

---

Identifikace	PP-0111/2013_P01	Číslo jednací	
Nahrazuje		Klasifikace	Veřejný
Platnost	8. 11. 2015	Účinnost	8. 11. 2015

---

## Příloha č. 1

# Základní příručka programu Crypta 2

# 1 Úvod

Cílem tohoto dokumentu je popsat jednoduše hlavní funkce programu Crypta 2. Předpokladem je zprovozněná aplikace dle manuálu, tzn. vytvořený profil a nainstalovaný certifikát.

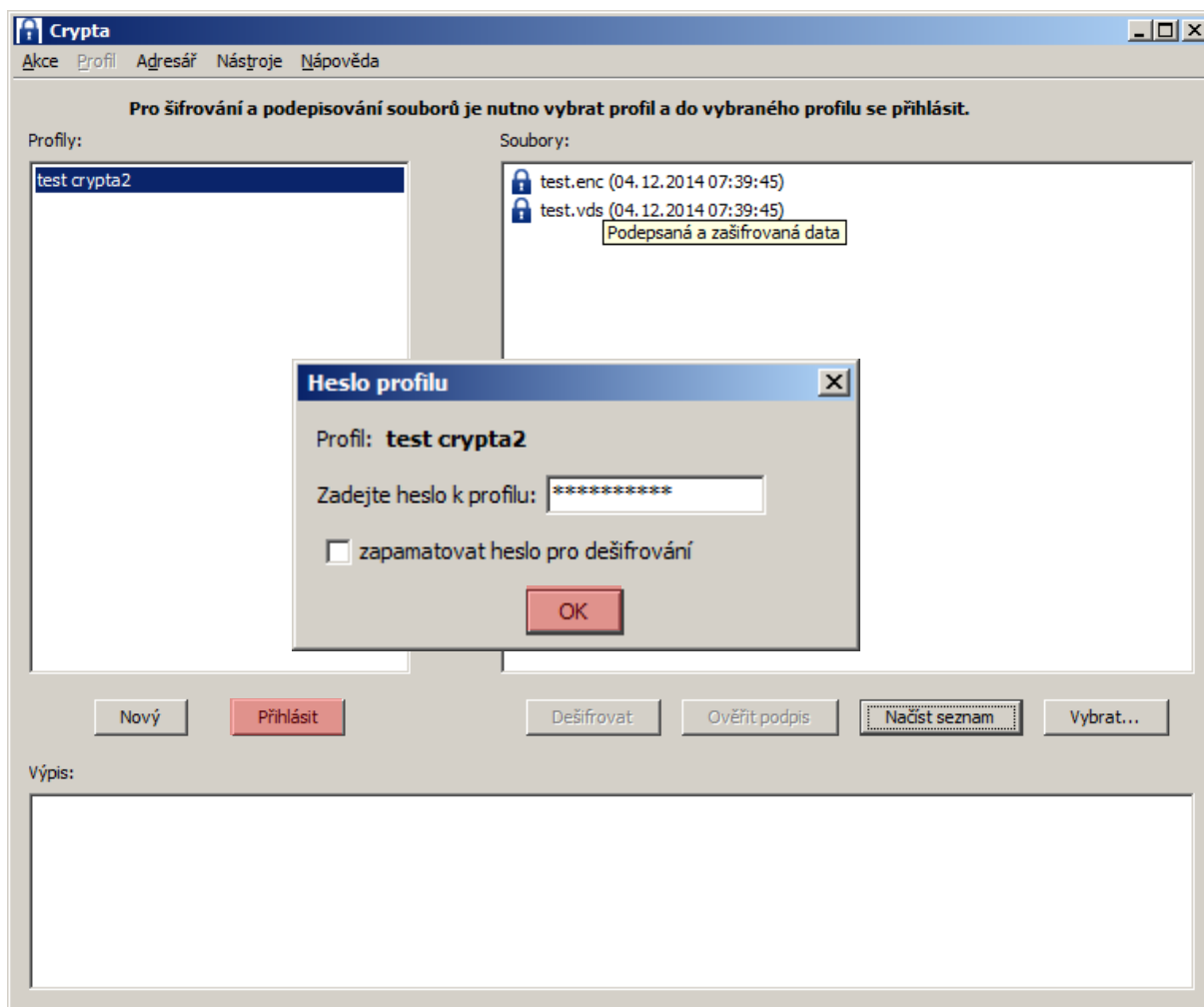
Obrázky v tomto dokumentu mohou být pouze orientační. Uvedené postupy počítají s ovládáním myši pravou rukou. Podobnost se jmény skutečných osob a organizací je čistě náhodná a neúmyslná. Účelem dokumentu není podrobné popsání všech funkcí aplikace Crypta.

Kompletní popis funkcí aplikace Crypta je v samostatném dokumentu nebo přímo v nápovědě programu po stisknutí klávesy F1.

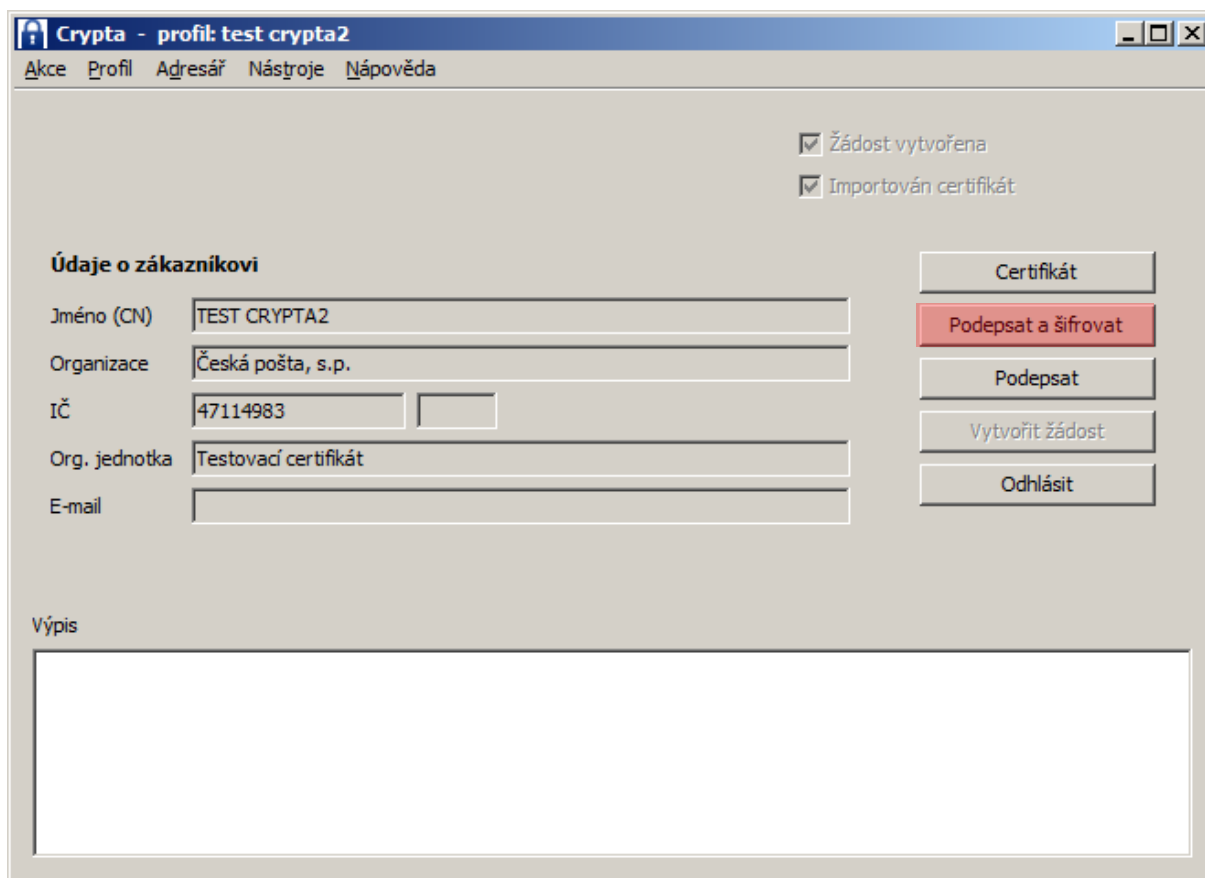
## 2 Šifrování

Postupné kroky pro šifrování:

1. Výběr profilu, pod kterým budete šifrovat přihlášení do profilu tlačítkem **Přihlásit**, dále zadáním hesla a stiskem tlačítka **OK**.

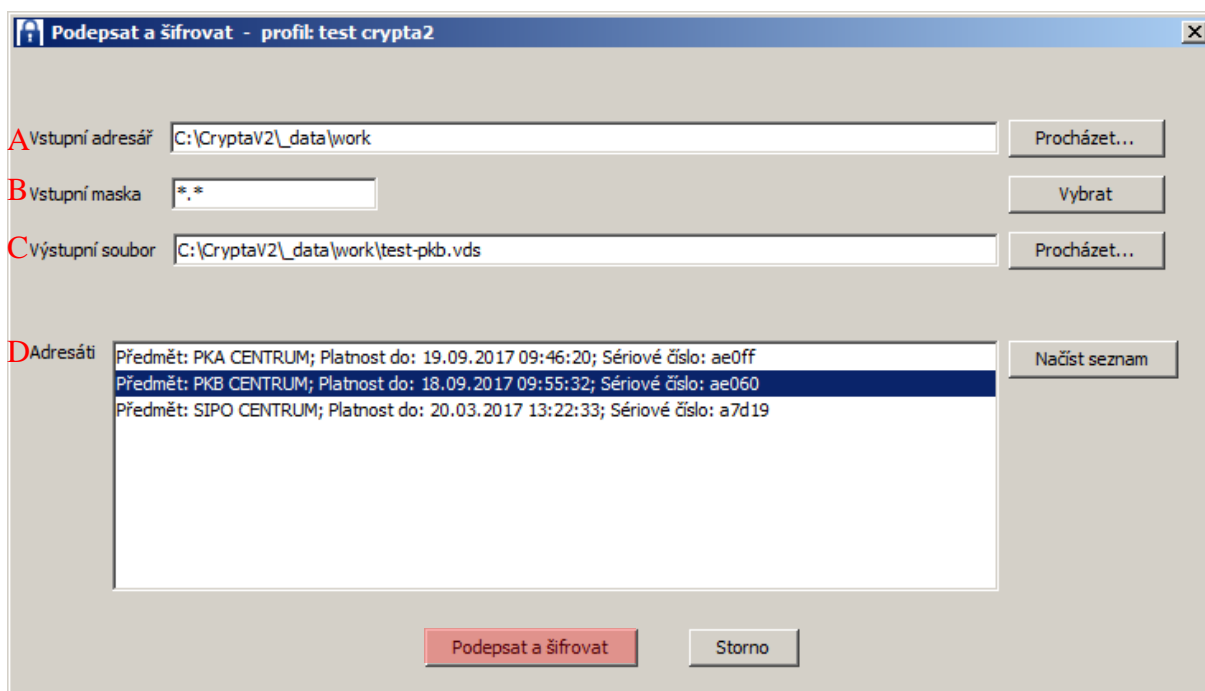


2. Dalším krokem je stisknutí tlačítka pro šifrování **Podepsat a šifrovat**



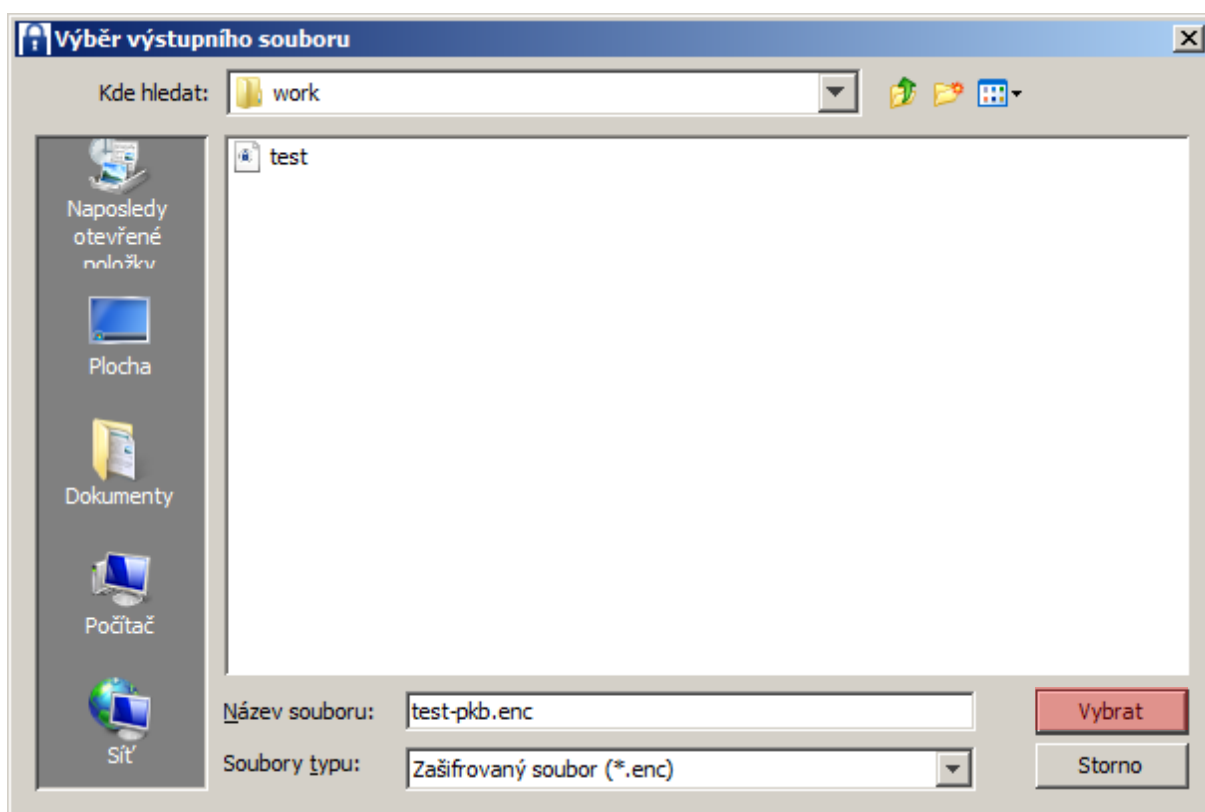
The screenshot shows the 'Crypta - profil: test crypta2' window. At the top, there are menu items: Akce, Profil, Adresář, Nástroje, and Nápověda. On the right, there are two checked checkboxes: 'Žádost vytvořena' and 'Importován certifikát'. Below these, there is a section titled 'Údaje o zákazníkovi' with several input fields: 'Jméno (CN)' containing 'TEST CRYPTA2', 'Organizace' containing 'Česká pošta, s.p.', 'IČ' containing '47114983', 'Org. jednotka' containing 'Testovací certifikát', and an empty 'E-mail' field. To the right of these fields are five buttons: 'Certifikát', 'Podepsat a šifrovat' (highlighted in red), 'Podepsat', 'Vytvořit žádost', and 'Odhlásit'. At the bottom left, there is a 'Výpis' label above a large empty text area.

3. Výběr souborů pro šifrování



The screenshot shows the 'Podepsat a šifrovat - profil: test crypta2' window. It features three input fields for file paths: 'A Vstupní adresář' with 'C:\CryptaV2\_data\work' and a 'Procházet...' button; 'B Vstupní maska' with '\*' and a 'Vybrat' button; and 'C Výstupní soubor' with 'C:\CryptaV2\_data\work\test-pkb.vds' and a 'Procházet...' button. Below these is a list of certificates under the 'D Adresáři' label, with the second entry selected: 'Předmět: PKB CENTRUM; Platnost do: 18.09.2017 09:55:32; Sériové číslo: ae060'. A 'Načíst seznam' button is to the right of the list. At the bottom, there are two buttons: 'Podepsat a šifrovat' (highlighted in red) and 'Storno'.

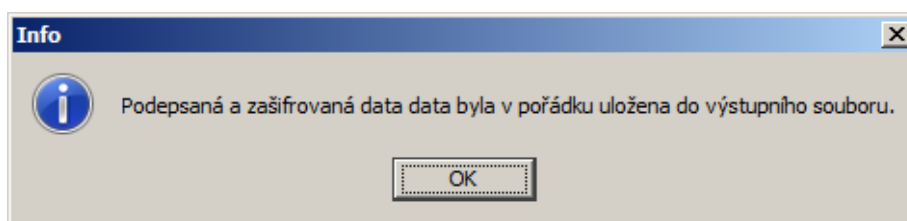
- A. Výběr vstupního adresáře provedete tlačítkem **Procházet...** V daném adresáři musí být uloženy soubory, které zamýšlíte zašifrovat a odeslat pro zpracování na pracoviště České pošty.
- B. Masku nastavíte dle potřeby například na **\*.txt** pro zašifrování všech souborů s příponou **txt**. Pokud chcete zašifrovat všechny soubory ve vybraném adresáři, ponechte přednastavenou masku na **\*.\*** nebo tlačítkem **Vybrat** vyberete konkrétní jeden soubor.
- C. Výstupní soubor vyberete tlačítkem **Procházet...** a název zapíšete do *Názvu souboru*:. Dále můžete vybrat typ souboru ENC nebo VDS. Pokud není požadovaný typ souboru v seznamu, můžete zapsat příponu přímo do názvu souboru. Po ukončení zadání stisknete tlačítko **Vybrat**



- D. V poslední řadě je potřeba vybrat Adresáta – pro koho budou soubory zašifrovány, např. SIPO CENTRUM, PKA CENTRUM, PKB CENTRUM, apod.

Nakonec stisknete tlačítko **Podepsat a šifrovat**

4. V případě úspěšného zašifrování bude výsledkem tato hláška:

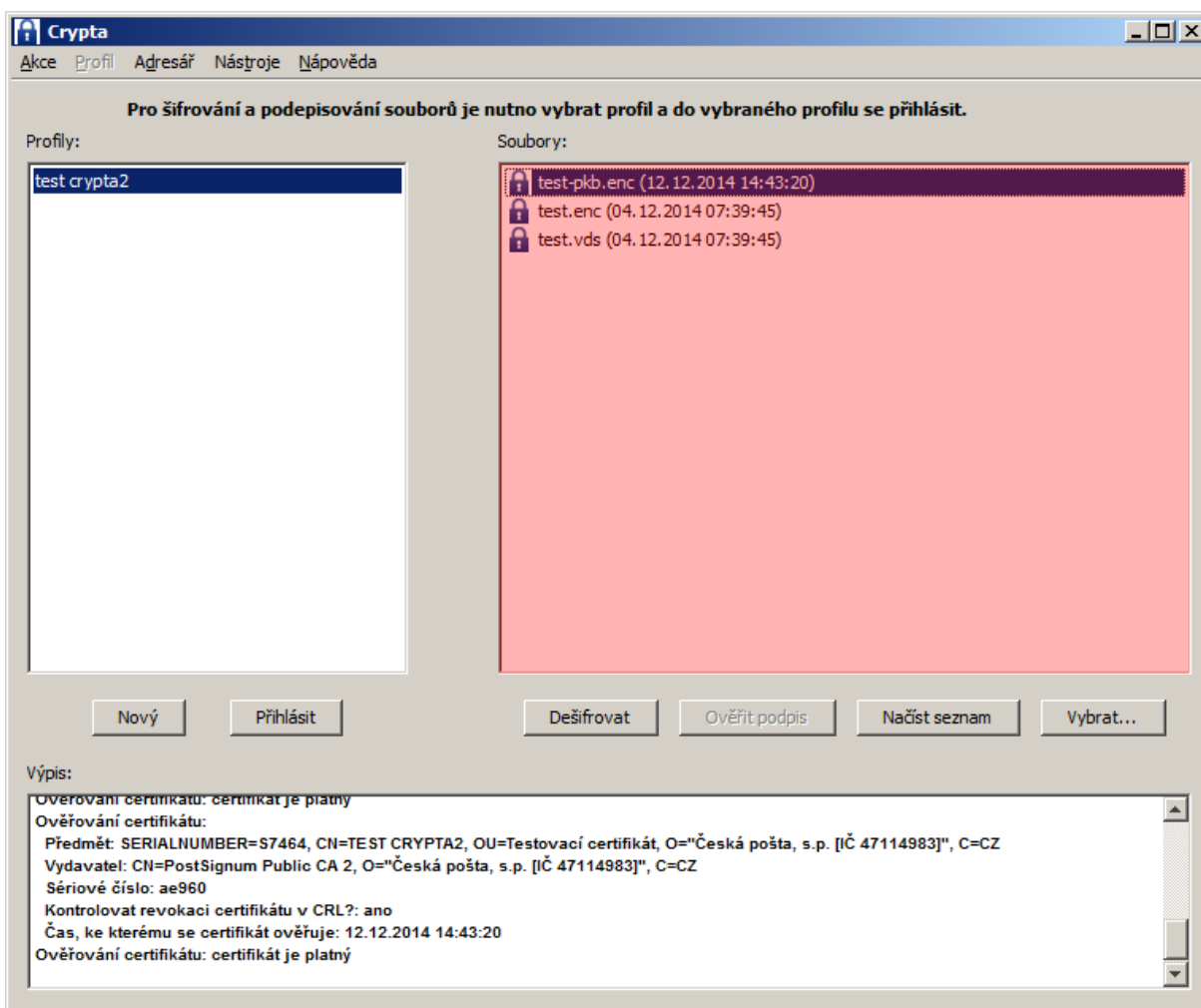


### 3 Dešifrování

Výběr souboru pro dešifrování můžete udělat dvěma způsoby:

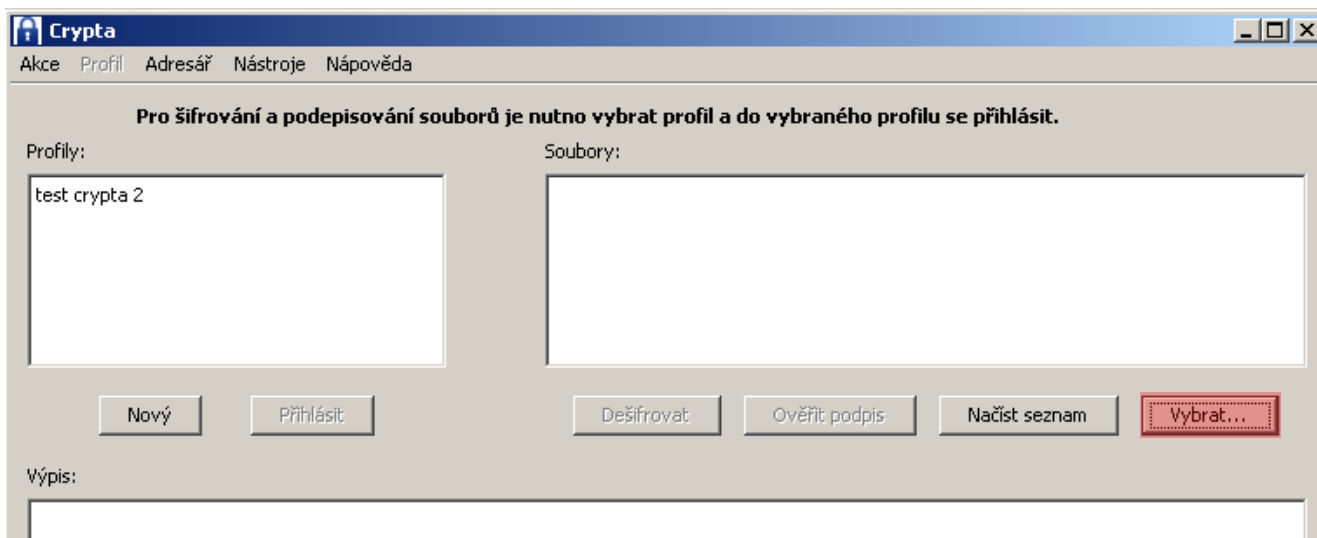
1. Z úvodní obrazovky programu. Není potřeba se hlásit do profilu.

Pokud jsou soubory pro dešifrování nahrány do provozního adresáře programu `_data\work`, tak jsou zobrazeny na úvodní obrazovce v rámečku *Soubory*:

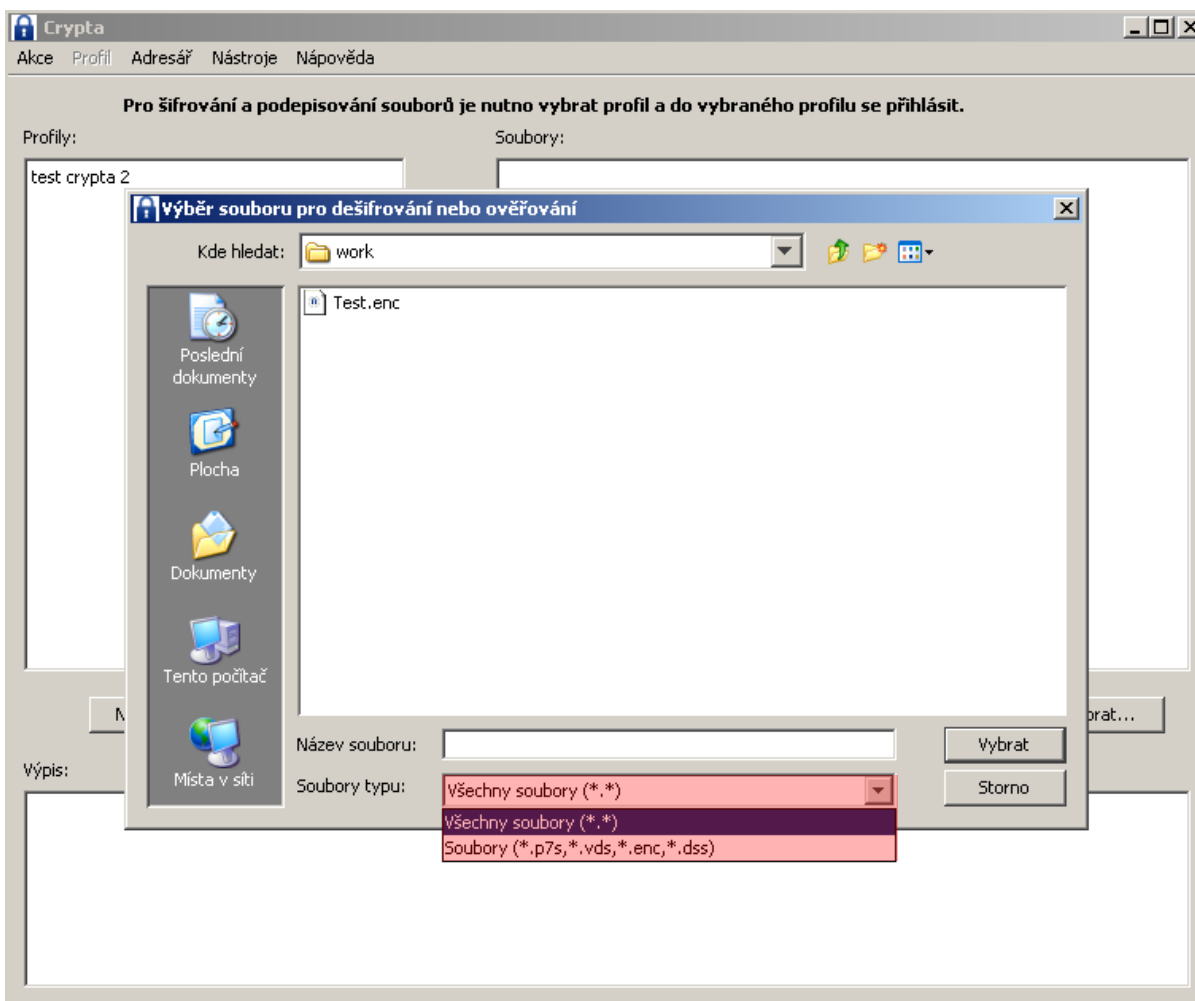


V tomto případě postačí vybrat příslušný soubor na úvodní obrazovce a stisknout tlačítko **Dešifrovat**. Program rozpozná, pro který profil je soubor zašifrován a zobrazí výzvu k zadání hesla pro příslušný profil. Po zadání hesla a stisku tlačítka **OK** se zobrazí okno s parametry pro dešifrování.

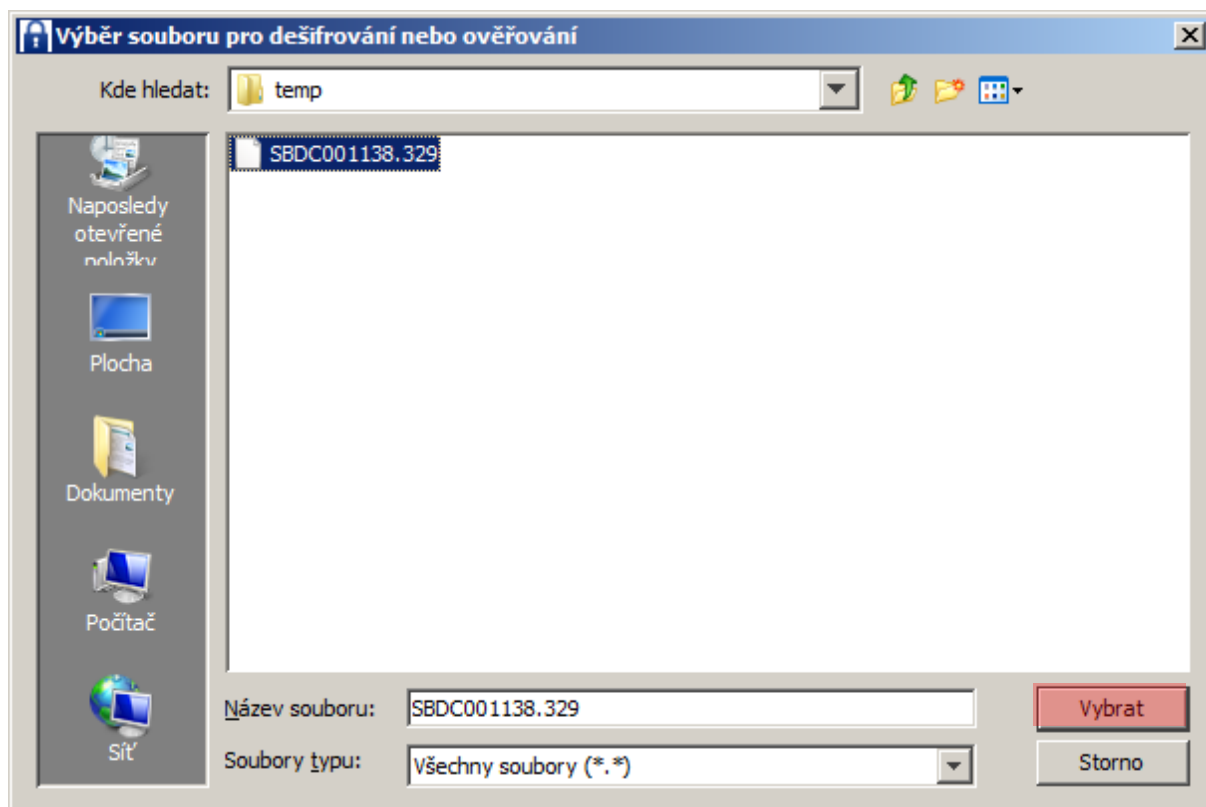
2. Soubor je možné vybrat přímo pomocí tlačítka **Vybrat...** .



Po stisknutí tlačítka se zobrazí okno s výběrem souboru pro dešifrování. Aby bylo možné zobrazit všechny soubory, je nutné změnit typ souboru.

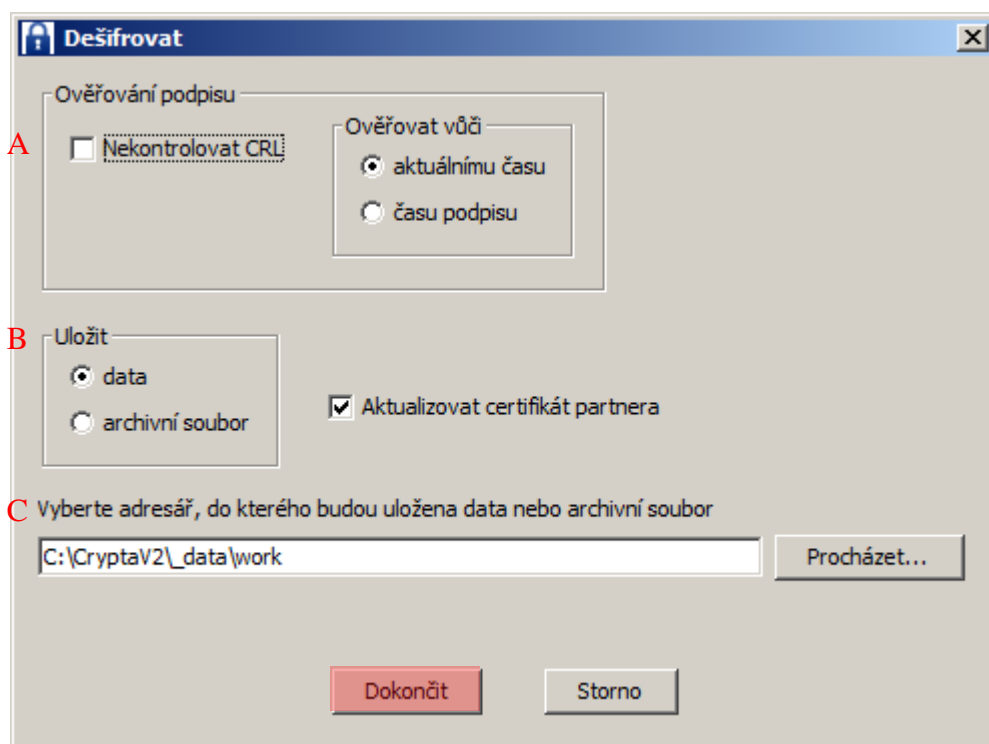


Po výběru souboru stisknete tlačítko **Vybrat**. Program rozpozná pro který profil je soubor zašifrován a zobrazí výzvu k zadání hesla pro příslušný profil. Po zadání hesla a stisku tlačítka **OK** se zobrazí okno s parametry pro dešifrování, viz následující stránka.





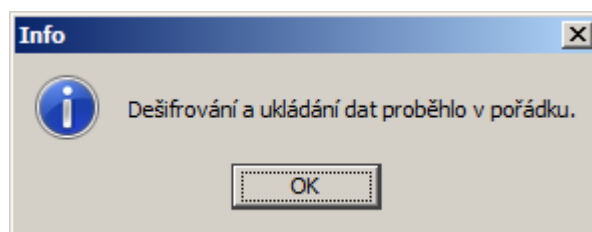
Okno dešifrování:



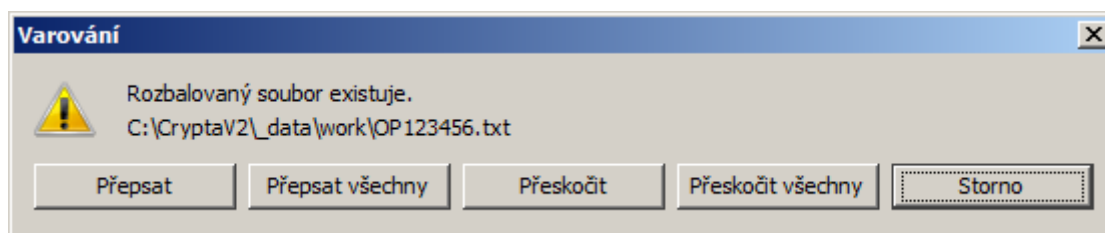
- A. Pokud nemáte momentálně přístup k internetu, je potřeba zaškrtnout volbu **Nekontrolovat CRL**, v opačném případě není potřeba měnit nic.
- B. Na ukládaném formátu není potřeba nic měnit.
- C. Tlačítkem **Procházet...** vyberete výstupní adresář, kam budou uloženy dešifrované soubory.

Po dokončení zadání všech parametrů stisknete tlačítko **Dokončit**

Po úspěšném dešifrování bude zobrazena hláška:



Pokud budou v cílovém adresáři již obsažené soubory se stejným názvem, bude zobrazena hláška:



V tomto případě se musíte rozhodnout pro nějakou akci.