

Generovanie žiadostí o certifikát
Užívateľská príručka pre prehliadač
Google Chrome

První certifikační autorita, a.s.

17.1.2011

Verze 7.06

Obsah

| | |
|--|----|
| 1. Úvod | 3 |
| 2. Požiadavky na softvér | 3 |
| 3. Inštalácia koreňového certifikátu I.CA | 4 |
| 4. Proces generovania žiadosti o certifikát | 7 |
| 4.1. Kontrola softwarového vybavenia..... | 7 |
| 4.1.1. Nepodporovaný operačný systém..... | 7 |
| 4.1.2. Nepodporovaný internetový prehliadač | 7 |
| 4.1.3. Podpora JavaScriptu | 8 |
| 4.1.4. Podpora Java Runtime Environment (JRE) | 9 |
| 4.1.5. Nainštalovaný Java Applet ICApki..... | 12 |
| 4.1.6. Ukladanie cookies..... | 13 |
| 4.2. Vyplnenie údajov o žiadateľovi | 15 |
| 4.3. Kontrola zadaných údajov | 18 |
| 4.4. Generovanie žiadosti o certifikát | 19 |
| 4.4.1. SecureStoreCSP | 19 |
| 4.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou súkromého kľúča. | 20 |
| 4.5. Uloženie žiadosti o certifikát | 23 |
| 5. Vystavenie certifikátu..... | 23 |
| 6. Inštalácia Java Runtime Environment (JRE)..... | 23 |
| 6.1. Spustenie inštalácie JRE pod prehliadačom Google Chrome | 23 |
| 7. Instalační program JRE | 24 |
| 8. Riešenie problémov..... | 26 |

1. Úvod

Tento dokument slúži ako návod, ako postupovať pri generovaní žiadosti o certifikát cez webové stránky.

2. Požiadavky na softvér

Počítač, na ktorom sa bude vykonávať generovanie žiadosti o certifikát, musí spĺňať nasledujúce požiadavky:

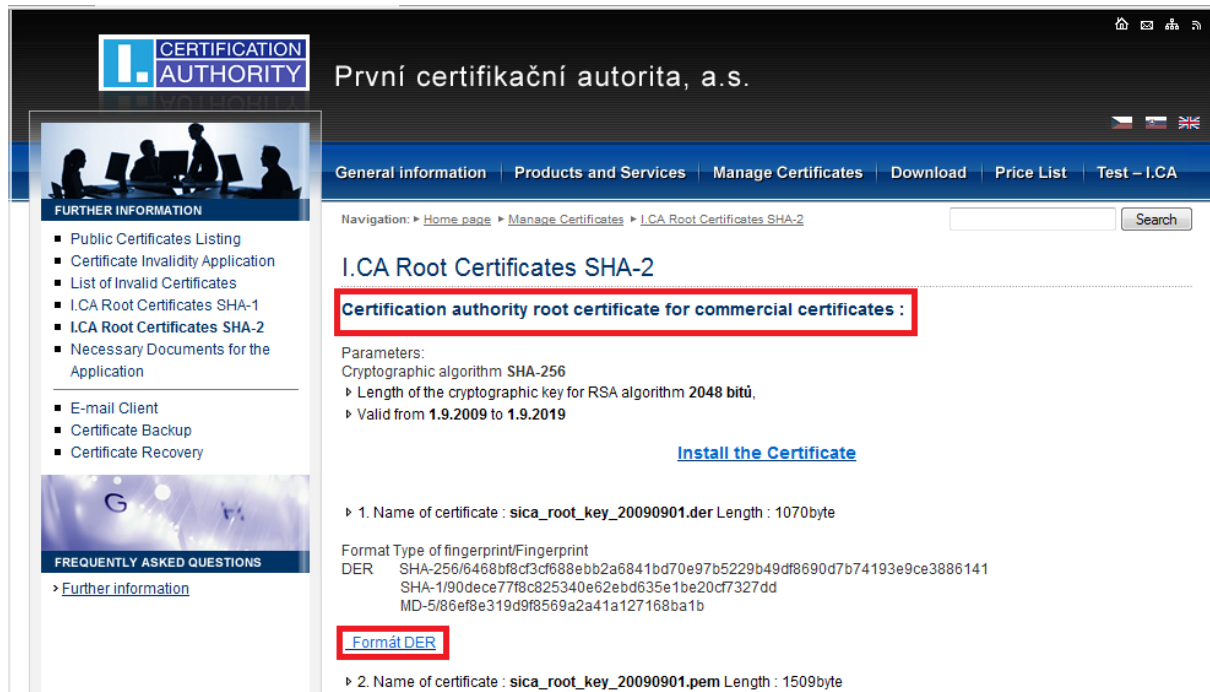
- Musí mať nainštalovaný a spustený operačný systém.
 - **Microsoft Windows XP**
 - **Windows Vista**
 - **Windows 7**
- Musí byť nainštalovaný a použitý niektorý z nasledujúcich prehliadačov (pre generovanie žiadosti).
 - **Microsoft Internet Explorer** (verzia 7 a vyššia).
 - **Mozilla Firefox** (verzia 3 a vyššia)
 - **Google Chrome** (verzia 2 a vyššia)
 - **Apple Safari** (verzia 4 a vyššia)
 - **Opera** (verzia 10 a vyššia)
- Musí mať nainštalovaný softvér **Java Runtime Environment** (ďalej **JRE**), aspoň verzia **1.6.0_21**, ktorý je potrebný pre správnu funkciu webových stránok pre generovanie žiadosti o certifikát.
 - Odporúčame používať najaktuálnejšiu verziu JRE.
 - Prítomnosť tohto softvéru detegujú stránky automaticky, ak zistia, že softvér prítomný nie je, vyzvú užívateľa k jeho stiahnutiu / inštalácii.
 - **V prípade, že máte nainštalovanú staršiu verziu JRE, ako je uvedená v požiadavkách, odinštalujte ju pred začatím generovania žiadosti o certifikát. Následne budete stránkami nasmerovaný na stiahnutie najaktuálnejšie verzie.**
- Vo vašom internetovom prehliadači musíte mať zapnutú podporu **skriptovania Javascript**, **zapnutú podporu jazyku Java**, **podporu ukládanie cookies**.

3. Inštalácia kořenového certifikátu I.CA

Pri spustení stránky so žiadosťou o certifikát vás môže váš prehliadač upozorniť, že vstupujete na nedôveryhodné stránky. Tento problém je spôsobený tým, že nemáte uložené v úložisku koreňové certifikáty I.CA.

Zadajte do prehliadača nasledujúcu URL: <http://www.ica.cz/cz/menu/112/prace-s-certifikaty/korenove-certifikaty-i-ca-sha-2/>

Zobrazí sa vám nasledujúca stránka:



První certifikační autorita, a.s.

General information | Products and Services | Manage Certificates | Download | Price List | Test – I.CA

Navigation: ▶ Home page ▶ Manage Certificates ▶ I.CA Root Certificates SHA-2

I.CA Root Certificates SHA-2

Certification authority root certificate for commercial certificates :

Parameters:
Cryptographic algorithm SHA-256
▶ Length of the cryptographic key for RSA algorithm 2048 bitů.
▶ Valid from 1.9.2009 to 1.9.2019

[Install the Certificate](#)

▶ 1. Name of certificate : sica_root_key_20090901.der Length : 1070byte

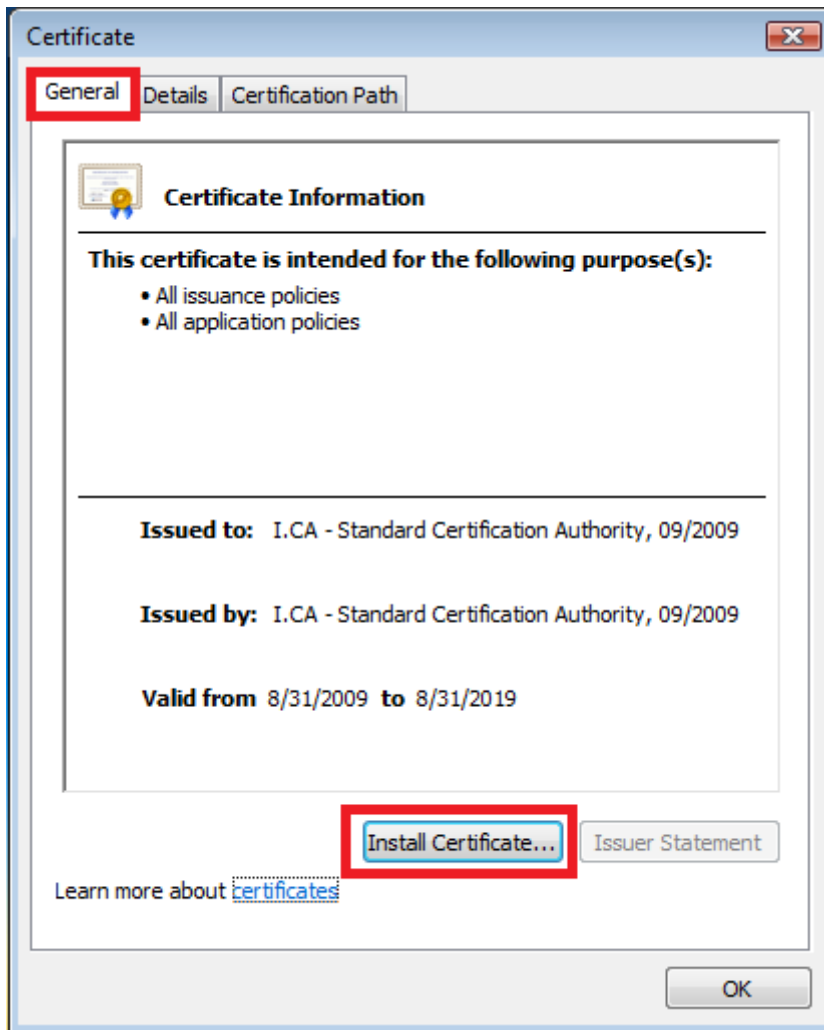
Format Type of fingerprint/Fingerprint
DER SHA-256/6468bf8cf3cf688ebb2a6841bd70e97b5229b49df8690d7b74193e9ce3886141
SHA-1/90dece77f8c825340e62ebd635e1be20cf7327dd
MD-5/86ef8e319d9f8569a2a41a127168ba1b

Formát DER

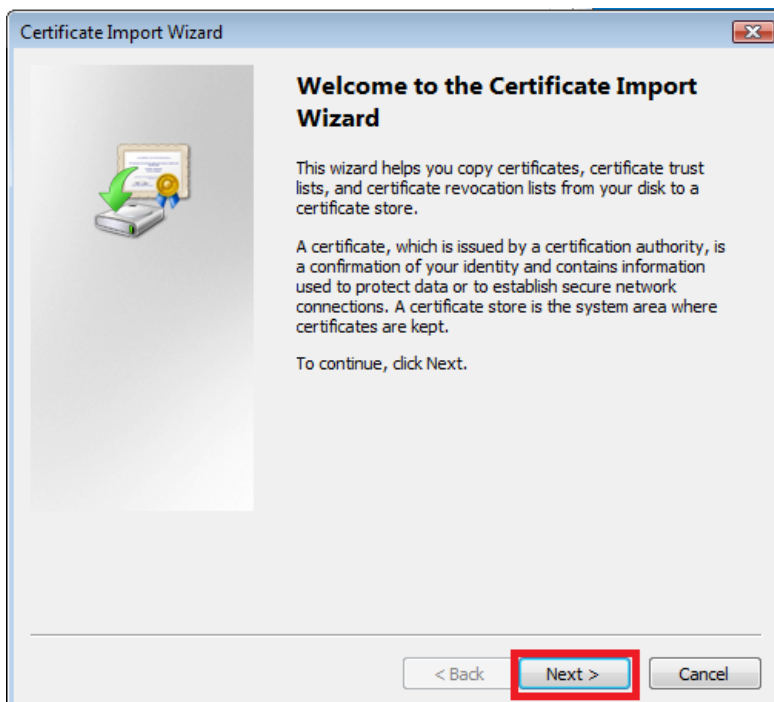
▶ 2. Name of certificate : sica_root_key_20090901.pem Length : 1509byte

Pod nadpisom **Koreňový certifikát certifikačnej autority pre vydávané komerčné certifikáty** kliknite na **Formát DER**. Zobrazí sa vám dialóg pre stiahnutie súboru. Súbor obsahujúci certifikát uložte na Váš pevný disk.

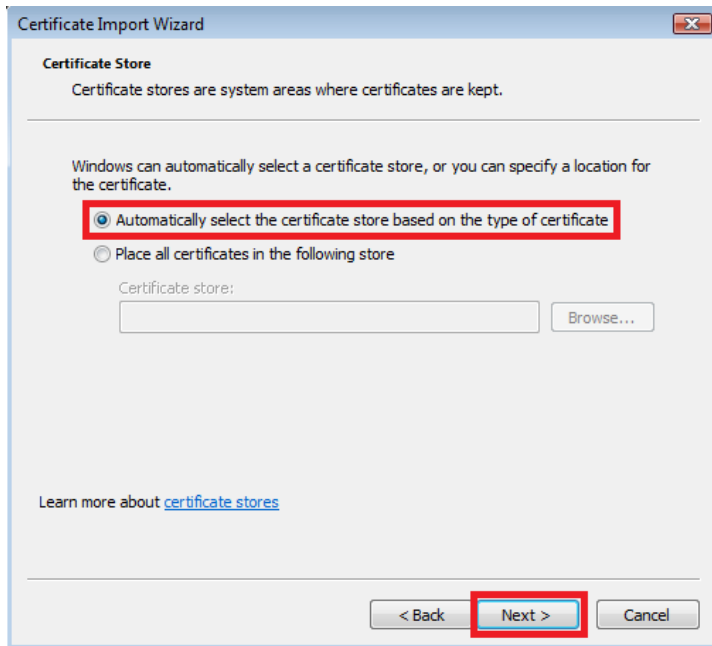
Dvojklikom otvorte súbor obsahujúci koreňový certifikát I. CA, ktorý ste uložili na pevný disk. Tým dôjde k zobrazeniu certifikátu. Na záložke **Všeobecné** kliknite na **Nainštalovať certifikát**.



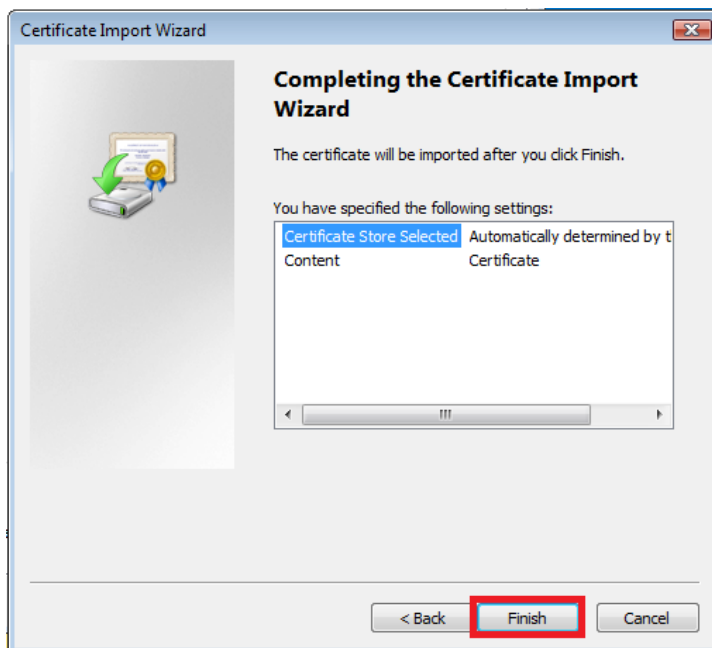
Spustí sa sprievodca inštaláciou certifikátu. Kliknite na tlačidlo **Ďalej**.



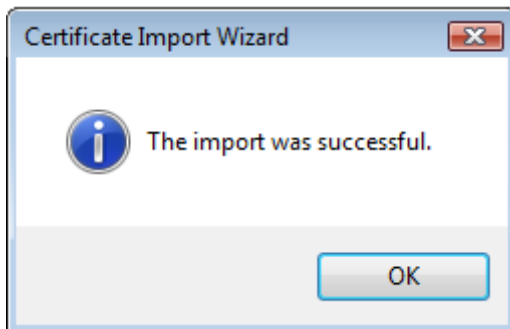
Skontrolujte, že je zaškrtnutá voľba **Automaticky vybrať úložisko certifikátov na základe typu certifikátu** a kliknite na tlačidlo **Ďalej**.



Kliknite na tlačidlo **Dokončiť**.



Sprievodca by vás mal informovať o úspešnom importe.



4. Proces generovania žiadosti o certifikát

Postup generovania žiadosti o prvotný certifikát je rozdelený do niekoľkých krokov:

- Kontrola softvérového vybavenia
- Vyplnenie údajov žiadateľa
- Kontrola vyplnených údajov
- Generovanie žiadosti o certifikát
- Uloženie žiadosti o certifikát

4.1.Kontrola softwarového vybavenia

Pre uľahčenie kontroly pripravenosti vášho počítača na generovanie žiadosti, je pri začatí generovania žiadosti zobrazená kontrolná stránka, ktorá overí prítomnosť kľúčových softvérových komponentov.

Checking required software, wait for its termination.

- ✓ Your operating system WinVista is supported
- ✓ Your browser Chrome version 10.0 is supported.
- ✓ JavaScript enabled.

Stránka otestuje počítač, test môže trvať desiatky sekúnd, a ohlási, či je niečo v neporiadku, prípadne vypíše chybové hlásenie. Ak nie sú detegované problémy, stránka zobrazí formulár pre vyplnenie osobných údajov.

Ak sa pri kontrole vyskytne chyba, nie je zobrazený formulár pre vyplnenie osobných údajov. Najskôr je potrebné odstrániť chybu, ktorá znemožňuje generovanie žiadosti. Význam chybových hlásení je uvedený v nasledujúcich kapitolách.

4.1.1.Nepodporovaný operačný systém

Pre generovanie žiadosti musíte použiť jeden z operačných systémov uvedených v kapitole **Chyba! Nenalezen zdroj odkazů.**


4.1.2. Nepodporovaný internetový prehliadač

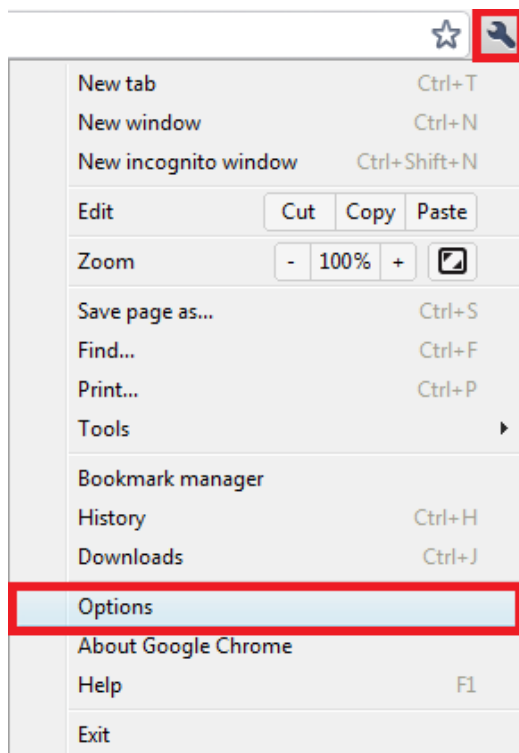
Pre generovanie žiadosti musíte použiť jeden z prehliadačov uvedených v kapitole **Chyba! Nenalezen zdroj odkazů.**

4.1.3. Podpora JavaScriptu

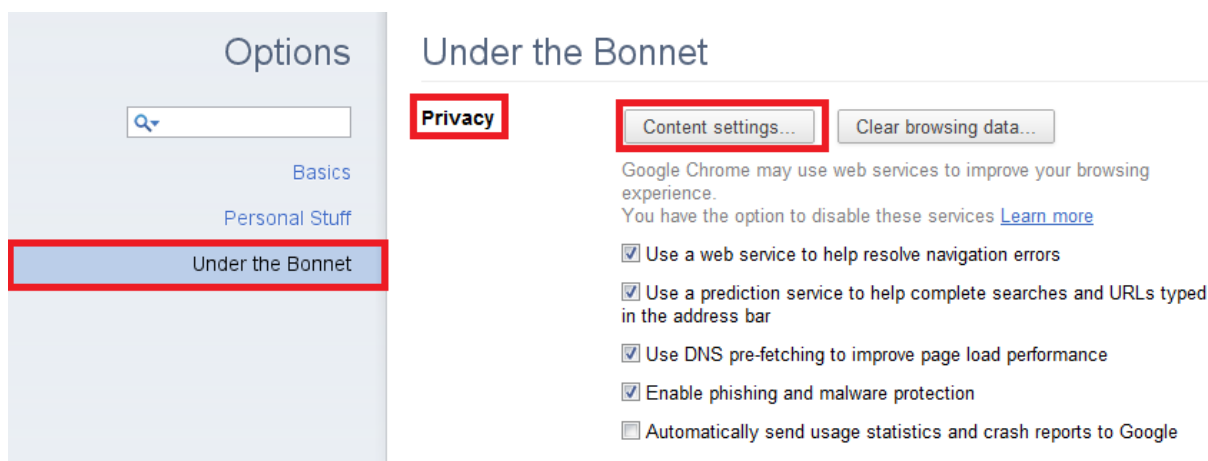
Stránky pre generovanie žiadosti o certifikát vyžadujú podporu skriptovania v jazyku JavaScript. Všetky podporované prehliadače majú túto podporu automaticky povolenú. Ak by táto kontrola zlyhala, znamená to s najväčšou pravdepodobnosťou, že je v nastavení prehliadača podpora skriptovania vypnutá. Povoľte podporu skriptovania v jazyku JavaScript vo vašom prehliadači.

4.1.3.1. Povolenie JavaScriptu v Google Chrome

Kliknite na ikonu kľúča  na lište prehliadača. Vyberte položku **Možnosti**.



Kliknite na záložku **Pod pokrievkou** a v časti **Ochrana osobných údajov** kliknite na tlačidlo **Nastavenie obsahu**.



Vyberte zo zoznamu možnosť **JavaScript** a zaškrtnite **Povolit všetkým webovým stránkam spúšťať JavaScript**.

(Prípadne kliknite na tlačidlo **Výnimky ...**, následne na tlačidlo **Pridať ...** do položky Vzor zadajte **s.ica.cz** pri položke akcie zvolíte **Povolit**)

Uzavrite všetky okná pomocou tlačidla **Zavrieť**.

Content Settings

Cookies

- Allow local data to be set (recommended)
- Block sites from setting any data
- Ignore exceptions and block third-party cookies from being set
- Clear cookies and other site data when I close my browser

[Manage exceptions...](#) [All cookies and site data...](#)

Images

- Show all images (recommended)
- Do not show any images

[Manage exceptions...](#)

JavaScript

- Allow all sites to run JavaScript (recommended)
- Do not allow any site to run JavaScript

[Manage exceptions...](#)

Plug-ins

- Run automatically (recommended)
- Block all


[Manage exceptions...](#)
[Disable individual plug-ins...](#)

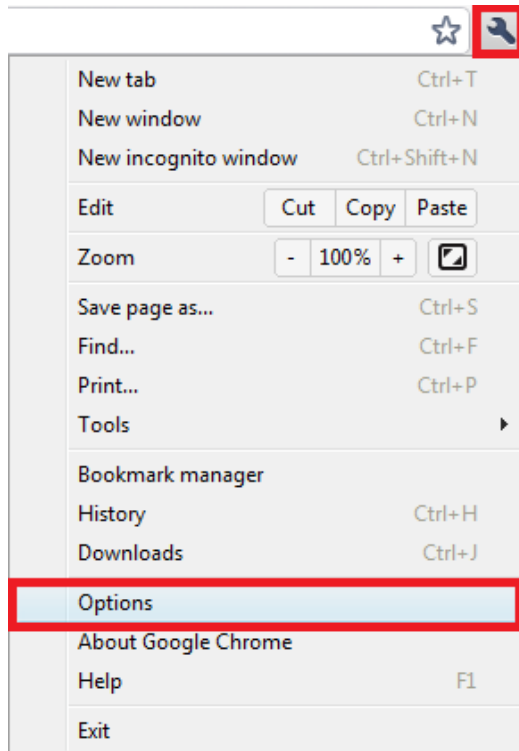
4.1.4.Podpora Java Runtime Environment (JRE)

Tieto stránky vyžadujú pre svoju funkčnosť nainštalovanú podporu jazyka Java. Uistite sa, že nemáte vo svojom prehliadači túto podporu vypnutú. Pokiaľ nemáte na svojom počítači JRE nainštalované, mal by vás prehliadač vyzvať na stiahnutie a inštaláciu JRE. Ak sa tak nestalo, kliknite na odkaz uvedený na stránke a manuálne stiahnite a nainštalujte aktuálnu verziu JRE. V každom prípade bude po inštalácii JRE treba zavrieť a znovu spustiť prehliadač, aby sa zmeny prejavili.

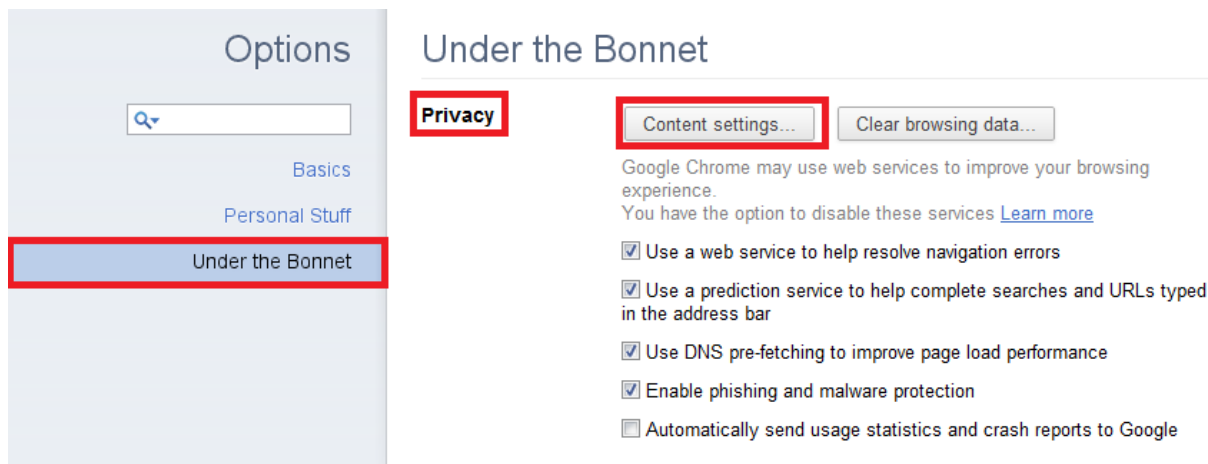
Inštalácia JRE je popísaná v **Kapitole 6**.

4.1.4.1.Povolenie Java v Google Chrome

Kliknite na ikonu kľúča  na lište prehliadača. Vyberte položku **Možnosti**.



Kliknite na záložku **Pod pokrievkou** a v časti **Ochrana osobných údajov** kliknite na tlačidlo **Nastavenie obsahu**.



Zvolte zo zoznamu možnosť **Pluginy** a kliknite na **Deaktivovať jednotlivé pluginy...**

Content Settings



Cookies

- Allow local data to be set (recommended)
- Block sites from setting any data
- Ignore exceptions and block third-party cookies from being set
- Clear cookies and other site data when I close my browser

[Manage exceptions...](#)

[All cookies and site data...](#)

Images

- Show all images (recommended)
- Do not show any images

[Manage exceptions...](#)

JavaScript

- Allow all sites to run JavaScript (recommended)
- Do not allow any site to run JavaScript

[Manage exceptions...](#)


Plug-ins

- Run automatically (recommended)
- Block all

[Manage exceptions...](#)

[Disable individual plug-ins...](#)

V zozname pluginov vyhľadajte **Java 6** a kliknite na **Aktivovať**. Uzavrite okno pomocou krížika.



Plug-ins

Plug-ins (8) [Details](#)

Flash - Version: 10.2.154.25
Shockwave Flash 10.2 r154
[Disable](#)

Java 6 (2 files) - Version: 6.0.240.7 (Disabled)
NPRuntime Script Plug-in Library for Java(TM) Deploy
[Enable](#)

Silverlight - Version: 2.0.40115.0 [Download Critical Security Update](#)
[Disable](#)

Chrome PDF Viewer
[Disable](#)

Google Gears 0.5.33.0 - Version: 0.5.33.0
These are the Gears that power the tubes! :-)
[Disable](#)

Google Update - Version: 1.2.183.39
[Disable](#)

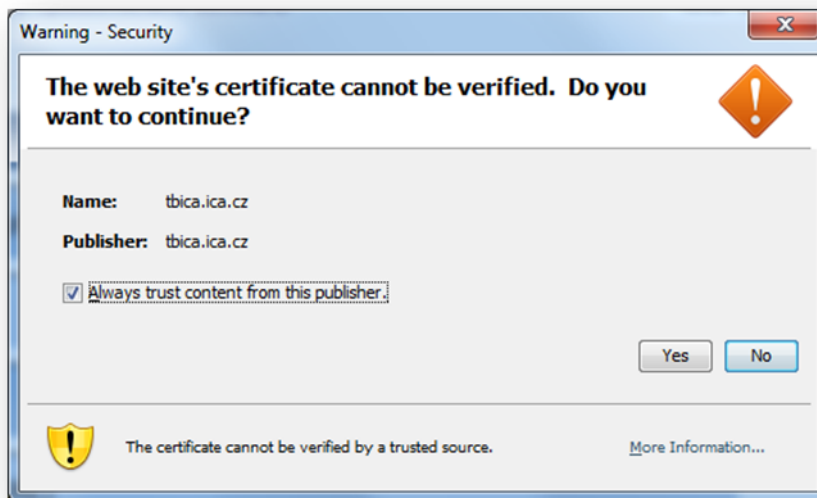
Windows Presentation Foundation
Windows Presentation Foundation (WPF) plug-in for Mozilla browsers
[Disable](#)

Default Plug-in - Version: 1
Provides functionality for installing third-party plug-ins
[Disable](#)

Uzavrite všetky okná pomocou tlačidla **Zavrieť**.

4.1.5. Nainštalovaný Java Applet ICApki

V tomto mieste sa kontrolná stránka pokúsi nainštalovať Java Applet ICApki, ktorý je potrebný pre funkčnosť stránok pre generovanie žiadosti o certifikát. Pri prvej inštalácii appletu na počítač, kde prebieha generovanie žiadosti o certifikát, budete vyzvaní na potvrdenie dôvery vydavateľovi Java applet. Vydavateľom appletu je První certifikační autorita, a.s. Dôveru appletu potvrdíte dialógom, ktorý znázorňuje nasledujúci obrázok. V tomto dialógu je dôležité zaškrtnúť voľbu **Always trust content from this publisher** a potom použiť tlačidlo **Yes**.



Nasleduje druhý dialóg, kde sa postupuje obdobne, a síce zaškrtnie sa voľba **Always trust content from this publisher** a potom sa použije tlačidlo **Run**.




Pri ďalšom spustení stránok na počítači, kde táto inštalácia prebehla, už nebudete k opätovnému potvrdzovanie Java Applet ICApki vyzývaní.

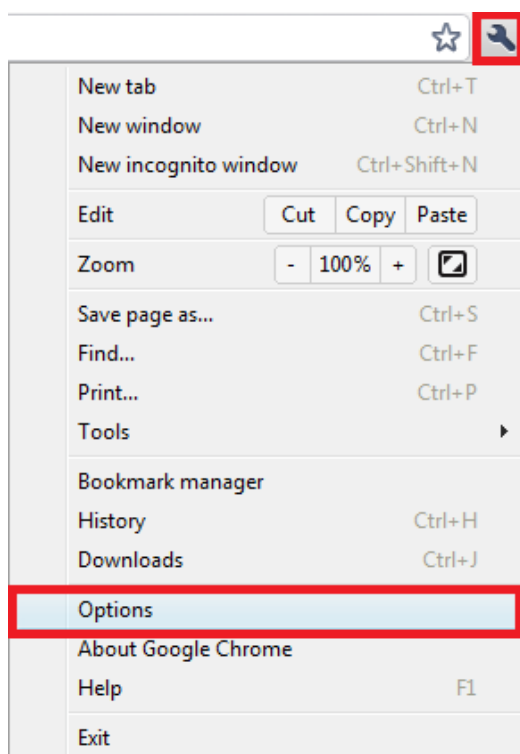
V prípade, že bude vydaná nová verzia Java Applet ICApki, bude klientom v tomto mieste okamžite automaticky stiahnutá a nainštalovaná. Táto inštalácia môže chvíľu trvať. Po jej skončení budú stránky pokračovať v normálnej práci.

4.1.6. Ukladanie cookies

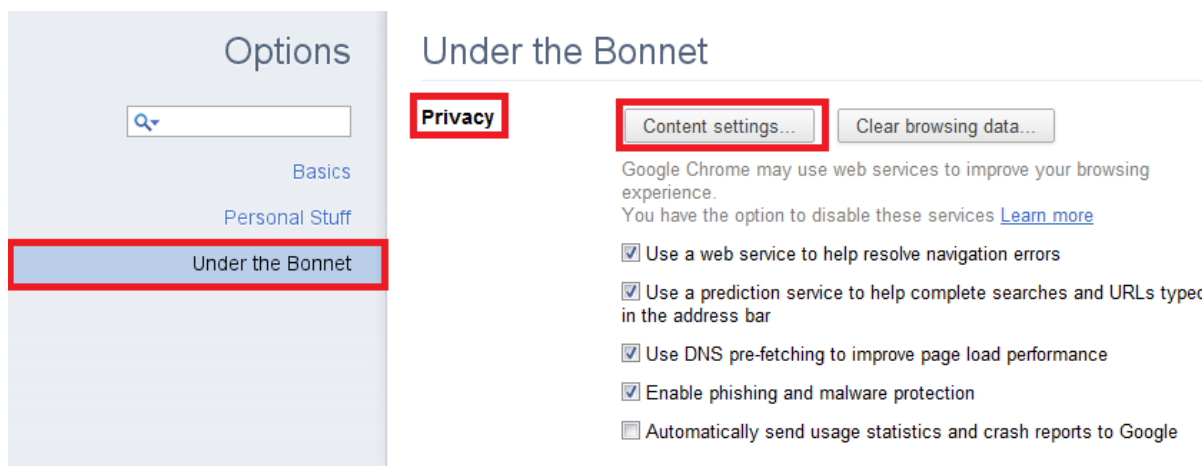
Pre správnu prácu stránok pre generovanie žiadostí je potrebné, aby váš prehliadač umožnil stránke ukladať cookies. Ak máte zakázané ukladanie cookies, povoľte ho.

4.1.6.1. Povolení cookies v Google Chrome

Kliknite na ikonu kľúča  na lište prehliadača. Vyberte položku **Možnosti**.



Kliknite na záložku **Pod pokrievkou** a v časti **Ochrana osobných údajov** kliknite na tlačidlo **Nastavenie obsahu**.



Vyberte zo zoznamu možnosť **Súbory cookie** a zaškrtnite **Povoliť nastavenie miestnych dát**.

(Prípadne kliknite na tlačidlo **Výnimky ...**, následne na tlačidlo **Pridať ...** do položky Vzor zadajte **s.ica.cz** pri položke akcie zvolte **Povoliť**)

Uzavrite všetky okná pomocou tlačidla **Zavrieť**.

Content Settings



Cookies

Allow local data to be set (recommended)

Block sites from setting any data

Ignore exceptions and block third-party cookies from being set

Clear cookies and other site data when I close my browser

Manage exceptions...

All cookies and site data...

Images

Show all images (recommended)

Do not show any images

Manage exceptions...

JavaScript

Allow all sites to run JavaScript (recommended)

Do not allow any site to run JavaScript

Manage exceptions...

Plug-ins

Run automatically (recommended)

Block all

Manage exceptions...

[Disable individual plug-ins...](#)

4.2. Vyplnenie údajov o žiadateľovi

Ak proces kontroly prebehol bez chýb, stránka zobrazí formulár, do ktorého vyplníte svoje osobné údaje.

| Heading | Your information | Example of completion |
|---|-------------------------------------|--|
| Select what type of applicant you are | | |
| <input checked="" type="radio"/> Current user (non-entrepreneurial) <input type="radio"/> Entrepreneur (Self-employed) <input type="radio"/> Employee <input type="radio"/> Pseudonym | | |
| Choose a repository for your private key | | |
| <input checked="" type="radio"/> Smart card I.CA <input type="radio"/> Other storage (PC, server, USB token, other smart card, etc.) | | |
| Information about the applicant | | |
| Degree (before name) | <input type="text"/> | Ing. |
| Name | <input type="text"/> | Jiřina |
| Surname | <input type="text"/> | Koutná |
| Degree (after name) | <input type="text"/> | Ph.D. |
| Generational resolution | <input type="text"/> | MI. |
| E-mail *) | <input type="text"/> | jirina_koutna@ica.cz |
| <input type="checkbox"/> The certificate is designed for communication with public authorities of the SR | | Mark the item if you require that the certificate can be used for communication with public authorities of the the SR and a private key to generate certified products according to Slovak legislation |
| Permanent Address | | |
| Street | <input type="text"/> | Česká |
| Street number/building identification number | <input type="text"/> | 11/22 |
| City/town | <input type="text"/> | Brno |
| Zip code | <input type="text"/> | 11150 |
| Province | <input type="text"/> | Jihomoravský |
| Country | Czech Republic <input type="text"/> | |
| Other options | | |
| Revocation password | <input type="text"/> | |
| Key Repository Type (CSP) | SecureStoreCSP <input type="text"/> | |
| <input type="checkbox"/> Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. | | |
| <input checked="" type="checkbox"/> Certificates for signing | | |
| <input type="checkbox"/> Certificates for encryption | | |
| *) The item is mandatory only if you intend to use the certificate in the email. | | |
| <input type="button" value="Continue"/> | | |

Položky zdôraznené tučným písmom a žltým podfarbením vstupného poľa sú povinné. Napríklad meno a priezvisko sú povinné, tituly povinné nie sú.

Heslo pre zneplatnenie:

Pokiaľ dôjde počas používania certifikátu ku kompromitácii privátneho kľúča, zmene údajov (zmena mena, bydliska ...) alebo sa vyskytnú ďalšie dôvody, prečo by nemal byť certifikát ďalej používaný, je Vašou zákonnou povinnosťou certifikát zneplatniť. Certifikát je možné zneplatniť cez webové rozhranie. Pri zneplatnení budete vyzvaní na zadanie hesla pre zneplatnenie. Toto heslo pre zrušenie určujete pri generovaní žiadosti o certifikát.

Dĺžka hesla pre zneplatnenie certifikátu musí byť 4 až 32 znakov. Povolené sú iba veľké a malé písmená bez diakritiky a číslice.

Typ úložisko ključa (CSP):

Pri položke **Typ úložisko ključa (CSP)** vyberte z ponuky SW modul zaisťujúci kryptografické služby (CSP), ktorý vygeneruje váš privátny ključ. Všetky tu zobrazené CSP podporujú podpisový algoritmus SHA2 a sú nainštalované vo vašom počítači.

Export privátneho ključa:

Ak vami zvolený typ úložiska ključa (CSP) podporuje export privátneho ključa, je vám ponúknutá voľba **povoliť export privátneho ključa**. Táto voľba umožní vykonať export certifikátu vrátane súkromného ključa. Súkromný ključ tak budete môcť prenášať medzi úložiskami. Správa ključa vyžaduje v takom prípade zvýšenú opatrnosť z dôvodu vyššieho rizika jeho krádeže / zneužitia.

Silná ochrana privátneho ključa:

Ak vami zvolený typ úložiska ključa (CSP) podporuje silnú ochranu privátneho ključa, je vám ponúknutá voľba **povoliť silnú ochranu privátneho ključa**. Pred každým použitím vášho ključa budete upozornení, že je váš ključ používaný. Následne máte možnosť vybrať si medzi: Stredná - vždy budete len upozornení informatívnym hlásením; Silná - pred každým použitím po Vás bude vyžadované zadanie hesla.

Po stlačení tlačidla **pokračovať** stránka vykoná kontrolu vami vyplnených údajov. Ak niektoré zadané údaje nespĺňajú podmienky, budete vyzvaní na ich opravu. Údaje vyžadujúce zmenu alebo doplnenie sú podfarbené červenou farbou.

| Heading | Your information | Example of completion |
|---|---|--|
| Select what type of applicant you are | | |
| <input checked="" type="radio"/> Current user (non-entrepreneurial) <input type="radio"/> Entrepreneur (Self-employed) <input type="radio"/> Employee <input type="radio"/> Pseudonym | | |
| Choose a repository for your private key | | |
| <input checked="" type="radio"/> Smart card I.CA <input type="radio"/> Other storage (PC, server, USB token, other smart card, etc.) | | |
| Information about the applicant | | |
| Degree (before name) | <input type="text"/> | Ing. |
| Name | <input type="text" value=""/> | Jiřina |
| Surname | <input type="text" value="Doe"/> | Koutn |
| Degree (after name) | <input type="text"/> | Ph.D. |
| Generational resolution | <input type="text"/> | III. |
| E-mail *) | <input type="text"/> | jirina_koutna@ica.cz |
| The certificate is designed for communication with public authorities of the SR | <input type="checkbox"/> | Mark the item if you require that the certificate can be used for communication with public authorities of the the SR and a private key to generate certified products according to Slovak legislation |
| Permanent Address | | |
| Street | <input type="text"/> | esk |
| Street number/building identification number | <input type="text"/> | 11/22 |
| City/town | <input type="text"/> | Brno |
| Zip code | <input type="text"/> | 11150 |
| Province | <input type="text"/> | Jihomoravsk |
| Country | <input type="text" value="Czech Republic"/> | |
| Other options | | |
| Revocation password | <input type="text" value="a"/> | Password for revocation may contain only the numbers and letters without accents. The password must be 4-32 characters. |
| Key Repository Type (CSP) | <input type="text" value="SecureStoreCSP"/> | |
| <input type="checkbox"/> Show advanced key usage settings (Recommended for experts). We do not recommend changing the default settings using the key. The change in the use of keys by the user's own risk. | | |
| Certificates for signing | <input checked="" type="checkbox"/> | |
| Certificates for encryption | <input type="checkbox"/> | |

Ak Vami zadan údaje splnj podmienky, zobraz sa vm strnka rekapitulujca vami zadan údaje.

4.3.Kontrola zadanch údajov

Na tejto strnke prosm skontrolujte vami zadan údaje.

| Recapitulated application | |
|---|-------------------------|
| Heading | Specified Value |
| Revocation password | aaaa |
| Period of validity | 365 days |
| Key Repository Type (CSP) | SecureStoreCSP |
| Algorithm thumbnails | sha256WithRSAEncryption |
| Allow exporting the private key | No |
| Allow the strong private key protection | No |
| Key length | 2048 |
| Certificates for signing | Yes |
| Certificates for encryption | No |
| Key name | 4d75ee7d94084 |
| Encoding type | UTF8_STRING |
| Items of the certificate request | |
| Full name | Jane Doe |
| E-mail | doe@ica.cz |
| Country | CZ |

The issued certificate is sent to the e-mail:

Certificate sent in the ZIP format:

Yes

No

Save the application in the card

Ak si prajete zasláť vydaný certifikát na e-mail, zadajte e-mailovú adresu, na ktorú vám bude certifikát zaslaný (položka **Vystavený certifikát zasláť na e-mail:**). Pozor: táto emailová adresa nie je súčasťou žiadosti o certifikát, teda nebude uvedená ani v samotnom certifikáte. E-mailovú adresu, ktorá bude obsiahnutá v certifikáte, je nutné vyplniť v údajoch o žiadateľovi (položka žiadosti o certifikát)!

Ak vami zvolený typ úložiska kľúča (CSP) podporuje uloženie žiadosti na kartu, môžete zatrhnúť možnosť **Uložiť žiadosť na kartu**. Ak zvolíte túto možnosť, stránka sa po vygenerovaní žiadosti pokúsi uložiť vygenerovanú žiadosť na kartu. Uistite sa, že na vašej karte je dostatok voľného miesta pre uloženie žiadosti. Ak uložíte žiadosť na kartu, operátor registračnej authority I. CA bude môcť načítať vašu žiadosť priamo z karty (nemusíte nosiť žiadosť na USB disku alebo inom médiu).

Kliknutím na tlačidlo **Vytvoriť žiadosť** spustíte generovanie žiadosti o certifikát.

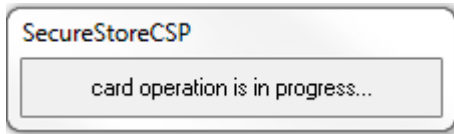
4.4. Generovanie žiadosti o certifikát

Nasledujúci postup sa pre jednotlivé typy úložiska kľúča (CSP) mierne líši.

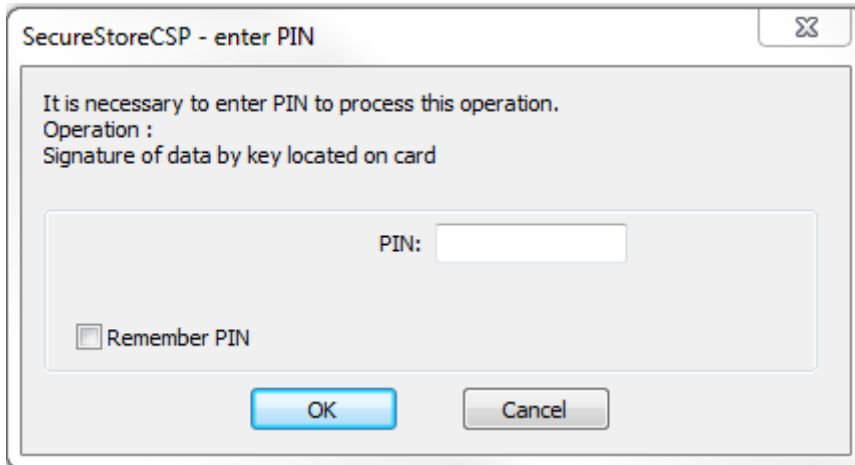
4.4.1. SecureStoreCSP

Ak pri vyplňovaní údajov o žiadateľovi zvolíte ako typ úložiska kľúča SecureStoreCSP, je postup generovania žiadosti nasledovný:

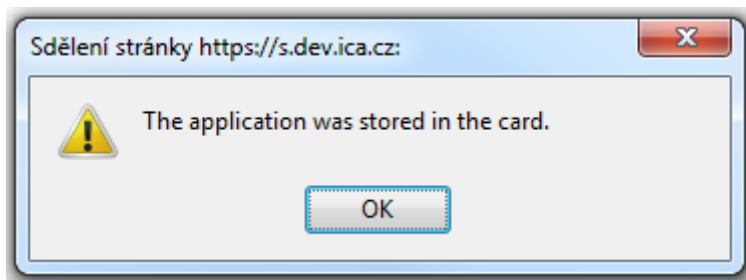
Najskôr sa vám zobrazí nasledujúci dialóg. V tomto momente sa generuje váš privátny kľúč. Tvorba privátneho kľúča môže trvať niekoľko desiatok sekúnd.



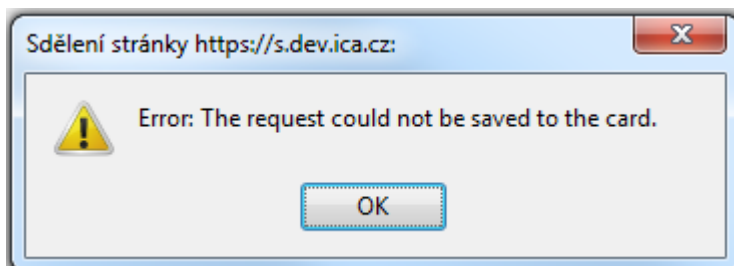
Potom čo je privátny kľúč vytvorený, ste vyzvaný na zadanie PINu k vašej karte.



Ak ste zvolili, že žiadosť má byť uložená na kartu, ste informovaný o výsledku uloženia. Ak bolo na karte dostatok miesta a žiadosť sa podarilo uložiť, je Vám zobrazený nasledujúci dialóg:



Ak na karte nebol dostatok voľného miesta a žiadosť sa nepodarilo uložiť, zobrazí sa nasledujúci dialóg (váš privátny kľúč je na karte uložený poriadku a nie je potreba znovu kľúč generovať):



V takom prípade sa žiadosť na karte nenachádza. Musíte žiadosť uložiť na USB flash disk alebo iné médium, ktoré predložíte na registračnej autorite I.CA.

4.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou súkromého kľúča.

Ak pri vyplňovaní údajov o žiadateľovi zvolíte ako typ úložisko kľúče Microsoft Enhanced RSA and AES Cryptographic Provider (prípadne Microsoft Enhanced RSA and AES Cryptographic Provider /

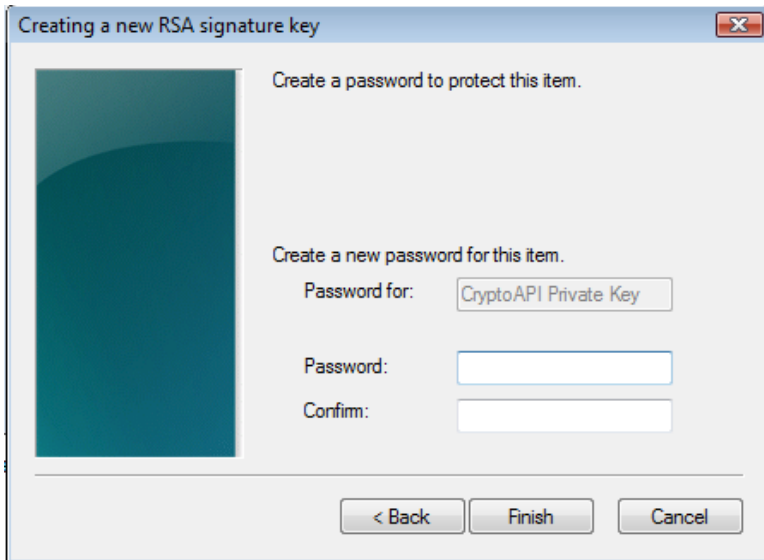
prototype /) a zaškrtnete voľbu Povolit' silnú ochranu kľúča, je postup generovania žiadosti nasledovný:



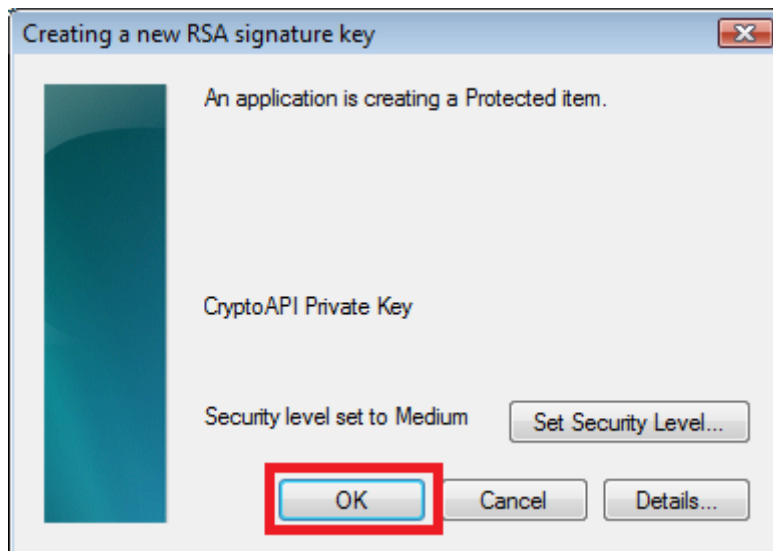
Ak kliknete na **Nastaviť úroveň zabezpečenia ...**, budete môcť zmeniť úroveň zabezpečenia.



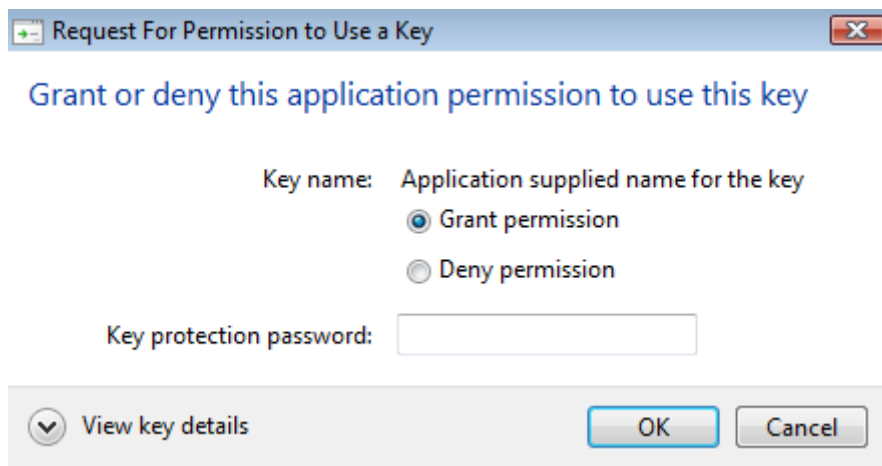
Ak zvolíte vysokú úroveň zabezpečenia, budete vyzvaný na zadanie hesla. Toto heslo bude potrebné zadať vždy, keď budete používať súkromný kľúč.



Po kliknutí na tlačidlo **Dokončiť** dôjde k zmene úrovne zabezpečenia. Teraz kliknite na tlačidlo **OK**.



V ďalšom dialógovom okne vyberte **Prideliť privilégiá**. Ak ste zvolili vysokú úroveň zabezpečenia, musíte zadať aj heslo.



4.5. Uloženie žiadosti o certifikát

Ak nedošlo pri generovaní žiadosti k chybe, stránka vám zobrazí vygenerovanú žiadosť vo formáte PKCS10. Kliknutím na tlačidlo **Uložiť žiadosť na disk** bude žiadosť uložená na váš pevný disk alebo iné médium, ktoré zvolíte.

The certificate request has been generated.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICnTCCAYUCAQAwIDERMA8GA1UEAwISmFuZSBEb2UxCzAJBgNVBAYTAkNaMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAI496mTv+wq8V1H/e1/hdWiNytYMs0VxjgREL9uQt
kq8WIGI5kak64Cvw6n+e0/cRHkspUIB8xvswWqJJ/j94bp2b9JtdWIDuPRtkFluhSzEgx4Gm
7X39UWAhTW1zVE+cwjrlUKESJmOMd+ZfnIYNTuV6A+ieyzCk9fbsJXay09T3F2smBbgIejj0
LJdLNUoWMDN3Zqst2GED1Md+cYdEU1e0GuVjhuhKWxchX0JkxyIpy3zgxkt1REnUIVDRNJ1M
aDAXCbQYt1s82pFO3rUZHvwSVRokLD+0I66YeqHxW2rh1YHU/jj6Jg0E+vq8mNvQgmFkw1dI
bzU1WVaCaSPspQIDAQABoDgwNgYJKoZIhvcNAQkOMSkwJzAObGgNVHQ8BAf8EBAMCBsAwFQYD
VR0RBA4wDIEKZG91QG1jY35jejANBgkqhkiG9w0BAQsFAAOCAQEAhCbQXSM9/ZaBoPpi1h5U
08Kt2ZFdHeL7EuyG+E6itf2IB43OCxJFifB7JNFqBGL1i2h6aoB24gpWQfuRGLUIdo8QwAX1
XXenfT0WLq0RM2j08FUZnnokgQ+KBL7Tv1EClyiDi0Nz52EgpiYzfhlYX/5ulluoVYniPrN7
hbqAxi8BYBIhK6uEpUqNSD1G53MvvsYS/x3WhRkCIRrPazVJ2m6GR6djk7zCJBE11GJFTtZm
PnMn5qdcUyh/pV1+cZian3kXCGfqKxiWx4Toq9VRE5ia4Vr31XheaRpsxU8wGXSw8bF188P4
D0VIQIokI+/Uq/qWY+YUv5q8HeAIDVDbfw==
-----END CERTIFICATE REQUEST-----
```

Save request to the disc

5. Vystavenie certifikátu

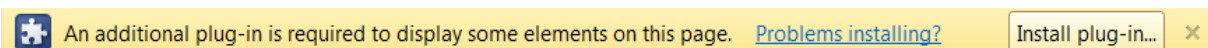
Potom, čo vytvoríte žiadosť o certifikát, je nutné navštíviť niektorú registračnú autoritu I. CA ([zoznam tu](#)). So sebou na registračnú autoritu I. CA prineste žiadosť, ktorú ste vygenerovali (napríklad na USB flash disku, uloženú na čipovej karte), a dokumenty potrebné na vystavenie certifikátu. Zoznam potrebných dokumentov nájdete [tu](#).

6. Inštalácia Java Runtime Environment (JRE)

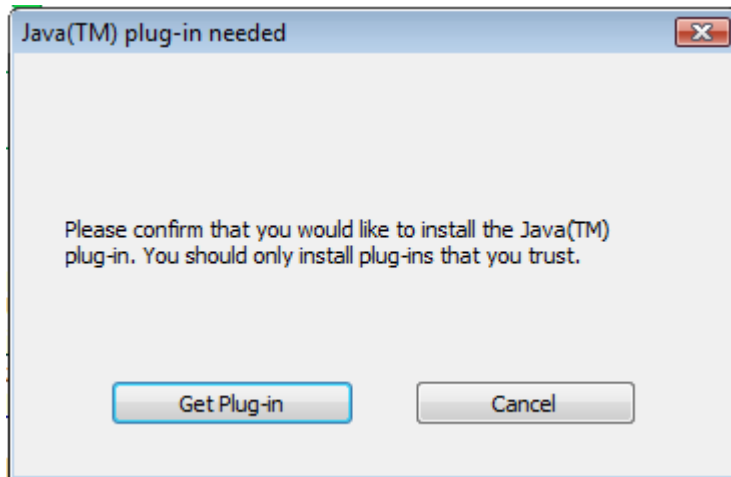
Inštalácia JRE prebieha v rámci jednotlivých prehliadačov rôznymi spôsobmi. Na jednom počítači nie je potrebné inštalovať JRE v každom prehliadači zvlášť, lebo po nainštalovaní funguje podpora JRE v rámci celého operačného systému a teda aj v prehliadači, v ktorom ste inštaláciu JRE nevykonávali.

6.1. Spustenie inštalácie JRE pod prehliadačom Google Chrome

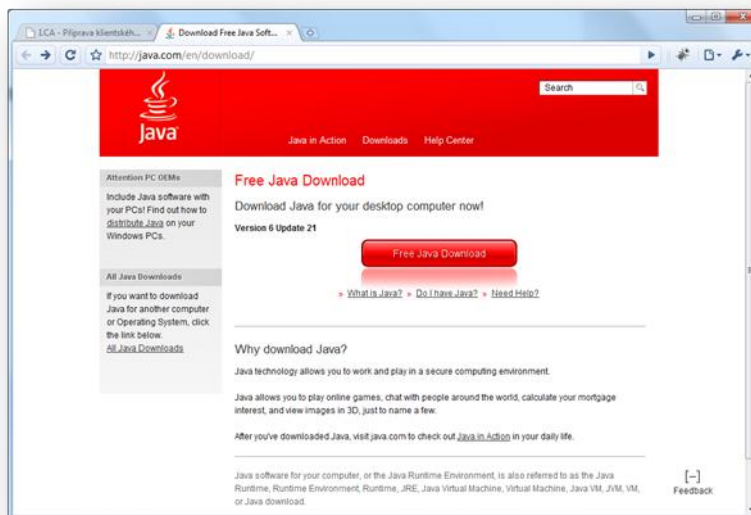
Ak nemáte nainštalovanú podporu Java Runtime Environment, budete pri prvom prístupe na stránky pre generovanie žiadosti o certifikát vyzvaný k jej inštalácii. V prehliadači Google Chrome sa zobrazí varovná lišta v hornej časti obrazovky prehliadača informujúca o nutnosti doinštalovať zásuvný modul.



Kliknutím na tlačidlo varovnej lišty **Inštalovať plugin...** sa zobrazí inštaláčny dialóg podobný tomu:



Tu zvolíte možnosť **Získať plugin** a otvorí sa stránka s ponukou na stiahnutie JRE.



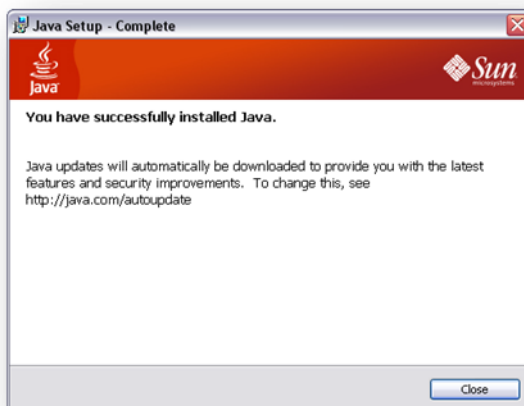
Na tejto stránke kliknite na červené tlačidlo **Free Java Download** a na nasledujúcej stránke na podobné červené tlačidlo **Agree and Start Free Download**, čím zahájite sťahovanie inštalačného programu. Po dokončení sťahovania ho spustíte; priebeh inštalačného programu je popísaný v **Kapitole 7**.

7. Instalační program JRE

Po spustení inštalačného programu JRE sa zobrazí prvé okno inštalačného programu.



Na úvodnej obrazovke zvolte tlačidlo **Install**. Ďalej je proces inštalácie až do konca automatický. Inštaláčny program si následne stiahne z internetu dodatočné súbory, ktoré potrebuje zavedenie JRE do vášho počítača.



Na záverečnej obrazovke kliknite na tlačidlo **Close**. V tejto chvíli odporúčame prehliadač vypnúť a zapnúť, aby sa prejavili zmeny.

8. Riešenie problémov

V prípade vzniku chyby počas procesu generovania žiadosti budete informovaný chybovou hláškou.



V treťom odseku nájdete popis chyby.

Niektoré chyby môžu byť závažnejšieho technického rázu. Môžu súvisieť so stavom hardvérového alebo softvérového vybavenia vášho počítača. Je dôležité opísať, urobiť screenshot, alebo inak uchovať informácie z podrobného výpisu chybového hlásenia, pretože tieto informácie sú kritické pre rýchle vyriešenie problémov s helpdeskom.