Uživatelská příručka

ELEKTRONICKÝ PODPIS

Elektronický nástroj
pro zadávání veřejných zakázek

CENT

verze 1.1.

SIGENO
veřejné zakázky a dotace s.r.o.

2018
Osigeno – veřejné zakázky a dotace s.r.o.

1 OBSAH

2 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.

Informace o akceptovaných certifikátech elektronického podpisu naleznete 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 hlášeni při podepisování uvádí kapitola „Chybova hlášení při podepsání“.

3 POŽADAVKY NA SYSTÉM

Pro práci s appletem pro elektronický podpis je zapotřebí mít v prohlížeči nainstalovánu a povolenu Javu verze 1.7 (často označovaná jako Java 7), případně novější vydanou verzi. Test můžete provést např. na stránce https://www.java.com/en/download/installed8.jsp; stažení nejnovější verze je k dispozici na adrese http://www.java.com.

Aby se v appletu zobrazovaly certifikáty nainstalované v systému Windows, je nutná minimálně Java 1.7 a vyšší.

4 ELEKTRONICKÝ PODPIS

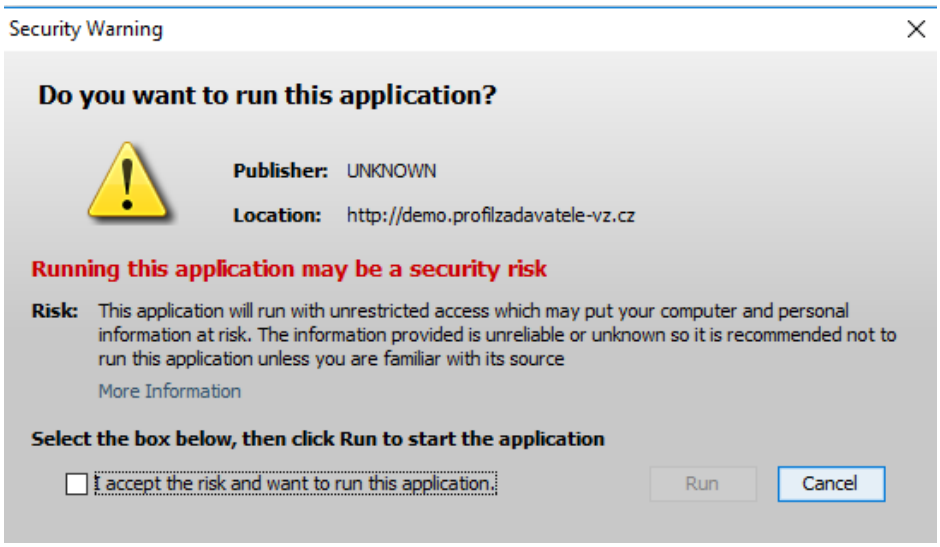
Podepisování je realizováno appletem „Signer“, jehož grafické rozhraní vidíte na obrázku č. 3 (blok s tlačítkem Podepsat).

Při prvním načtení stránky s podepisovacím appletem (v rámci jednoho spuštění prohlížeče) je zapotřebí nejdříve povolit spuštění appletu (jedná se o aplikaci pro internetové stránky) a to tak, že zaškrtnete volbu „accept the risk and want to run this app“ a následně kliknete na tlačítko Run v dialogu viz. obr. č. 2. Pokud zaškrtnete i volbu „do not show this again for this app“, nebudete již příště dotazováni na povolení spuštění appletu.

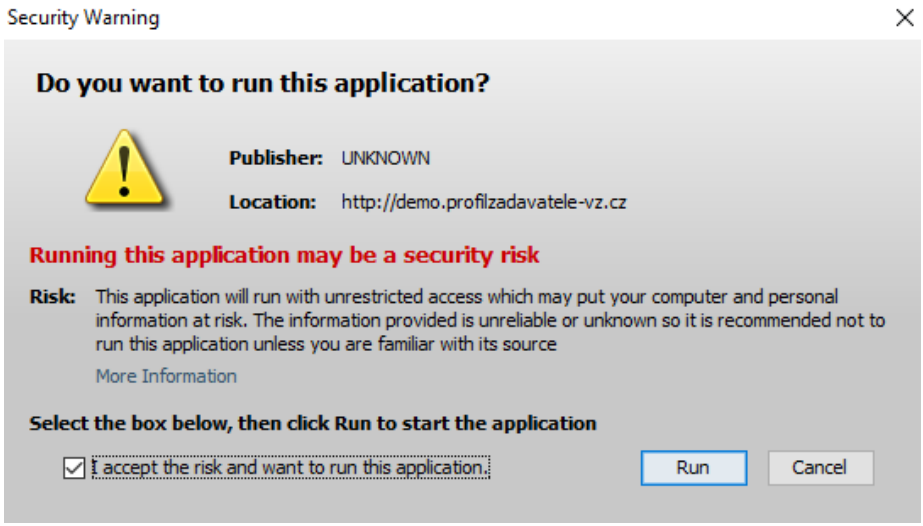
V případě, že je applet použit na zabezpečených (šifrovaných HTTPS) stránkách, můžete být dotázáni na povolení stažení appletu z těchto stránek – viz. obrázek č. 1. V tomto případě klikněte na Continue (kliknutím na Show Options se zobrazí ještě volba „Always trust connections to websites identified by

this certificate“, po jejímž zaškrtnutí již nebude příště toto upozornění zobrazováno).

Obrázek č. 1 - Dialog pro povolení přístupu na zašifrovanou stránku (https)

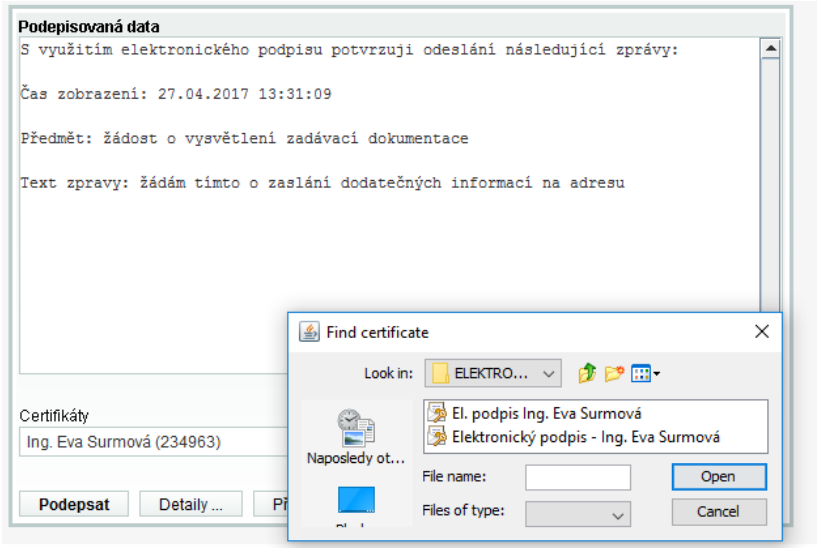


Obrázek č. 2 - Dialog pro povolení spuštění nástroje (appletu) elektronického podpisu



V některých případech můžete být zobrazeno ještě další bezpečnostní upozornění z následujícího obrázku – v daném případě klikněte na tlačítko Don‘t Block (Neblokovat).

Obrázek č. 3 - Applet pro elektronický podpis



Jestliže máte certifikáty nainstalovány v systému, objeví se jejich seznam v boxu appletu pod přepínačem Certifikát mám uložen v systému. ***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 na jakémkoli datovém úložišti** (externí disk Token) – v tom případě použijte přepínač Certifikát ze souboru... a tento soubor nastavte pomocí tlačítka „...“. Musíte také zadat Heslo k tomuto certifikátu v souboru. Podporovány jsou certifikáty v souborech typu P12 (resp. PKCS12) a PFX.

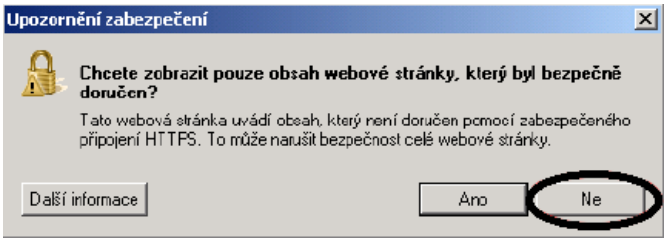
Po výběru certifikátu (a případně zadání hesla) použijte tlačítko Podepsat viz. obr. č. 3: Applet pro elektronický podpis

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

5 POVOLENÍ SPUŠTĚNÍ JAVA APPLETU

Při přechodu na šifrovanou stránku můžete být prohlížečem dotázáni na zobrazení (resp. Blokování) obsahu, který byl přenesen nešifrovaně, viz. obrázek č. 4. Pokud serveru důvěřujete, klikněte na Ne.

Obrázek č. 4 - Dialog pro stahování nešifrovaného obsahu stránky



V závislosti na nastavení zabezpečení Vašeho prohlížeče může být automatické spouštění javaappletů (resp. běhového prostředí Java SE Runtime Environment) a jiných aktivních prvků na stránkách blokováno.

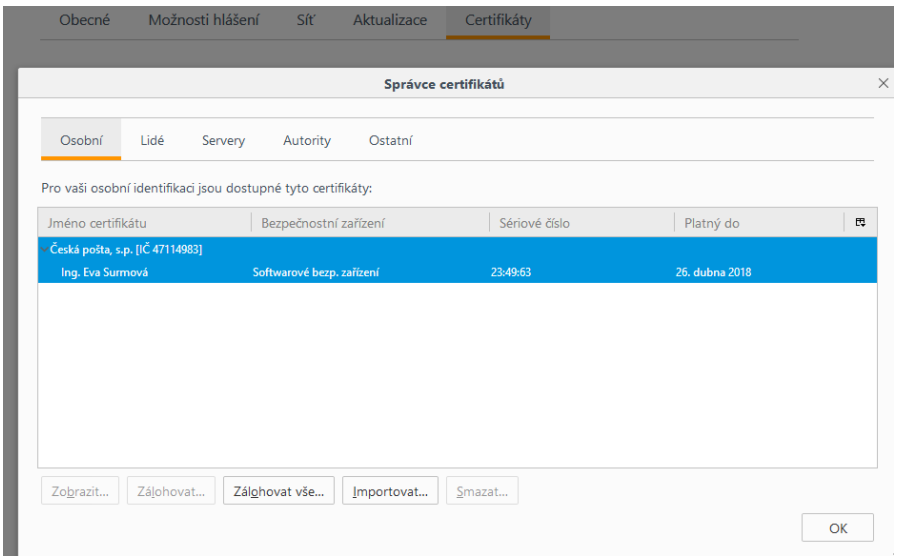
Pro spuštění podepisovacího java appletu v internetovém prohlížeči je nutné povolit tento doplněk pomocí tlačítka Povolit. Pro danou verzi podepisovacího appletu je v daném prohlížeči nutné tuto operaci provést jen jednou. V některých případech můžete být dotázáni, zda si přejete applet spustit v rámci novější (aktuální) verze javy, kterou máte v systému nainstalovánu, viz následující obrázek. V takovém případě klikněte na tlačítko Run with the latest version.

6 CERTIFIKÁT V SOUBORU

V případě, že 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 zapotřebí certifikát nejdříve 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 č. 5. Zde v sekci Rozšířené na záložce Šifrování 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.*

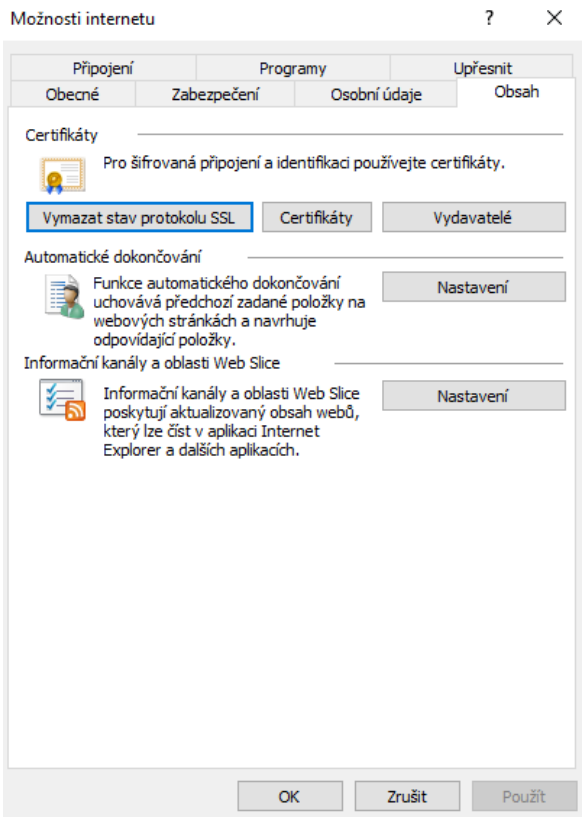
Obrázek č. 5 - Správa certifikátů v prohlížeči Firefox



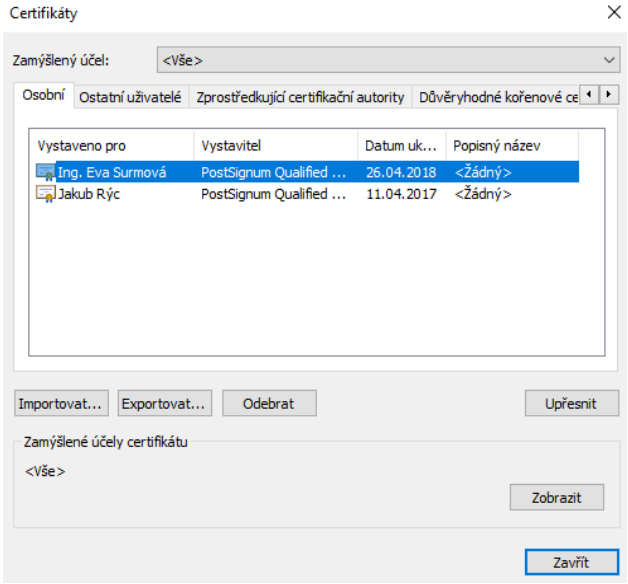
V případě Microsoft Internet Exploreru použijte v menu Nástroje→Možnosti Internetu, v konfiguračním nástroji z obrázku č. 6 zvolte záložku **Obsah** a v sekci **Certifikáty** pak stejnojmenné tlačítko. Certifikáty jsou opět rozděleny do několika záložek, pro nás je podstatný obsah záložky **Osobní**. 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 Microsoft Internet Exploreru po jednotlivých krocích zachycují následující obrázky č. 6 – 12.

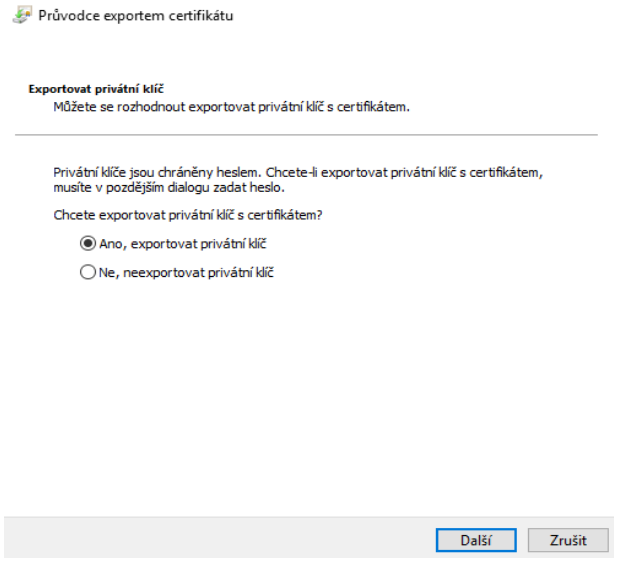
Obrázek č. 6 - Správa certifikátů v MS Internet Exploreru



Obrázek č. 7 - Výběr certifikátu k exportu

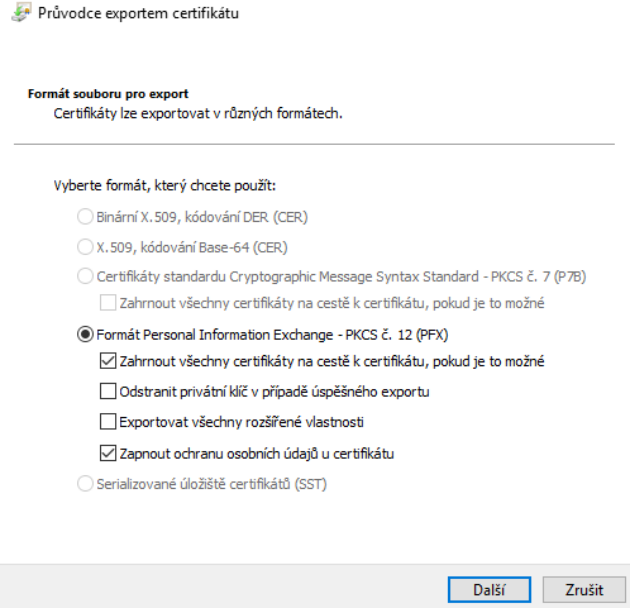


Obrázek č. 8 - Volba exportu soukromého klíče

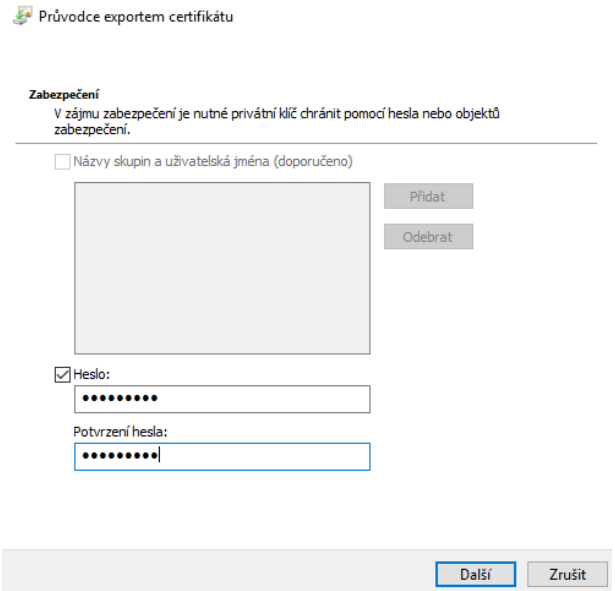


Pokud vám tato možnost není nabídnuta, byl certifikát elektronického podpisu nainstalován do systému/prohlížeče bez možnosti exportu soukromého klíče – v tom případě exportovaný certifikát nebude v CENTu použitelný!

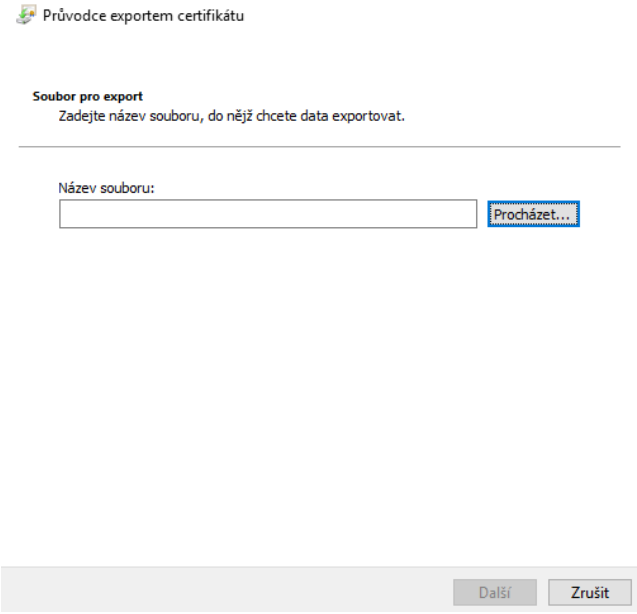
Obrázek č. 9 - Do exportovaného certifikátu je nutné zahrnout všechny certifikáty na cestě k certifikátu, jinak exportovaný certifikát nebude v CENTu použitelný



Obrázek č. 10 - Certifikát s exportovaným soukromým klíčem je nutno chránit bezpečným heslem

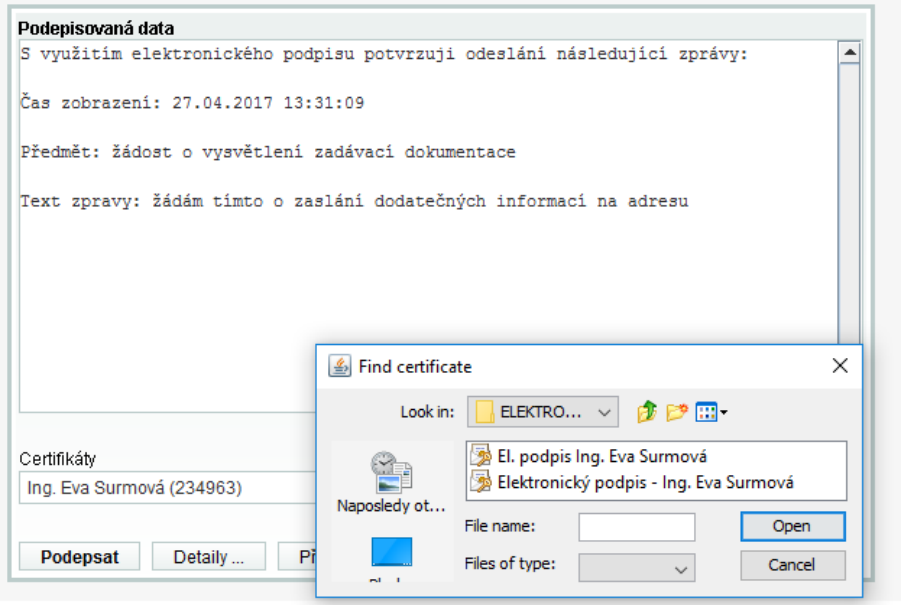


Obrázek č. 11 - V posledním kroku umístění a název exportovaného certifikátu



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 č. 12 - Dialog pro výběr souboru obsahujícího certifikát elektronického podpisu



7 AKCEPTOVATELNÉ CERTIFIKÁTY

V souladu s právní úpravou je vyžadováno podepisování zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu. K 1. 9. 2011 vydávali kvalifikované certifikáty 3 kvalifikovaní poskytovatelé certifikačních služeb:

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

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

8 KONTROLA SPRÁVNOSTI INSTALACE CERTIFIKÁTU

Správně nainstalovaný kvalifikovaný certifikát, který je vyžadován podepisovacím appletem, obsahuje v certifikační cestě zpravidla jeden až dva další certifikáty (kromě vašeho certifikátu ještě certifikát(y) vydávající autority – kořenové autority a popř. ještě kvalifikované vydávající autority). Dále musí být Váš certifikát správně spojen s odpovídajícím privátním nebo-li soukromým klíčem.

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

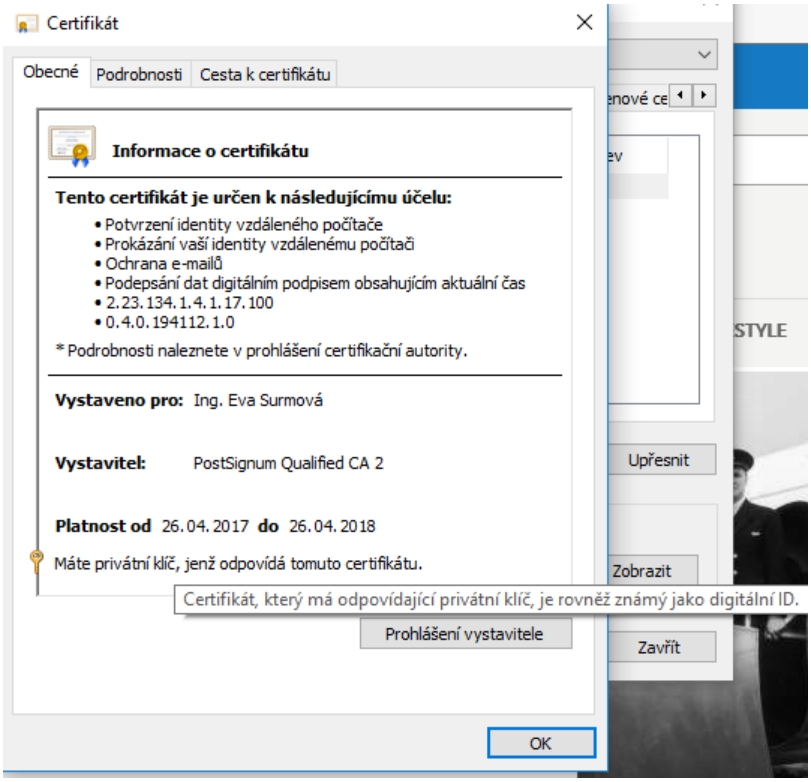
Obecný postup správné instalace certifikátu elektronického podpisu je následující:

- 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,
- import kořenových certifikátů autority vydávající kvalifikované certifikáty, viz. kapitola „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.

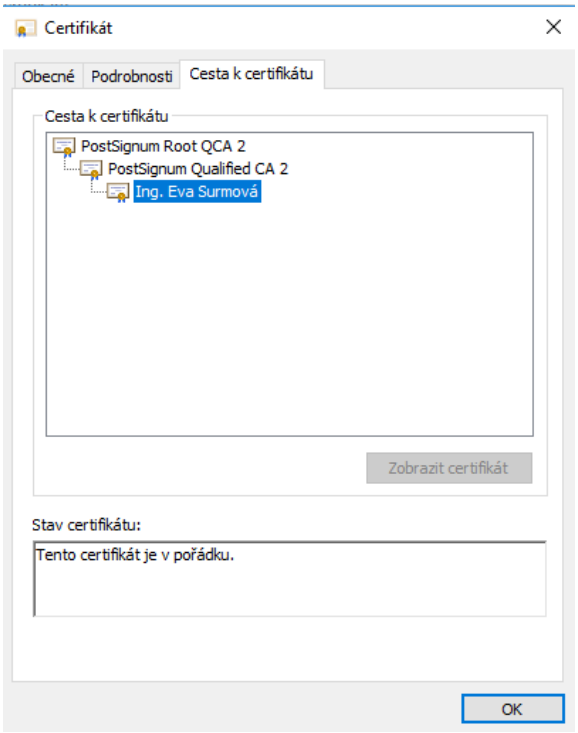
- Detail certifikátu s propadlou platností obr. č. 15

Ověření bodu 1 vidíte na obrázku č.13.

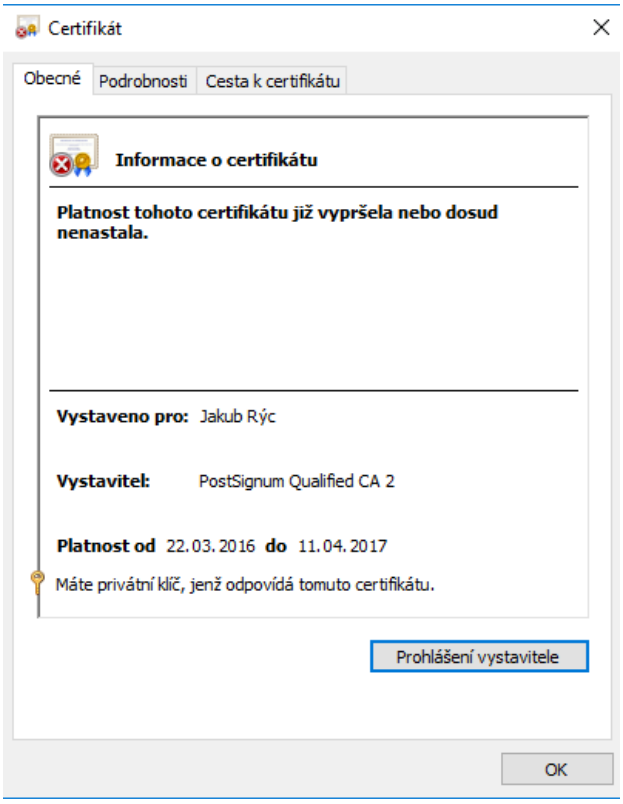
Obrázek č. 13 - Informace o certifikátu - certifikát má odpovídající soukromý klíč, MS Internet Explorer



Obrázek č. 14 - Detail certifikátu s úplnou cestou k certifikátu, MS Internet Explorer



Obrázek č. **15 - Certifikát s vypršenou platností**



9 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“.

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, viz. kapitola „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.

10 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, 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.

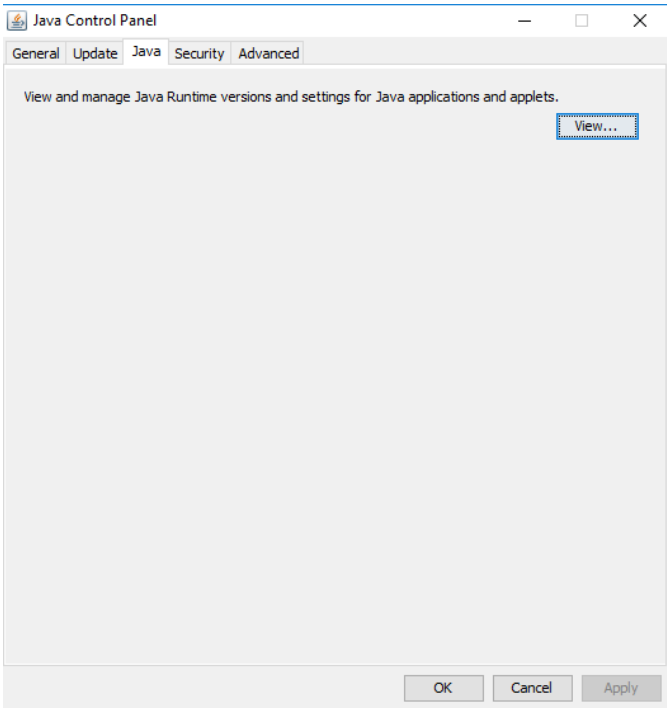
11 NASTAVENÍ JAVY VE WINDOWS

Otevřete kontrolní panel Javy (Configure Java) – 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 klikněte na ikonku Java.

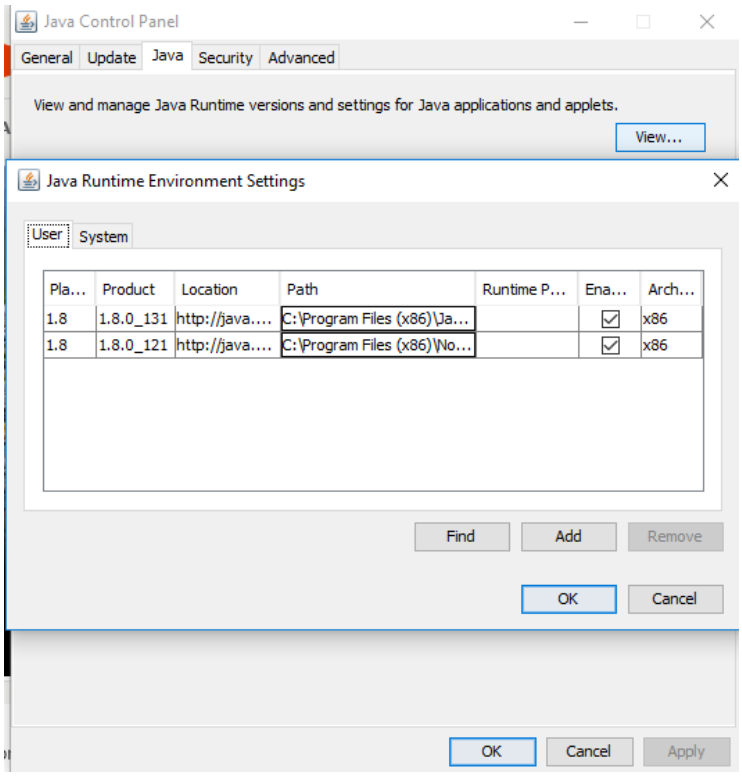
Otevře se Vám dialog jako na obrázku č. 16. Vyberte záložku Java a klikněte na tlačítko View... Tím se otevře tabulka z obrázku č. 17.

Pro Vámi používanou verzi Javy ve sloupci 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 č. 16 - Dialog nástroje jcontrol ve Windows



Obrázek č. 17 - 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.

12 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:

- 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 – zkontrolujte správnost nainstalování certifikátu, vizte kapitolu „Kontrola správnosti instalace certifikátu“, nebo vyberte jiný certifikát k podepsání,
- Exception in thread "Thread-38" 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 nebo vytvořte print screen do e-mailu a zašlete ho na adresu info@osigeno.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.

13 FAQ – ČASTO KLADENÉ OTÁZKY

Otázka

Nespustil se mi applet pro elektronický podpis.

Odpověď

Důvodů může být několik:

- nemáte nainstalovánu nebo povolenu Javu – viz. kapitola „Požadavky na systém“
- máte nainstalovánu starou verzi Javy – viz. kapitola „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

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

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, viz. obrázek č. 7, 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

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

Odpověď

Vizte kapitolu „Podepisování velkého objemu dat“.