extended Attributes Create Files/Write Data Create Folders/Append Data Write Attributes Write Extended Attributes Read Permissions

pro adresář **<root_crypta>\keys**

Name:	Users
Aply onto:	This folder, subfolders and files
Permissions:	Traverse Folder/Execute File List Folder/Read Data Read Attributes Read Extended Attributes Create Files/Write Data Create Folders/Append Data Write Attributes Write Extended Attributes Read Permissions

(V obou případech však uživatelé nebudou mít stále právo mazání souborů).

Poznámka:
Pokud potřebujete monitorovat práci uživatelů s programem Crypta, doporučujeme aktivování auditu souborů **<root_crypta>\keys*.p12** (Při vytvoření nového uživatele je pak potřeba přidat audit i nově vzniklému souboru P12).

5.6 Správa certifikátů

Protože se může stát, že se vám podaří přejmenovat certifikát či zapomenout na to, kdo se pod daným certifikátem skrývá, je výhodné mít k dispozici nástroj, kterým si můžete prohlédnout obsah certifikátu. Máte na výběr ze dvou možností:

1. použít funkci zabudovanou do programu crypta, která je však přístupná pouze z příkazové řádky (program cryptacmd.exe), nebo
2. použít součást aplikace MS Explorer verze 4.0 a vyšší (doporučujeme verzi 5), kterou vyvoláte v průzkumníkovi poklepáním na soubor s certifikátem.

5.7 Upgrade programu Crypta z verze 1.0

Protože jednou z nově zapracovaných změn je jiný typ ukládání vašeho vlatního certifikátu - ve verzi 1.0 byl uložen jako samostatný soubor, nyní je již správně uložen v `*.p12` souboru s klíčem, není možné přejít z verze 1.0 na verzi 1.2 pouhým odinstalováním staré verze a nainstalováním nové. Musíme použít postup shodný s tím, který poté použijeme, když přijedeme s nově vydaným certifikátem:

1. Nejprve uděláte zálohu adresáře s programem Crypta pro případ, že by se něco nepodařilo.
2. Odinstalujete program Crypta verze 1.0. Nyní by na disku měly zůstat uživatelské soubory uložené v adresáři `<root_crypta>\keys` a certifikáty partnerů v adresáři `<root_crypta>\certs`. Ostatní soubory doporučujeme smazat.
3. Nainstalujete program Crypta verze 1.3 do adresáře, v němž jste měli nainstalovánu starší verzi.

4. Provedete nastavení prostředí podle bodu 3.1
5. Nyní si vytvoříte disketu, jako byste právě přišli od operátora CA. Pokud tuto disketu stále máte, potom jděte rovnou na bod 6
    a. z adresáře **<root_crypta>\keys** na disketu nakopírujete svůj certifikát;
    b. z adresáře **<root_crypta>\keys** na disketu nakopírujete soubor **ca.crl**;
    c. certifikát CA se však v původním tvaru nikde nenachází (je umístěn ve struktuře databáze certifikátů - soubor **<root_crypta>\keys\ca.cdb**). Proto jej musíte nejprve z této struktury dostat ven. Provedete export certifikátu z databáze pomocí programu cryptacmd.exe s následujícími parametry: **cryptacmd ecdb ca a:\ca.crt** a pro export zvolíte 1. certifikát.
6. Provedete natažení certifikátu podle bodu 3.4
7. Vypočítáte databázi integrity podle bodu 3.5
8. Můžete šifrovat.

5.8 Upgrade programu Crypta z verze 1.1

Rozdíly mezi verzemi 1.2 a 1.1 spočívají v různém ukládání certifikátů autorit a CRL):

Oblast	Verze 1.1	Verze 1.3
Ukládání certifikátů autorit	Program používá jednu databázi certifikátů autorit pro všechny uživatele - soubor **ca.cdb**	Každý uživatel má svou vlastní databázi autorit - soubor **jmeno_uzivatele.cdb**. Formát je nezměněn.
Ukládání CRL	V celém programu se používá jedno CRL - soubor **ca.crl**	Program nově pracuje s adresářem, do kterého se ukládají CRL všech v programu používaných autorit.

Postup je tedy velice jednoduchý:

1. Nejprve uděláte zálohu adresáře s programem Crypta pro případ, že by se něco nepodařilo.
2. Odinstalujete program Crypta verze 1.1. Nyní by na disku měly zůstat uživatelské soubory uložené v adresáři **<root_crypta>\keys** a certifikáty partnerů v adresáři **<root_crypta>\certs**. Ostatní soubory doporučujeme smazat.
3. Nainstalujete program Crypta verze 1.3 do adresáře, v němž jste měli nainstalovánu starší verzi.
4. Soubor **ca.crl** nakopírujete do adresáře vyhrazeného pro ukládání CRL
5. Soubor **ca.cdb** přejmenujete/překopírujete tak, aby jeho jméno bylo shodné se jménem každého uživatele (pro více uživatelů si tedy musíte udělat více kopií tohoto souboru).
6. Provedete nastavení prostředí podle bodu 3.1
7. Vypočítáte databázi integrity podle bodu 3.5
8. Můžete šifrovat.

5.9 Upgrade programu Crypta z verze 1.2

Tento upgrade bude nejjednodušší, protože oproti verzi 1.2 nedošlo k žádným zásahům do adresářové struktury.

1. Nejprve uděláte zálohu adresáře s programem Crypta pro případ, že by se něco nepodařilo.
2. Odinstalujete program Crypta verze 1.2. Nyní by na disku měly zůstat uživatelské soubory uložené v adresáři **<root_crypta>\keys** a certifikáty partnerů v adresáři **<root_crypta>\certs**. Ostatní soubory doporučujeme smazat.
3. Nainstalujete program Crypta verze 1.3 do adresáře, v němž jste měli nainstalovánu starší verzi.
4. Provedete nastavení prostředí podle bodu 3.1
5. Můžete šifrovat.

5.10 Řešení problémů a zodpovídání dotazů

Pokud se při používání tohoto programu dostaví problémy, nebo budete mít dotazy či připomínky, kontaktujte, prosím, lokálně příslušného operátora CA (systémovou podporu), který buď na vaše dotazy odpoví a nebo je předá řešitelům, kteří se pokusí dotazy zodpovědět a věcné připomínky zapracovat do programu.

Poznámka:V případě výskytu vážnějšího problému (mj. tehdy, když bude váš dotaz přesměrován na řešitele) je podmínkou rychlého vyřešení problému znalost okolností výskytu chyby a vašeho nastavení programu. Proto vás v tomto případě prosíme o zaslání následujících údajů (nejlépe e-mailem):

1. přesný popis problému (tzn. kdy a jak se chyba projevuje) - nejlepší je poslat alespoň pár posledních řádků logu běhu programu;

2. důležité soubory s údaji popisujícími vaše nastavení. Tyto soubory získáte spuštěním dávky **`error.bat`**, která se nachází v programovém adresáři. Tato dávka vytvoří adresář **`c:\crypta.err`**, kam nakopíruje všechny potřebné soubory. Tyto soubory, které neobsahují žádné citlivé informace (např. soubory s klíči **`*.p12`** se nekopírují; dávka je okomentovaná - můžete se přesvědčit), potom pošlete osobě, která se zabývá vaším problémem. Soubory doporučujeme zkomprimovat programem ARJ nebo ZIP.

6. Přílohy

Vypracoval:

Česká pošta, státní podnik
OZ VAKUS
L.P. 2001

Příloha č. 1

Vlastnosti a HW+SW požadavky programu Crypta

- Program umožňuje šifrování jednoho či více souborů z jednoho adresáře.
- Program provádí kompresi dat kompatibilní s formátem gzip.
- Vlastní data program šifruje algoritmem TripleDES o síle 112 bitů (CBC mód) nebo RC2 o síle 128 bitů.
- Používá hašovací funkci SHA-1.
- Provádí generování asymetrických RSA klíčů.
- RSA klíče o síle 1024 nebo 2048 bitů program ukádá ve formátu PKCS#12, kde jsou uloženy v zašifrovaném tvaru s použitím TripleDES algoritmu.
- Pro distribuci asymetrických RSA klíčů využívá program centralizovaný model výměny klíčů postavený na certifikační autoritě – používá žádosti o certifikát dle standardu PKCS#10 a certifikáty dle standardu X.509v3 v DER formátu.
- Podporuje práci s více CA (i v hierarchické struktuře).
- Podporuje ověřování platnosti certifikátů pomocí CRL.
- Podporuje šifrování souboru až pro 32 příjemců zároveň.
- Podporuje šifrování souboru i na více disket nebo do více souborů.
- Podporuje formát zašifrovaného souboru podle PKCS#7.
- Umí stahovat certifikáty z veřejně přístupného LDAP serveru prostřednictvím protokolu TCP/IP (podporuje práci s více LDAP servery - až 10).
- Umí pracovat jak v grafickém, tak i v příkazovém režimu.
- Pracuje pouze v prostředí Win32, tedy pod operačními systémy MS Windows95 SR2, MS Windows98, MS WindowsME, MS Windows2000 a MS WindowsNT. Zde je doporučena podpora českého prostředí, jinak může dojít k problémům se zobrazováním češtiny, nicméně pro vlastní funkčnost programu toto nutné není.
- Program vyžaduje pro vlastní instalaci cca 5 MB na pevném disku a další prostor pro dočasné soubory, který je rovný dvojnásobku zpracovávaných dat v nekomprimovaném stavu.
- Program pracuje s datovými údaji z intervalu let 1980 až 2038. Zobrazené časové hodnoty jsou v zimním čase.
- Program je postaven na komerčních kryptografických knihovnách PKI-Plus firmy Baltimore Ltd. a používá GNU knihovny ZLIB autorů Jean-loup Gaillyho a Marka Adlera.
- Program je zpětně kompatibilní s verzemi 1.1 a 1.2

Vypracoval:

Česká pošta, státní podnik
OZ VAKUS
L.P. 2001

Příloha 2

Parametry programu `CryptaCmd.exe`

Program **`CryptaCmd.exe`** nabízí tyto funkce:

- kompresi (volitelná), šifrování (volitelné) a podepsání (povinné) dat, následné
- dešifrování, ověření podpisu a dekompresi dat,
- dešifrování, ověření podpisu a archivaci dat,
- výpis obsahu databáze certifikátů,
- export certifikátu z databáze certifikátů,
- výpis údajů uložených v certifikátu,
- uložení hesla k tajménu klíči v zašifrovaném souboru.

Pro svou funkci dostává program **`CryptaCmd.exe`** data z příkazové řádky (případně se na některá – jako heslo – přímo dotáže) a ze souboru **`crypt.ini`**, uloženého v adresáři programu. Cestu k tomuto programu získává program z cesty příkazu, kterým je vyvolán, takže je výhodné tento program spouštět buď přímo z adresáře, kde je nainstalován a nebo zadávat celou jeho cestu.

Šifrování dat

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

- komprimuje, šifruje a podepisuje soubor,
- volitelný znak **2**/**d**/**7** určuje formát výstupního souboru: **2** pro "verzi 2", **d** pro formát "diskety" a **7** pro formát "PKCS#7"; pokud není žádný z těchto znaků uveden, používá se původní "formát 1"
- volitelný znak +/- označuje kompresi (+) či bez komprese (-); pokud znaménko není uvedeno, používá se komprese
- položka vstupní soubory obsahuje celou cestu a masku souboru (např. **c:\windows*.txt**)
- soubor s heslem - jedná se o soubor vytvořený pomocí níže uvedené funkce "Uložení hesla do souboru"

Podepisování dat

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

- komprimuje a podepisuje soubor,
- volitelný znak **2**/**d**/**7** určuje formát výstupního souboru: **2** pro "verzi 2", **d** pro formát "diskety" a **7** pro formát "PKCS#7"; pokud není žádný z těchto znaků uveden, používá se původní "formát 1"
- volitelný znak **+**/**-** označuje kompresi (**+**) či bez komprese (**-**); pokud znaménko není uvedeno, používá se komprese
- položka vstupní soubory obsahuje celou cestu a masku souboru (např. **`c:\windows\*.txt`**)
- soubor s heslem - jedná se o soubor vytvořený pomocí níže uvedené funkce "Uložení hesla do souboru"

Dešifrování dat

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

- dešifruje, ověří podpis a dekomprimuje soubor
- soubor s heslem - jedná se o soubor vytvořený pomocí níže uvedené funkce "Uložení hesla do souboru"

Archivace dat

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

- dešifruje soubor
- soubor s příponou **arch-** uloží do výstupního adresáře
- soubor s heslem - jedná se o soubor vytvořený pomocí níže uvedené funkce "Uložení hesla do souboru"

Dávkové stahování certifikátů nebo CRL

CryptaCmd ln jmeno {cislo_LDAP_serveru}

- dávkově stahuje certifikáty nebo CRL z LDAP serveru
- stažené certifikáty jsou uloženy do pracovního adresáře
- stažené CRL je uloženo do soukromého adresáře
- položka jméno může obsahovat buď text "crl" a tehdy se stahuje CRL a nebo hledaný text ve jméně certifikátu
- položka číslo LDAP serveru může obsahovat pořadové číslo LDAP serveru v seznamu LDAP serverů. Pokud tato položka chybí, je automaticky použit první LDAP server.

Uložení hesla do souboru

CryptaCmd sp soubor_s_heslem

- ukládá heslo k tajnému klíči do souboru v nečitelné formě

Výpis obsahu databáze certifikátů

CryptaCmd lcdb jmeno_uzivatele

- vypisuje všechny certifikáty CA uložených v databázi certifikátů
- jmeno_uzivatele - jméno uživatele, jehož databázi certifikátů chcete zobrazit

Export certifikátu z databáze certifikátů

CryptaCmd ecdb jmeno_uzivatele jmeno_souboru

- exportuje vybraný certifikát z databáze certifikátů a ukládá jej do souboru *jmeno_souboru*
- volba certifikátu pro export se provádí v programu zvolením jeho pořadového čísla (od 1.)
- jmeno_uzivatele - určuje jméno uživatele, z jehož databáze certifikátů bude export probíhat

Výpis informací z certifikátu

CryptaCmd pcrt jmeno_souboru

- vypisuje na obrazovku informace o certifikátu uloženém v zadaném souboru

Kopírování CRL

CryptaCmd cc jmeno_souboru

- zadaný soubor uloží do adresáře s CRL, přejmenovaný podle interních pravidel

---

Vypracoval:

Česká pošta, státní podnik
OZ VAKUS
L.P. 2001

Příloha č. 3

Historie změn programu Crypta

verze 1.0

```
první veřejně uvolněná verze
```

---

verze 1.1

```
+ přidáno
! opraveno
- vypuštěno
```

Engine:
```
+ přidány další symetrické šifry (3DES-CBC, 3DES-ECB, RC2)
+ kontrola natahovaných certifikátů
+ odesílatel je automaticky přidáván k příjemcům
+ při šifrování i dešifrování jsou vypisovány zpracovávané soubory
+ funkce na správu databáze certifikátů
+ funkce na výpis informací z certifikátu
! uživatelské certifikáty jsou ukládány přímo do souboru p12 (formát PKCS#12)
! soubory p12 jsou šifrovány algoritmem TripleDES
! ověřování databáze integrity pro soubory v adresáři obsahujícím v názvu mezeru
! zvýšen limit stahovaných certifikátů v dávkovém stahování na 512 certifikátů
! šifrování z disku na disk pod OS Windows NT
! nevytváří se pomocný soubor *.out
! testování přepisu existujících souborů
! podmínky pro ukládání certifikátu odesilatele na disk při dešifrování nebo archivaci
```

CryptaTool:
```
+ přidán soubor nápovědy
+ v tvorbě uživatelů: kontrola existence jména uživatele, kontrola mezer za posledními
znaky
```

CryptaGUI:
```
+ přidána možnost dočasného pamatování hesla
+ přidán tento soubor nápovědy
! šifrování z rootu disku
```

CryptaCmd:
```
+ možnost uložení šifrovaného hesla na disk (pro další použití v CryptaCMD)
+ přidána správa databáze certifikátů CA (tisk, export)
! při zadávání hesla v CryptaCMD nejsou zobrazovány znaky (jsou zobrazovány *)
```

---

verze 1.2

```
+ přidáno
! opraveno
- vypuštěno
```

Engine:
```
! podpora více certifikačních autorit (pro každého uživatele zvlášť)
+ podpora hierarchické struktury certifikačních autorit (ověřování celého tzv.
certificate chain)
+ kontrola certifikátů oproti více CRL zároveň
+ možnost stahování certifikátů a CRL z více LDAP serverů
+ kontrola času platnosti jednotlivých CRL (+ možnost jejího potlačení)
! funkce pro slučování souborů
```

---

verze 1.3

```
+ přidáno
! opraveno
- vypuštěno
```

Engine:
```
! funkce pro výpočet data
+ podpora formátu PCS#7
+ možnost dělení zašifrovaných souborů na části o velikosti 1.44 MB (formát "diskety")
+ funkce kopírování CRL souboru do adresáře <root_crypta>\crls
! odkaz na P12 soubor v POL souboru již není dán absolutní cestou (pouze pro nově
generované klíče)
```

CryptaTool:
```
! zpřístupněna volba symetrické šifry v Nastavování prostředí
+ přidáno kopírování certifikátů partnerů v Natahování certifikátu
+ tlačítko Kopírování CRL
```

CryptaGUI:
```
! zpřístupněna volba symetrické šifry
+ možnost výběru formátu výstupního šifrovaného souboru (verze 1, verze 2, diskety,
PKCS#7)
```

CryptaCmd:
```
! parametry ecdb a lcdb již vyžadují pouze zadání uživatelského jména namísto plné
cesty k CDB souboru
```

Dokumentace:
```
! přepracování HTML dokumentu se seznamem chybových hlášek
```

Vypracoval:

Česká pošta, státní podnik
OZ VAKUS
L.P. 2001

Chyby, jejich příčiny a náprava v programu Crypta v1.3

Seznam chybových hlášení je rozdělen podle místa jejich výskytu. Stačí si pouze nalistovat tu činnost programu, ve které k chybě došlo, a **měli byste** nalézt řešení. Neuspějete-li, zkuste si chybovou hlášku vyhledat pomocí funkce **Najít (CTRL+F)** ve vašem internetovém prohlížeči; třeba se nachází v jiné sekci. Kromě znění chybové hlášky porovnávejte i její umístění v chybovém logu; v tabulkách jsou většinou uvedeny části logu s danou chybou, nebo jsou uvedeny přímo celé výpisy těchto logů.

Pokud není vaše chyba v seznamu zahrnuta, požádejte o pomoc operátora CA.

Poznámka:
V textu vycházíme z toho, že jste ponechali přednastavenou adresářovou strukturu, tedy že:

soukromý adresář s klíči:	**<root_crypta>\keys**
adresář s certifikáty partnerů:	**<root_crypta>\certs**
dočasný adresář:	**<root_crypta>\temp**
adresář s CRL:	**<root_crypta>\crls**

Pokud jste v **Nastavování prostředí** změnili některý nastavený adresář, přizpůsobte řešení problému svému nastavení.

(Doporučené rozlišení pro tento dokument je 1024x768 bodů)

Obsah:

Obecné chybové hlášky

Chyba:	Vyber adresare s programem
Příčina:	Toto okno se objeví po spuštění programu CryptaGui nebo CryptaTool. Příčinou může být chybějící přístupové právo zápisu do registru (Windows NT, 2000) nebo chybějící položka "PrgDir" v klíči registru "HKEY_LOCAL_MACHINE\Software\CzechPost\Crypta".
Náprava:	Oprava přístupových práv je v uživatelské dokumentaci, kapitole 5.3, chybějící položku si program sám doplní, až mu zadáte adresář **<root_crypta>\bin**.

Chyba:	failed to set data for 'PrgDir'
Příčina:	Tato hláška se objeví po spuštění programu CryptaGui nebo CryptaTool. Způsobuje ji chybějící přístupové právo zápisu do registru.
Náprava:	Viz uživatelská dokumentace, kapitola 5.3

Chyba:	ERROR: Nepovedlo se nacist knihovnu CryptaLib.dll ci nsldapssl32v30.dll (CryptaGui a CryptaTool) ***ERROR: nepovedlo se nacist dll knihovnu - cislo chyby : 1157 (CryptaCmd)
Příčina:	Programu se nepodařilo načíst některý nebo oba zmíněné soubory.

Náprava:	Zkontrolujte existenci těchto souborů v adresáři **<root_crypta>\bin** a zda máte příslušná přístupová práva (Windows NT, 2000). Tyto soubory mohou být i poškozené - pak je potřeba přeinstalovat program.

Nastavování prostředí

Chyba:	Není zadaný popis LDAP serveru
Příčina:	Klikli jste na tlačítko "Přidej", ale nevyplnili jste popis LDAP serveru.
Náprava:	Doplňte popis LDAP serveru, který jej bude charakterizovat.

Chyba:	Není zadaná adresa LDAP serveru
Příčina:	Klikli jste na tlačítko "Přidej", ale nevyplnili jste adresu LDAP serveru.
Náprava:	Doplňte buď IP adresu nebo DNS jméno LDAP serveru.

Chyba:	Není zadaný port LDAP serveru
Příčina:	Klikli jste na tlačítko "Přidej", ale nevyplnili jste port LDAP serveru.
Náprava:	Doplňte port LDAP serveru (standardně 389).

Chyba:	Nemohu otevrit soubor pro zapis
Příčina:	Objeví se po kliknutí na tlačítko "Nastav". Program nemůže vytvořit nebo zapsat do souboru **<root_crypta>\bin\crypt.ini**.
Náprava:	Ověřte, zda tento soubor nemá zapnut atribut "jen ke čtení", nebo zda máte přístupové právo zápisu do tohoto souboru resp. adresáře (Windows NT, 2000).

Tvorba nového uživatele

Chyba:	Nemáš zadané Uživatelské jméno Nemáš zadané Jméno certifikátu Nemáš zadanou Organizaci Nemáš zadané Město
Příčina:	Uvedená položka je prázdná.
Náprava:	Vyplňte tuto položku.

Chyba:	ERROR: spatne jmeno politiky
Příčina:	Jméno uživatele je používáno pro pojmenování generovaných souborů. Ve vámi zadaném jménu uživatele se však vyskytují znaky, které nelze použít (např. /, \, <, >, ?, *, :, atd.).
Náprava:	Zvolte si jiné jméno uživatele.

Chyba:	Politika s takovym jmenem jiz existuje - zvolte jine jmeno
Příčina:	Uživatel s vámi zvoleným jménem již byl vytvořen. Bez tohoto varování by došlo k jeho přepsání.
Náprava:	Zvolte si jiné jméno uživatele.

Chyba:	Heslo musí mít alespoň 8 znaků
Příčina:	Program vyžaduje délku hesla alespoň 8 znaků.
Náprava:	Zvolte si jiné, delší heslo.

Chyba:	Heslo musí obsahovat jeden malý znak a jeden velký znak či číslo
Příčina:	Program vyžaduje hesla, obsahující malé znaky s alespoň jedním velkým znakem nebo číslem.
Náprava:	Zvolte si jiné heslo, které bude splňovat uvedená kritéria.

Chyba:	Hesla si neodpovídají
Příčina:	Hesla v položkách "Heslo" a "Ověřovací heslo" si neodpovídají.
Náprava:	Zadejte znovu zvolené heslo.

Chyba:	V poli "?????" jsou nepovolene znaky
Příčina:	Nepovolené znaky (diakritika, oddělovníky, atd.) mohou při generování certifikátu způsobovat problémy (ačkoliv generování klíče + žádosti o certifikát proběhlo v pořádku). Proto jsou znaky, povolené pro zadávání hodnot, značně omezené.
Náprava:	Používejte pouze základní znaky bez diakritiky, čísla a znaky ".", "@", "-", "/".

Chyba:	V poli ????? je posledním znakem mezera.
Příčina:	Tato mezera může při generování certifikátu způsobit problémy (a operátor CA ji může přehlédnout).
Náprava:	Odmažte mezeru v uvedeném poli.

Chyba:	Nemohu otevrit soubor pro zapis
Příčina:	Objeví se po zvolení umístění a jména souboru REQ se žádostí o certifikát. Program nemůže vytvořit nebo zapsat do tohoto souboru.
Náprava:	Ověřte, zda nejsou ve jméně nepovolené znaky (\ / : atd.), zda máte oprávnění tento soubor vytvořit (Windows NT, 2000) a zda již tento soubor neexistuje a nemá zapnutý atribut "jen ke čtení". Ukládáte-li soubor na disketu, zkontrolujte, zda není zablokovaná proti zápisu.

Chyba:	Nemohu zapsat do souboru
Příčina:	Objevuje se po pokusu uložit žádost o certifikát (soubor *.REQ). Tato chyba vzniká v případě, kdy se nepodaří vytvořit soubory uživatele (nedostatečná oprávnění nebo neexistující ***soukromý adresář s klíči*** (standardně **<root_crypta>\keys**).
Náprava:	Zkontrolujte, zda založení adresáře nebrání např. stejnojmenný soubor. Pokud takový adresář existuje, zkontrolujte pro něj přístupová práva (Windows NT, 2000).

Chyba:	Cannot create file ?????\crypta\bin\error.log.
Příčina:	Program nemohl vytvořit uvedený soubor.
Náprava:	Zkontrolujte, zda v adresáři **<root_crypta>\bin** neexistuje stejnojmenný soubor se zapnutým atributem "jen ke čtení" a zda máte přístupové právo vytvářet v adresáři soubory (Windows NT, 2000).

Obnova klíče

ERROR: Spatne jmeno politiky	viz **Tvorba nového uživatele**
ERROR: politika s takovym jmenem jiz existuje - zvolte jine jmeno	viz **Tvorba nového uživatele**
Heslo musí mít alespoň 8 znaků	viz **Tvorba nového uživatele**
Heslo musí obsahovat jeden malý znak a jeden velký znak či číslo	viz **Tvorba nového uživatele**
Hesla si neodpovídají	viz **Tvorba nového uživatele**
Cannot create file ?????\crypta\bin\error.log.	viz **Tvorba nového uživatele**

Chyba:	Nemáš zadaného uživatele
Příčina:	Nezadali jste jméno uživatele.
Náprava:	Doplňte uživatelské jméno.

Chyba:	Nemáš zadaného nového uživatele
Příčina:	Nezadali jste jméno pro nového uživatele.
Náprava:	Doplňte uživatelské jméno novému uživateli.

Chyba:	ERROR: chyba pri otevirani politiky
Příčina:	Program nemohl otevřít soubor s politikou zadaného uživatele (soubor *jmeno_uzivatele*.pol) v ***soukromém adresáři s klíči*** (standardně **<root_crypta>\keys**).
Náprava:	Zkontrolujte existenci tohoto souboru a zda k němu máte správná přístupová práva (Windows NT, 2000). A nezadali jste jméno uživatele špatně?

Chyba:	Jmeno noveho uzivatele nesmi byt shodne se jmenem stareho
Příčina:	Zadali jste stejné jméno původního i nového uživatele, Crypta nedovoluje přepsání starého uživatele novým.
Náprava:	Zvolte si jiné jméno uživatele.

Chyba:	Access violation at address ????? in module 'CRYPTALIB.DLL'. Read of address ?????.
Příčina:	Poškozený soubor s politikou původního uživatele.
Náprava:	Proveďte vygenerování uživatele přes volbu "Tvorba nového uživatele". Pokud byl původní uživatel vygenerován ještě v Cryptě 1.0, může být v jeho POL souboru uložen nekorektní údaj. Vyeditujte soubor ***jmeno_uzivatele*.pol** v ***soukromém adresáři s klíči*** (standardně **<root_crypta>\keys**) a vyhledejte znak "," (čárka) - nejčastěji bývá ve jméně organizace. Smažte jej, uložte změny a zkuste opět obnovu klíče. V opačném případě

Natahování certifikátu

ERROR: Chyba pri otevirani politiky	viz **Obnova klíče**
Cannot create file ?????\crypta\bin\error.log.	viz **Tvorba nového uživatele**

Chyba:	Nemáš nastaveného uživatele
Příčina:	Nevyplnili jste položku Uživatel - Jméno.
Náprava:	Zvolte jméno uživatele.

Chyba:	Nemáš zadané heslo
Příčina:	Nezadali jste heslo uživatele.
Náprava:	Doplňte toto heslo.

Chyba:	ERROR: spatne heslo
Příčina:	Zadané heslo uživatele není správné.
Náprava:	Opravte toto heslo. Zkontrolujte si zvolený jazyk klávesnice (Česká-Anglická), zapnutý CAPS-LOCK, vypnutý NUM-LOCK, apod.

Chyba:	Nemáš vybraný svůj certifikát
Příčina:	Nevyplnili jste položku Uživatelův certifikát.
Náprava:	Zadejte nebo nalistujte soubor s certifikátem, který vám byl vydán (**jméno_uživatele.crt**).

Chyba:	Nemáš zadaný žádný certifikát a CRL autority
Příčina:	Nezadali jste certifikát a CRL certifikační autority, dlouhé okno vlevo od kláves s šipkami nahoru a dolů je prázdné.
Náprava:	Zadejte/nalistujte soubory s certifikátem a CRL autority a klikněte na tlačítko "Přidej".

Chyba:	Nemáš vybraný adresář s certifikáty partnerů
Příčina:	Nezadali (resp. smazali) jste položku **Adresář s certifikáty partnerů**.
Náprava:	Zadejte do položky takový adresář, v němž máte certifikáty partnerů uloženy. Pokud chcete kopírování certifikátů provést ručně, zadejte libovolný adresář, v němž se nenachází soubory s příponou CRT.

Chyba:	Vybrany soubor s certifikatem autority neexistuje
Příčina:	Objevuje se po kliknutí na tlačítko "Přidej". Program nemohl otevřít zadaný soubor s certifikátem autority, nebo jste jej nazadali.
Náprava:	Doplňte soubor, příp. zkontrolujte existenci zadaného souboru a přístupová práva k němu (Windows NT, 2000).

Chyba:	Vybrany soubor s CRL autority neexistuje
Příčina:	Objevuje se po kliknutí na tlačítko "Přidej". Program nemohl otevřít zadaný soubor s CRL autority, nebo jste jej nazadali.
Náprava:	Doplňte soubor, příp. zkontrolujte existenci zadaného souboru a přístupová práva k němu (Windows NT, 2000).

Chyba:	Soubor s tvým certifikátem neexistuje
Příčina:	Objevuje se po kliknutí na tlačítko "Natáhni". Program nemohl otevřít zadaný soubor s uživatelovým certifikátem.
Náprava:	Zkontrolujte existenci zadaného souboru a přístupová práva k němu (Windows NT, 2000).

Dotaz:	Jiz existuje databaze certifikatu pod stejnym jmenem. Pokud budete pokracovat, bude prepsana. Pokracovat?
Příčina:	Program našel existující soubor **<root_crypta>\keys\jméno_uživatele.cdb**.
Náprava:	Je možné, že tento uživatel již má natažený certifikát, nebo proces natahování skončil chybou po vytvoření tohoto souboru. Můžete klidně potvrdit přepsání souboru a pokračovat v natahování certifikátu.

Upozornění:	ERROR: akce prerusena uzivatelem
Příčina:	Nejedná se o chybu, ale o upozornění, že uživatel přerušil práci programu.
Náprava:	N/A

Chyba:	ERROR: nekorespodujici verejny a tajny klic - snaha o import spatneho certifikatu
Příčina:	Certifikát byl vydán pro jiného uživatele, než je právě zvolený.
Náprava:	Soubor s uživatelským certifikátem by se měl jmenovat jako uživatel, pro kterého byl tento certifikát vydán. Zkontrolujte, zda jste nezvolili špatného uživatele. Pokud máte více uživatelů, zkuste zadat jiného. V případě přetrvávajícího problému kontaktujte hotline Crypty.

Chyba:	ERROR: certifikat byl zneplatnen
Příčina:	Uživatelský certifikát byl zneplatněn.
Náprava:	Zvolte platný uživatelský certifikát. Pokud máte pochybnosti o důvodu zneplatnění certifikátu, kontaktujte operátora CA.

Chyba:	ERROR: certifikat nebyl overen zadnym certifikatem CA
Příčina:	Certifikát byl vydán jinou autoritou než tou, kterou jste zadali (jako první při zadávání více autorit). Většinou je zadán špatně certifikát uživatele a/nebo certifikát autority.
Náprava:	Opravte zadané soubory s uživatelovým certifikátem a certifikátem autority.

Chyba:	ERROR: CRL nebylo overeno zadnym certifikatem CA
Příčina:	Oproti zadanému certifikátu autority jste zvolili takové CRL autority, které "patří" jiné autoritě.
Náprava:	Vymažte zadané soubory s certifikátem a CRL autority tlačítkem "Odeber". Zadejte správně tyto soubory. Postup je popsán v uživatelské dokumentaci, kapitole 3.4

Chyba:	ERROR: nebylo mozne overit retez certifikatu CA
Příčina:	V seznamu certifikátů a CRL autorit není zadán jeden nebo více souborů správně.
Náprava:	Vymažte zadané soubory s certifikáty a CRL autorit tlačítkem "Odeber". Zadejte správně tyto soubory. Postup je popsán v uživatelské dokumentaci, kapitole 3.4

Dotaz:	Certifikat autority "?????" neni korenovy, coz muze zpusobovat problemy. Pokracovat?
Příčina:	V seznamu certifikátů a CRL autorit jsou zadány (jedna nebo více) pouze tzv. podřízené autority - chybí kořenová autorita, která vydala certifikát těmto podřízeným autoritám.
Náprava:	Odmítněte pokračování kliknutím na tlačítko "NE". Doplňte do seznamu soubory s certifikátem a CRL kořenové autority. Celý postup natahování certifikátu je popsán v uživatelské dokumentaci, kapitole 3.4

Chyba:	ERROR: nemohu vytvorit vystupni adresar ukladani CRL
Příčina:	Program nemohl uložit CRL soubory do *adresáře s CRL* (umístění adresáře zjistíte v **Nastavování prostředí**).
Náprava:	Zkontrolujte, zda tento adresář existuje, zda místo něj neexistuje stejnojmenný soubor a zda máte do něj právo zápisu. Doporučujeme nastavit tento adresář na **<root_crypta>\crls**.

Chyba:	CHYBA: Natazeni certifikatu probehlo v poradku, ale nepodarilo se nakopirovat certifikaty prijemcu(). Provedte nakopirovani rucne.
Příčina:	Program nemohl uložit soubory do adresáře **<root_crypta>\certs**.
Náprava:	Zkontrolujte, zda tento adresář existuje, zda místo něj neexistuje stejnojmenný soubor a zda máte do něj právo zápisu. Po vyřešení těchto obtíží do něj ručně nakopírujte certifikáty partnerů, které jste dostali s vydaným uživatelovým certifikátem.

Chyba:	ERROR: interni chyba v krypto knihovne Unknown DER tag
Příčina:	Některý soubor s certifikátem/CRL je poškozený. Přesnější určení tohoto souboru lze zjistit z chybového logu aplikace.
Náprava:	Požádejte operátora CA o opětovné zaslání souboru s certifikátem/CRL.

Chyba:	Access violation at address ????? in module 'CRYPTALIB.DLL'. Read of address ?????.
Příčina:	Poškozený soubor s politikou uživatele (**<root_crypta>\keys\jméno_uživatele.pol**).
Náprava:	Pokuste se obnovit soubor ze zálohy. Pokud ji nemáte, je teoreticky možné použít jiný POL soubor; poraďte se s operátorem CA.

Chyba:	ERROR: interni chyba v krypto knihovne pkcs12_obj_fromfile() failed
Příčina:	Soubor **<root_crypta>\keys\jméno_uživatele.p12** je poškozený.
Náprava:	Tento soubor lze pouze obnovit ze zálohy. Pokud ji nemáte, musíte si vygenerovat nového uživatele a požádat o nový certifikát.

Chyba:	ERROR: interni chyba v krypto knihovne failed to locate any key pairs
Příčina:	Program nemohl otevřít soubor **jméno_uživatele.p12**.
Náprava:	Program hledá tento soubor podle odkazu v souboru **<root_crypta>\keys\jméno_uživatele.pol**. Vyeditujte si tedy tento soubor a zkontrolujte tento odkaz, je hned na začátku souboru. Obsahuje-li plnou cestu k souboru, vymažte ji a ponechte pouze jméno souboru a příponu P12. Soubor se pak bude hledat pod uvedeným jménem ve stejném adresáři jako POL soubor uživatele. Zkopírujte jej (ten P12 soubor) sem, příp. opravte jméno, nebo zkontrolujte přístupová práva k souboru (Windows NT, 2000).

Změna hesla

Nemáš zadaného uživatele	viz **Obnova klíče**
Heslo musí mít alespoň 8 znaků	viz **Tvorba nového uživatele**
Heslo musí obsahovat jeden malý znak a jeden velký znak či číslo	viz **Tvorba nového uživatele**
Hesla si neodpovídají	viz **Tvorba nového uživatele**
ERROR: Chyba pri otevirani politiky	viz **Obnova klíče**
ERROR: Spatne heslo	viz **Natahování certifikátu**
Access violation at address ????? in module 'CRYPTALIB.DLL'. Read of address ?????.	viz **Natahování certifikátu**
ERROR: interni chyba v krypto knihovne pkcs12_obj_fromfile() failed	viz **Natahování certifikátu**
ERROR: interni chyba v krypto knihovne failed to locate any key pairs	viz **Natahování certifikátu**
Cannot create file ?????\crypta\bin\error.log.	viz **Tvorba nového uživatele**

Chyba:	Nemáš zadané původní heslo
Příčina:	Nevyplnili jste položku Staré heslo.
Náprava:	Doplňte heslo zvoleného uživatele.

Výpočet databáze integrity

Nemáš zadaného uživatele	viz **Obnova klíče**
Nemáš zadané heslo	viz **Natahování certifikátu**
ERROR: Chyba pri otevirani politiky	viz **Obnova klíče**
ERROR: Spatne heslo	viz **Natahování certifikátu**
Access violation at address ????? in module 'CRYPTALIB.DLL'. Read of address ?????.	viz **Natahování certifikátu**
ERROR: interni chyba v krypto knihovne pkcs12_obj_fromfile() failed	viz **Natahování certifikátu**
ERROR: interni chyba v krypto knihovne failed to locate any key pairs	viz **Natahování certifikátu**
Cannot create file ?????\crypta\bin\error.log.	viz **Tvorba nového uživatele**

Chyba:	ERROR: certifikat neni podepsan CA - provedte natazeni certifikatu
Příčina:	Uživateli jste nenatáhli certifikát.
Náprava:	Proveďte natažení certifikátu. Postup je popsán v uživatelské dokumentaci, kapitole 3.4

Chyba:	Soubor ????? neexistuje
Příčina:	Program nenalezl uvedený soubor.

Náprava:	Ověřte, zda jste soubor zadali správně a zda máte příslušná přístupová práva (Windows NT, 2000).

Dávkové stahování certifikátů

Cannot create file ?????\crypta\bin\error.log.	viz **Tvorba nového uživatele**

Chyba:	Natahuji soubory z CDB - zadny soubor s certifikaty autorit nebyl nalezen ERROR: obecna chyba
Příčina:	V adresáři **<root_crypta>\keys** se nenachází žádné soubory *.cdb - tj. neexistuje ještě žádný uživatel, nebo žádný uživatel ještě nemá natažen certifikát.
Náprava:	Vygenerujte si uživatele (uživatelská dokumentace, kapitola 3.2) a proveďte natažení certifikátu (uživatelská dokumentace, kapitola 3.4).

Chyba:	Natahuji soubory z CDB .... hotovo. ERROR: obecna chyba
Příčina:	Patrně špatně nastavený port a/nebo adresa zvoleného LDAP serveru.
Náprava:	Zkontrolujte si v **Nastavování prostředí** zadané parametry LDAP serverů.

Chyba:	Natahuji soubory z CDB ..ERROR: spatny format souboru
Příčina:	V adresáři **<root_crypta>\keys** se nachází alespoň jeden poškozený soubor *.cdb.
Náprava:	Poškozený soubor opravíte natažením certifikátu danému uživateli (uživatelská dokumentace, kapitola 3.4). Mnohem těžší je zjistit, který soubor je poškozen (pokud máte více uživatelů). Nejjednodušší je asi "vylučovací metoda", kdy v adresáři vždy ponecháte pouze jeden CDB soubor, ostatní přesunete jinam, a spustíte opět dávkové stahování. U poškozeného souboru se opět objeví tato chyba.

Chyba:	ERROR: nalezen LDAP objekt bez certifikatu
Příčina:	Jedná se o obecnější chybu.
Náprava:	Kontaktujte operátora CA.

Chyba:	ERROR: nemohu se nalogovat na LDAP server ldap_result call timeout.
Příčina:	Zvolený server není LDAP server nebo je momentálně nedostupný.
Náprava:	Zkontrolujte si nastavení tohoto serveru (adresu a port) v **Nastavování prostředí**. Kontaktujte operátora CA.

Chyba:	ERROR: interni chyba v krypto knihovne
Příčina:	Program zkolaboval při stahování dat z LDAP serveru.
Náprava:	Na vině je interní chyba v LDAP serveru. Kontaktujte operátora CA, aby byla zajištěna její oprava.

Chyba:	Access violation at address ????? in module 'CRYPTALIB.DLL'. Read of address ?????.
Příčina:	Program zkolaboval při stahování dat z LDAP serveru.
Náprava:	Na vině je interní chyba v LDAP serveru. Kontaktujte operátora CA, aby byla zajištěna její oprava.

Chyba:	ERROR: neni zadny vysledek LDAP hledani
Příčina:	Program nenašel na LDAP serveru certifikát se zadanými parametry.
Náprava:	Zadaný certifikát nemusí být na serveru uložen. Pokud si jste jisti, že na něm existuje, pokuste se upřesnit parametry certifikátu v poli "Hledaný řetězec ze jména certifikátu", příp. se obraťte na operátora CA.

Chyba:	Certifikát byl podle logu nalezen, ale neuložen (např. 1 souborů nalezeno, 0 uloženo).
Příčina:	Program považuje tento certifikát za neplatný: zneplatněn, vypršení platnosti.
Náprava:	Vlastník tohoto certifikátu musí provést obnovu klíče a požádat o vydání nového certifikátu. Pokud jste přesvědčeni, že daný certifikát je platný, kontaktujte operátora CA.

Interaktivní stahování certifikátů

Natahuji soubory z CDB - zadny soubor s certifikaty autorit nebyl nalezen ERROR: obecna chyba	viz **Dávkové stahování certifikátů**
Natahuji soubory z CDB .... hotovo. ERROR: obecna chyba	viz **Dávkové stahování certifikátů**
Natahuji soubory z CDB ..ERROR: spatny format souboru	viz **Dávkové stahování certifikátů**
ERROR: nalezen LDAP objekt bez certifikatu	viz **Dávkové stahování certifikátů**
ERROR: nemohu se nalogovat na LDAP server ldap_result call timeout.	viz **Dávkové stahování certifikátů**
ERROR: interni chyba v krypto knihovne	viz **Dávkové stahování certifikátů**
Access violation at address ?? in module 'CRYPTALIB.DLL'. Read of address ??.	viz **Dávkové stahování certifikátů**
ERROR: neni zadny vysledek LDAP hledani	viz **Dávkové stahování certifikátů**
Cannot create file ?????\crypta\bin\error.log.	viz **Tvorba nového uživatele**

Chyba:	Certifikát byl podle logu nalezen, ale nepřidán do nalezených certifikátů (např. 1 souborů nalezeno, 0 uloženo).
Příčina:	Program považuje tento certifikát za neplatný: zneplatněn, vypršení platnosti.
Náprava:	Vlastník tohoto certifikátu musí provést obnovu klíče a požádat o vydání nového certifikátu. Pokud jste přesvědčeni, že daný certifikát je platný, kontaktujte operátora CA.

Kopírování CRL

Chyba:	Neni zadany soubor
Příčina:	Nezadali jste soubor s CRL
Náprava:	Zadejte jej - ručně nebo nalistováním přes tlačítko [...]

Chyba:	ERROR: nemohu vytvorit vystupni adresar ukladani CRL
Příčina:	Program nemohl vytvořit *adresář s CRL* (zadaný v **Nastavování prostředí**).
Náprava:	Ověřte, jak je tento adresář zadán (např. UNC cesty nejsou podporovány) a zda místo adresáře neexistuje stejnojmenný soubor. Zkontrolujte přístupová práva (Windows NT, 2000).

Chyba:	Access violation at address ????? in module 'CRYPTALIB.DLL'. Read of address ?????.
Příčina:	Zvolený soubor ke kopírování je poškozený.
Náprava:	Požádejte operátora CA o zaslání nového CRL.

Převod PEM/DER

Chyba:	Neni zadany vstupni soubor
Příčina:	Nezadali jste vstupní soubor.
Náprava:	Zadejte jej - ručně nebo nalistováním přes tlačítko [...]

Chyba:	Není zadaný výstupní soubor
Příčina:	Nezadali jste výstupní soubor.
Náprava:	Zadejte jej - ručně nebo nalistováním přes tlačítko [...]

Chyba:	ERROR: spatna pripona souboru
Příčina:	Program převádí pouze soubory s příponou CRT.
Náprava:	Zvolte jiný, správný soubor, nebo současnému změňte (např. v Průzkumníku) příponu.

Chyba:	ERROR: spatny format souboru Unknown DER tag
Příčina:	Vstupní soubor je poškozený nebo se nejedná o soubor s certifikátem.
Náprava:	Zvolte jiný, správný soubor, nebo požádejte operátora o zaslání nového certifikátu.

Chyba:	ERROR: spatny format souboru Attempt to get the name from GeneralName when it is not holding that type of name
Příčina:	Objevuje se v případě, že vstupní soubor je ve formátu DER, ale vy máte zvolen formát PEM.
Náprava:	Změňte formát na DER a opakujte převod.

Chyba:	ERROR: spatny format souboru
Příčina:	Objevuje se v případě, že vstupní soubor je ve formátu PEM, ale vy máte zvolen formát DER. Tato chyba se objevuje i v případě, kdy program neuspěje při otevírání vstupního souboru.
Náprava:	Změňte formát na PEM a opakujte převod. Bude-li se chyba opakovat, zkontrolujte existenci vstupního souboru, příp. přístupová oprávnění k němu (Windows NT, 2000).

SHA-1 a MD5

Chyba:	Neni zadany soubor
Příčina:	Chyba se objeví po kliknutí na tlačítko "Počítej" v sekci Kód ze souboru. Nezadali jste soubor, jehož hash kód chcete spočítat.
Náprava:	Doplňte položku Vstupní soubor.

Šifrování

ERROR: Chyba pri otevirani politiky	viz **Obnova klíče**
ERROR: Spatne heslo	viz **Natahování certifikátu**
Access violation at address ?? in module 'CRYPTALIB.DLL'. Read of address ??.	viz **Natahování certifikátu**
ERROR: interni chyba v krypto knihovne pkcs12_obj_fromfile() failed	viz **Natahování certifikátu**
ERROR: interni chyba v krypto knihovne failed to locate any key pairs	viz **Natahování certifikátu**
ERROR: certifikat neni podepsan CA - provedte natazeni certifikatu	viz **Výpočet databáze integrity**
ERROR: akce prerusena uzivatelem	viz **Natahování certifikátu**
Cannot create file ?????\crypta\bin\error.log.	viz **Tvorba nového uživatele**

Chyba:	Nemas zadane uzivatelske jmeno
Příčina:	Není vyplněna položka Uživatel - Jméno.
Náprava:	Doplňte jméno uživatele (ručně nebo přes tlačítko [...]).

Chyba:	Nemas zadane heslo.
Příčina:	Není vyplněna položka Uživatel - Heslo.
Náprava:	Doplňte heslo uživatele.

Chyba:	Nemas zadany vstupni adresar.
Příčina:	Není vyplněna položka Vstupní adresář.
Náprava:	Zvolte adresář se soubory, které chcete zašifrovat.

Chyba:	Nemas zadanou masku vstupnich souboru.
Příčina:	Není vyplněna položka Vstupní maska.
Náprava:	Zvolte masku souborů, která identifikuje soubory k zašifrování (např. ***.*** pro všechny soubory).

Chyba:	Nemas zadany vystupni soubor.
Příčina:	Není vyplněna položka Výstupní soubor.
Náprava:	Doplňte adresářovou cestu a jméno souboru, do nějž se soubory zašifrují.

Chyba:	Nemas zadane prijemce.
Příčina:	Není vyplněna položka Adresáti.
Náprava:	Doplňte adresáta/y, pro nějž se mají soubory zašifrovat.

Upozornění:	VAROVANI: Tento format neni zpetne kompatibilni!
Příčina:	Minulé verze programu mohou dešifrovat pouze soubory ve formátu "verze 1".
Náprava:	Pokud příjemce používá Cryptu 1.2 (resp. nižší verzi), používejte pouze formát "verze 1". V opačném případě můžete podle potřeby použít i jiný formát, např "diskety" pro rozdělení šifrovaného souboru na velikost jedné 3.5" diskety.

Upozornění:	Platnost vaseho certifikatu skonci za ? dni.
Příčina:	Program začíná upozorňovat 14 dní před vypršením platnosti certifikátu.
Náprava:	Vygenerujte si nového uživatele a požádejte operátora CA o obnovení certifikátu. Nový certifikát si natáhněte do Crypty a můžete jej začít používat místo starého.

Upozornění:	Platnost certifikatu prijemce skonci za ? dnu.
Příčina:	Program začíná upozorňovat 14 dní před vypršením platnosti certifikátu.
Náprava:	Kontaktujte příjemce a požádejte jej o zaslání nového certifikátu, nebo certifikát zkuste stáhnout z LDAP serveru (máte-li možnost).

Dotaz:	Platnost vaseho certifikatu jiz skoncila. Prijemce nemusi byt schopen zpracovat vami podepsana data. Pokracovat?
Chyba:	ERROR: certifikat uz neni platny
Příčina:	Platnost vašeho certifikátu vypršela. Chyba se objeví po kliknutí na tlačítko NE v dotazu.
Náprava:	Rozhodnutí je nyní na vás. Rozhodně si však co nejdříve vygenerujte nového uživatele a požádejte operátora CA o obnovení certifikátu. Nový certifikát si natáhněte do Crypty a používejte jej místo starého.

Chyba:	Natahovani certifikatu prijemcu nacitam soubor ???\certs\???.crt : neni platny - ERROR: certifikat uz neni platny
Příčina:	Certifikátu příjemce už skončila platnost - nelze pro něj již šifrovat.
Náprava:	Kontaktujte příjemce a požádejte jej o zaslání nového certifikátu, nebo certifikát zkuste stáhnout z LDAP serveru (máte-li možnost).

Chyba:	ERROR: chces sifrovat, ale nemas prijemce
Příčina:	Buď jste korektně nezadali adresáta nebo je tato chyba "zaviněna" nějakou další chybou.
Náprava:	Zkontrolujte položku **Adresáti**, zda jste správně zadali adresáty, nebo error log na přítomnost nějaké "dřívější" chyby.

Dotaz:	Ve vystupnim adresari jiz existuje soubor se shodnym nazvem. Prepsat?
Příčina:	Soubor, zadaný v položce Výstupní soubor, již existuje.
Náprava:	Pokud nechcete soubor přepsat, klikněte na tlačítko "NE" a pak změňte položku Výstupní soubor nebo existující soubor přesuňte do jiného adresáře. Pokud jej chcete přepsat, klikněte na tlačítko "ANO".

Dotaz:	Problemy s integritou souboru - pokracovat?
Příčina:	Uživatelova databáze integrity neexistuje (byla smazána?) nebo neodpovídá současnému stavu (některý ze sledovaných souborů byl modifikován).
Náprava:	Přepočítejte databázi integrity v programu **CryptaTool**. Měli byste však také zjistit, proč k modifikaci souborů došlo, zda to bylo úmyslné či ne, apod. Program nahlásí bližší podrobnosti po odkliknutí tlačítka NE jako další chybovou hlášku.

Chyba:	Kontrola integrity prostredi ... Zkontrolujte soubory a vytvorte novou integritni DB ERROR: nemohu otevrit soubor pro cteni
Příčina:	Objeví se po odkliknutí tlačítka NE v dotazu "Problemy s integritou souboru - pokracovat?". Program nemohl otevřít soubor s databází integrity **<root_crypta>\keys*jméno_uživatele*.idb**.
Náprava:	Pokud soubor neexistuje, vytvořte jej v **CryptaTool - Výpočet databáze integrity**. V opačném případě zkontrolujte přístupová práva k tomuto souboru (Windows NT, 2000).

Výskyt chyby v error logu:	`**OK   : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu    : RSA`
	`Velikost klicu       : 1024`
	`Vlastnik klice      : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru          : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru        : test.p12`

	`Otevirani trezoru ... hotovo.`
	
	`**OK : Natahovani klicu skoncilo v poradku`
	
	`Kontrola integrity prostredi ... Zkontrolujte soubory a vytvorte novou integritni DB`
	`ERROR: nemohu otevrit soubor pro cteni`

Chyba:	Kontrola integrity prostredi ... Zkontrolujte soubory a vytvorte novou integritni DB ERROR: nebyla overena integrita souboru v IDB problematicky soubor: ?????.idb
Příčina:	Objeví se po odkliknutí tlačítka NE v dotazu "Problemy s integritou souboru - pokracovat?". Hash kód uvedeného souboru nesouhlasí s kódem v databázi integrity - soubor byl patrně pozměněn.
Náprava:	Přepočítejte databázi integrity v programu **CryptaTool**. Měli byste však také zjistit, proč k modifikaci souboru došlo, zda to bylo úmyslné či ne, apod.

Chyba:	Kontrola integrity prostredi ... Zkontrolujte soubory a vytvorte novou integritni DB ERROR: nebyla overena integrita samotneho IDB souboru problematicky soubor: ?????.idb
Příčina:	Objeví se po odkliknutí tlačítka NE v dotazu "Problemy s integritou souboru - pokracovat?". Hash kód samotného souboru s databází integrity nesouhlasí s uloženým kódem v databázi - soubor byl patrně pozměněn.
Náprava:	Přepočítejte databázi integrity v programu **CryptaTool**. Měli byste však také zjistit, proč k modifikaci souboru došlo, zda to bylo úmyslné či ne, apod.

Chyba:	ERROR: nemohu otevrit soubor pro cteni soubor s CDB
Příčina:	Program nemohl načíst soubor **<root_crypta>\keys*jméno_uživatele*.cdb**.
Náprava:	Zkontrolujte, zda tento soubor existuje; pokud ano, ověřte přístupová práva (Windows NT, 2000). Pokud neexistuje, obnovte jej ze zálohy, nebo proveďte natažení certifikátu (-provedli jste jej vůbec?). Provádí se v **CryptaTool - Natahování certifikátu** a postup je popsán v uživatelské dokumentaci v kapitole 3.4.

Výskyt chyby v error logu:	`**OK : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu : RSA`
	`Velikost klicu : 1024`
	`Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru : test.p12`
	
	`Otevirani trezoru ... hotovo.`
	
	`**OK : Natahovani klicu skoncilo v poradku`
	
	`Kontrola integrity prostredi ... Natahuji certifikaty autorit ...ERROR: nemohu otevrit soubor pro cteni soubor s CDB`

Chyba:	ERROR: spatny format souboru soubor s CDB
Chyba:	ERROR: interni chyba v krypto knihovne soubor s CDB
Příčina:	Soubor **<root_crypta>\keys*jméno_uživatele*.cdb** je poškozený.
Náprava:	Obnovte jej ze zálohy (pokud máte), nebo proveďte opětovné natažení certifikátu. Provádí se v **CryptaTool - Natahování certifikátu** a postup je popsán v uživatelské dokumentaci v kapitole 3.4.

Výskyt chyby v error logu:	`**OK : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu : RSA`
	`Velikost klicu : 1024`
	`Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru : test.p12`
	
	`Otevirani trezoru ... hotovo.`
	
	`**OK : Natahovani klicu skoncilo v poradku`
	
	`Kontrola integrity prostredi ... Natahuji certifikaty autorit ...ERROR: spatny format souboru soubor s CDB`

Dotaz:	CRL vydane autoritou ????? jiz neni aktualni. Pokracovat?
Chyba:	ERROR: CRL uz neni platne
Příčina:	Platnost CRL souboru v adresáři **<root_crypta>\crls** skončila. Většinou je CRL platné 24 hodin.
Náprava:	Stáhněte si nové CRL z LDAP serveru (máte-li možnost), požádejte operátora CA o pravidelné zasílání CRL souborů e-mailem (denní, týdenní, měsíční), nebo deaktivujte kontrolu platnosti CRL v **CryptaTool** v **Nastavování prostředí**.

Chyba:	Natahuji soubory s CRL - zadny soubor nebyl nalezen ERROR: obecna chyba
Příčina:	Program nenašel žádný CRL soubor v **<root_crypta>\crls** nebo přímo samotný adresář.
Náprava:	Stáhněte si CRL z LDAP serveru (máte-li možnost), obnovte CRL soubory ze zálohy pomocí **Kopírování CRL** v **CryptaTool**, nebo požádejte operátora CA jejich zaslání. Pokud v uvedeném adresáři CRL soubory existují, zkontrolujte jejich přístupová práva (Windows NT, 2000).

Chyba:	Natahuji soubory s CRL ERROR: interni chyba v krypto knihovne Unknown DER tag
Příčina:	Některý z CRL souborů v *adresáři s CRL* je poškozen.
Náprava:	Stáhněte si CRL z LDAP serveru (máte-li možnost), obnovte CRL soubory ze zálohy pomocí **Kopírování CRL** v **CryptaTool**, nebo požádejte operátora CA jejich zaslání.

Výskyt chyby v error logu:	`**OK   : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu    : RSA`
	`Velikost klicu       : 1024`
	`Vlastnik klice       : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru          : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru        : test.p12`
	
	`Otevirani trezoru ... hotovo.`
	
	`**OK   : Natahovani klicu skoncilo v poradku`
	
	`Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo.`
	`Natahuji soubory s CRL -+ERROR: interni chyba v krypto knihovne`
	`Unknown DER tag`

Chyba:	Natahovani certifikatu prijemcu nacitam soubor ???\certs\???.crt : neni platny - ERROR: neni k dispozici CRL potrebne k overeni
Chyba:	Natahovani certifikatu prijemcu nacitam soubor ???\certs\???.crt : WARNING: certifikat z retezu certifikatu se nepodarilo overit nebot chybi CRL vydane autoritou ????? neni platny - ERROR: nebylo mozne overit retez certifikatu CA
Příčina:	Program nemohl načíst soubor s CRL pro ověření platnosti certifikátu příjemce. Soubor chybí, nebo k němu nemáte dostatečná přístupová práva.
Náprava:	Zkontrolujte *adresář s CRL*, zda v něm máte uloženy všechny potřebné CRL soubory a zda k nim máte patřičná přístupová práva (Windows NT, 2000). Pokud můžete, zkuste stáhnout CRL z LDAP serveru.

Chyba:	Natahovani certifikatu prijemcu nacitam soubor ???\certs\???.crt : neni platny - ERROR: certifikat nebyl overen zadnym certifikatem CA
Příčina:	Uživatel nemá ve svém CDB souboru uložen certifikát autority, která vydala certifikát příjemci. Jeho certifikát vydala jiná autorita.
Náprava:	Sežeňte si od příjemce certifikát "jeho" autority a naimportujte si jej do svého CDB souboru pomocí programu **CryptaCmd** příkazem: **`cryptacmd icdb jméno_uživatele certifikát_nové_autority`** (Po importu si musíte přepočítat databázi integrity a do *adresáře s CRL* přidat CRL vydané touto autoritou.)

Dotaz:	Uzivatelsky certifikat byl overen certifikatem ve vasi databazi certifikatu, ale nepodarilo se overit cely retez certifikatu CA. Pokracovat? (Potencialne nebezpecna akce)
Chyba:	Natahovani certifikatu prijemcu nacitam soubor ???\certs\???.crt : neni platny - ERROR: nebylo mozne overit retez certifikatu CA
Příčina:	Ve vašem CDB souboru chybí certifikáty některých autorit, které autorizují certifikát příjemce. Chyba se zobrazí po kliknutí na tlačítko NE v dotazu.
Náprava:	Znovu natáhněte svému uživateli certifikát a sežeňte si certifikáty všech "příjemcových" autorit. Naimportujte si je do CDB souboru pomocí programu **CryptaCmd** příkazem: **`cryptacmd icdb jméno_uživatele certifikát_nové_autority`**

	(Po importu si musíte přepočítat databázi integrity a do *adresáře s CRL* přidat CRL vydaná těmito autoritami.)

Chyba:	Natahovani certifikatu prijemcu nacitam soubor ???\certs\???.crt : neni platny - ERROR: certifikat byl zneplatnen
Příčina:	Certifikát příjemce byl zneplatněn.
Náprava:	Požádejte příjemce o zaslání nového, platného certifikátu, nebo si jej stáhněte z LDAP serveru (máte-li možnost) pomocí **Dávkového / Interaktivního stahování certifikátů** v **CryptaTool**.

Chyba:	nacitam soubor ???\certs\???.crt : ERROR: interni chyba v krypto knihovne pridavani certifikatu
Příčina:	Uvedený soubor s certifikátem příjemce je poškozený.
Náprava:	Požádejte příjemce o zaslání nového certifikátu, nebo soubor obnovte ze zálohy, nebo si jej stáhněte z LDAP serveru (máte-li možnost) pomocí **Dávkového / Interaktivního stahování certifikátů** v **CryptaTool**.

Chyba:	ERROR: nemohu vytvorit vystupni adresar
Příčina:	Program nemohl vytvořit *dočasný adresář*, zadaný v **Nastavování prostředí** v **CryptaTool**.
Náprava:	Zkontrolujte, zda je tento adresář zadán správně, zda místo něho neexistuje stejnojmenný soubor, nebo zda máte dostatečná přístupová práva (Windows NT, 2000). Crypta neumí UNC cesty! (\\počítač\sdílený_adresář)

Výskyt chyby v error logu:	`**OK   : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu    : RSA`
	`Velikost klicu       : 1024`
	`Vlastnik klice       : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru          : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru        : test.p12`
	
	`Otevirani trezoru ... hotovo.`
	
	`**OK   : Natahovani klicu skoncilo v poradku`
	
	`Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo.`
	`Natahuji soubory s CRL -++ hotovo.`
	
	`Natahovani certifikatu prijemcu`
	`nacitam soubor C:\Crypta\certs\prijemce.crt : je platny`
	
	`**OK   : Spusteno sifrovani souboru`
	
	`Verze souboru        : 1.0`
	`Soubor vytvoren      : 01.01.2000 00:00`
	`Identifikace souboru : vystup.enc`
	`Komprese             : zapnuto`
	`Sifrovani            : TripleDES v1`
	`Hash funkce          : SHA-1`
	
	`ERROR: nemohu vytvorit vystupni adresar`

Chyba:	Probiha slucovani dat ERROR: chyba v kondensacni funkci - nejsou vstupni soubory
Příčina:	Program nenašel žádný soubor k zašifrování.
Náprava:	Zkontrolujte, zda **Vstupní adresář** existuje a zda **Vstupní masce** odpovídají nějaké existující soubory ve **Vstupním adresáři**. Ověřte přístupová práva (Windows NT, 2000).

Chyba:	ERROR: chyba v kondensacni funkci - nemohu otevrit soubor pro cteni
Příčina:	Program nemůže nemůže načíst některý soubor, který je určen k zašifrování a je uložen ve **Vstupním adresáři**. Jméno souboru je uvedeno před chybovou hláškou.
Náprava:	Zkontrolujte přístupová práva souboru (Windows NT, 2000). Na jiných operačních systémech tento problém neočekáváme.

Výskyt chyby v error logu:	`**OK   : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu    : RSA`
	`Velikost klicu       : 1024`
	`Vlastnik klice       : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru          : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru        : test.p12`
	
	`Otevirani trezoru ... hotovo.`
	
	`**OK   : Natahovani klicu skoncilo v poradku`

```
Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo.
Natahuji soubory s CRL -++ hotovo.

Natahovani certifikatu prijemcu
nacitam soubor C:\Crypta\certs\prijemce.crt : je platny

**OK   : Spusteno sifrovani souboru

Verze souboru        : 1.0
Soubor vytvoren      : 01.01.2000 00:00
Identifikace souboru : vystup.enc
Komprese             : zapnuto
Sifrovani            : TripleDES v1
Hash funkce          : SHA-1

Probiha slucovani dat
  file.1
  file.2
  file.3ERROR: chyba v kondensacni funkci - nemohu otevrit soubor pro cteni
```

Chyba:	Probiha slucovani dat ERROR: chyba v kondensacni funkci - nemohu otevrit soubor pro zapis
Chyba:	Probiha komprese dat ERROR: chyba v kompresni funkci - nemohu otevrit GZ soubor pro zapis
Příčina:	Program nemůže vytvořit pracovní soubor v *dočasném adresáři* (nastaven v **CryptaTool** v **Nastavování prostředí**).
Náprava:	Smažte všechno (soubory/podadresáře) v tomto adresáři a zkontrolujte pro něj přístupová práva (Windows NT, 2000). Zkontrolujte nastavení tohoto adresáře v **CryptaTool**, UNC cesty (\\počítač\sdílený_adresář) nejsou podporovány.

Chyba:	ERROR: chyba v kondensacni funkci - nemohu zapsat do souboru
Příčina:	Program nemůže zapisovat do pracovního souboru v *dočasném adresáři* (nastaven v **CryptaTool** v **Nastavování prostředí**). To mohlo být způsobeno nedostatkem místa na disku.
Náprava:	Zkuste uvolnit další místo na disku, kde máte *dočasný adresář*, nebo jej přesměrujte na "větší" disk (pak musíte ale přepočítat databázi integrity všem uživatelům) a spusťte znovu šifrování.
Výskyt chyby v error logu:	**OK : Spusteno natahovani klicu Nahravani politiky ... hotovo. NASTAVENI PROSTREDI: Typ dvojice klicu : RSA Velikost klicu : 1024 Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123 Typ trezoru : soubor typu PKCS#12 (WWW browser) Jmeno trezoru : test.p12 Otevirani trezoru ... hotovo. **OK : Natahovani klicu skoncilo v poradku Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo. Natahuji soubory s CRL -++ hotovo. Natahovani certifikatu prijemcu nacitam soubor C:\Crypta\certs\prijemce.crt : je platny **OK : Spusteno sifrovani souboru Verze souboru : 1.0 Soubor vytvoren : 01.01.2000 00:00 Identifikace souboru : vystup.enc Komprese : zapnuto Sifrovani : TripleDES v1 Hash funkce : SHA-1 Probiha slucovani dat file.1ERROR: chyba v kondensacni funkci - nemohu zapsat do souboru

Chyba:	ERROR: chyba v kompresni funkci - doslo k vyskytu chyby v ZIP knihovne ?????\condensed.tmp.gz: file error
Příčina:	Program nemůže zapisovat do uvedeného pracovního souboru v *dočasném adresáři* (nastaven v **CryptaTool** v **Nastavování prostředí**). To mohlo být způsobeno nedostatkem místa na disku.
Náprava:	Zkuste uvolnit další místo na disku, kde máte *dočasný adresář*, nebo jej přesměrujte na "větší" disk (pak musíte ale přepočítat databázi integrity všem uživatelům) a spusťte znovu šifrování.
Výskyt chyby v error logu:	**OK : Spusteno natahovani klicu Nahravani politiky ... hotovo. NASTAVENI PROSTREDI: Typ dvojice klicu : RSA Velikost klicu : 1024

```
Vlastnik klice       : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123
Typ trezoru          : soubor typu PKCS#12 (WWW browser)
Jmeno trezoru        : test.p12

Otevirani trezoru ... hotovo.

**OK   : Natahovani klicu skoncilo v poradku

Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo.
Natahuji soubory s CRL -++ hotovo.

Natahovani certifikatu prijemcu
nacitam soubor C:\Crypta\certs\prijemce.crt : je platny

**OK   : Spusteno sifrovani souboru

Verze souboru        : 1.0
Soubor vytvoren      : 01.01.2000 00:00
Identifikace souboru : vystup.enc
Komprese             : zapnuto
Sifrovani            : TripleDES v1
Hash funkce          : SHA-1

Probiha slucovani dat
  file.1
Probiha komprese dat ERROR: chyba v kompresni funkci - doslo k vyskytu chyby v ZIP knihovne
C:\Crypta\temp\condensed.tmp.gz: file error
```

Chyba:	Probiha komprese dat ERROR: nemohu vytvorit vystupni adresar
Příčina:	Program nemohl vytvořit adresář, do nějž se má uložit zašifrovaný soubor, zadaný v položce **Výstupní soubor**.
Náprava:	Zkontrolujte, zda je tento adresář zadán správně, zda místo něho neexistuje stejnojmenný soubor, nebo zda máte dostatečná přístupová práva (Windows NT, 2000). Pokud šifrujete na disketu, nemáte ji chráněnou proti zápisu? Samozřejmě můžete zkusit šifrovat do jiného adresáře.

Výskyt chyby v error logu:	**OK : Spusteno natahovani klicu
	
	Nahravani politiky ... hotovo.
	
	NASTAVENI PROSTREDI:
	Typ dvojice klicu : RSA
	Velikost klicu : 1024
	Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123
	Typ trezoru : soubor typu PKCS#12 (WWW browser)
	Jmeno trezoru : test.p12
	
	Otevirani trezoru ... hotovo.
	
	**OK : Natahovani klicu skoncilo v poradku
	
	Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo.
	Natahuji soubory s CRL -++ hotovo.
	
	Natahovani certifikatu prijemcu
	nacitam soubor C:\Crypta\certs\prijemce.crt : je platny
	
	**OK : Spusteno sifrovani souboru
	
	Verze souboru : 1.0
	Soubor vytvoren : 01.01.2000 00:00
	Identifikace souboru : vystup.enc
	Komprese : zapnuto
	Sifrovani : TripleDES v1
	Hash funkce : SHA-1
	
	Probiha slucovani dat
	  file.1
	  file.2
	Probiha komprese dat
	ERROR: nemohu vytvorit vystupni adresar

Chyba:	Probiha komprese dat ERROR: nemohu otevrit soubor pro zapis
Příčina:	Program nemohl vytvořit soubor, zadaný v položce **Výstupní soubor**.
Náprava:	Zkontrolujte, zda je tento soubor zadán správně (ve tvaru *disk:\adresář\jméno.přípona*), zda místo něho neexistuje stejnojmenný adresář, nebo zda již soubor neexistuje a nemá zapnut atribut "jen pro čtení", nebo zda máte dostatečná přístupová práva (Windows NT, 2000). Pokud šifrujete na disketu, nemáte ji chráněnou proti zápisu? Samozřejmě můžete zkusit šifrovat do jiného souboru.
Výskyt chyby v	**OK : Spusteno natahovani klicu Nahravani politiky ... hotovo.

error logu:

```
NASTAVENI PROSTREDI:
Typ dvojice klicu    : RSA
Velikost klicu       : 1024
Vlastnik klice       : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123
Typ trezoru          : soubor typu PKCS#12 (WWW browser)
Jmeno trezoru        : test.p12

Otevirani trezoru ... hotovo.

**OK   : Natahovani klicu skoncilo v poradku

Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo.
Natahuji soubory s CRL -++ hotovo.

Natahovani certifikatu prijemcu
nacitam soubor C:\Crypta\certs\prijemce.crt : je platny

**OK   : Spusteno sifrovani souboru

Verze souboru        : 1.0
Soubor vytvoren      : 01.01.2000 00:00
Identifikace souboru : vystup.enc
Komprese             : zapnuto
Sifrovani            : TripleDES v1
Hash funkce          : SHA-1

Probiha slucovani dat
  file.1
  file.2
Probiha komprese dat
ERROR: nemohu otevrit soubor pro zapis
```

Chyba:	Probiha sifrovani dat ERROR: nemohu otevrit soubor pro zapis
Příčina:	Chyba se objeví pokud jste zvolili formát "diskety". Program nemohl vytvořit soubor s částí šifrovaného souboru, který je zadaný v položce **Výstupní soubor**. Tyto části přejímají název souboru a připojují k němu příponu part??? (part001, part002 atd.). Program nemohl vytvořit samotný soubor nebo adresář (v případě zápisu do adresáře na vyměnitelném médiu).
Náprava:	Zkontrolujte, zda místo souboru neexistuje stejnojmenný adresář, nebo zda již soubor neexistuje a nemá zapnut atribut "jen pro čtení", nebo zda máte dostatečná přístupová práva (Windows NT, 2000). Pokud šifrujete na disketu, nemáte ji chráněnou proti zápisu a není na některé stejnojmenný soubor jako je adresář, do nějž se má zašifrovaná část uložit? Samozřejmě můžete zkusit šifrovat do jiného souboru.

Výskyt chyby v error logu:	**OK : Spusteno natahovani klicu
	
	Nahravani politiky ... hotovo.
	
	NASTAVENI PROSTREDI:
	Typ dvojice klicu : RSA
	Velikost klicu : 1024
	Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123
	Typ trezoru : soubor typu PKCS#12 (WWW browser)
	Jmeno trezoru : test.p12
	
	Otevirani trezoru ... hotovo.
	
	**OK : Natahovani klicu skoncilo v poradku
	
	Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo.
	Natahuji soubory s CRL -++ hotovo.
	
	Natahovani certifikatu prijemcu
	nacitam soubor C:\Crypta\certs\prijemce.crt : je platny
	
	**OK : Spusteno sifrovani souboru (verze 2)
	
	Verze souboru : 2.0
	Soubor vytvoren : 01.01.2000 00:00
	Identifikace souboru : vystup.enc
	Komprese : zapnuto
	Sifrovani : TripleDES (CBC mod)
	Hash funkce : SHA-1
	
	Probiha slucovani dat
	  file.1
	  file.2
	Probiha komprese dat
	Generovani tajneho klice pro tento soubor
	Probiha sifrovani dat ERROR: nemohu otevrit soubor pro zapis

Chyba:	Probiha sifrovani dat ERROR: nemohu zapsat do souboru
Příčina:	Při vytváření šifrovaného souboru z dočasných souborů nastala **najednou** chyba zápisu. Pokud cílové umístění ukazuje nyní volné místo 0 bajtů, byl šifrovaný soubor větší než volné místo na disku.

Náprava:	Zkuste uvolnit další místo na disku a zašifrujte soubor znovu.

Dotaz:	Na cilovem mediu je malo mista. Vlozte nove medium nebo ukoncete program
Příčina:	Objeví se při šifrování ve formátu "diskety" na vyměnitelné médium, když dojde k uložení celé jedné části zašifrovaného souboru. Objevuje se i v případě, kdy nelze zapsat na médium první část, neboť většinu kapacity zabírají jiná data.
Náprava:	Vložte prázdné médium a klikněte na tlačítko "Médium", nebo operaci přerušte kliknutím na tlačítko "Storno".

Dešifrování/Archivace

Mnoho chyb je shodných s těmi během šifrování. Proto zde budou uvedeny jen ty, které jsou specifické jen pro dešifrovací proces. Jelikož je archivování souboru prakticky totožné s dešifrováním, nebude mu věnována samostatná sekce.
Pokud zde nenaleznete některou chybovou hlášku, podívejte se ještě do sekce **Šifrování**.

Chyba:	Nemas zadany vstupni soubor.
Příčina:	Není vyplněna položka Vstupní soubor.
Náprava:	Zvolte soubor, který chcete dešifrovat.

Chyba:	Nemas zadany vystupni adresar.
Příčina:	Není vyplněna položka Výstupní adresář.
Náprava:	Doplňte adresář, do nějž chcete uložit dešifrované soubory .

Chyba:	ERROR: nejsi prijemce
Příčina:	Zašifrovaný soubor je určen pro jiného uživatele.
Náprava:	Pokud máte v Cryptě více uživatelů, zkuste soubor dešifrovat jiným uživatelem. Pokud jste prováděli obnovu certifikátu, může být soubor zašifrován pro starého uživatele. Selžou-li všechny pokusy, dohodněte se s operátorem CA na novém zašifrování souborů pro správného uživatele, nebo kontaktujte hotline Crypty, který může určit oprávněného příjemce souboru.

Upozornění:	Platnost vaseho certifikatu jiz skoncila.
Příčina:	Vašemu certifikátu skončila platnost.
Náprava:	Soubor můžete stále dešifrovat, ale co nejdříve si vygenerujte nového uživatele a požádejte operátora CA o obnovu certifikátu.

Dotaz:	Certifikat odesilatele souboru uz neni platny. Pokracovat? (Potencialne nebezpecna akce)
Chyba:	Overuji podpis dat ..ERROR: certifikat uz neni platny certifikat odesilatele uz neni platny
Příčina:	Certifikátu odesílatele již skončila platnost - obsah zašifrovaného souboru již nemusíte pokládat za důvěryhodný.
Náprava:	Je na vašem rozhodnutí, zda budete pokračovat s dešifrováním, nebo požádáte odesílatele o opětovné zašifrování jeho novým certifikátem.

Dotaz:	Soubor existuje - prepsat?
Příčina:	Ve **Výstupním adresáři** již existuje stejnojmenný soubor (jméno uvedeno v posledním řádku logu). Rozhodněte, zda jej chcete přepsat.
Náprava:	Zvolte ANO nebo NE - v obou případech bude dešifrování pokračovat dále a soubor se přepíše nebo ne.

Dotaz:	Ve zpracovavanem souboru byla poskozena integrita hlavicky. K teto udalosti muze dojit pouze u archivovanych souboru, jinak se jedna o neopravnene poruseni integrity souboru. Pokracovat ve zpracovani?
Příčina:	Okno se objeví při pokusu dešifrovat zaarchivovaný soubor. Pokud se jedná o klasický zašifrovaný soubor, berte tento dotaz jako znamení porušení integrity tohoto souboru.
Náprava:	Klikněte na tlačítko ANO a pokračujte v dešifrování souboru, pokud se opravdu jedná o archivovaný soubor, jinak si od odesilatele zažádejte o zaslání nového zašifrovaného souboru.

Dotaz:	Vlozte medium s dalsi casti souboru (cislo ?) nebo ukoncete program
Příčina:	Okno se objeví při dešifrování souboru, který je rozdělen na více částí a požadovaná část není právě k dispozici (např. je na jiném výměnném médiu - disketě).

Náprava:	Vložte správné médium-disketu a zvolte "Médium", nebo klikněte na tlačítko "Storno" pro přerušení operace.

Chyba:	Probiha desifrovani dat ERROR: vlozena neocekavana cast rozdeleneho souboru
Příčina:	Chyba se objeví u souboru, zašifrovaného do více částí. Část, kterou program právě načítal, nesla sice správné pojmenování (správnou příponu), ale přesto nenavazuje na předchozí část.
Náprava:	Je možné, že došlo k poškození souboru. Požádejte odesílatele, ať vám rozdělený zašifrovaný soubor pošle znovu.

Chyba:	ERROR: nemohu otevrit soubor pro cteni
Příčina:	Program nemohl načíst zašifrovaný soubor, zadaný v položce **Vstupní soubor**.
Náprava:	Zkontrolujte, zda je tento soubor zadán správně, nebo zda máte dostatečná přístupová práva (Windows NT, 2000).

Výskyt chyby v error logu:	`**OK   : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu    : RSA`
	`Velikost klicu       : 1024`
	`Vlastnik klice      : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru          : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru        : test.p12`
	
	`Otevirani trezoru ... hotovo.`
	
	`**OK   : Natahovani klicu skoncilo v poradku`
	
	`Kontrola integrity prostredi ... Natahuji certifikaty autorit ...  hotovo.`
	`Natahuji soubory s CRL -++ hotovo.`
	`ERROR:  nemohu otevrit soubor pro cteni`

Chyba:	ERROR: nemohu vytvorit vystupni adresar
Příčina1:	Program nemohl vytvořit adresář, zadaný v položce **Výstupní adresář**.
Náprava1:	Zkontrolujte, zda je tento adresář zadán správně, zda místo něho neexistuje stejnojmenný soubor, nebo zda máte dostatečná přístupová práva (Windows NT, 2000). Pokud šifrujete na disketu, nemáte ji chráněnou proti zápisu? Samozřejmě můžete zkusit šifrovat do jiného adresáře.
Příčina2:	Program nemohl vytvořit *dočasný adresář*, zadaný v **Nastavování prostředí** v **CryptaTool**.
Náprava2:	Zkontrolujte, zda je tento adresář zadán správně, zda místo něho neexistuje stejnojmenný soubor, nebo zda máte dostatečná přístupová práva (Windows NT, 2000). Crypta neumí UNC cesty! (\\počítač\sdílený_adresář)

Výskyt chyby v error logu:	`**OK   : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu    : RSA`
	`Velikost klicu       : 1024`
	`Vlastnik klice      : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru          : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru        : test.p12`
	
	`Otevirani trezoru ... hotovo.`
	
	`**OK   : Natahovani klicu skoncilo v poradku`
	
	`Kontrola integrity prostredi ... Natahuji certifikaty autorit ...  hotovo.`
	`Natahuji soubory s CRL -++ hotovo.`
	
	`**OK   : Spusteno desifrovani souboru`
	
	`ERROR: nemohu vytvorit vystupni adresar`

Chyba:	Overuji podpis dat ..ERROR: neni k dispozici CRL potrebne k overeni
Chyba:	WARNING: certifikat z retezu certifikatu se nepodarilo overit nebot chybi CRL vydane autoritou ????? neni platny - ERROR: nebylo mozne overit retez certifikatu CA
Příčina:	Program nemohl načíst soubor s CRL pro ověření platnosti certifikátu odesílatele. Soubor chybí, nebo k němu nemáte dostatečná přístupová práva.
Náprava:	Zkontrolujte *adresář s CRL*, zda v něm máte uloženy všechny potřebné CRL soubory a zda k nim máte patřičná přístupová práva (Windows NT, 2000). Pokud můžete, zkuste stáhnout CRL z LDAP serveru.

Chyba:	ERROR: certifikat nebyl overen zadnym certifikatem CA
Příčina:	Uživatel nemá ve svém CDB souboru uložen certifikát autority, která vydala certifikát odesílateli. Jeho certifikát vydala jiná autorita.

Náprava:	Sežeňte si od odesílatele certifikát "jeho" autority a naimportujte si jej do svého CDB souboru pomocí programu **CryptaCmd** příkazem: **`cryptacmd icdb jméno_uživatele certifikát_nové_autority`** (Po importu si musíte přepočítat databázi integrity a do *adresáře s CRL* přidat CRL vydané touto autoritou.)

Dotaz:	Uzivatelsky certifikat byl overen certifikatem ve vasi databazi certifikatu, ale nepodarilo se overit cely retez certifikatu CA. Pokracovat? (Potencialne nebezpecna akce)
Chyba:	ERROR: nebylo mozne overit retez certifikatu CA
Příčina:	Ve vašem CDB souboru chybí certifikáty některých autorit, které autorizují certifikát odesílatele. Chyba se zobrazí po kliknutí na tlačítko NE v dotazu.
Náprava:	Znovu natáhněte svému uživateli certifikát a sežeňte si certifikáty všech "příjemcových" autorit. Naimportujte si je do CDB souboru pomocí programu **CryptaCmd** příkazem: **`cryptacmd icdb jméno_uživatele certifikát_nové_autority`** (Po importu si musíte přepočítat databázi integrity a do *adresáře s CRL* přidat CRL vydaná těmito autoritami.)

Chyba:	ERROR: certifikat byl zneplatnen
Příčina:	Certifikát odesílatele byl zneplatněn.
Náprava:	Požádejte odesílatele, aby vám soubory zašifroval pomocí platného certifikátu.

Chyba:	ERROR: chyba v dekondensacni funkci - nemohu otevrit soubor pro zapis
Příčina:	Program nemůže nemůže uložit některý soubor ze zašifrovaného souboru do **Výstupního adresáře**. Jméno souboru je uvedeno před chybovou hláškou.
Náprava:	Zkontrolujte, zda ve **Výstupním adresáři** neexistuje stejnojmenný adresář nebo soubor se zapnutým atributem "jen pro čtení". Zkontrolujte přístupová práva souboru (Windows NT, 2000).

Výskyt chyby v error logu:	`**OK   : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu    : RSA`
	`Velikost klicu       : 1024`
	`Vlastnik klice      : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru          : soubor typu PKCS#12 (WWW browser)`
	`Jmeno trezoru        : test.p12`
	
	`Otevirani trezoru ... hotovo.`
	
	`**OK   : Natahovani klicu skoncilo v poradku`
	
	`Kontrola integrity prostredi ... Natahuji certifikaty autorit ...  hotovo.`
	`Natahuji soubory s CRL -++ hotovo.`
	
	`**OK   : Spusteno desifrovani souboru`
	
	`INFORMACE O SOUBORU:`
	`Verze souboru        : 1.0`
	`Soubor vytvoren      : 01.07.2000 00:00`
	`Identifikace souboru : vystup.enc`
	`Komprese             : zapnuto`
	`Sifrovani            : TripleDES v1`
	`Hash funkce          : SHA-1`
	`Odesilatel dat       : c=cz, o=test, ou=test, l=test, st=test, cn=test, email=test, telephoneNumber=123`
	`ID odesilatele       : test`
	
	`**OK   : Potvrzeni integrity hlavicky souboru`
	
	`Probiha desifrovani dat`
	`Probiha dekomprese souboru`
	`Probiha rozbalovani souboru`
	`  file.1`
	`  file.2`
	`  file.3 ERROR: chyba v dekondensacni funkci - nemohu otevrit soubor pro zapis`

Chyba:	ERROR: nemohu otevrit soubor pro zapis
Příčina:	Tato chyba se objeví při archivování souboru (zaškrtnuté políčko "Archivace"). Program nemůže nemůže uložit zaarchivovaný soubor.
Náprava:	Zkontrolujte, zda ve **Výstupním adresáři** neexistuje stejnojmenný adresář nebo soubor se zapnutým atributem "jen pro čtení". Zkontrolujte přístupová práva souboru (Windows NT, 2000).

Výskyt chyby v error logu:	`**OK   : Spusteno natahovani klicu`
	
	`Nahravani politiky ... hotovo.`
	
	`NASTAVENI PROSTREDI:`
	`Typ dvojice klicu    : RSA`
	`Velikost klicu       : 1024`
	`Vlastnik klice      : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123`
	`Typ trezoru          : soubor typu PKCS#12 (WWW browser)`

```
Jmeno trezoru        : test.p12

Otevirani trezoru ... hotovo.

**OK   : Natahovani klicu skoncilo v poradku

Kontrola integrity prostredi ... Natahuji certifikaty autorit ...  hotovo.
Natahuji soubory s CRL -++ hotovo.

**OK   : Spusteno archivovani souboru

INFORMACE O SOUBORU:
Verze souboru        : 1.0
Soubor vytvoren      : 01.01.2000 00:00
Identifikace souboru : vystup.enc
Komprese             : zapnuto
Sifrovani            : TripleDES v1
Hash funkce          : SHA-1
Odesilatel dat       : c=cz, o=test, ou=test, l=test, st=test, cn=test, email=test, telephoneNumber=123
ID odesilatele       : test

**OK   : Potvrzeni integrity hlavicky souboru

Probiha desifrovani dat
ERROR: nemohu otevrit soubor pro zapis
```

Chyba:	ERROR: nemohu otevrit soubor pro zapis
Příčina:	Program nemůže vytvořit pracovní soubor v *dočasném adresáři* (nastaven v **CryptaTool** v **Nastavování prostředí**).
Náprava:	Smažte všechno (soubory/podadresáře) v tomto adresáři a zkontrolujte pro něj přístupová práva (Windows NT, 2000). Zkontrolujte nastavení tohoto adresáře v **CryptaTool**, UNC cesty (\\počítač\sdílený_adresář) nejsou podporovány.
Výskyt chyby v error logu:	**OK : Spusteno natahovani klicu Nahravani politiky ... hotovo. NASTAVENI PROSTREDI: Typ dvojice klicu : RSA Velikost klicu : 1024 Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123 Typ trezoru : soubor typu PKCS#12 (WWW browser) Jmeno trezoru : test.p12 Otevirani trezoru ... hotovo. **OK : Natahovani klicu skoncilo v poradku Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo. Natahuji soubory s CRL -++ hotovo. **OK : Spusteno desifrovani souboru INFORMACE O SOUBORU: Verze souboru : 1.0 Soubor vytvoren : 01.07.2000 00:00 Identifikace souboru : vystup.enc Komprese : zapnuto Sifrovani : TripleDES v1 Hash funkce : SHA-1 Odesilatel dat : c=cz, o=test, ou=test, l=test, st=test, cn=test, email=test, telephoneNumber=123 ID odesilatele : test **OK : Potvrzeni integrity hlavicky souboru ERROR: nemohu otevrit soubor pro zapis

Chyba:	Probiha dekomprese souboru ERROR: chyba v kompresni funkci -
Příčina:	Program nemůže vytvořit pracovní soubor v *dočasném adresáři* (nastaven v **CryptaTool** v **Nastavování prostředí**).
Náprava:	Smažte všechno (soubory/podadresáře) v tomto adresáři a zkontrolujte pro něj přístupová práva (Windows NT, 2000). Zkontrolujte nastavení tohoto adresáře v **CryptaTool**, UNC cesty (\\počítač\sdílený_adresář) nejsou podporovány.
Výskyt chyby v error logu:	**OK : Spusteno natahovani klicu Nahravani politiky ... hotovo. NASTAVENI PROSTREDI: Typ dvojice klicu : RSA Velikost klicu : 1024 Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123 Typ trezoru : soubor typu PKCS#12 (WWW browser) Jmeno trezoru : test.p12 Otevirani trezoru ... hotovo. **OK : Natahovani klicu skoncilo v poradku

```
Kontrola integrity prostredi ... Natahuji certifikaty autorit ...  hotovo.
Natahuji soubory s CRL -++ hotovo.

**OK   : Spusteno desifrovani souboru

INFORMACE O SOUBORU:
Verze souboru        : 1.0
Soubor vytvoren      : 01.07.2000 00:00
Identifikace souboru : vystup.enc
Komprese             : zapnuto
Sifrovani            : TripleDES v1
Hash funkce          : SHA-1
Odesilatel dat       : c=cz, o=test, ou=test, l=test, st=test, cn=test, email=test, telephoneNumber=123
ID odesilatele       : test

**OK   : Potvrzeni integrity hlavicky souboru

Probiha desifrovani dat
Probiha dekomprese souboru ERROR: chyba v kompresni funkci -
```

Chyba:	Probiha dekomprese souboru ERROR: chyba v kompresni funkci -
Příčina:	Program nemůže zapisovat do pracovního souboru v *dočasném adresáři* (nastaven v **CryptaTool** v **Nastavování prostředí**). To mohlo být způsobeno nedostatkem místa na disku.
Náprava:	Zkuste uvolnit další místo na disku, kde máte *dočasný adresář*, nebo jej přesměrujte na "větší" disk (pak musíte ale přepočítat databázi integrity všem uživatelům) a spusťte znovu šifrování.
Výskyt chyby v error logu:	**OK : Spusteno natahovani klicu Nahravani politiky ... hotovo. NASTAVENI PROSTREDI: Typ dvojice klicu : RSA Velikost klicu : 1024 Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123 Typ trezoru : soubor typu PKCS#12 (WWW browser) Jmeno trezoru : test.p12 Otevirani trezoru ... hotovo. **OK : Natahovani klicu skoncilo v poradku Kontrola integrity prostredi ... Natahuji certifikaty autorit ... hotovo. Natahuji soubory s CRL -++ hotovo. **OK : Spusteno desifrovani souboru INFORMACE O SOUBORU: Verze souboru : 1.0 Soubor vytvoren : 01.07.2000 00:00 Identifikace souboru : vystup.enc Komprese : zapnuto Sifrovani : TripleDES v1 Hash funkce : SHA-1 Odesilatel dat : c=cz, o=test, ou=test, l=test, st=test, cn=test, email=test, telephoneNumber=123 ID odesilatele : test **OK : Potvrzeni integrity hlavicky souboru Probiha desifrovani dat Probiha dekomprese souboru ERROR: chyba v kompresni funkci -

Chyba:	Probiha desifrovani dat ERROR: nemohu zapsat do souboru
Příčina:	Program nemůže zapisovat do pracovního souboru v *dočasném adresáři* (nastaven v **CryptaTool** v **Nastavování prostředí**). To mohlo být způsobeno nedostatkem místa na disku.
Náprava:	Zkuste uvolnit další místo na disku, kde máte *dočasný adresář*, nebo jej přesměrujte na "větší" disk (pak musíte ale přepočítat databázi integrity všem uživatelům) a spusťte znovu šifrování.
Výskyt chyby v error logu:	**OK : Spusteno natahovani klicu Nahravani politiky ... hotovo. NASTAVENI PROSTREDI: Typ dvojice klicu : RSA Velikost klicu : 1024 Vlastnik klice : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123 Typ trezoru : soubor typu PKCS#12 (WWW browser) Jmeno trezoru : test.p12 Otevirani trezoru ... hotovo. **OK : Natahovani klicu skoncilo v poradku

```
Kontrola integrity prostredi ... Natahuji certifikaty autorit ...  hotovo.
Natahuji soubory s CRL -++ hotovo.

**OK   : Spusteno desifrovani souboru

INFORMACE O SOUBORU:
Verze souboru        : 1.0
Soubor vytvoren      : 01.01.2000 00:00
Identifikace souboru : test.enc
Komprese             : zapnuto
Sifrovani            : TripleDES v1
Hash funkce          : SHA-1
Odesilatel dat       : c=cz, o=test, ou=test, l=test, st=test, cn=test, email=test, telephoneNumber=123
ID odesilatele       : test

**OK   : Potvrzeni integrity hlavicky souboru

Probiha desifrovani dat ERROR:  nemohu zapsat do souboru
```

Chyba:	ERROR: chyba v dekondensacni funkci - nemohu zapsat do souboru
Příčina:	Při dešifrování souborů ze zašifrovaného souboru do **Výstupního adresáře** nastala **najednou** chyba zápisu. Pokud cílové umístění ukazuje nyní volné místo v řádu několika kilobajtů, byla velikost všech zašifrovaných souborů větší než volné místo na disku.
Náprava:	Zkuste uvolnit další místo na disku a dešifrujte soubor znovu, nebo změňte umístění **Výstupního adresáře**.
Výskyt chyby v error logu:	

```
**OK   : Spusteno natahovani klicu

Nahravani politiky ... hotovo.

NASTAVENI PROSTREDI:
Typ dvojice klicu    : RSA
Velikost klicu       : 1024
Vlastnik klice       : c=cz, cn=test, o=test, ou=test, l=test, st=test, email=test, telephoneNumber=123
Typ trezoru          : soubor typu PKCS#12 (WWW browser)
Jmeno trezoru        : test.p12

Otevirani trezoru ... hotovo.

**OK   : Natahovani klicu skoncilo v poradku

Kontrola integrity prostredi ... Natahuji certifikaty autorit ...  hotovo.
Natahuji soubory s CRL -++ hotovo.

**OK   : Spusteno desifrovani souboru

INFORMACE O SOUBORU:
Verze souboru        : 1.0
Soubor vytvoren      : 01.01.2000 00:00
Identifikace souboru : test.enc
Komprese             : zapnuto
Sifrovani            : TripleDES v1
Hash funkce          : SHA-1
Odesilatel dat       : c=cz, o=test, ou=test, l=test, st=test, cn=test, email=test, telephoneNumber=123
ID odesilatele       : test

**OK   : Potvrzeni integrity hlavicky souboru

Probiha desifrovani dat
Probiha dekomprese souboru
Probiha rozbalovani souboru
  file.1 ERROR: chyba v dekondensacni funkci - nemohu zapsat do souboru
```

Chyba:	ERROR: spatny typ souboru
Příčina:	Zašifrovaný soubor je poškozen.
Náprava:	Požádejte odesílatele, aby vám poslal nový. Pokud jste soubor obdrželi e-mailem, může být na vině nastavené kódování souborů ve vašem a/nebo odesílatelově poštovním klientovi, doporučujeme je nastavit na formát UUENCODE.

Vypracoval:

Česká pošta, státní podnik
OZ VAKUS
L.P. 2001