Uživatelská příručka zadavatele

ELEKTRONICKÝ PODPIS

Elektronický nástroj
pro zadávání veřejných zakázek

CENT

verze 1.2

SIGENO
veřejné zakázky a dotace s.r.o.

2023
Osigeno – veřejné zakázky a dotace s.r.o.

Obsah

1 ÚVOD

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

V případě, že si při zadávání nového zadávacího řízení zapnete volbu „Vyžadovat u VZ elektronický podpis“ , bude nástroj vyžadovat podepisování u některých úkonů, jako je např. odesílání zpráv v rámci nástroje CENT, podání elektronické nabídky / žádosti o účast atd. a to ze strany dodavatele i zadavatele.

Samotné podepisování je v nástroji CENT realizováno podpisovou aplikací, která umožní práci s uznávaným elektronickým podpisem a to jak z datového úložiště operačního systému, tak ze souboru s certifikátem ve formátu P12 / PFX.

2 POŽADAVKY NA SYSTÉM

CENT je tzv. webovou aplikací, pro jeho provozování na straně uživatele postačí běžně používané operační systémy (MS Windows 8 a novější, Linux, macOS), které umí spustit Javu JRE a aktuální verze běžně používaných prohlížečů Internetu.

V případě využití elektronického podpisu v nástroji CENT, je nutné mít nainstalovanou Javu verze 8 Update 241 a vyšší ve Vašem zařízení. Bez nainstalované Javy JRE se Vám nespustí podepisovací Java applet.

Instalaci Javy JRE je možné provést na URL adrese: https://www.java.com viz podkapitola 2.2.

Stažení a užívání Javy je zdarma, pozor si ale dejte z jakých stránek stažení provedete. Software instalujte přímo od vydavatele viz adresa výše, nikoli z pop up stránek, které se objevují na mnoha stránkách.

2.1 KDE PROVÉST TEST PŘIPRAVENOSTI PROSTŘEDÍ

Zda máte Javu ve Vašem zařízení již nainstalovanou, popř. jakou její verzi používáte, zjistíte např. na stránce https://www.java.com/en/download/installed8.jps.

Na stránkách nástroje CENT si pak funkčnost podpisu můžete vyzkoušet v testu připravenosti prostředí, který je dostupný na URL adrese https://www.profilzadavatele-vz.cz/test (CENT → menu → test nastavení).

2.2 KDE A JAK STÁHNOUT NEJNOVĚJŠÍ VERZI JAVY?

Stažení nejnovější verze je k dispozici na adrese http://www.java.com. Jakmile do adresního řádku v prohlížeči zadáte tuto URL adresu, bude Vám automaticky nabídnuta poslední aktuální verze Javy určená pro ten prohlížeč, ze kterého jste aktuálně na stránkách Javy. Stránky samy poznají, zda potřebujete stáhnout 32 bitvou nebo 64 bitovou verzi. Z tohoto důvodu není vhodné stahovat Javu v jiném prohlížeči, než který budete používat pro práci s elektronickým nástrojem CENT.

2.3 REINSTALACE JAVY

Nadaří se Vám úspěšné podepsání? Pokud nechcete dlouze hledat možné příčiny problému s podpisem, doporučujeme Javu kompletně renistalovat a naistalovat nejnovější verzi. Např. postup pro operační systém Microsoft Windows je následující:

1. Start -> Ovládací panely -> Programy a funkce -> vybrat v seznamu Javu (i staré verze, pokud nejsou používané) -> Odinstalovat.
2. Spustit prohlížeč a nainstalovat aktuální verzi Javy z adresy: http://www.java.com
3. Po instalaci Javy si zkontrolujte funkčnost v našem testu ověření kompatibility: https://www.profilzadavatele-vz.cz/test

3 ELEKTRONICKÝ PODPIS

Podepisování je realizováno podpisovou aplikací, která umožní práci s uznávaným elektronickým podpisem v elektronickém nástroji CENT v běžně používaných operačních systémech a v aktuálních verzích běžně používaných prohlížečů Internetu.

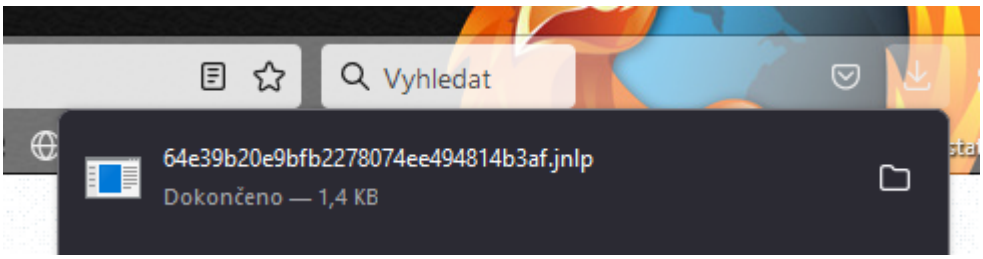
Podpisová aplikace umožňuje použití kvalifikovaného certifikátu jak z datového úložiště operačního systému, tak ze souboru s certifikátem ve formátu PFX/P12.

Elektronický nástroj Vás v místě vyžadující elektronické podepsání (např. při dešifraci přijaté elektronické nabídky se jedná o tlačítko „podepsat pro odemknutí nabídky“) vyzve ke stažení a spuštění souboru s příponou .jnlp.

Obrázek 1: Výzva k elektronickému podepsání při dešifraci přijatých elektronických nabídek

Stažený soubor se zobrazí v sekci stahovaní ve Vámi používaném prohlížeči. V prohlížeči Mozilla Firefox vypadá soubor po stažení následovně:

Obrázek 2: Stažení souboru s příponou jnlp



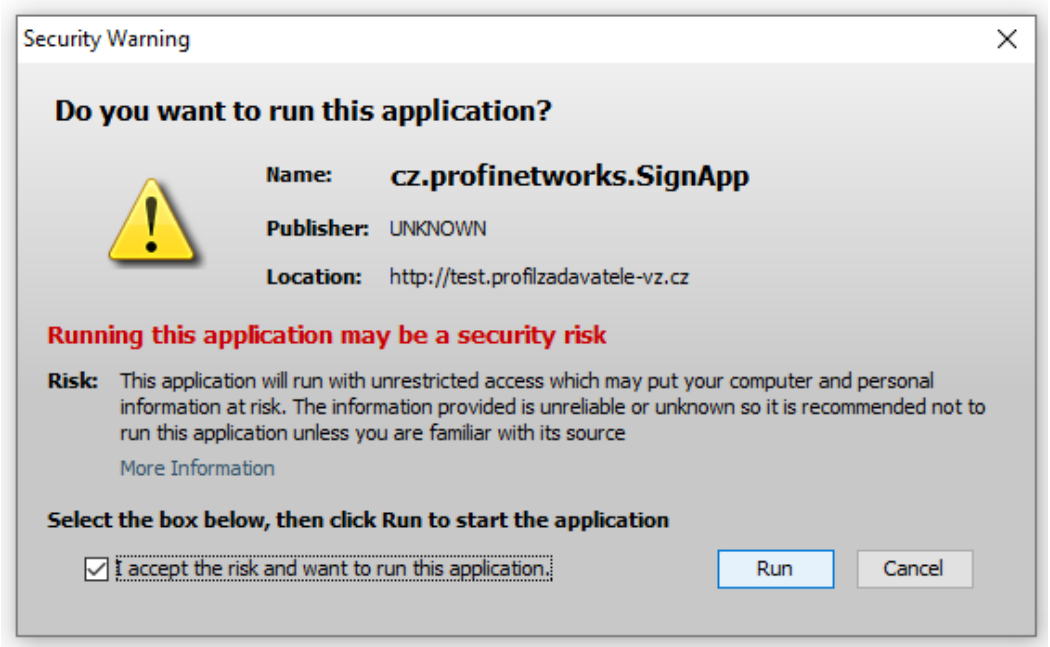
Tento soubor s příponou .jnlp obsahuje HASH žádost, která po kliknutí na název souboru spustí Javu s podepisovacím appletem viz Obrázek 5.

Na stránce nástroje CENT je zobrazeno hlášení, které Vás informuje o správném postupu.

Obrázek 3: Informační hláška

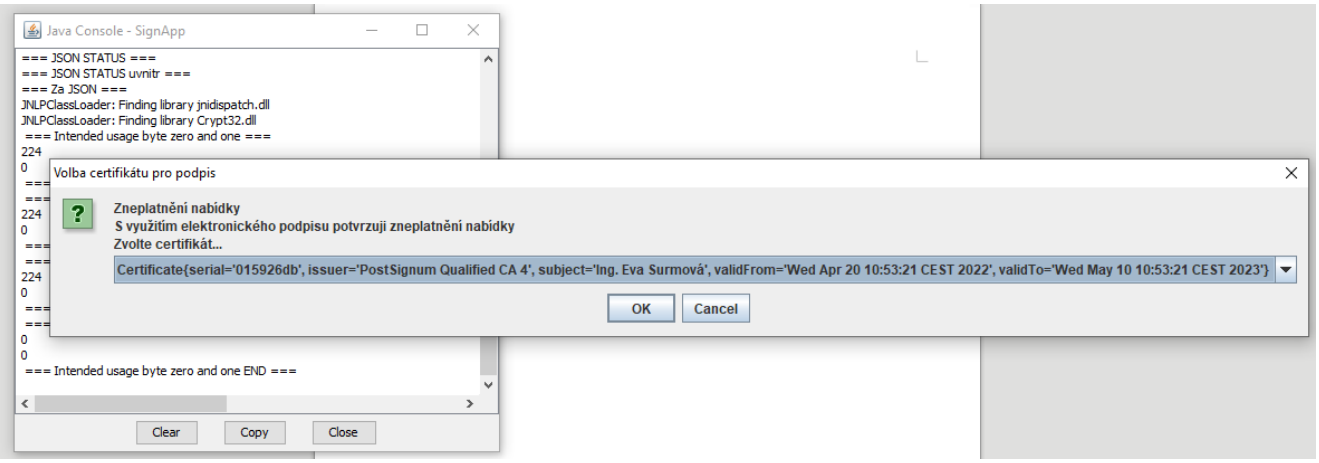
Stažený soubor je nutné spustit - spuštění provedete kliknutím na název souboru . Po kliknutí se spustí podepisovací Java applet. Nejprve je ale nutné povolit spuštění appletu (jedná se o aplikaci pro internetové stránky) a to tak, že zaškrtnete volbu *„I accept the risk and want to run this application“* a následně kliknete na tlačítko *„Run“* v dialogu viz obrázek níže.

Obrázek 4: Povolení spuštění podpisového appletu



Po udělení souhlasu se otevře dialogové okno *„Volba certifikátu pro podpis“*, ve kterém se zobrazí seznam Vašich certifikátů, které máte nainstalovány v systému.

Obrázek 5: Výběr certifikátu v dialogovém okně "Volba certifikátu"



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 informační hlášení Vás následně informuje o výsledku.

Obrázek 6: Informační hlášení - výsledek podpisu - úspěšné podepsání

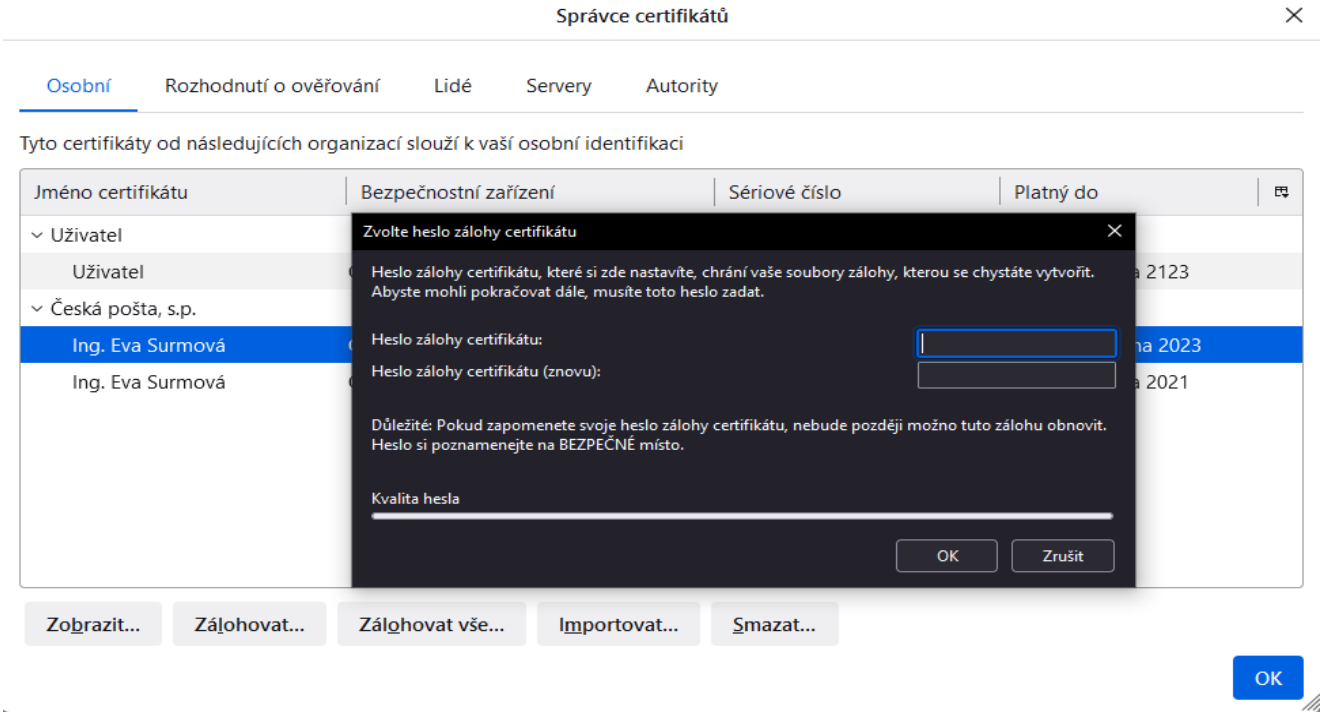
Obrázek 7: Informační hlášení - výsledek testu - neúspěšné podepsání

4 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 Microsoft Mozilla v menu rozklikněte nabídku aplikace (tři čárky) → nastavení → soukromí a zabezpečení → zabezpečení → certifikáty → zobrazit certifikáty → zobrazí se správce certifikátů s přehledem → osobní.

Obrázek 8: Správce souboru



Označte požadovaný certifikát a stiskněte tlačítko „Zálohovat“. Zadejte název souboru, umístění a poté si stanovte 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.

5 AKCEPTOVATELNÉ CERTIFIKÁTY

V souladu s právní úpravou je vyžadováno podepisování zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu. Uznávané elektronické podpisy vydávají tři poskytovatelé:

1. Česká pošta, s.p. (www.postsignum.cz),
2. eIdentity, a.s. (www.eidentity.cz),
3. První certifikační autorita, a.s. (www.ica.cz).

6 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“.

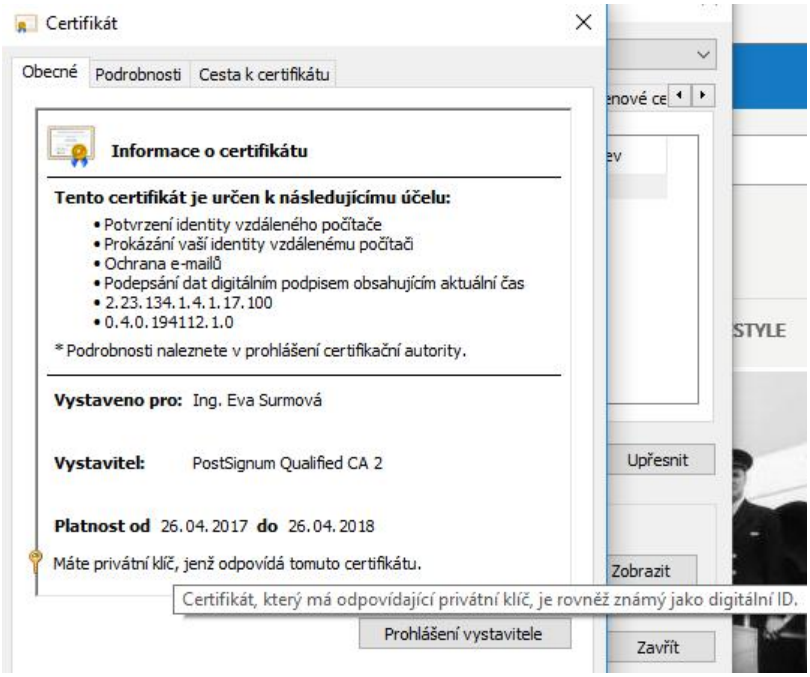
Obecný postup správné instalace certifikátu elektronického podpisu je následující:

- 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.

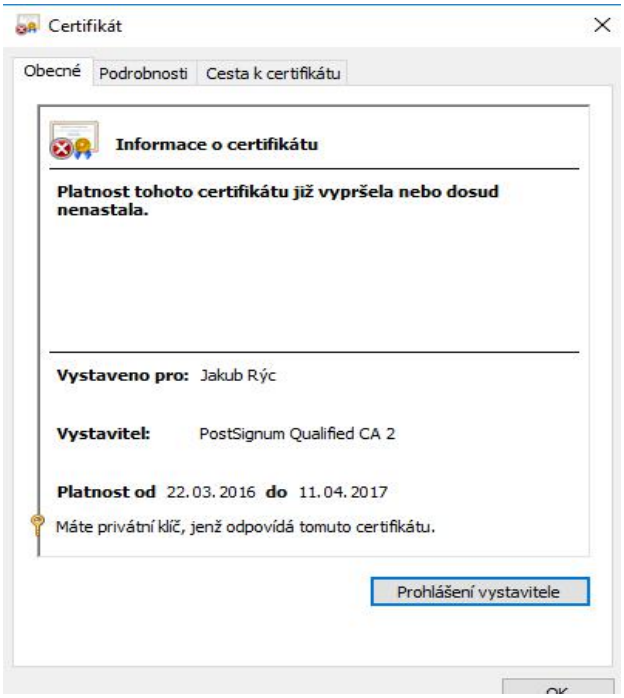
- Detail certifikátu s propadlou platností viz obrázek 10.

Ověření bodu 1 vidíte na obrázku Obrázek 9.

Obrázek 9: Informace o certifikátu - certifikát má odpovídající soukromý klíč



Obrázek 10: Detail certifikátu s uplynulou platností



7 CHYBOVÁ HLÁŠENÍ PO PODEPSÁNÍ

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:

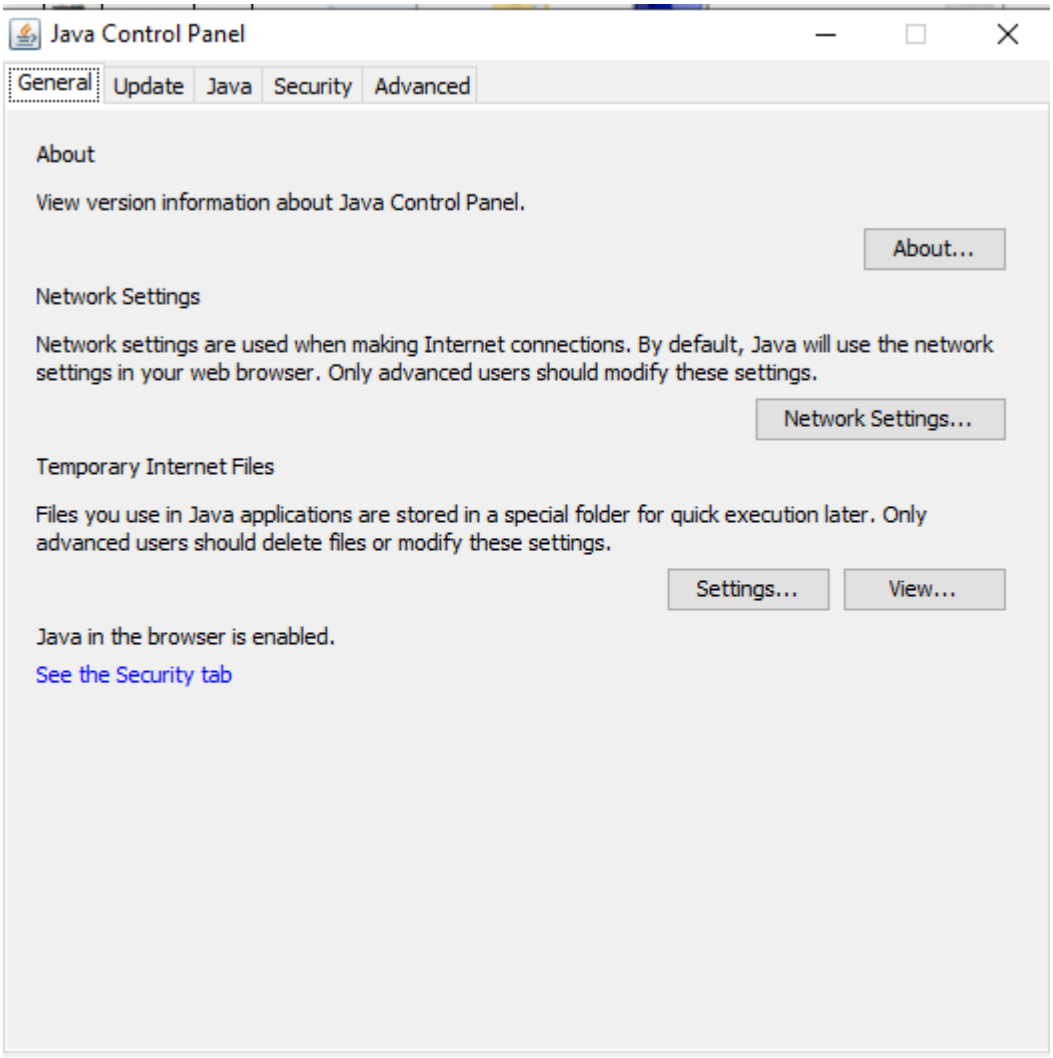
- Certifikát elektronického podpisu není kvalifikovaný, nebo neobsahuje úplnou certifikační cestu. Prosím použijte správný certifikát – certifikát není správně nainstalován, chybí certifikáty vydávající autority.
- Podepisování selhalo – Vybraný certifikát už není platný
- Validation failed (...), Path 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.

8 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 níže.

Obrázek 11: Java Control Panel



Vyberte záložku Security a přidejte stránku nástroje CENT do vyjímek. Provedete: Exception Site List → Edit Side List… → Add → do okna vepište přesnou URL adresu, v případě použití základní verze nástroje se jedná o adresu: http://www.profilzadavatele-vz.cz/, pokud využíváte individuální URL adresy bude místo „www“ vepsán název předmětné obce, města či příspěvkové organizace např. https://praha7.profilzadavatele-vz.cz/ → akci potvrdíte OK.

Aby změna nastavení začala fungovat, je nutné zavřít všechna okna prohlížeče a spustit jej znovu (restart prohlížeče), popř. restart celého zařízení.

9 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,
- 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 Vám 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.