SHA2CHECK

Nástroj pro opravu digitálních certifikátů a kontrolu nastavení Internet Exploreru

---

Autor:	AQUASOFT spol. s r.o., Němec Radek
Název projektu:	ECR brána
Poslední aktualizace:	27.6.2016
Jméno souboru:	SHA2Check
Počet stran:	10
Důvěrnost dokumentu:	Nízká

HISTORIE DOKUMENTU

Verze	Datum	Podpis
1.0	31. 3. 2014	Úvodní verze
1.1	16. 2. 2015	Změny verze 3.1.0.0
1.2	2. 6. 2015	Změny verze 3.2.0.0
1.3	27. 6. 2016	Změny verze 4.0.0.0

OBSAH

1. ÚVOD

SHA2Check je nástroj, který slouží ke:

- změně hodnoty vlastnosti Cryptographic Service Provider (dále jen CSP) v podepisovacích certifikátech uložených v osobním úložišti aktuálně přihlášeného uživatele tak, aby tyto certifikáty bylo možné použít pro digitální podpis s využitím algoritmů SHA-2. Tato vlastnost certifikátu určuje, který kryptografický modul se má při práci s daným certifikátem používat a přímo tedy ovlivňuje množinu algoritmů, které lze pro digitální podpis s využitím tohoto certifikátu použít.
- změně CSP v uloženém PFX souboru při přenosu certifikátů mezi Microsoft Windows XP a jiným systémem MS Windows podporujícím algoritmy SHA2 (Windows Vista a novější)
- kontrole nastavení Internet Exploreru tak, aby bylo možné použít ActiveX komponentu pro digitální podpis

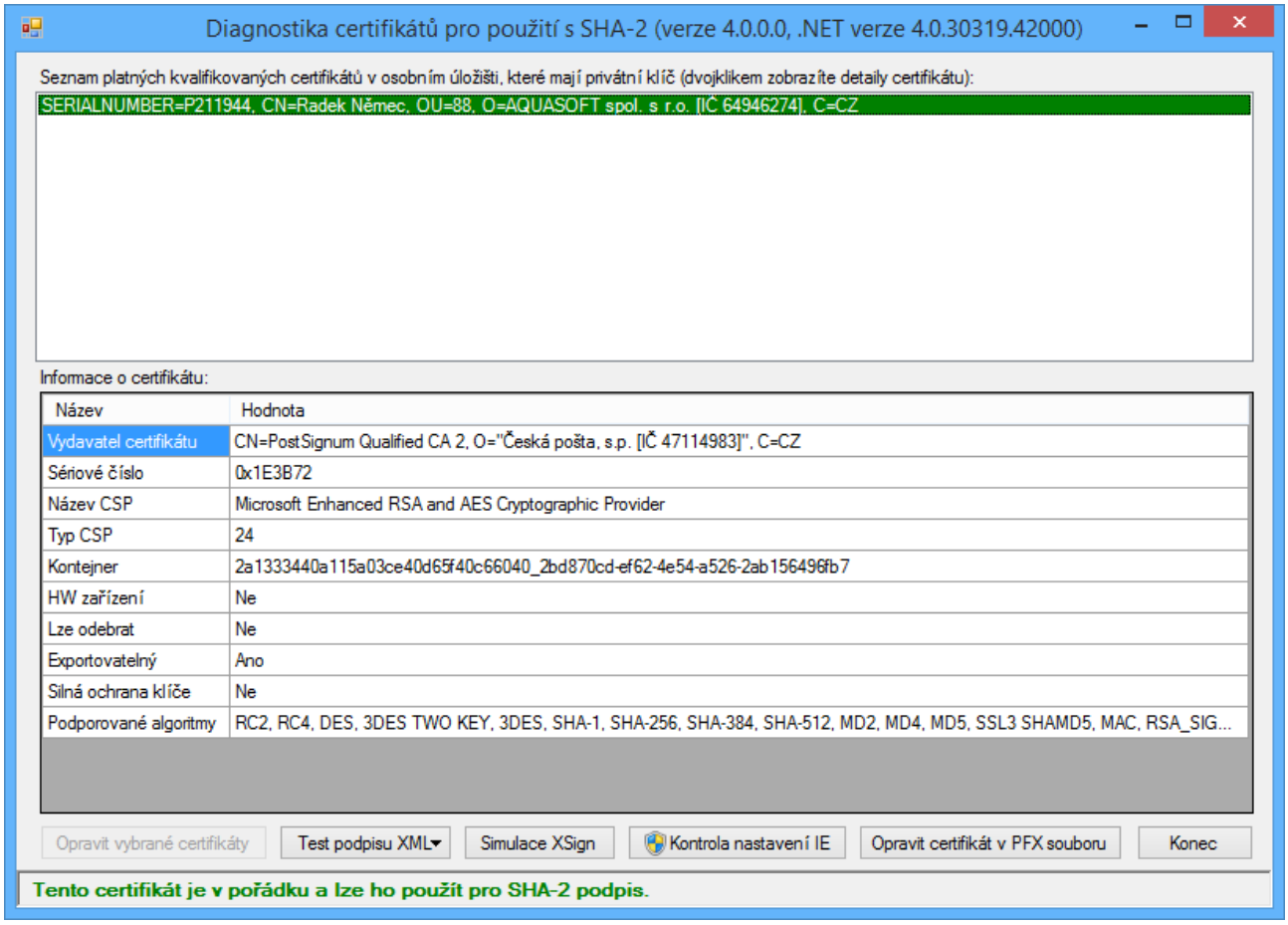
Program ke svému běhu používá Microsoft .NET Framework (dále FW) verze 2.0 nebo 4.5 (ZIP soubor obsahuje obě verze, které jsou funkčně identické, liší se jen verzí frameworku, pod kterým běží). Důvod pro vytvoření 2 verzí je snaha o možnost spuštění programu bez nutnosti instalovat příslušnou verzi FW. Seznam předinstalovaných verzí FW v operačních systémech je následující:

Verze OS	Předinstalovaná verze FW	Nejvyšší vydaná verze FW
Windows XP	Žádná (ale pravděpodobně se nainstalovala přes Windows Update)	4.0
Windows Vista, Windows 7	3.5.1 (obsahuje 2.0, 3.0 SP2 a 3.5 SP1)	4.6
Windows 8.0	4.5 (3.5 SP1 lze instalovat jako volitelnou součást systému)	
Windows 8.1	4.5.1 (3.5 SP1 lze instalovat jako volitelnou součást systému)	
Windows 10	4.6 (3.5 SP1 lze instalovat jako volitelnou součást systému)	

Z výše uvedeného je patrné, že:

- ve Windows 8.0 a vyšší bude vždy fungovat verze pro FW 4.5
- ve Windows Vista a Windows 7 záleží, zda je nainstalován FW 4.5; verze pro FW 2.0 bude fungovat vždy
- ve Windows XP bude fungovat jen verze pro FW 2.0 a to jen v případě, že je nainstalován

2. HLAVNÍ OKNO PROGRAMU



Obrázek č. 1

2.1. SPUŠTĚNÍ PROGRAMU

Po spuštění program zkontroluje, zda běží na podporovaném operačním systému (z hlediska SHA-2 podpory), pokud tomu tak není, zobrazí upozornění a ukončí se.

2.2. HLAVNÍ OKNO PROGRAMU

2.2.1 SEZNAM CERTIFIKÁTŮ

Seznam certifikátů obsahuje všechny digitální certifikáty v osobním úložišti aktuálně přihlášeného uživatele, které jsou označeny jako podepisovací (příznak, který do certifikátu zapisuje vydávající certifikační autorita (CA)) a mají privátní klíč (lze s nimi tedy provést digitální podpis). Dvojklikem lze zobrazit standardní okno s vlastnostmi certifikátu. Barva písma řádky seznamu může být jedna z 3 následujících:

- Zelená – certifikát je v pořádku a lze s ním provést SHA-2 podpis
- Červená – certifikát je sice v pořádku, ale jeho CSP neumožňuje provádět digitální podpis algoritmy SHA-2. Certifikát je však možno opravit stisknutím tlačítka „Opravit vybraný certifikát“.

- Šedivá – certifikát nelze použít pro SHA-2 podpis a nelze ho ani opravit. Tato situace nastává buď v případě, že je certifikát naimportován do úložiště certifikátů špatně, nebo se jedná o certifikát, jehož privátní klíč je uložen na externím médiu (čipová karta, USB token,…). V případě, že se jedná o certifikát uložený na externím médiu, je nutné zjistit podporu pro SHA-2 u výrobce/dodavatele daného HW zařízení, nástroj SHA2Check takovéto certifikáty nedokáže opravit.

2.2.2 Detaily certifikátu

Tato tabulka obsahuje detailní vlastnosti certifikátu. Jejími nejdůležitějšími údaji jsou řádky *Název CSP* a *Typ CSP*. Pokud se jedná o certifikát uložený v úložišti certifikátů Windows (tj. nejedná se o certifikát na čipové kartě nebo USB tokenu), pak (aby bylo možné použít certifikát pro podpis algoritmem SHA-2) je nutné, aby *Název CSP* byl roven hodnotě „Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)“ pro Windows XP SP3, nebo „Microsoft Enhanced RSA and AES Cryptographic Provider“ pro všechny ostatní systémy; *Typ CSP* musí být vždy 24.

2.3. Tlačítko „Opravit vybraný certifikát“

Pokud je zvolen certifikát, který lze opravit (je v seznamu certifikátů uveden červeně), lze stiskem tohoto tlačítka certifikát opravit. Certifikát je opraven přímo v úložišti a po dokončení opravy by měl v seznamu změnit barvu na zelenou.

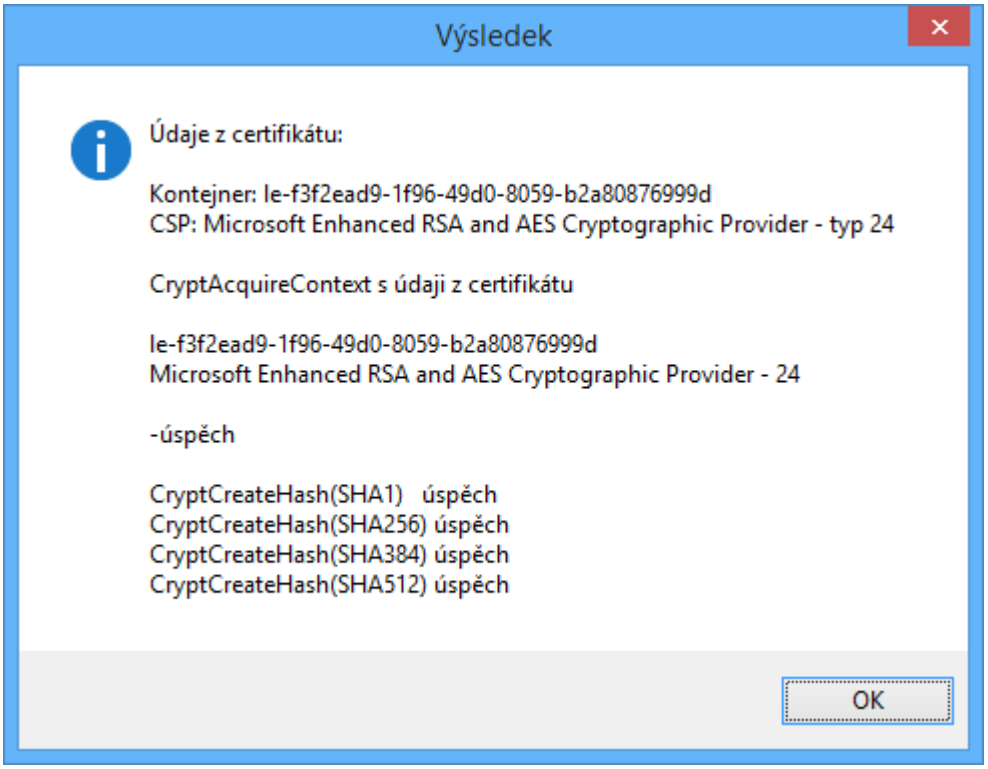
2.4. Tlačítko „Test podpisu XML“

Stiskem tlačítka se nabídne test podpisu XML souboru pomocí jedné z nainstalovaných ActiveX komponent pro podpis (pro ECR obálku 2.0 se používá jiná komponenta než pro 3.0). V případě, že se nezdaří inicializace ActiveX komponenty (např. pokud není nainstalována), zobrazí program upozornění. Výsledek testu je uložen do ZIP souboru.

POZOR: Vzhledem k tomu, že při spuštění ActiveX komponent v aplikaci SHA2Check běží tyto komponenty s jinou (menší) úrovní zabezpečení než při spuštění v Internet Exploreru, pak to, že se v aplikaci SHA2Check podaří úspěšně provést test podpisu pomocí jedné z komponent, neznamená, že podepisování zpráv danou komponentou bude automaticky fungovat i v Internet Exploreru (kde může být spuštění ActiveX blokováno, viz kapitola 2.6). Obrácená logika ale platí: pokud se test podpisu nezdaří v aplikaci SHA2Check, pak určitě daná ActiveX komponenta nebude fungovat s vybraným certifikátem ani v Internet Exploreru.

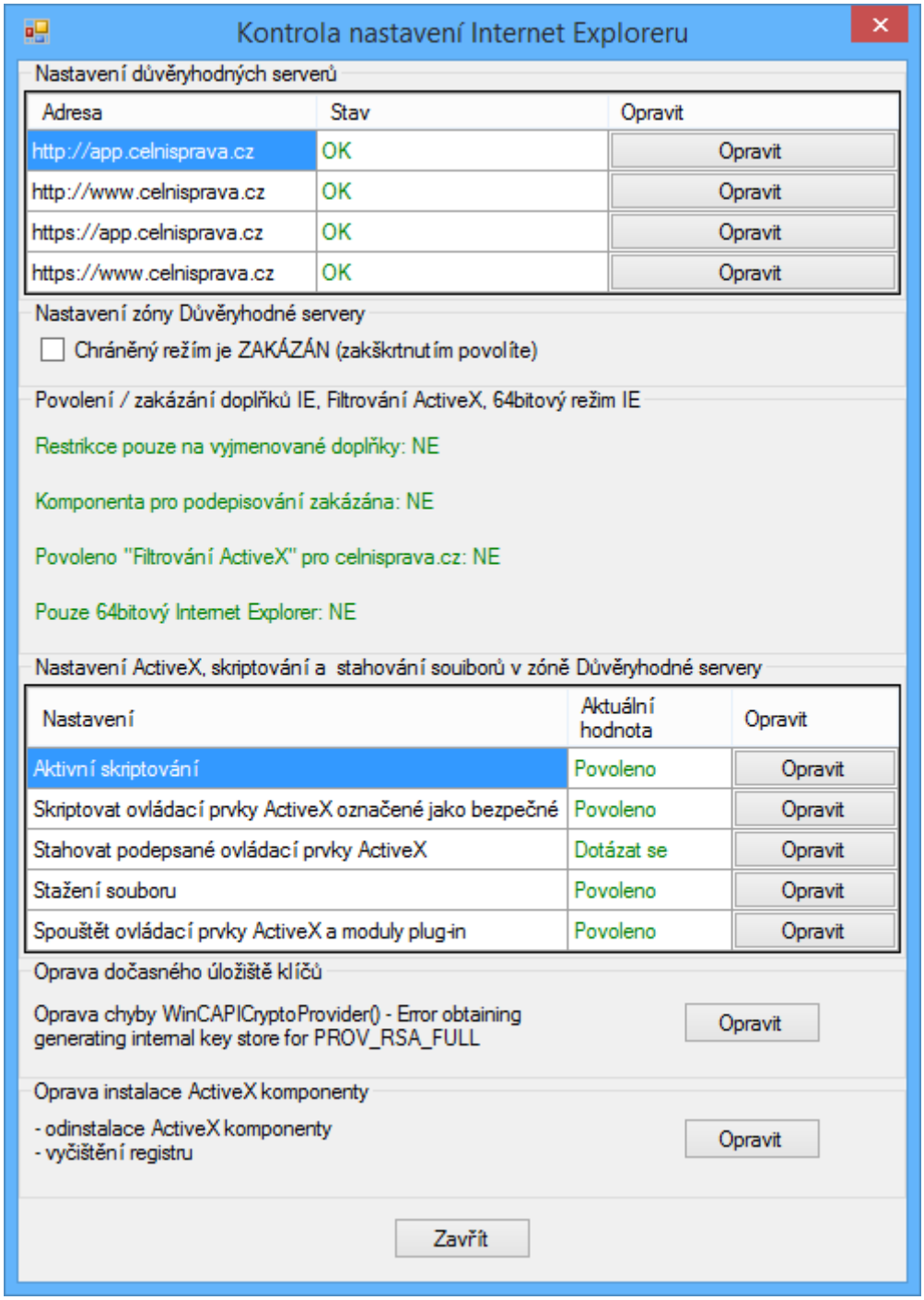
2.5. TLAČÍTKO „SIMULACE XSIGN“

Toto tlačítko umožňuje simulovat průběh podpisu bez použití samotné ActiveX komponenty pro podpis, slouží tedy k ověření, zda lze na daném počítači vůbec používat SHA-2 algoritmy v souvislosti s digitálními podpisy. Po stisknutí se zobrazí seznam certifikátů aktuálního uživatele, u vybraného certifikátu se pak program pokusí zavolat Windows funkce CryptAcquireContext a CryptCreateHash. Aby bylo možné použít vybraný certifikát pro SHA-2 podpis, je nutné, aby alespoň u jedné z řádek s SHA256, SHA384 a SHA512 bylo uvedeno slovo „úspěch“ (algoritmus SHA1 není součástí „rodiny“ algoritmů SHA-2).



Obrázek č. 2

2.6. Tlačítko „Kontrola nastavení IE“



Obrázek č. 3

Aby podepisovací ActiveX komponenta správně fungovala, je nutné, aby bylo umožněno webovým stránkám celní správy tuto komponentu spouštět a umožnit jí pracovat s úložištěm certifikátů na počítači uživatele. K tomu je nutné splnit několik podmínek (viz Obrázek č. 3 a jednotlivé podkapitoly níže). Všechny opravy v okně „Kontrola nastavení Internet Exploreru“ je nutné provádět s vypnutým Internet Explorerem. Pokud je program spuštěn v prostředí, kde je zapnuta funkce „Řízení uživatelských účtů“ (UAC) a program nebyl spuštěn pomocí volby „Spustit jako správce“ (tento stav je indikován obrázkem štítu u tlačítka „Kontrola nastavení IE“, viz Obrázek č. 1), je nutno program restartovat se zvýšenými právy (program o tento restart po stisknutí tlačítka sám požádá, není nutno ho ukončovat a znovu spouštět ručně).

2.6.1 Nastavení důvěryhodných serverů

Pro správnou funkci webových aplikací CS používajících pro digitální podpis ActiveX komponentu je nutné, aby všechny části webové stránky zobrazené uživateli byly považovány za důvěryhodné, tj. aby jejich zdrojový web server byl důvěryhodný. Vzhledem k tomu, že na web CS lze přistupovat pomocí protokolu http i https a tomu, že některé aplikace používají kromě webové adresy www.celnisprava.cz i adresu app.celnisprava.cz, je nutné, aby všechny 4 kombinace byly považovány za důvěryhodné. Pokud je tedy u serveru uvedeno „Není důvěryhodný“ je nutné stiskem tlačítka Opravit tento server přidat do důvěryhodných serverů.

2.6.2 Nastavení zóny důvěryhododné servery

Pro správnou funkci ActiveX komponenty je nutné, aby u zóny Důvěryhodné servery byl vypnut Chráněný režim (kolonka není zaškrtnuta a je zobrazeno „Chráněný režim je ZAKÁZÁN (zaškrtnutím povolíte)“, viz Obrázek č. 3). Protože však v minulosti platil přesný opak (bylo nutné, aby chráněný režim byl pro zónu Důvěryhodné servery povolen), není u tohoto nastavení barevně označeno, která hodnota je „správná“.

2.6.3 Povolení/Zakázání doplňků IE, Filtrování ActiveX, 64bitový režim IE

2.6.3.1 Povolení/Zakázání doplňků IE

V Internet Exploreru lze pro doplňky nastavit 3 druhy omezení:

- správce může globálně omezit povolené doplňky jen na ty, které jsou uvedeny v seznamu povolených doplňků; všechny ostatní doplňky jsou zakázány
- pro konkrétní doplněk lze nastavit, zda je: zakázán (uživatel nemůže povolit), zakázán (uživatel může povolit), nebo povolen
- uživatel může doplněk povolit/zakázat v konfiguraci.

Pokud je jedno z těchto omezení nastaveno správcem (první bod výše), nějakým programem zakazujícím jemu neznámé (potenciálně škodlivé) doplňky, nebo přímo uživatelem, je u příslušné řádky zobrazeno tlačítko Opravit, které je nutno stisknout. V prvním případě dojde k odstranění restrikce na vyjmenované doplňky, v druhém případě se po stisknutí „Opravit“ nastaví, že podepisovací komponenta pro ActiveX je povoleným doplňkem. V posledním případě se uživatelské nastavení doplňku změní na „Povoleno“.

2.6.3.2 Filtrování ActiveX

Novější verze Internet Exploreru obsahují technologii Filtrování ActiveX, která, pokud je povolena, implicitně blokuje všechny „neznámé“ ActiveX komponenty a tím znemožňuje funkci podepisovací komponenty. Pro povolení podepisovací komponenty, je možno použít ikonu v adresní řádce prohlížeče, nebo použít tlačítko Opravit na příslušné řádce.

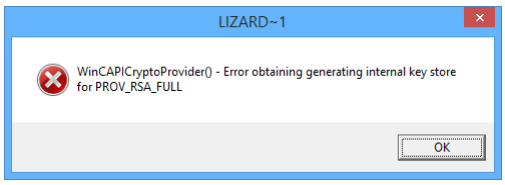
2.6.3.3 64bitový režim IE

V 64bitovém operačním systému existuje nastavení pro Internet Explorer, které znemožňuje spuštění 32bitové verze Internet Exploreru (a to i v případě, že je iexplore.exe spouštěn z adresáře „Program Files (x86)“). Pro správnou funkci podepisovací komponenty je třeba toto nastavení zakázat (stisknutím tlačítka Opravit).

2.6.4 Nastavení ActiveX, skriptování a stahování souborů, filtrování ActiveX

Tato nastavení mohou mít několik stavů: „Zakázáno“, „Povoleno“ (tyto 2 stavy existují ve všech nastaveních), „Schválené správcem“ a „Dotázat se“. Pokud je některé z vyjmenovaných nastavení zobrazeno červeně, nemusí podepisovací komponenta fungovat správně a je tedy nutné stiskem tlačítka Opravit na příslušné řádce nastavit správnou hodnotu (většinou „Povoleno“, u filtrování ActiveX je naopak důležité nastavit „Zakázáno“). Hodnoty „Dotázat se“ a „Schválené správcem“ jsou též v pořádku. Nastavení „Stažení souboru“ nemá přímý vliv na funkčnost podepisovací ActiveX komponenty, ale je nutné pro povolení stahování podepsaných souborů na disk. Nastavení „Filtrování ActiveX“ není zobrazeno, pokud je instalován Internet Explorer verze 8 či starší (filtrování ActiveX komponent není v těchto verzích implementováno).

2.6.5 Oprava dočasného úložiště klíčů



Obrázek č. 4

Pokud se při práci s podepisovací komponentou objeví hlášení výše (viz Obrázek č. 4), je nutné opravit, resp. smazat dočasné úložiště klíčů stiskem příslušného tlačítka Opravit.

2.6.6 Oprava instalace ActiveX komponenty

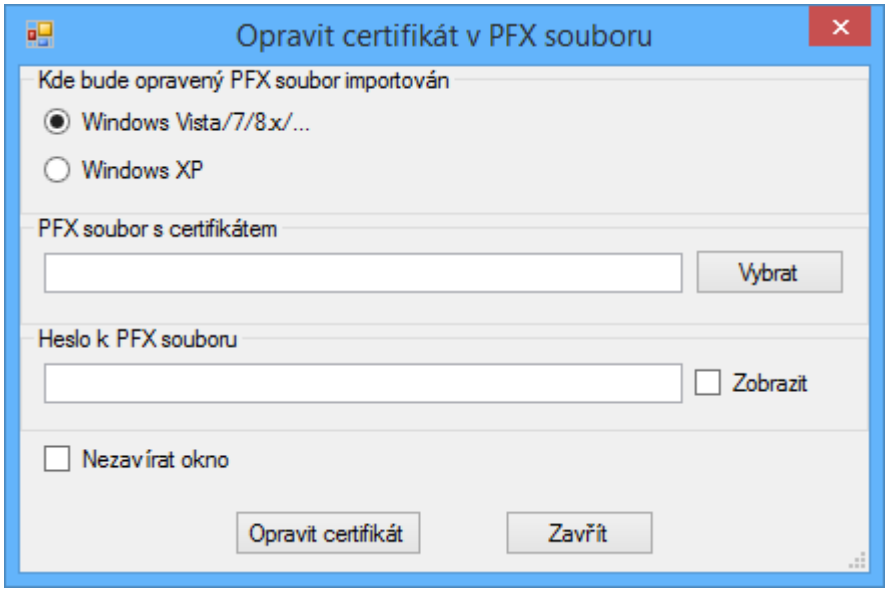
Poznámka: Tato kapitola popisuje pouze opravu instalace ActiveX komponenty používané pro podpis ECR obálky 2.0 (LizardLabsXSignAX Control). Opravu instalace komponenty ActiveXSigner provedete jedině tak, že pomocí nástrojů OS Windows danou komponentu odinstalujete (je uvedena v seznamu nainstalovaných aplikací) a pak pomocí Internet Exploreru (či MSI balíčku) znovu nainstalujete.

Pokud jsou všechna nastavení Internet Exploreru správně (žádná řádka není zobrazena červeně a chráněný režim pro zónu „Důvěryhodné weby“ je zakázán), certifikát je v seznamu (v hlavním okně) zobrazen zeleně (lze s ním provést SHA-2 podpis) a přesto podpis nefunguje, lze provést úplnou odinstalaci všech výskytů podepisovací ActiveX komponenty. Tato akce provede následující kroky:

- pokud byla provedena jakákoliv instalace podepisovací komponenty ručně pomocí MSI balíčku, spustí se její odinstalace (zobrazí se dialog odinstalace, který je bezobslužný a nelze přerušit)
- smazání všech zbývajících souborů, které zbydou po provedení předchozího bodu
- smazání všech relevantních odkazů na ActiveX komponentu v registru Windows
- zobrazení informace o dokončení odinstalace a ukončení programu

Pozor: Tento krok komponentu pouze odinstaluje, opětovnou instalaci je nutno provést zobrazením příslušné stránky v Internet Exploreru.

2.7. TLAČÍTKO „OPRAVIT CERTIFIKÁT V PFX SOUBORU“



Obrázek č. 5

Tato část programu umožňuje opravit CSP v souboru s certifikátem (přípona PFX). Někdy totiž není možné opravit certifikát, který je umístěn v úložišti certifikátů, protože do něj nelze PFX soubor s certifikátem vůbec naimportovat. Toto nastává zejména v momentě, kdy byl proces žádosti o certifikát proveden na Windows XP, poté byl certifikát vyexportován do PFX souboru a nyní je třeba ho naimportovat na počítači se systémem Windows Vista nebo novějším. Stejný problém nastane i v momentě, kdy je směr přenosu opačný (z Windows Vista či novější na Windows XP). Při opravě certifikátu v PFX souboru postupujeme následovně:

- vybereme verzi OS, na které bude opravený PFX soubor importován (nezáleží tedy vůbec na verzi Windows, ze kterých byl proveden export do PFX souboru)
- tlačítkem Vybrat zvolíme PFX soubor, který chceme opravit
- vyplníme heslo, které bylo použito pro export certifikátu do PFX souboru (zaškrtnutím Zobrazit lze heslo zobrazit v čitelné formě)
- stiskneme Opravit a vyčkáme, až se oprava provede
- pokud nastane nějaký problém (nejčastějším problémem je špatně zadané heslo), lze pomocí zaškrtnutí „Nezavírat okno“ nechat zobrazit výstup externího programu
- pokud je vše OK, program zobrazí nové jméno PFX souboru, kam uložil opravený certifikát. Heslo k tomuto PFX souboru je stejné jako heslo původního PFX souborus
- importujeme nově vygenerovaný PFX soubor do úložiště Windows pomocí standardního postupu. Po importu je nutné ověřit, že certifikát byl naimportován se správným CSP a pokud tomu tak není (některé verze Windows ignorují nově nastavené CSP v opraveném PFX souboru, ale PFX lze naimportovat), opravit pomocí tlačítka „Opravit vybraný certifikát“