

Podepisování elektronického podání – SHA-2

Od 1.1.2011 je dle vyhlášky MV ČR č. 378/2006 Sb. stanovena povinnost používat při vytváření elektronických podpisů dokumentů výhradně hashovací funkce třídy SHA-2. Další informace k problematice lze nalézt na stránkách Ministerstva vnitra v dokumentech:

"Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu" na URL:

<http://www.mvcr.cz/clanek/informace-k-prechodu-k-bezpecnejsim-kryptografickym-algoritmem-v-oblasti-elektronickeho-podpisu.aspx>,

"Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu" na URL:

<http://www.mvcr.cz/clanek/zmena-v-kryptografickych-algoritmech-ktere-jsou-pouzivany-pro-vytvoreni-elektronickeho-podpisu.aspx>.

Obsah

1. SYSTÉMOVÉ POŽADAVKY A ULOŽENÍ PODEPISOVACÍCH CERTIFIKÁTŮ A KLÍČŮ	1
2. NASTAVENÍ PODPISU.....	2
3. CERTIFIKÁT A KLÍČ VE WINDOWS	3
3.1. Změna CSP u certifikátu ve Windows.....	3
4. CERTIFIKÁT A KLÍČ NA KARTĚ/TOKENU.....	4

1. Systémové požadavky a uložení podepisovacích certifikátů a klíčů

K využití hashovacích funkcí třídy SHA-2 musí být počítač vybaven odpovídajícími verzemi SW vybavení:

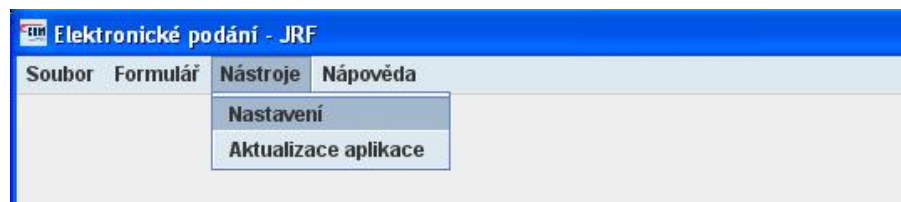
- **Minimální verze Windows je XP SP3,**
(U starších verzí Windows nelze zaručit funkčnost SHA-2.)
nebo
Linux
nebo
Mac OS X
- **Aktuální verze aplikace JRF – v. 2.0 nebo vyšší,**
- **Minimální verze Javy je 1.6.0_18.**

Je-li aplikace JRF spouštěna přímo programem EXE, který byl instalován již dříve (v r. 2008), je třeba aplikaci JRF nainstalovat znovu, nestačí provést jen aktualizaci. Java je součástí aplikace JRF.

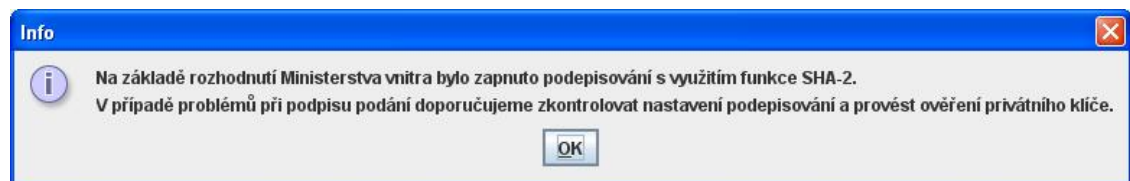
2. Nastavení podpisu

V aktuální verzi aplikace JRF doporučujeme zkontrolovat nastavení podpisu a provést ověření privátního klíče.

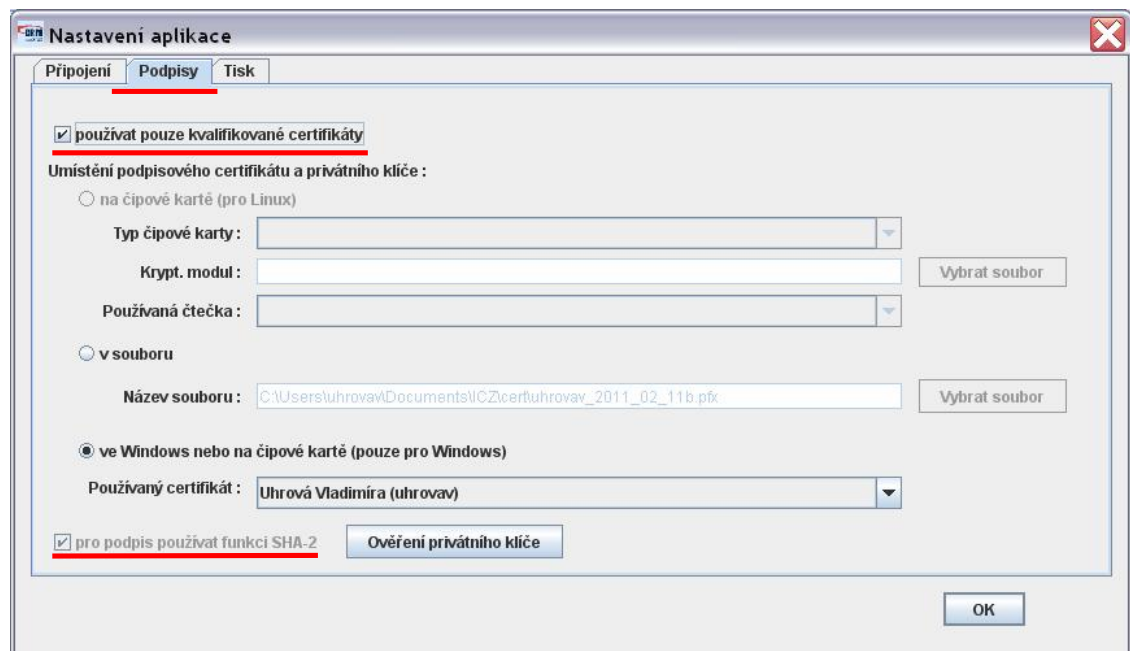
V nabídce aplikace JRF je třeba zvolit volbu Nástroje / Nastavení.



Při prvním spuštění se otevře okno s informací o zapnutí podepisování s využitím funkce SHA-2.

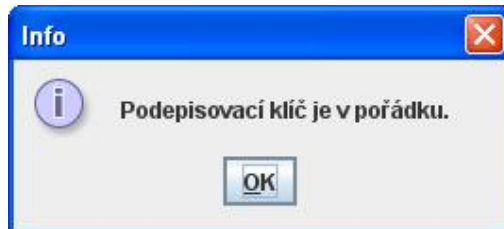


Parametry podpisu najdete na záložce Podpisy. Nové parametry "používat pouze kvalifikované certifikáty" a "pro podpis používat funkci SHA-2" jsou standardně zatrženy.



V případě nastavení parametru "pro podpis používat funkci SHA-2" je třeba před prvním použitím spustit test schopnosti PC používat SHA-2 pomocí tlačítka **Ověření privátního klíče**.

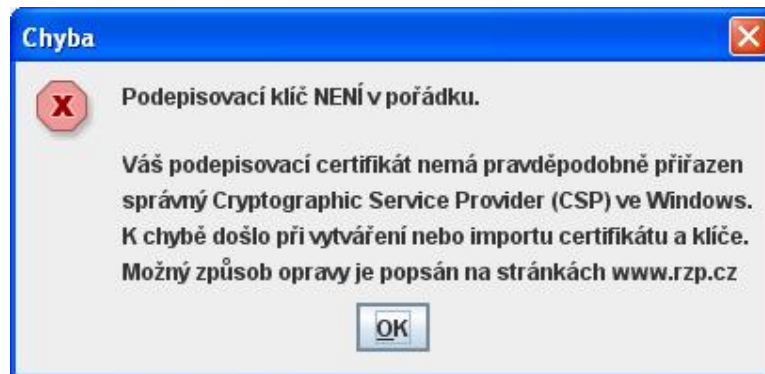
Test podepisovacího klíče a nastavení PC v případě správného nastavení vypíše následující potvrzovací okno.



Od 1.7.2011 nelze zrušit nastavení parametru "pro podpis používat funkci SHA-2", tj. nelze používat při podepisování hashovací funkci třídy SHA-1.

3. Certifikát a klíč ve Windows

Pokud je podepisovací klíč uložen ve Windows, musí být certifikátu přiřazen správný Cryptographic Service Provider (CSP), a to "Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)" ve Windows XP SP3, resp. "Microsoft Enhanced RSA and AES Cryptographic Provider" v novějších verzích Windows (Vista, Win7). Pokud je certifikát přiřazen k nevhodnému CSP, zobrazí se při testu podpisu tlačítkem **Ověření privátního klíče** chybové hlášení.



Chybu lze odstranit exportem certifikátu a klíče a jeho opětovným importem do správného CSP.

3.1. Změna CSP u certifikátu ve Windows

Změna CSP u daného certifikátu a klíče se provede jeho exportem a importem do správného CSP.

Export certifikátu a klíče se provede běžným postupem v prohlížeči MSIE pomocí Nástroje / Možnosti internetu / záložka Obsah / tlačítko Certifikáty / tlačítko Exportovat...

V průvodci exportem certifikátu je třeba nastavit, že se má exportovat i soukromý klíč (parametr Ano, exportovat soukromý klíč) a není třeba zahrnovat všechny certifikáty na cestě (parametr Zahrnout všechny certifikáty na cestě k certifikátu ...).

Výsledkem je soubor s příponou .PFX.

Po exportu je vhodné certifikát z Windows smazat a ukončit všechny aplikace.

Import lze provést dvěma způsoby v závislosti na tom, zda je na PC nainstalován program "certutil". Pokud není certutil nainstalován, je potřeba použít program "OpenSSL" (k dispozici ke stažení je na www.openssl.org, www.openssl.org/related/binaries.html). Adresář uložení programů "certutil", "OpenSSL" musí být uveden v cestě pro vyhledávání spustitelných programů (parametr "PATH" v systému) nebo tyto programy musí být spuštěny přímo z adresáře, kde jsou nainstalovány.

a) Postup na PC s nainstalovaným programem certutil (exportovaný klíč a certifikát se nacházejí v souboru mycert.pfx):

Spustit na příkazovém řádku Windows příkaz:

```
certutil -user -csp "Název CSP" -importpfx mycert.pfx
```

b) Postup na PC s nainstalovaným programem OpenSSL (exportovaný klíč a certifikát se nacházejí v souboru mycert.pfx):

- na příkazovém řádku Windows spustit příkazy:

```
openssl pkcs12 -in mycert.pfx -out tmp.pem  
openssl pkcs12 -export -in tmp.pem -out mycert.pfx -CSP "Název CSP"
```

- naimportovat soubor mycert.pfx do Windows např. "doubleclickem" na souboru mycert.pfx, nebo spuštěním příkazu z příkazového řádku:

```
mycert.pfx
```

Název CSP

pro Windows XP SP3:

"Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)",

pro Windows Vista a Windows 7:

"Microsoft Enhanced RSA and AES Cryptographic Provider"

4. Certifikát a klíč na kartě/tokenu

V případě technických problémů je potřeba kontaktovat dodavatele karet/tokenů.