Crypta verze 2 pro SIPO přichází

Česká pošta nasazuje pro komunikaci se SIPO nový šifrovací program Crypta verze 2.2. Do konce ledna 2015 jím má být zcela nahrazen současně používaný Crypta verze 1.3. Pokud jste ještě neobdrželi e-mailem výzvu k přechodu na novou Cryptu verze 2.2, očekávejte ji každým dnem.

Ačkoliv se zdánlivě jedná jen o změnu čísla verze, ve skutečnosti je Crypta verze 2 (CRYPTAV2) zcela nový program naprogramovaný v jazyce Java a je tedy nutno změnit Vaše mnohé postupy. Chci Vám tímto poskytnout některé užitečné informace.

## Opatření vlastního programu CRYPTAV2

Program je volně ke stažení na internetu na adrese <http://www.postsignum.cz/programy_ke_stazeni.html?step=02> Z nabídky si musíte vybrat verzi odpovídající Vašemu systému (zpravidla Windows 32-bitové nebo 64-bitové) a stáhnout si ji na svůj počítač a spustit instalační program. Doporučujeme standardní nastavení neměnit a pokračovat pouze stiskem tlačítek „Další“ až do nainstalování programu Crypta. Podrobný postup instalace najdete ve formě dokumentu také na této stránce.

Získání šifrovacího certifikátu pro CRYPTAV2

Původní certifikáty Crypta verze 1.3 Vám v žádném případě nebudou fungovat! Je potřeba získat certifikáty nové. Česká pošta nabízí 2 cesty, jak se k nim propracovat. Zkoušeli jsme obě, jsou schůdné a zdá se nám, že jsou zhruba rovnocenné.

1. Požádat internetem. Předpokládá se, že máte funkční Cryptu 1.3 (starou) , stále ještě platný certifikát a tím samozřejmě i smlouvu o certifikačních službách s Českou poštou. Vytvoříte požadavek na certifikát CryptaV2, vyplníte příslušné dokumenty. Pořídíte si sken mandátní smlouvy, pověření starosty a plnou moc a to vše odešlete zakryptované na adresu crypta2.postsignum@cpost.cz. Podrobnější postup s příslušnými dokumenty najdete na <http://www.postsignum.cz/inca/?step=04>.
2. S návštěvou pobočky České pošty. Stačí vlastnit mandátní smlouvu a smlouvu o certifikačních službách České pošty. Vytvoříte požadavek na certifikát CryptaV2, vyplníte příslušné dokumenty. Vezmete si mandátní smlouvu, pověření starosty, plnou moc a osobní průkaz a dostavíte se na pobočku České pošty. Na flash disku si můžete přinést požadavek na vystavení certifikátu a poznamenané ID číslo odeslaného požadavku. Podrobněiší postup s příslušnými dokumenty najdete na <http://www.postsignum.cz/inca/?step=02>.

V obou případech dostanete výsledný certifikát pravděpodobně e-mailem. K jeho instalaci Vás opět odkazujeme na příslušnou dokumentaci, která je k nalezení na uvedených adresách. Pro další předpokládáme, že máte nainstalovaný program CryptaV2 s vytvořeným profilem a načteným. Platným certifikátem

## Použití v programu SBN Klasik (DOSový, starý program)

Přestože CryptaV2 je zcela nový program, jak jsme již uváděli, programátoři se snažili o maximální zpětnou kompatibilitu a změny nejsou nijak zásadní. Přesto existují.

Pro správnou funkci SBN a CRYPTAV2 je potřeba nainstalovat novou verzi programů SIPO2000.RDB a SIPO2000.TTT v adresáři SIPO2000 (jednoduchým překopírováním souborů z přílohy). Vlastní vytvoření změn je zcela identické s předchozí verzí. Změna nastane až v okamžiku doplňování parametrů pro šifrování.



1. Je potřeba upravit cestu k programu CryptaCmd.exe. Při běžné instalaci se nachází jak je na obrázku naznačeno na „C:\CRYPTAV2\CRYPTA~1.EXE“.
2. Zcela nový je dotaz „Používat CRYPTA verze 2 (NOVÁ)?“. V našem případě tedy „A“ (ANO).
3. „Uživatelské jméno“ se v CRYPTĚV2 nazývá „Jméno profilu“. Napíšete jméno svého profilu pořízeného v CRYPTAV2. Nezapomeňte na uvozovky, teď jsou povinné!
4. „Adresát-certifikát“ je jméno partnera, kterému je zakryptovaný soubor určen. Pro CRYPTUV2 se používá „SIPO CENTRUM“. Opět v uvozovkách!
5. Ostatní parametry se nemění.
6. Nyní kryptování trvá o něco déle, předchází mu totiž načtení seznamu odvolaných certifikátů („CLR“).



1. Teprve po načtení se objeví výzva „Heslo:“. Zapište heslo pro Váš profil a stiskněte ENTER. V této verzi se zapisované heslo nezobrazuje (ani hvězdičky) a je nutno ho zapsat na první dobrou.
2. Tím je šiftování dokončeno a na výstupu by se měl objevit soubor ZMxxxxxx.ENC, který odešlete.

Pozor! V programu CRYPTAV2 se na výstupním místě nesmí nalézat soubor se shodným jménem, do kterého kryptujete, tedy ZMxxxxxx.ENC! V takovém případě skončí kryptování chybou!! Pro jistotu výstupní adresář (flash disk) vždy vymažte. A není na škodu si před odesláním ověřit datum a čas vzniku souboru ZMxxxxxx.ENC!

## Změny v programu SBNW

Vytvoření změnového souboru je stejné jako v předchozí verzi. Před vlastním zakryptováním je nutné zkontrolovat a upravit označené parametry.



1. Je potřeba upravit cestu k programu CryptaCmd.exe. Při běžné instalaci se nachází jak je na obrázku naznačeno na „C:\CRYPTAV2\CryptaCmd.exe“. Můžete použít tlačítko se složkou vpravo.
2. „Příjemce“ se v CRYPTĚV2 nazývá „Jméno profilu“. Napíšete jméno svého profilu pořízeného v CRYPTAV2.
3. „Příjemce“ je jméno partnera, kterému je zakryptovaný soubor určen. Pro CRYPTUV2 a SIPO se používá „SIPO CENTRUM“.
4. Podmínkou správného fungování je, že program CRYPTAV2 je instalován ve složce „CryptaV2“. Standardní instalací CRYPTAV2 je toto automaticky splněno.



Vytvoříte soubory změn a uložíte je do pracovního adresáře. Tento postup je shodný pro obě CRYPTY.

****

Jste požádáni o vložení hesla ke svému profilu a to se objevuje ve formě náhradních znaků. Také toto je shodné pro CRYPTU 1 i pro CRYPTUV2.

****

Jestliže je vše provedeno správně, objeví se hlášení o správném zakryprování.

****

V opačném případě Vám program oznámí, že došlo k chybě a NENÍ zakryptováno. V adresáři CryptaV2 najdete soubor „JCRYPTA.LOG“, kde se můžete dočíst k jaké závadě došlo.

Jednou z nejčastějších závad je chybějící kontrola odvolaných certifikátů na serveru POSTSIGNUM, kterou tato verze CRYPTA vyžaduje. Je k tomu určena nová funkce, kterou najdete v menu k „Výměně dat“ (viz obr.).



Stisknete a po zodpovězení dotazu:



Probíhá stahování seznamu odvolaných certifikátů.



Nakonec se objeví zpráva o dokončení.

Pokud by Vás to obtěžovalo, můžete si kontrolu odvolaných certifikátů vypnout v programu CRYPTA.EXE volbou „Nástroje“ z hlavního menu a potom „Nastavit aplikaci“. Objeví se formulář:



Nastavíte zatrhávátko „Nekontrolovat CRL“ a potvrdíte „Uložit“, jak je naznačeno.

Je ovšem potřeba dodat, že takové nastavení má negativní vliv na bezpečnost kryptování.

Za SH servis AV

Jiří Mosz