SignerApplet

applet pro elektronický podpis

uživatelská příručka, verze 1.9

2011
QCM, s.r.o.

Obsah

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.

Rychlé odkazy

Informace o akceptovaných certifikátech elektronického podpisu najdete v kapitole „Akceptované certifikáty“.

Problémy při elektronickém podepisování jsou nejčastěji způsobeny nesprávnou nebo neúplnou instalací certifikátu elektronického podpisu. Jak ověřit správnost jeho instalace se dozvíte v kapitole „Kontrola správnosti instalace certifikátu“.

Přehled chybových hlášení při podepisování uvádí kapitola „Chybová hlášení při podepsání“.

Odpovědi na často kladené otázky naleznete v kapitole „FAQ – často kladené dotazy“.

Požadavky na systém

Pro práci s appletem pro elektronický podpis je potřeba mít v prohlížeči nainstalovánu a povolenu **SUN(ORACLE) Javu verze 1.5, doporučujeme vyšší** (test můžete provést např. na stránce http://java.com/en/download/help/testvm.xml; 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.

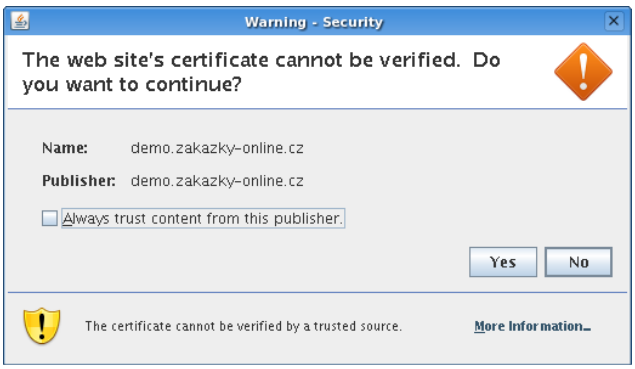
Elektronický podpis

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 stažení appletu z těchto stránek – vizte 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.



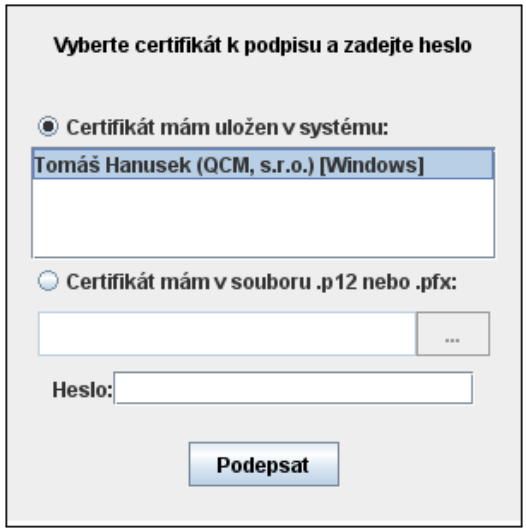
Obrázek 1: Dialog pro povolení přístupu na zašifrovanou stránku (https)

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 určený pro podepisování, 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 15). 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**.

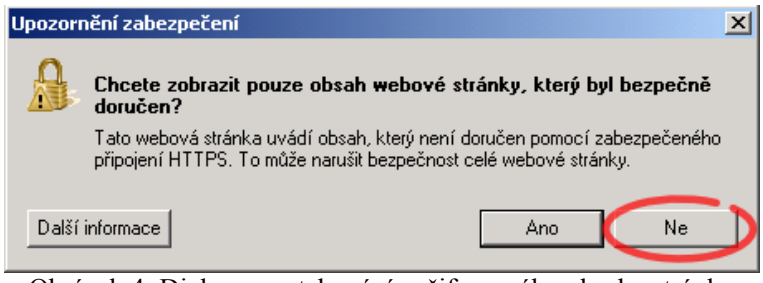


Obrázek 3: Applet pro elektronický podpis

Jestliže se vám nezobrazí java applet z obrázku 3, ani dialogy z obrázků 1 či 2, podívejte se do kapitoly „Povolení spuštění java appletu“.

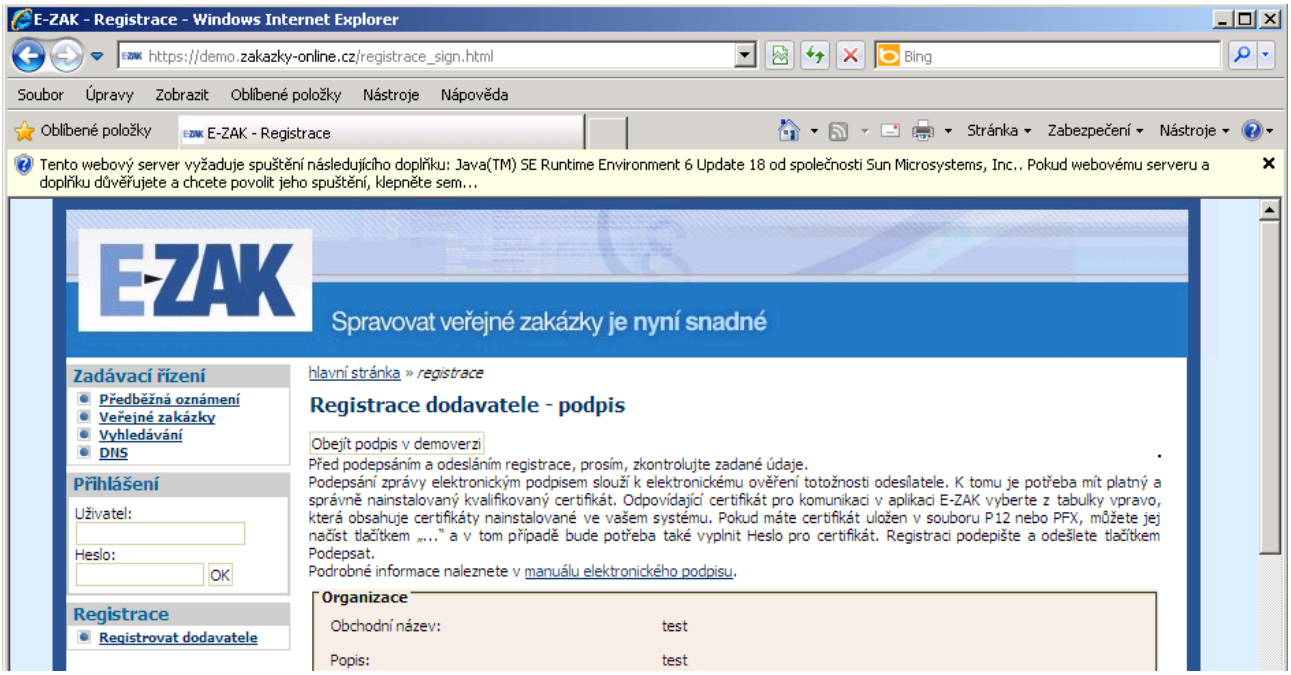
Povolení spuštění java appletu

Při přechodu na šifrovanou stránku můžete být prohlížečem dotázáni na zobrazení obsahu, který byl přenesen nešifrovaně, vizte obrázek 4. Pokud serveru důvěřujete, klikněte na Ne, jinak klikněte na Ano.



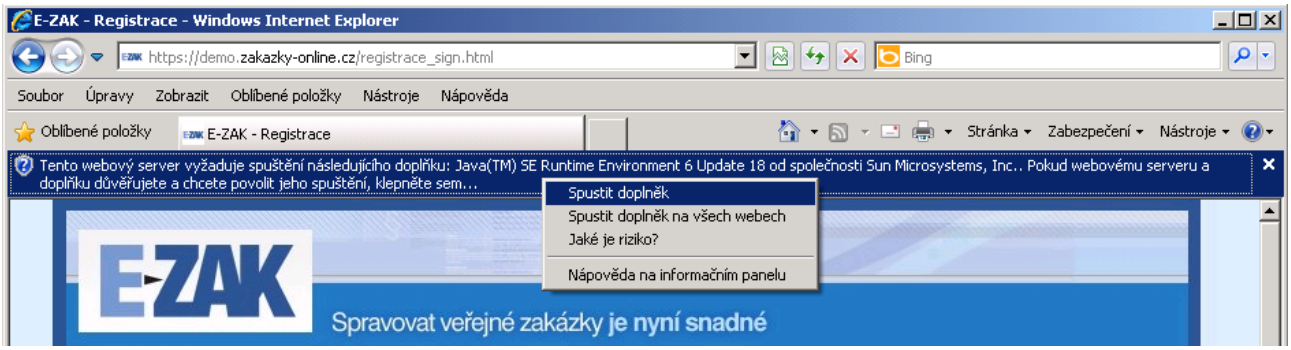
Obrázek 4: Dialog pro stahování nešifrovaného obsahu stránky

V závislosti na nastavení zabezpečení vašeho prohlížeče může být automatické spouštění java appletů a jiných aktivních prvků na stránkách blokováno. Na obrázku 5 je nad stránkou zobrazen žlutý pruh s upozorněním „*Tento webový server vyžaduje spuštění následujícího doplňku ...*“.



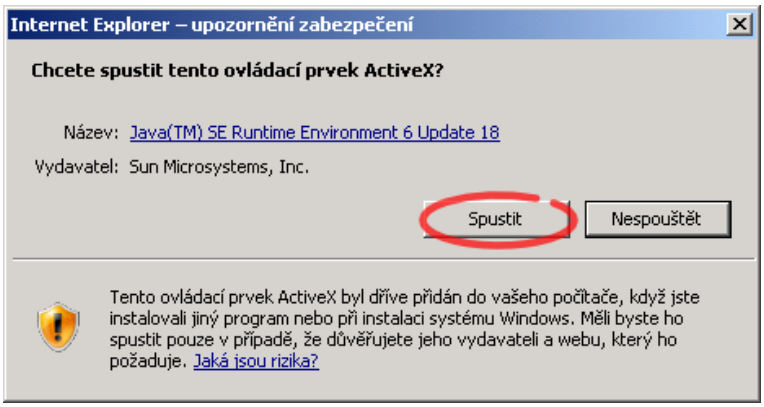
Obrázek 5: Upozornění Internet Exploreru 8 na požadavek spuštění doplňku – java appletu.

Pro spuštění podepisovacího java appletu v Internet Exploreru je nutné na tento pruh kliknout levým tlačítkem myši a ve zobrazeném menu vybrat položku „Spustit doplněk“ nebo „Spustit doplněk na všech webech“, vizte obrázek 6.



Obrázek 6: Povolení spuštění doplňku v MS IE 8.

Internet Explorer poté zobrazí ještě jeden dialog pro potvrzení spuštění java appletu, vizte obrázek 7.



Obrázek 7: Dialog souhlasu se spuštěním aktivního prvku.

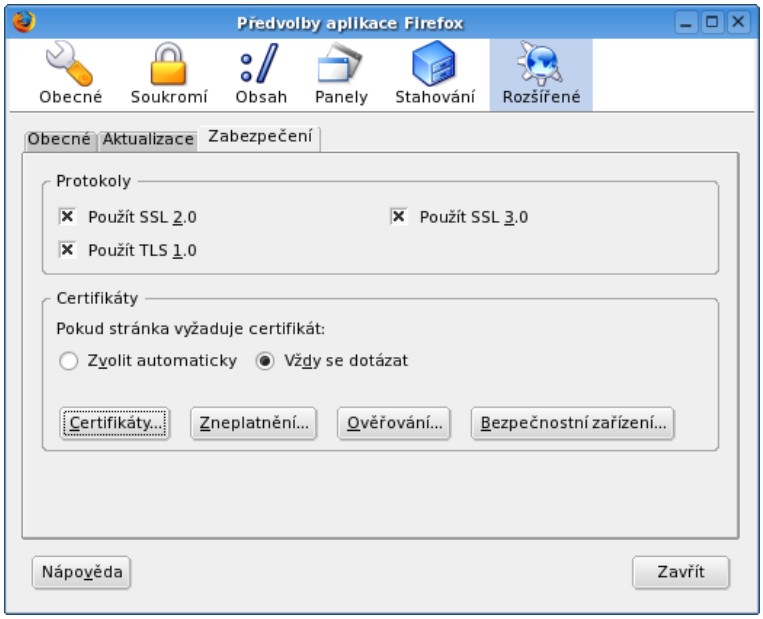
Pro danou verzi podepisovacího appletu je v daném prohlížeči nutné tuto operaci provést jen

jednou.

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.

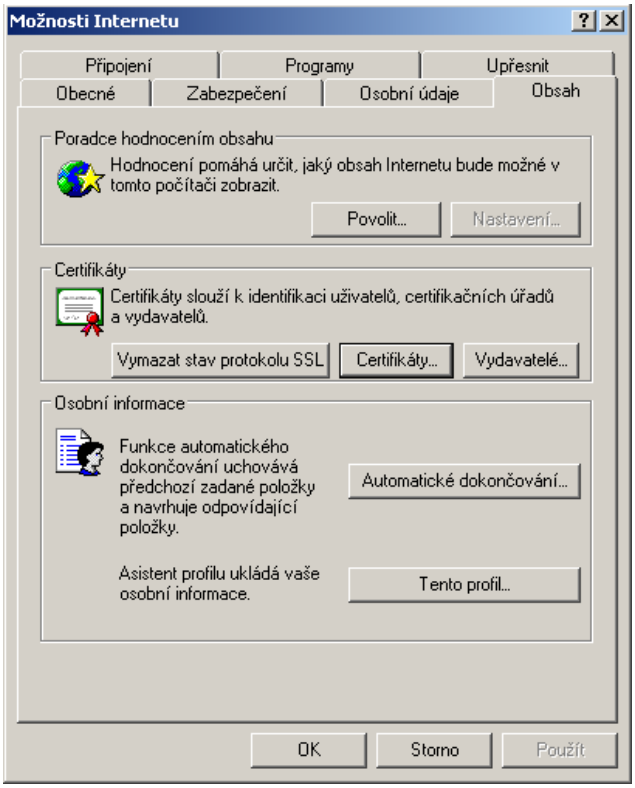
V případě prohlížeče Firefox najdete nainstalované certifikáty v nastavení (z menu prohlížeče vyberte *Úpravy→Předvolby* nebo *Nástroje→Možnosti* podle verze), zobrazí se konfigurační nástroj jako na obrázku 8. Zde v sekci *Rozšířené* na záložce *Zabezpečení* použijte tlačítko **Certifikáty**. Tím se zobrazí seznam certifikátů nainstalovaných v prohlížeči a to podle typu roztříděných 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.



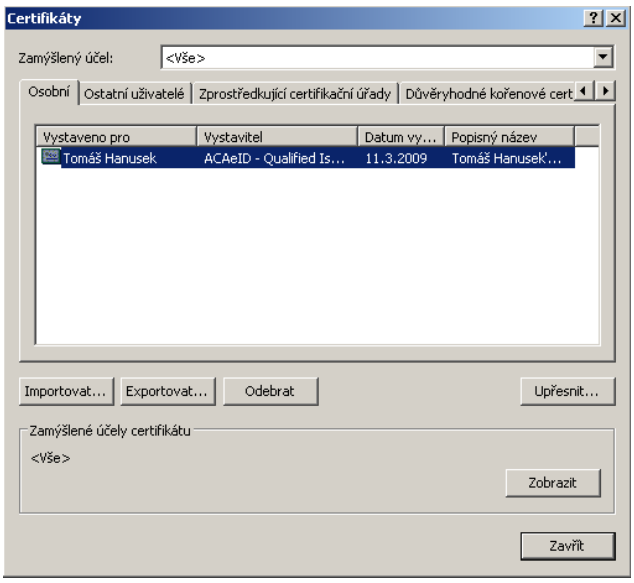
Obrázek 8: Správa certifikátů v prohlížeči Firefox (verze 1.5.0.7)

V případě Microsoft Internet Exploreru použijte v menu *Nástroje→Možnosti Internetu*, v konfiguračním nástroji z obrázku 9 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).

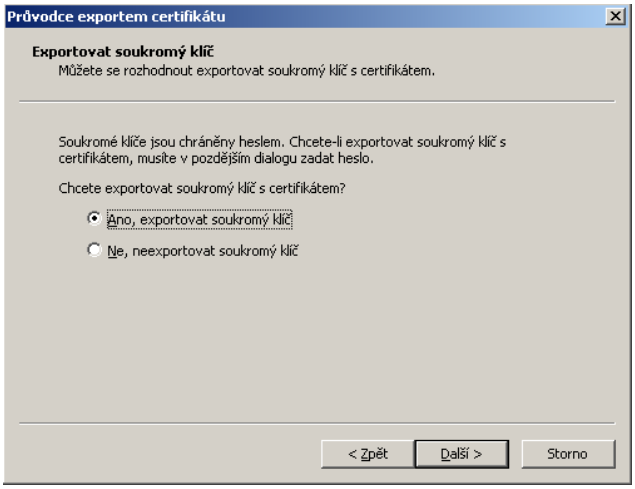
Postup exportu certifikátu v MSIE po jednotlivých krocích zachycují následující obrázky.



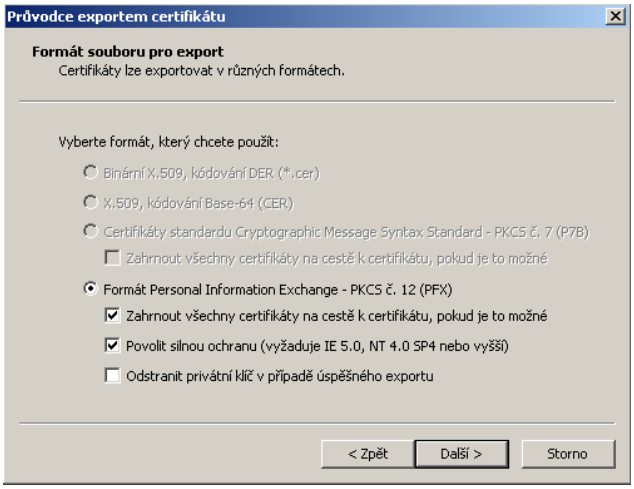
Obrázek 9: Správa certifikátů v MS Internet Exploreru



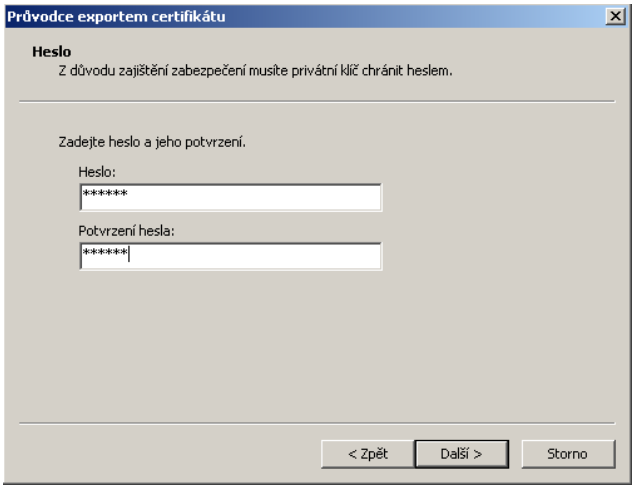
Obrázek 10: Výběr certifikátu k exportu



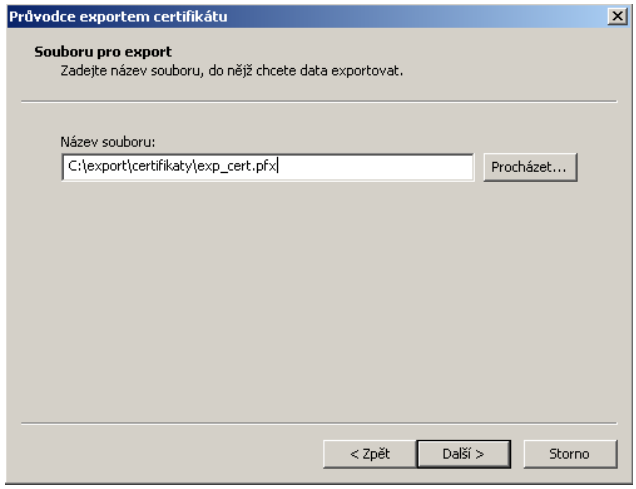
Obrázek 11: Volba exportu soukromého klíče – pokud vám tato možnost není nabídnuta, byl certifikát elektronického podpisu nainstalován do systému/prohlížeče bez možnosti exportu soukromého klíče – v tom případě exportovaný certifikát nebude v podepisovacím appletu použitelný



Obrázek 12: Do exportovaného certifikátu je nutné zahrnout všechny certifikáty na cestě k certifikátu, jinak exportovaný certifikát nebude v podepisovacím appletu použitelný

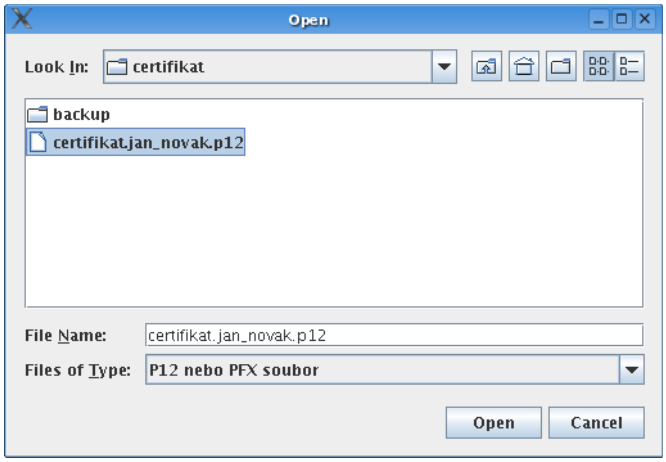


Obrázek 13: Certifikát s exportovaným soukromým klíčem je nutno chránit bezpečným heslem



Obrázek 14: 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 15: Dialog pro výběr souboru obsahujícího certifikát elektronického podpisu

Akceptované certifikáty

V souladu s právní úpravou je při podepisování vyžadován zaručený elektronický podpis založený na kvalifikovaném certifikátu. V době vydání této příručky vydávali kvalifikované certifikáty tři akreditovaní 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)

POZOR! V elektronickém nástroji E-ZAK nelze použít certifikáty umístěné na čipových kartách či tokenech.

Aktuální seznam akreditovaných certifikačních autorit naleznete na stránkách http://www.mvcr.cz.

Kontrola správnosti instalace certifikátu

Správně nainstalovaný kvalifikovaný certifikát, který je vyžadován podepisovacím appletem, obsahuje v certifikační cestě zpravidla další dva certifikáty (kromě vašeho certifikátu ještě dva

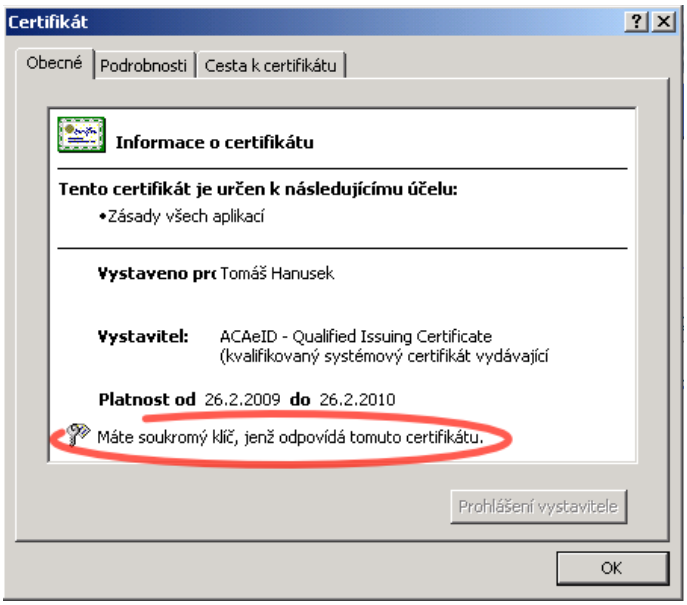
certifikáty vydávající autority – kořenový a kvalifikovaný) a váš certifikát je správně spojen s privátním klíčem.

Kontrolu těchto vlastností provedete na místě, kde jsou ukládány a zobrazovány certifikáty, tj. obvykle přes internetový prohlížeč, vizte též kapitolu „Certifikát v souboru“.

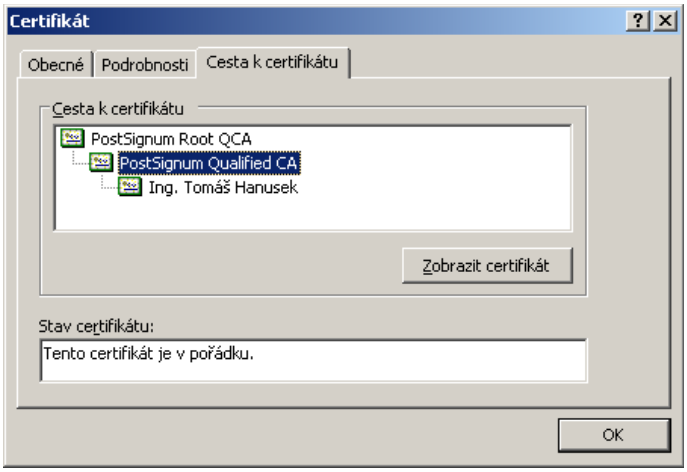
Obecný postup správné instalace certifikátu elektronického podpisu je následující:

1. import certifikátu, který vám byl vydán certifikační autoritou, do prohlížeče či nástroje, kde jste vygenerovali žádost o certifikát; jedině tak dojde ke správnému spojení privátního klíče s certifikátem,
2. import kořenových certifikátů autority vydávající kvalifikované certifikáty, vizte kapitolu „Akceptované certifikáty“; kořenové (angl. root) certifikáty naleznete na stránkách příslušné certifikační autority – hledejte stránky jako „certifikáty autorit“, „kořenové certifikáty“ apod. a na těchto stránkách pak certifikát kořenové certifikační autority a certifikát podřízené certifikační autority vydávající kvalifikované certifikáty.

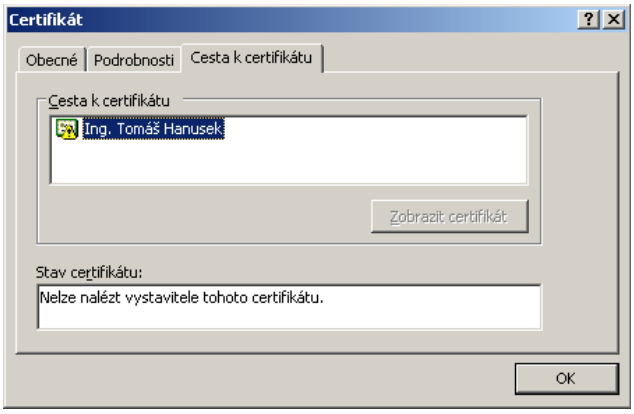
Ověření bodu 1 vidíte na obrázku 16, ověření bodu 2 pak na obrázku 17. V případě, že neprovedete správně a úplně postup uvedený v bodu 2 nebo naimportujete nesprávné kořenové certifikáty, bude výsledek obdobný obrázku 18 či 19.



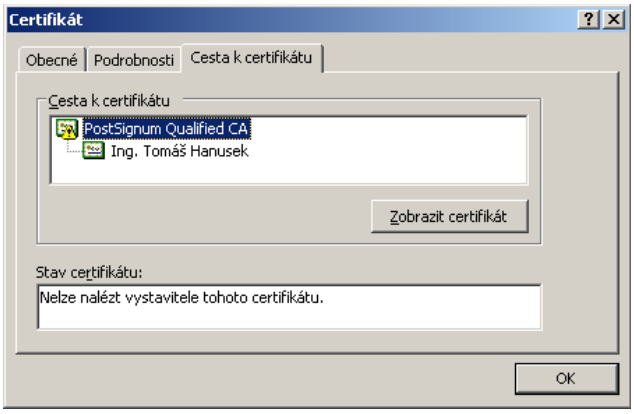
Obrázek 16: Informace, že certifikát má odpovídající soukromý klíč, MS Internet Explorer



Obrázek 17: Detail certifikátu s úplnou cestou k certifikátu, MS Internet Explorer



Obrázek 18: Neúplná certifikační cesta k certifikátu (chybí kořenový certifikát a certifikát vydávající autority), MS Internet Explorer



Obrázek 19: Neúplná certifikační cesta k certifikátu (chybí kořenový certifikát), MS Internet Explorer

Chybová hlášení po podepsání

V případě, že se během podepisování SignerApplet „zasekne“ a v jeho záhlaví zůstane vypsáno „Načítám certifikát“ nebo „Podepisuji“ nebo „Applet nemá práva“, podívejte se do kapitoly „Java console – informace při potížích“.

Po dokončení podepisování v prohlížeči jsou data ihned odeslána na server k okamžitému ověření platnosti podpisu. Výsledkem je buď úspěch a systém pokračuje v normální činnosti, nebo je podpis shledán neplatným a uživateli je zobrazeno některé z následujících chybových hlášení:

- *Certifikát elektronického podpisu není kvalifikovaný, nebo neobsahuje úplnou certifikační cestu. Prosím použijte správný certifikát. / Validation failed (...), The certification chain is too short. It should consist of at least 2 certiicates.* – certifikát není správně nainstalován, chybí certifikáty vydávající autority, vizte kapitolu „Kontrola správnosti instalace certifikátu“.
- *Použitý certifikát elektronického podpisu již vypršel. Prosím použijte platný certifikát / Validation failed (...), timestamp check failed* – použitý certifikát má již prošlou platnost.
- *Validation failed (...), Path does not chain with any of the trust anchors* – server nepřijímá certifikáty dané autority; pokud byl váš certifikát vydán některou z autorit uvedenou v kapitole „Akceptované certifikáty“, kontaktujte prosím provozovatele systému.

Podepisování 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, vizte dále.

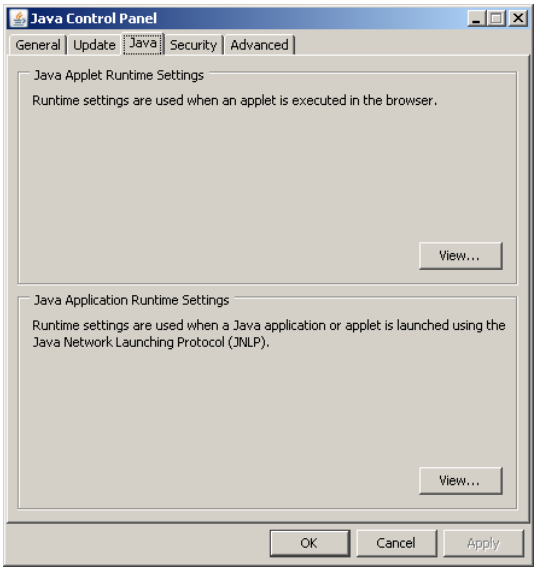
Samotné podepisování je otázkou několika vteřin, avšak přenos velkého objemu dat mezi prohlížečem a serverem může trvat i delší dobu v závislosti na rychlosti vašeho připojení k internetu. Např. přenos 10 MB dat při rychlosti připojení 1 Mbit/sec (rychlost pro UPLOAD DAT!) může trvat i 10 minut. Po celou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

Nastavení Javy ve Windows

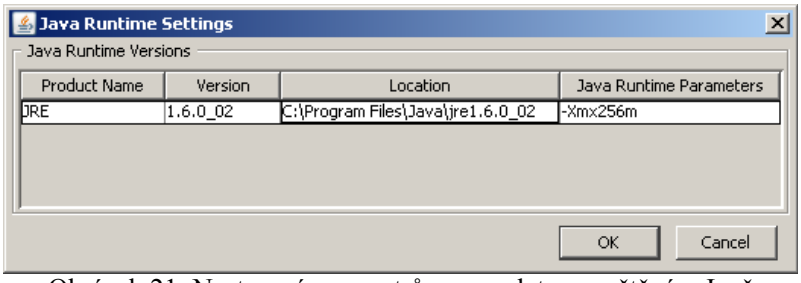
Otevřete kontrolní panel Javy – pokud je Java spuštěna, pak v systémové liště (system tray) klikněte pravým tlačítkem myši na ikonku Javy a zvolte „Open Control Panel“; jinak přes Nastavení systému v Ovládacích panelech poklikejte na ikonku Java.

Otevře se vám dialog jako na obrázku 20. Vyberte záložku *Java* a v bloku *Java Applet Runtime Settings* klikněte na tlačítko *View*... Tím se otevře tabulka z obrázku 21.

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 20: Dialog nástroje jcontrol ve Windows

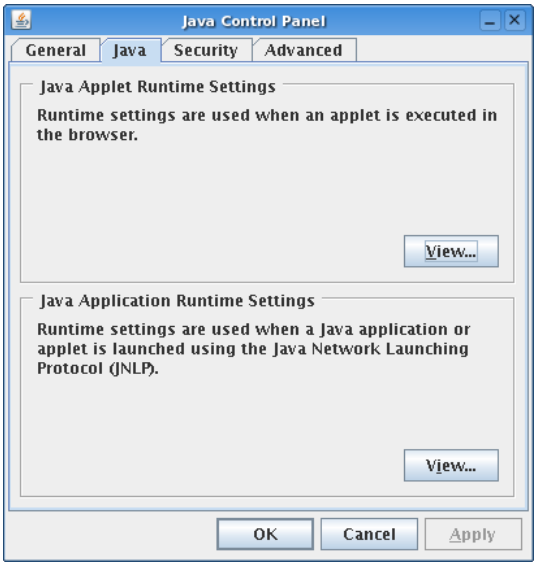


Obrázek 21: Nastavení parametrů pro applety spouštěné v Javě

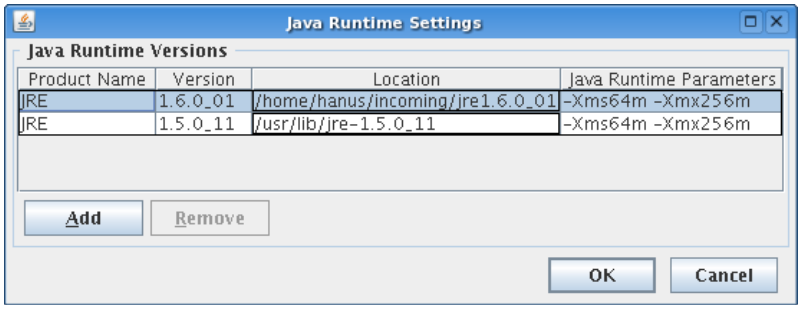
Aby změna nastavení začala fungovat, je nutné zavřít všechna okna prohlížeče a spustit jej znovu (restart prohlížeče). Dostupné množství paměti pro Javu si můžete ověřit např. na stránce http://www.duckware.com/support/javahelp.html.

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 22. Vyberte záložku *Java* a v bloku *Java Applet Runtime Settings* klikněte na tlačítko *View*... Tím se otevře tabulka z obrázku 23, která bude pravděpodobně prázdná.



Obrázek 22: Dialog nástroje jcontrol v Linuxu



Obrázek 23: 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`!

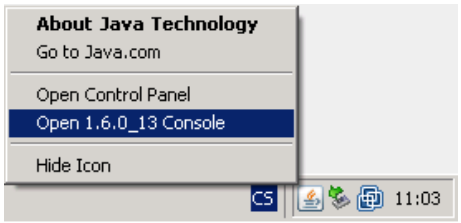
Java console – informace při potížích

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:

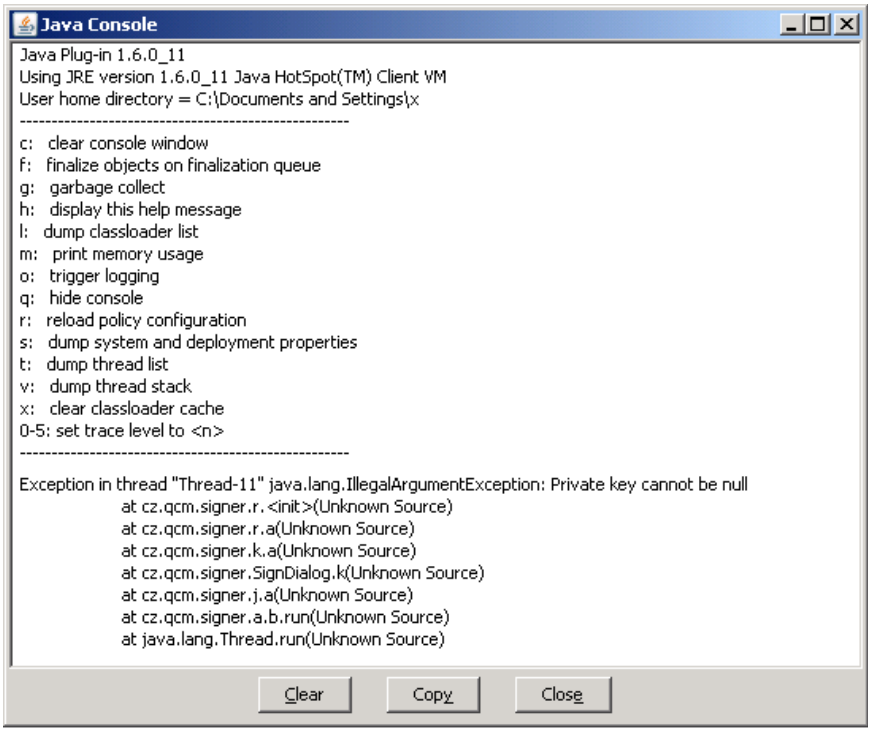
- Načítám certifikát
- Podepisuji
- Applet nemá práva

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, vizte obrázek 24. 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, vizte obrázek 25.



Obrázek 24: Otevření Java Console pomocí ikonky ze systémové části dolního panelu



Obrázek 25: 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 *Nástoje→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 zkratek. Pod nimi se pak zobrazují jednotlivé výpisy. Následující seznam uvádí chybová hlášení, která mohou souviset s podepisovacím appletem:

- **java.lang.IllegalArgumentException: Private key cannot be null** – certifikát použitý k podpisu neobsahuje privátní klíč; nejedná se o správný certifikát určený k podepisování – zkontrolujte správnost nainstalování certifikátu, vizte kapitolu „Kontrola správnosti instalace certifikátu“, nebo vyberte jiný certifikát k podepsání
- **java.lang.OutOfMemoryError: Java heap space** – paměť přidělená javě v rámci vašeho prohlížeče byla vyčerpána; pro řešení vizte kapitolu „Podepisování velkého objemu dat“
- **access denied (java.security.SecurityPermission putProviderProperty.XMLDSig)** – java applet nemá potřebná oprávnění, zkontrolujte instalaci javy používané v prohlížeči
- **failed to decrypt safe contents entry: java.io.IOException: getSecretKey failed: Password is not ASCII** – heslo k certifikátu v souboru nebo k úložišti certifikátů obsahuje znaky, které java neumí zpracovat, např. české znaky s diakritikou; změňte heslo, aby neobsahovalo takové znaky, popř. znovu vyexportujte certifikát do souboru a při zadávání hesla nepoužívejte takové znaky

V případě, že se v java consoli objeví **jiné** chybové hlášení, než jsou výše uvedená, zkopírujte

obsah konzole do e-mailu a zašlete ho na adresu podpora@qcm.cz spolu s informací, na které www adrese došlo k problému, jaký používáte prohlížeč a jeho verzi, jakou verzi javy používá prohlížeč a jaký operační systém a jeho verzi máte.

FAQ – často kladené dotazy

Otázka

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

Odpověď

Důvodů může být několik:

► nemáte nainstalovánu nebo povolenu Javu – vizte kapitolu „Požadavky na systém“

► máte nainstalovánu starou verzi Javy – vizte kapitolu „Požadavky na systém“

► nepovolili jste spuštění appletu – pokud jste přihlášeni 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. Podrobnosti naleznete v kapitole „Akceptované certifikáty“.

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 10, a jen tyto certifikáty lze použít k podepisování.

Certifikát použitý ze souboru musí rovněž obsahovat privátní klíč, vizte kapitolu Certifikát v souboru.

Podívejte se také do kapitoly „Kontrola správnosti instalace certifikátu“.

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 podepisovací applet 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 chlásí 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“.