

SignerApplet

applet pro elektronický podpis

uživatelská příručka, verze 1.4



2009
QCM, s.r.o.

Obsah

Úvod.....	3
Požadavky.....	3
Elektronický podpis.....	3
Certifikát v souboru.....	4
Podepisování velkého objemu dat.....	6
Nastavení Javy ve Windows.....	7
Nastavení Javy v Linuxu.....	8
Java console – informace při potížích.....	8
Otevření Java Console ve Windows.....	9
Otevření Java Console v Linuxu.....	9
Informace z Java Console.....	9
FAQ – často kladené dotazy.....	11

Úvod

Podepsání dat elektronickým podpisem slouží k elektronickému ověření totožnosti odesílatele. K tomu je potřeba mít platný a správně nainstalovaný kvalifikovaný certifikát, případně mít certifikát uložen v souboru P12 nebo PFX.

Požadavky

Pro práci s appletem pro elektronický podpis je potřeba mít v prohlížeči nainstalovánu a povolenu **Java verze 1.5, doporučujeme vyšší** (test můžete provést např. na stránkách <http://java.com/en/download/installed.jsp> – tlačítko **Verify Java Version**; stažení nejnovější verze je k dispozici na adrese <http://www.java.com>).

Aby se v appletu zobrazovaly certifikáty nainstalované v systému Windows, je nutná Java 1.6 či novější.

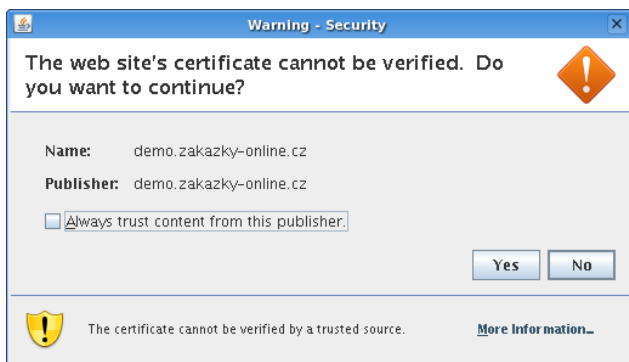
Elektronický podpis

Podepisování je realizováno appletem „Signer“, jehož grafické rozhraní vidíte na obrázku 3 (blok s tlačítkem **Podepsat**).

Při prvním načtení stránky s podepisovacím appletem (v rámci jednoho spuštění prohlížeče) je potřeba nejprve povolit spuštění appletu (jedná se o aplikaci pro internetové stránky) a to kliknutím na tlačítko **Run** v dialogu z obrázku 2. Pokud zaškrtnete volbu „Always trust content from this publisher“, nebudete již příště dotazováni na povolení spuštění appletu.

V případě, že je applet použit na zabezpečených (šifrovaných) stránkách, můžete být dotázáni na povolení přístupu na tyto stránky – viz dialog z obrázku 1. V tomto případě klikněte na **Yes**.

První spuštění podepisovacího appletu může nějakou dobu trvat – nejprve se totiž musí v prohlížeči/systému spustit samotná Java. Další načtení appletu v rámci jednoho spuštění prohlížeče je již podstatně rychlejší.



Obrázek 1: Dialog pro povolení přístupu na zašifrovanou stránku (https)

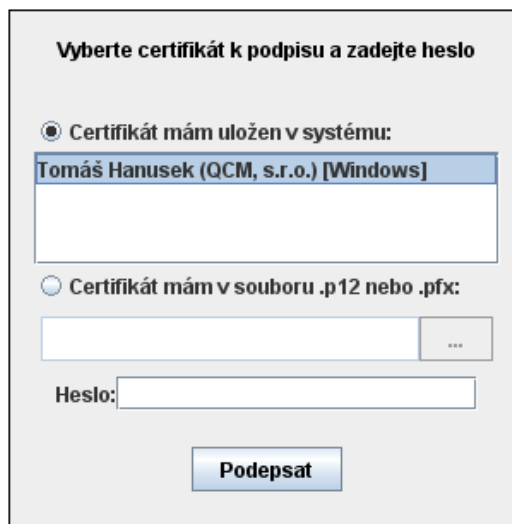


Obrázek 2: Dialog pro povolení spuštění nástroje (appletu) elektronického podpisu

Jestliže máte certifikáty nainstalovány v systému, objeví se jejich seznam v boxu appletu pod přepínačem *Certifikát mám uložen v systému*. **Tato funkce je podporována až s Javou verze 1.6.** Na požadovaný certifikát musíte pro jeho použití nejprve kliknout.

Jestliže je tento seznam prázdný, nebo neobsahuje certifikát vhodný pro podepisování v nástroji E-ZAK, můžete použít certifikát uložený v souboru – v tom případě použijte přepínač *Certifikát mám v souboru...* a tento soubor nastavte pomocí tlačítka „...“ (objeví se dialog z obrázku 11). Musíte také zadat *Heslo* k tomuto certifikátu v souboru. Podporovány jsou certifikáty v souborech typu P12 (resp. PKCS12) a PFX.

Po výběru certifikátu (a případně zadání hesla) použijte tlačítko **Podepsat**.

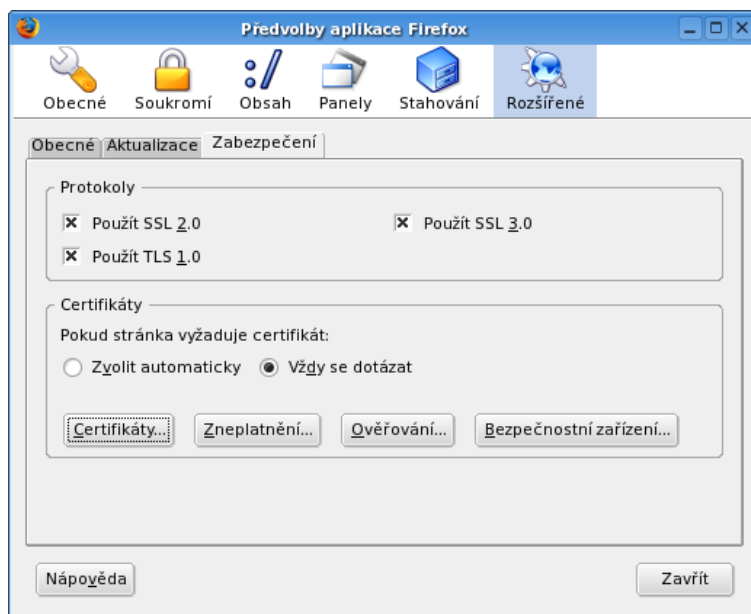


Obrázek 3: Applet pro elektronický podpis

Certifikát v souboru

Jestliže máte certifikát nainstalován v prohlížeči, nikoli však v systému, a není tudíž zobrazen v appletu, nebo máte starší verzi Javy, která nepodporuje přístup do systémového úložiště certifikátů, je potřeba certifikát nejprve uložit do souboru typu PK12 nebo PFX a ten poté nastavit v appletu spolu s heslem.

V případě prohlížeče Firefox najdete nainstalované certifikáty v nastavení (z menu prohlížeče vyberte *Úpravy*→*Předvolby* nebo *Nástroje*→*Možnosti* podle verze), zobrazí se konfigurační nástroj jako na obrázku 4. Zde v sekci *Rozšířené* na záložce *Zabezpečení* použijte tlačítko **Certifikáty**. Tím se zobrazí seznam certifikátů nainstalovaných v prohlížeči a to podle typu rozříděných do záložek **Osobní certifikáty**, **Servery** aj. Vyberte prvně jmenovanou záložku **Osobní**, označte požadovaný certifikát a stiskněte tlačítko **Zálohovat**. Zadejte název souboru, umístění a poté heslo k souboru s certifikátem. Jelikož se do souboru ukládá spolu s certifikátem také váš privátní klíč, je potřeba si tento soubor dobře chránit – jednak použít silné heslo a dále mít soubor uložen na bezpečném místě.

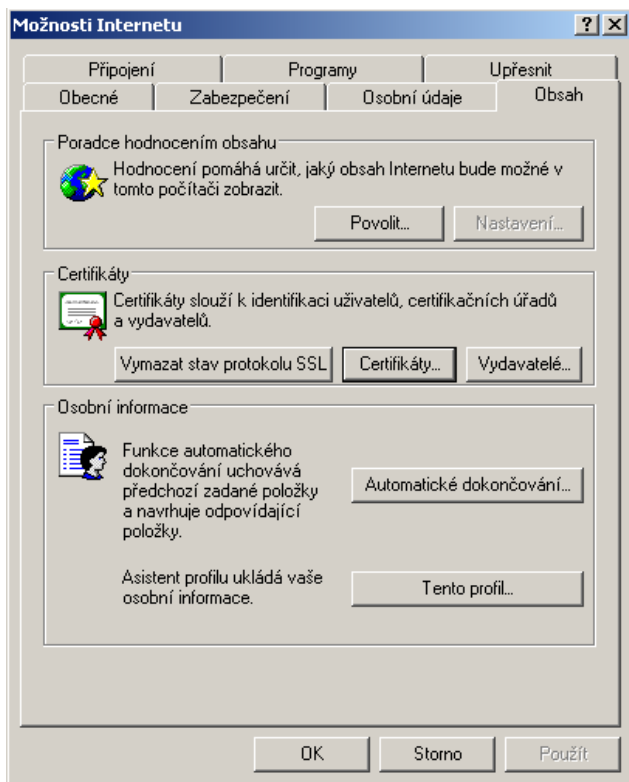


Obrázek 4: Správa certifikátů v prohlížeči Firefox (verze 1.5.0.7)

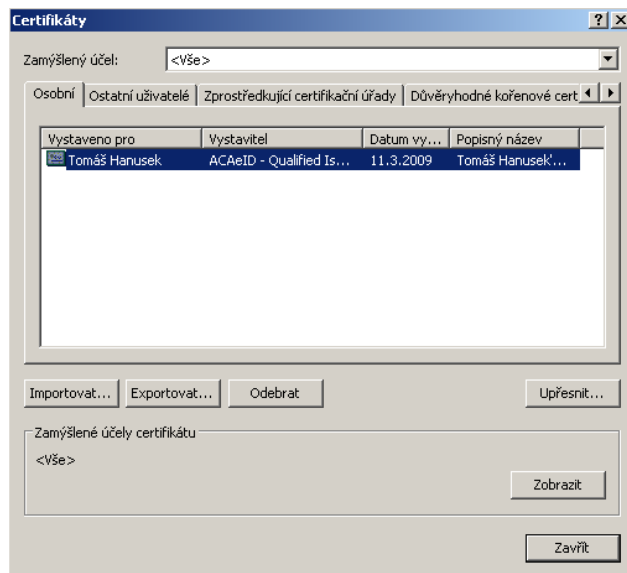
V případě Microsoft Internet Exploreru použijte v menu *Nástroje*→*Možnosti Internetu*, v

konfiguračním nástroji z obrázku 5 zvolte záložku *Obsah* a v sekci *Certifikáty* pak stejnojmenné tlačítko. Certifikáty jsou opět rozděleny do několika záložek, pro nás je podstatný obsah záložky **Osobní**. K zálohování/exportu certifikátu použijte tlačítko **Exportovat**, vyberte možnost „Ano, exportovat soukromý klíč“, zadejte heslo a dále umístění a název souboru (certifikát s klíčem bude uložen do souboru typu PFX).

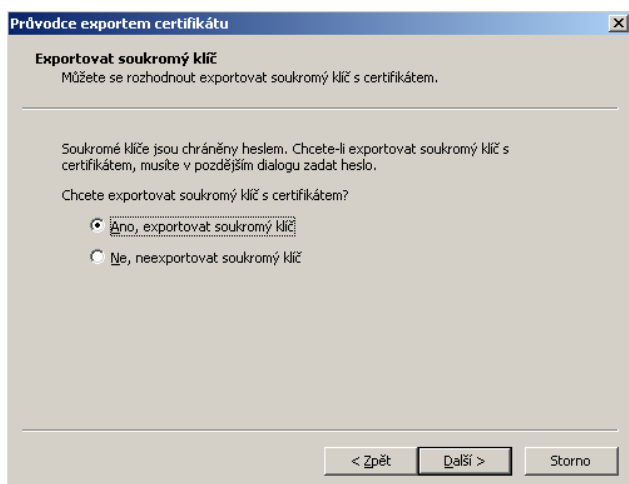
Postup exportu certifikátu v MSIE po jednotlivých krocích zachycují následující obrázky.



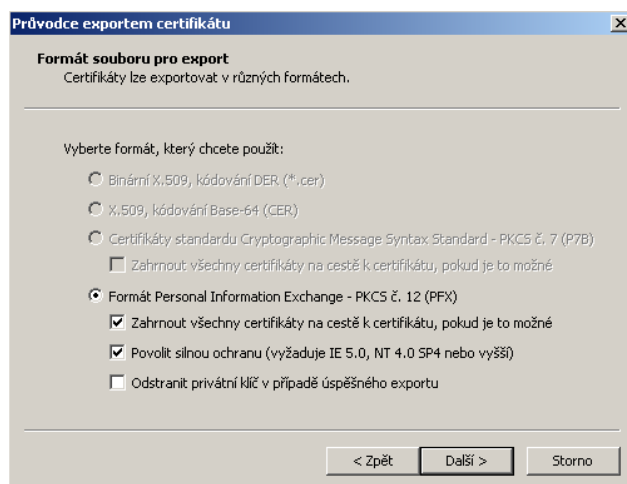
Obrázek 5: Správa certifikátů v MS Internet Exploreru



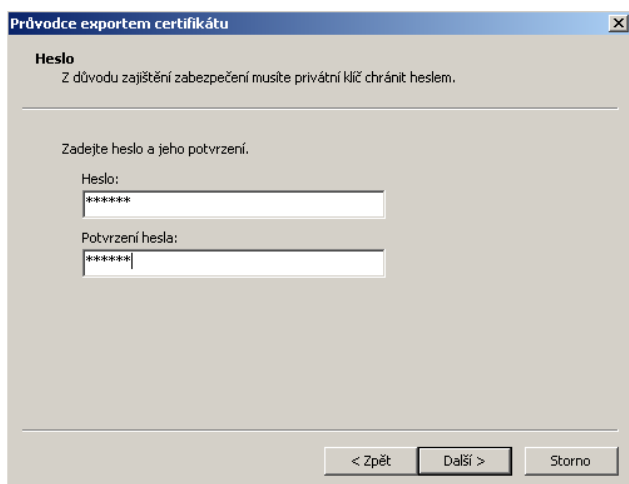
Obrázek 6: Výběr certifikátu k exportu



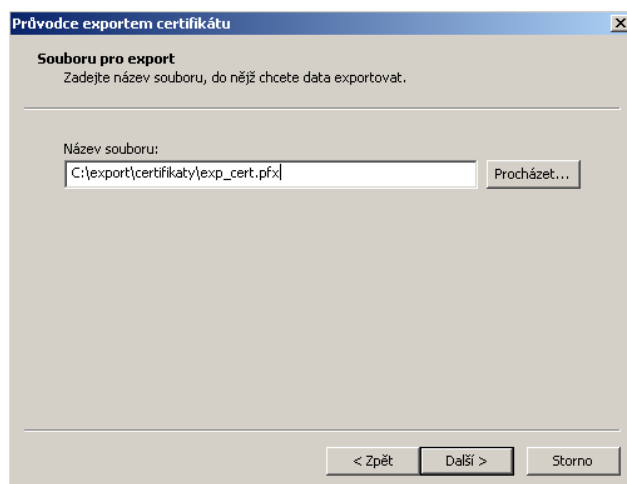
Obrázek 7: Volba exportu soukromého klíče – pokud vám tato možnost není nabídnuta, byl certifikát elektronického podpisu nainstalován do systému/prohlížeče bez možnosti exportu soukromého klíče – v tom případě exportovaný certifikát nebude v E-ZAKu použitelný



Obrázek 8: Do exportovaného certifikátu je nutné zahrnout všechny certifikáty na cestě k certifikátu, jinak exportovaný certifikát nebude v E-ZAKu použitelný

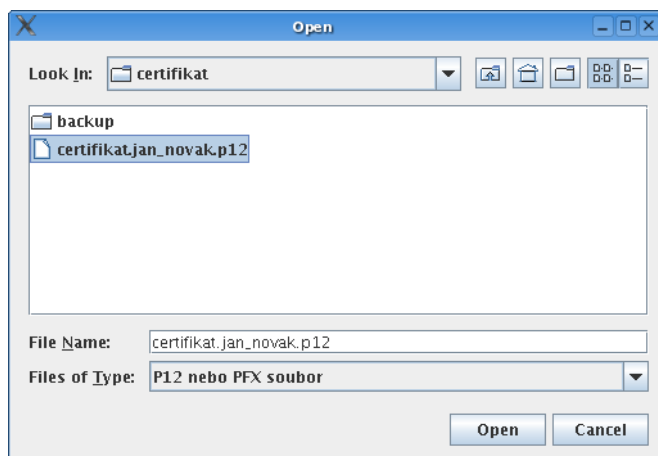


Obrázek 9: Certifikát s exportovaným soukromým klíčem je nutno chránit bezpečným heslem



Obrázek 10: V posledním kroku nastavte umístění a název exportovaného certifikátu

Po úspěšném vyexportování certifikátu do souboru (P12 či PFX) je možné tento soubor nastavit v podepisovacím appletu a zadat *Heslo*, které jste uvedli při exportu/zálohování certifikátu.



Obrázek 11: Dialog pro výběr souboru obsahujícího certifikát elektronického podpisu

K 1.12.2007 vydávali kvalifikované certifikáty 3 kvalifikovaní poskytovatelé certifikačních služeb:

- Česká pošta, s.p. (<http://qca.postsignum.cz>)
- eIdentity, a.s. (<http://www.eidentity.cz>)
- První certifikační autorita, a.s. (<http://www.ica.cz>)

Aktuální seznam naleznete na stránkách <http://www.mvcr.cz>

Podpisování velkého objemu dat

V případě podepisování dat o značném objemu (řádově megabajty) může dojít k situaci, že podepisovací applet přestane reagovat (při hlášení „Podepisuji“), neboť vyčerpá veškerou paměť, která je Javě v prohlížeči přidělena. V takovém případě je potřeba v prohlížeči zvětšit paměť pro Javu, viz dále.

Samotné podepisování je otázkou několika vteřin, avšak přenos velkého objemu dat mezi prohlížečem a serverem může trvat i delší dobu v závislosti na rychlosti vašeho připojení k internetu. Např. přenos 10 MB dat při rychlosti připojení 1 Mbit/sec (rychlost pro UPLOAD DAT!) může trvat i 10 minut. Po celou tuto dobu applet vypisuje „Požadavek podepsán, přenáším data“. Vyčkejte, dokud se přenos

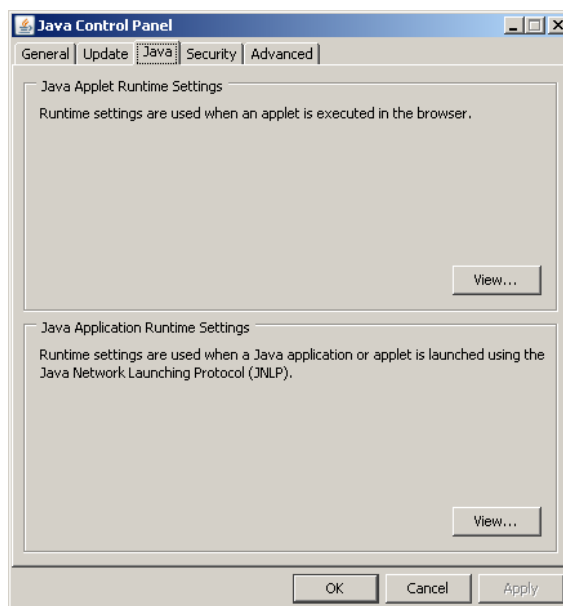
nedokončí.

Nastavení Javy ve Windows

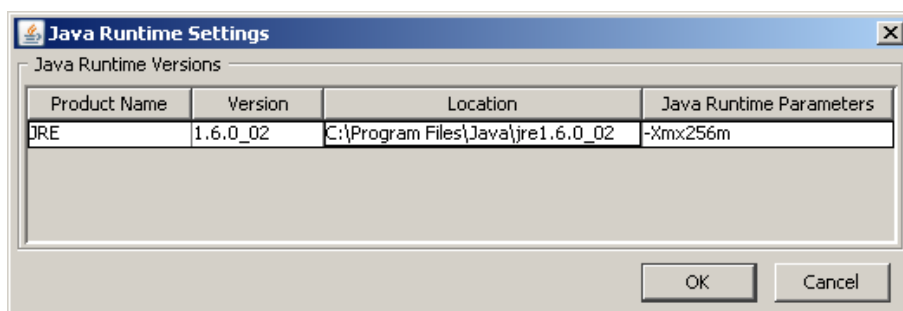
Otevřete kontrolní panel Javy – pokud je Java spuštěna, pak v systémové liště (system tray) klikněte pravým tlačítkem myši na ikonku Javy a zvolte „Open Control Panel“; jinak přes Nastavení systému v Ovládacích panelech poklikejte na ikonku Java.

Otevře se vám dialog jako na obrázku 12. Vyberte záložku *Java* a v bloku *Java Applet Runtime Settings* klikněte na tlačítko *View...* Tím se otevře tabulka z obrázku 13.

Pro vámi používanou verzi Javy v posledním sloupci *Java Runtime Parameters* nastavte parametr např. „-Xmx256m“ pro maximální paměť pro Javu 256 MB. Můžete přidat též parametr např. „Xms64m“ pro nastavení 64 MB paměti jako výchozí pro Javu.



Obrázek 12: Dialog nástroje jcontrol ve Windows

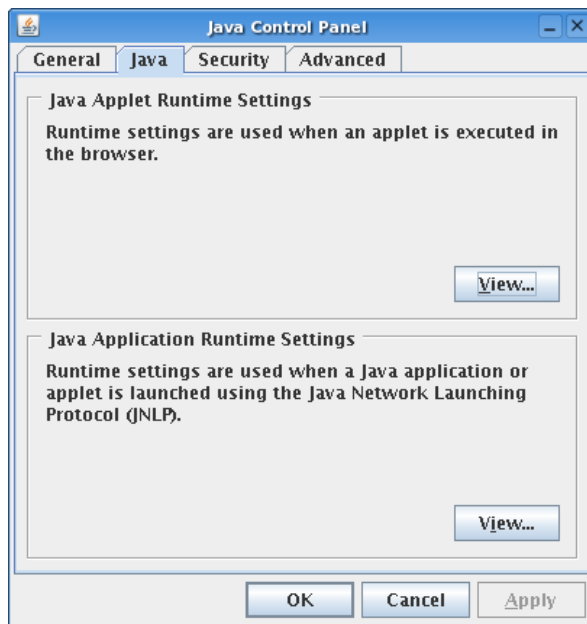


Obrázek 13: Nastavení parametrů pro applety spouštěné v Javě

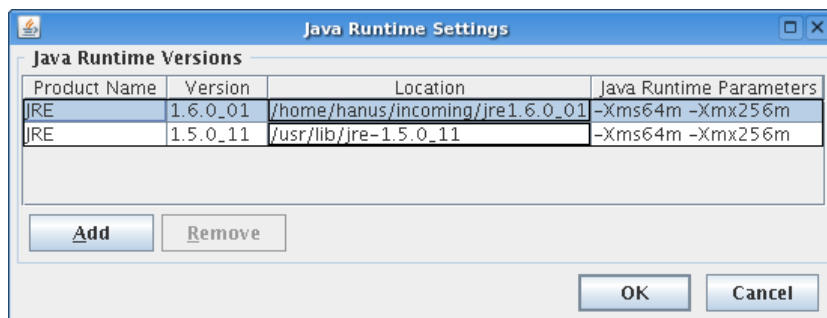
Aby změna nastavení začala fungovat, je nutné zavřít všechna okna prohlížeče a spustit jej znovu (restart prohlížeče). Dostupné množství paměti pro Javu si můžete ověřit např. na stránce <http://www.duckware.com/support/javahelp.html>.

Nastavení Javy v Linuxu

Spusťte nástroj `jcontrol` pro nastavení parametrů Javy (pokud ho nenajdete v menu vašeho systému, použijte stejnojmenný příkaz v příkazové řádce v konzoli/emulátoru terminálu). Otevře se vám dialog jako na obrázku 14. Vyberte záložku *Java* a v bloku *Java Applet Runtime Settings* klikněte na tlačítko *View...* Tím se otevře tabulka z obrázku 15, která bude pravděpodobně prázdná.



Obrázek 14: Dialog nástroje jcontrol v Linuxu



Obrázek 15: Nastavení parametrů pro applety spouštěné v Javě

Pomocí *Add* přidejte záznam pro vámi používanou verzi Javy, kdy v posledním sloupci *Java Runtime Parameters* nastavte parametr např. „-Xmx256m“ pro maximální paměť pro Javu 256 MB. Můžete přidat též parametr např. „-Xms64m“ pro nastavení 64 MB paměti jako výchozí pro Javu.

Aby změna nastavení začala fungovat, je nutné zavřít všechna okna prohlížeče a spustit jej znovu (restart prohlížeče). Dostupné množství paměti pro Javu si můžete ověřit např. na stránce <http://www.duckware.com/support/javahelp.html>.

Nastavení platí pouze pro uživatele, pod jehož účtem jste spustili aplikaci `jcontrol`!

Java console – informace při potížích

V případě, že podepisovací applet nereaguje delší dobu (řádově minuty), je potřeba zjistit proč. K tomu slouží tzv. *Java Console*, do níž vypisují chybová hlášení spuštěné java applety. Jedná se zejména o případy, kdy podepisovací applet zůstane v nečinném stavu s hlášením jako je:

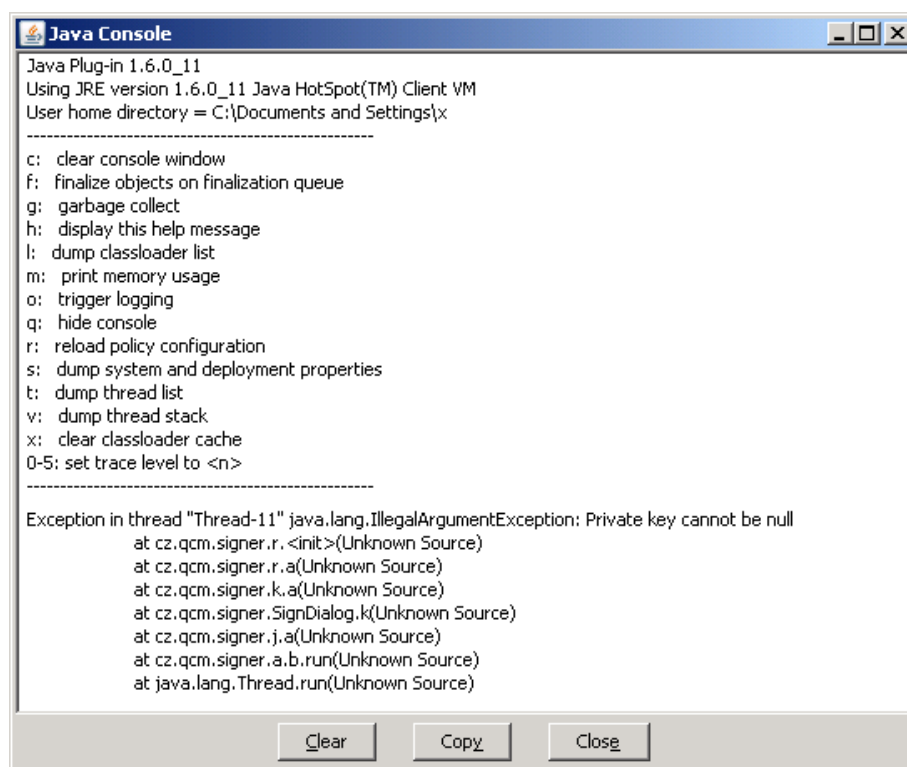
- Načítám certifikát
- Podepisuji

Otevření Java Console ve Windows

V systému Windows se po spuštění java appletu v prohlížeči objeví v systémové části dolního panelu ikonka javy vzhledem připomínající šálek kouřící kávy. Po kliknutí pravým tlačítkem myši na tuto ikonku se otevře kontextové menu, viz obrázek 16. Z nabídnutých položek vyberte „Open X.Y.Z Console“ (X.Y.Z představuje číslo verze nainstalované javy, kterou používá prohlížeč), čímž vyvoláte okno java konzoly, viz obrázek 17.



Obrázek 16: Otevření Java Console pomocí ikonky ze systémové části dolního panelu



Obrázek 17: okno Java Console

Dále přejděte na kapitolu „[Informace z Java Console](#)“.

Otevření Java Console v Linuxu

V Linuxu se Java Console otevírá přímo z menu prohlížeče, záleží tedy na jednotlivých prohlížečích, kde v menu ji naleznete. Např. ve Firefoxu je to *Nástroje*→*Java Console*, v Galeonu *WWW*→*Java konzole*, v Opeře pak *Nástroje*→*Rozšířené*→*Java console*.

Dále přejděte na kapitolu „[Informace z Java Console](#)“.

Informace z Java Console

V java konzoli jsou obvykle na začátku zobrazeny informace o verzi javy a seznam klávesových zkratk. Pod nimi se pak zobrazují jednotlivé výpisy. Následující seznam uvádí chybová hlášení, která mohou souviset s podepisovacím appletem:

- **Exception in thread "Thread-11" java.lang.IllegalArgumentException: Private key cannot be null** – certifikát použitý k podpisu neobsahuje privátní klíč; nejedná se o správný certifikát určený k podepisování, musíte vybrat jiný
- **Exception in thread "Thread-38" java.lang.OutOfMemoryError: Java heap space** – paměť přidělená javě v rámci vašeho prohlížeče byla vyčerpána; řešení viz kapitola „[Podepisování velkého objemu dat](#)“

FAQ – často kladené dotazy

Otázka

Nespustil se mi applet pro elektronický podpis (nenaběhl blok z obrázku [3](#)).

Odpověď

Důvodů může být několik:

- ▶ nemáte nainstalovány nebo povolenu Javu – viz kapitolu „[Požadavky](#)“
- ▶ máte nainstalovány starou verzi Javy – viz kapitolu „[Požadavky](#)“
- ▶ nepovolili jste spuštění appletu – pokud jste přihlášení v nějakých webových aplikacích, odhlaste se, zavřete všechna okna prohlížeče, spusťte znovu prohlížeč a přečtěte si úvod kapitoly „[Elektronický podpis](#)“

Otázka

Mám elektronický podpis, ale přesto se nemůžu zaregistrovat/podpis není akceptován.

Odpověď

Applet pracuje se zaručeným elektronickým podpisem založeným na **kvalifikovaném** certifikátu.

Tyto certifikáty v současné době vydávají v ČR pouze tři akreditované certifikační autority a pouze jejich kvalifikované certifikáty lze v systému E-ZAK používat:

- ▶ [PostSignum QCA - Česká pošta](#)
- ▶ [eIdentity](#)
- ▶ [První certifikační I.CA](#)

Otázka

Mám zaručený elektronický podpis založený na kvalifikovaném certifikátu, ale přesto nemůžu podepisovat. Podepisovací applet zůstane ve stavu „Načítám certifikát“.

Odpověď

Certifikát elektronického podpisu musí být do prohlížeče/systému nainstalován včetně soukromého (privátního) klíče. Takovéto certifikáty se v prohlížeči objeví v záložce *Osobní*, vizte obrázek [6](#), a jen tyto certifikáty lze použít k podepisování.

Certifikát použitý ze souboru musí rovněž obsahovat privátní klíč, vizte kapitolu [Certifikát v souboru](#).

Otázka

Mám kvalifikovaný certifikát od I.CA vydaný jako Twins, ale přesto se nemůžu zaregistrovat/podpis není akceptován.

Odpověď

Produkt Twins od I.CA představuje současné vydání komerčního i kvalifikovaného certifikátu. Pokud máte v systému zaregistrovány oba, je možné, že E-ZAK má přístup pouze ke komerčnímu certifikátu. Odeberte ze systému komerční certifikát a ponechte v systému pouze kvalifikovaný certifikát.

Otázka

Podepisovací applet hlásí "Chybně zadané heslo certifikátu"

Odpověď

Jestliže je Váš kvalifikovaný certifikát chráněn heslem, je potřeba ho zadat do pole "Heslo:" v podepisovacím appletu.

Pokud jste si jisti, že znáte správné heslo, avšak podepisovací applet hlásí chybné heslo, ujistěte se, že při jeho zadávání nezapisujete číslice pomocí klávesy SHIFT (v případě české klávesnice). Některé verze Javy s tímto mají potíže. Použijte numerickou oblast na klávesnici nebo se přepněte na anglickou klávesnici.

Otázka

Podepisovací java applet dlouho nereaguje, je v něm vypsáno „Podepisuji“.

Odpověď

Vizte kapitolu „[Podepisování velkého objemu dat](#)“.

Otázka

Podepisovací java applet dlouho nereaguje, je v něm vypsáno „Načítám certifikát“.

Odpověď

Vizte kapitolu „[Java console – informace při potížích](#)“.