

			\smile
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:

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

🔐 Crypta	
Akce Profil Adresář Nástroje	<u>N</u> ápověda
Pro šifrování a po	depisování souborů je nutno vybrat profil a do vybraného profilu se přihlásit.
Profily:	Soubory:
test crypta2	 test.enc (04. 12. 2014 07: 39: 45) test.vds (04. 12. 2014 07: 39: 45) Podepsaná a zašifrovaná data
	Heslo profilu
	Profil: test crypta2
	Zadejte heslo k profilu: ********
	🔽 zapamatovat heslo pro dešifrování
	ОК
Nový Přih	lásit Dešifrovat Ověřit podpis Načist seznam Vybrat
Výpis:	



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

🔒 Crypta - pro	ofil: test crypta2		
<u>Akce Profil Adr</u>	esář Nás <u>t</u> roje <u>N</u> ápověda		
	ন ন	 Žádost vyt Importovár 	vořena n certifikát
Údaje o záka	zníkovi		Certifikát
Jméno (CN)	TEST CRYPTA2		Podepsat a šifrovat
Organizace	Česká pošta, s.p.		Podepsat
IČ	47114983	[Vytvořit žádost
Org. jednotka E-mail		_ [Odhlásit
Linda	,		
Výpis			

3. Výběr souborů pro šifrování

Podepsat a	ŝifrovat - profil: test crypta2	×
AVstupní adresář	C:\CryptaV2_data\work	Procházet
B Vstupní maska	*,*	Vybrat
C Výstupní soubor	C:\CryptaV2_data\work\test-pkb.vds	Procházet
DAdresáti Předm Předm Předm	ět: PKA CENTRUM; Platnost do: 19.09.2017 09:46:20; Sériové číslo: ae0ff ět: PKB CENTRUM; Platnost do: 18.09.2017 09:55:32; Sériové číslo: ae060 ět: SIPO CENTRUM; Platnost do: 20.03.2017 13:22:33; Sériové číslo: a7d19	Načíst seznam
	Podepsat a šifrovat Storno	

Česká pošta, s.p., se sídlem Politických vězňů 909/4, 225 99 Praha 1, IČ: 471 14 983, zapsaný v Obchodním rejstříku u Městského soudu v Praze, spisová značka A7565 Tento dokument je považován za vlastnictví podniku Česká pošta, s.p., a může být užíván výhradně způsobem stanoveným v tomto dokumentu.



- 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:*

Akce Profil Adresář Nástroje Nápověda		
Akce Profil Adresář Nástroje Nápověda Pro šifrování a podepisování soube Profily: test crypta2	orů je nutno vybrat profil a do vybraného profilu se přihlásit. Soubory:	
Nový Přihlásit	Dešifrovat Ověřit podpis Načíst seznam Vybrat	
Vypis: Overovaní čertifikátu: Ověřování certifikátu: Předmět: SERIALNUMBER=S7464, CN=TEST CRYF Vydavatel: CN=PostSignum Public CA 2, O="Česk Sériové číslo: ae960 Kontrolovat revokaci certifikátu v CRL?: ano Čas, ke kterému se certifikát ověřuje: 12.12.2014 Ověřování certifikátu: certifikát je platný	PTA2, OU=Testovací certifikát, O="Česká pošta, s.p. [lČ 47114983]", C=CZ (á pošta, s.p. [lČ 47114983]", C=CZ I 14:43:20	ł

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... .

😭 Crypta		<u>- 0 ×</u>
Akce Profil Adresář Nástroje Nápověda		
Pro šifrování a podepisování souborů je	nutno vybrat profil a do vybraného profilu se přihlásit.	
Profily:	Soubory:	
test crypta 2		
Nový Přihlásit	Dešifrovat Ověřit podpis Načíst seznam Vybrat.	
Výpis:		

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

🔒 Crypta				<u> </u>
Akce Profil Adresář Nás	stroje Nápověda			
Pro šifrování	a podepisování souborů je i	nutno vybrat profil a do vybran	ného profilu se přihlásit.	
Profily:		Soubory:		
test crypta 2				
🔐 Výběr so	ouboru pro dešifrování nebo	ověřování		×
Kde H	nledat: 🛅 work		💌 🤣 📂 🖽 -	
Posledr dokumer Plocha Plocha	ní nty nty			
Tento pod	litač		Vybra	prat
Výpis: Místa v s	siti Souboru tupu	1 1 Abraha		
	Všect Soubory typu: Všect Soub	hny soubory (*.*) nny soubory (*.*) ory (*.p7s,*.vds,*.enc,*.dss)		



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.

🔒 Výběr soubor	u pro dešifrován	í nebo ověřování				×
Kde hledat:	🍌 temp]	- 🕫 🛛	🤊 🛄 -	
Naposledy otevřené noložkv Plocha Plocha Dokumenty Počítač	SBDC001138	3.329				
	Název souboru:	SBDC001138.329				Vybrat
Síť	Soubory typu:	Všechny soubory (*.	*)		•	Storno



Okno dešifrování:

6	Dešifrovat	×
Α	Ověřování podpisu Ověřovat vůči Nekontrolovat CRL Ověřovat vůči C aktuálnímu času C času podpisu	
В	Uložit	
C١	Vyberte adresář, do kterého budou uložena data nebo archivní soubor	.
I	C:\CryptaV2_data\work Procházet	
	Dokončit Storno	

- 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:

Varování				×
Rozbalovan C:\CryptaV	ý soubor existuje. 2_data\work\OP12345	6.txt		
Přepsat	Přepsat všechny	Přeskočit	Přeskočit všechny	Storno

V tomto případě se musíte rozhodnout pro nějakou akci.