Generovanie žiadosti o certifikát

Užívateľská príručka pre prehliadač

Opera

První certifikační autorita, a.s.

17.1.2011

Verzia 7.06

Obsah

1. Úvod

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

2. Požiadavky na software

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

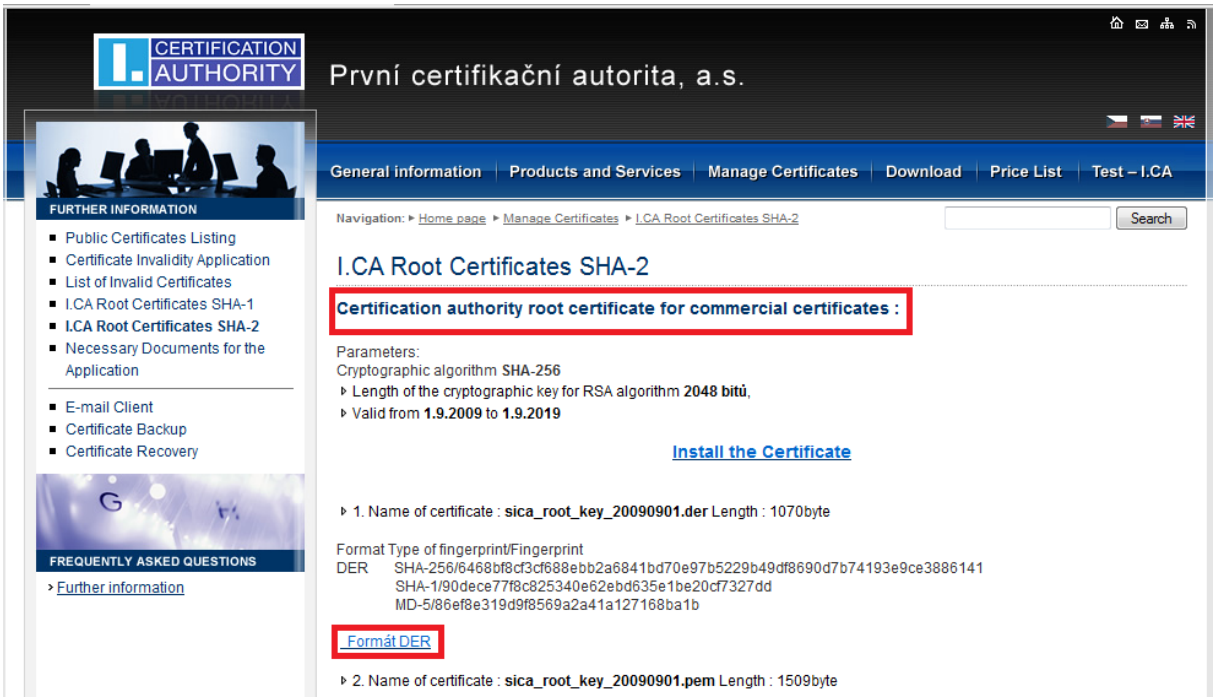
- Musí mať nainštalovaný a spustený operačný systém
    - **Microsoft Windows XP**
    - **Windows Vista**
    - **Windows 7**
- Musí byť nainštalovaný a použitý niektorý z nasledujúcich prehliadačov (pre generovanie žiadosti)
    - **Microsoft Internet Explorer** (verzia 7 a vyššie).
    - **Mozilla Firefox** (verzia 3 a vyššie)
    - **Google Chrome** (verzia 2 a vyššie)
    - **Apple Safari** (verzia 4 a vyššie)
    - **Opera** (verzia 10 a vyššie)
- 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 zistí, že softvér prítomný nie je, vyzve užívateľa k jeho stiahnutiu / inštaláciu.
    - **V prípade, že máte nainštalovanú staršiu verziu JRE, ako je** uvedená v požiadavkách, odinštalujte ju pred začatím generovania žiadosti o certifikát. Následne budete stránkami nasmerovaní na stiahnutie najaktuálnejšie verzie.
- Vo vašom internetovom prehliadači musíte mať zapnutú **podporu Javascript, zapnutú podporu jazyku Java, podporu ukladanie cookies.**

3. Inštalácia koreňového 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, ženemáte uložené v úložisku koreňové certifikáty I.CA.

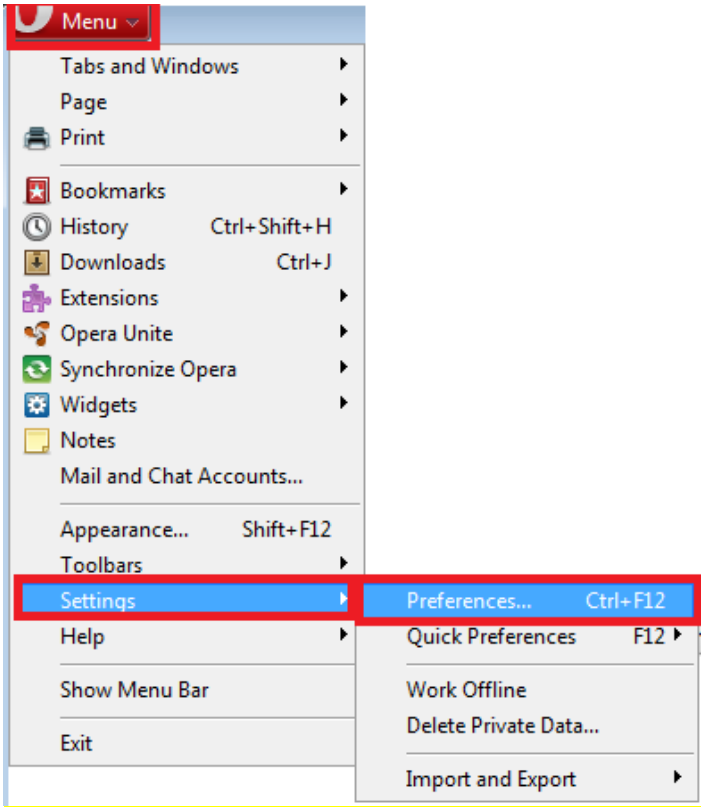
Zadajte do prehliadača nasledovné URL: http://www.ica.cz/cz/menu/112/prace-s-certifikaty/korenove-certifikaty-i-ca-sha-2/

Zobrazí sa vám nasledujúca stránka:

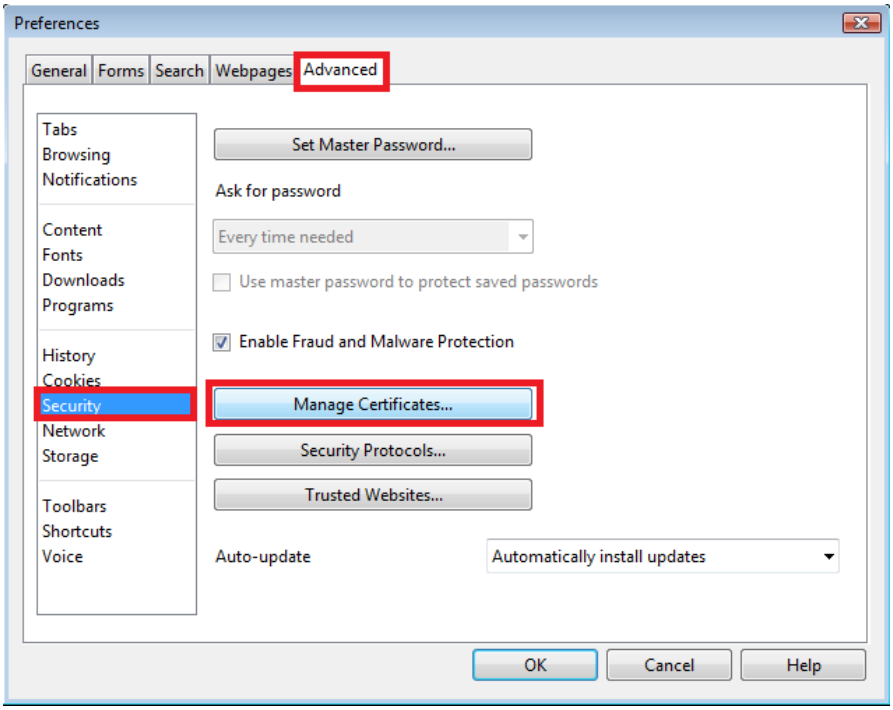


Pod nadpisom **Koreňový certifikát certifikačnej autority pre vydávané komerčné certifikáty** kliknite na **Formát DER**. Zobrazí sa vám dialóg pre stiahnutie súboru. Súbor obsahujúci certifikát uložte na Váš pevný disk.

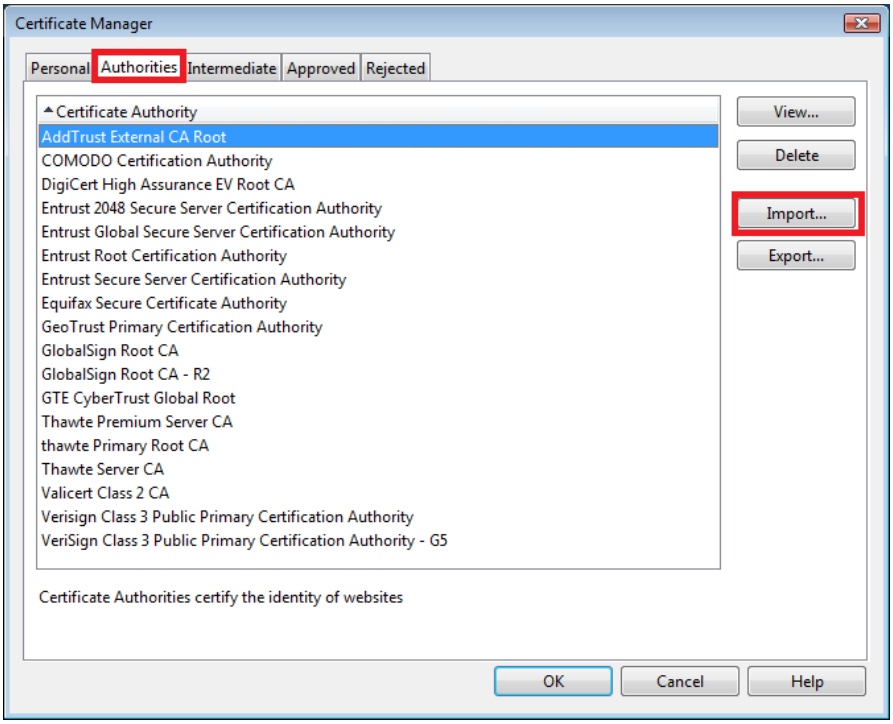
V prehliadači Opera kliknite na **Menu**, vyberte **Nastavenia** a ďalšie ponuky **Nastavenia** ...



Zvoľte záložku **Pokročilej voľby**. Zo zoznamu vyberte položku **Zabezpečenie** a kliknite na tlačidlo **Správca certifikátov ...**

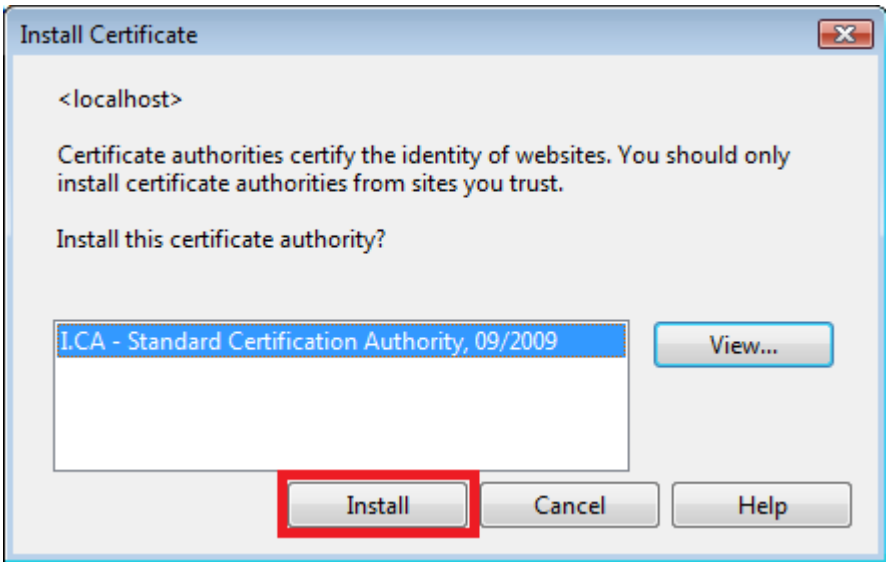


Zvoľte záložku **Certifikačné autority** a kliknite na tlačidlo **Importovať...**

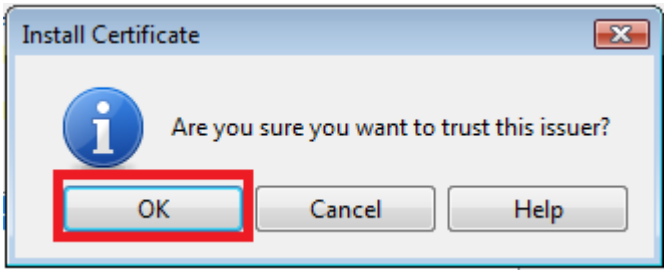


Vyberte certifikát, ktorý ste uložili na pevný disk.

Kliknite na tlačítko **Inštalovať.**



Potvrďte stlačením tlačítka **OK**



Všetky otvorené okná zatvorte stlačením tlačidla OK **OK**.

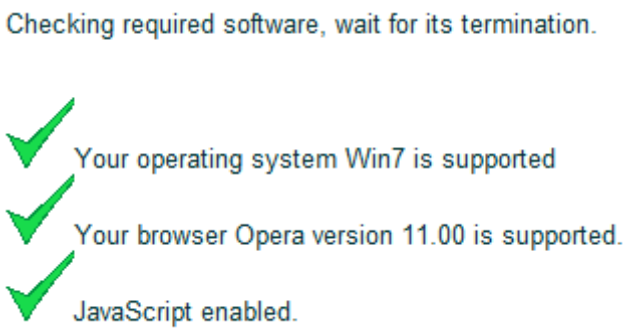
4. Proces generovania žiadosti o certifikát

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.



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 0.

4.1.2.Nepodporovaný internetový prehliadač

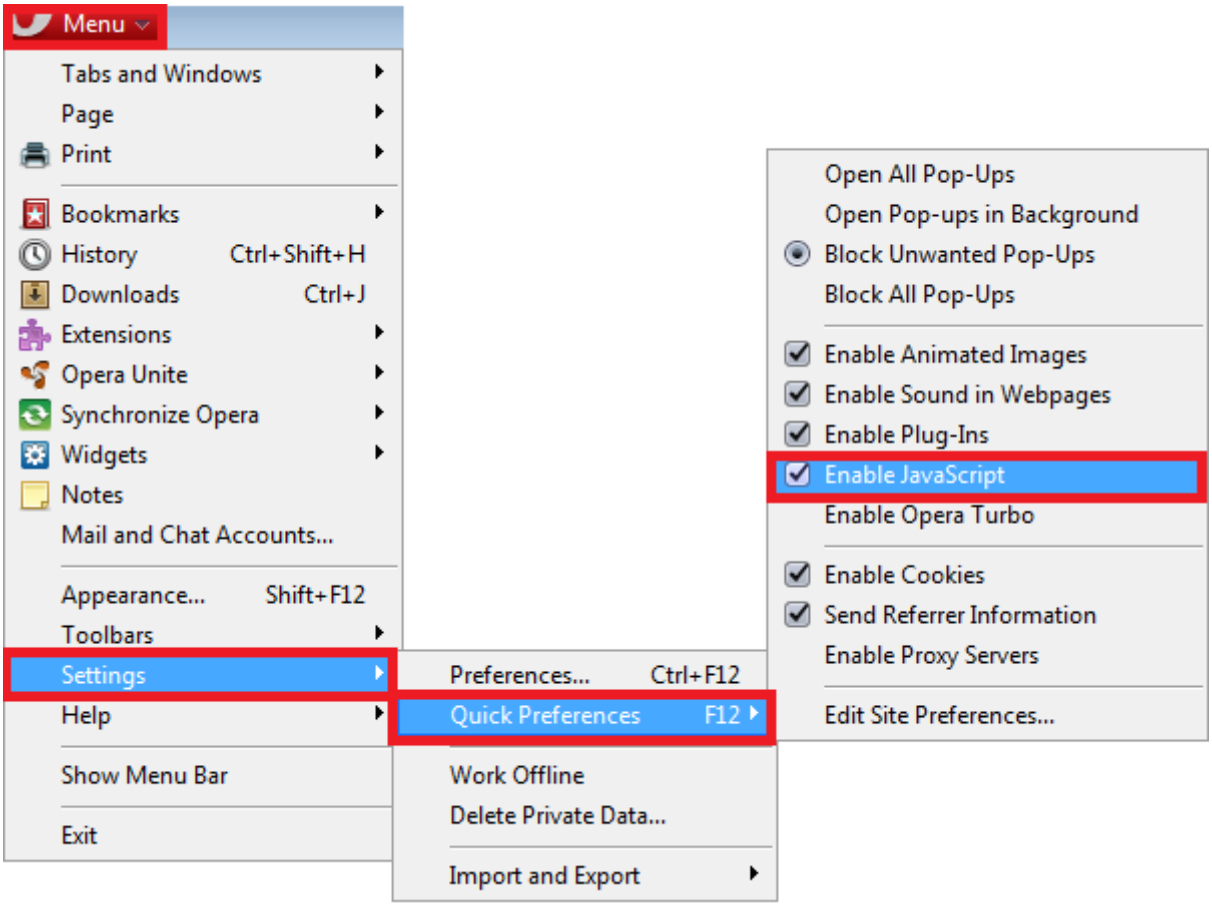
Pre generovanie žiadosti musíte použiť jeden z prehliadačov uvedených v kapitole 0.

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 Opera

Kliknite na **Menu**, v ponuke vyberte **Nastavenia**, objaví sa ďalšia ponuka, z ktorej vyberte **Rýchle nastavenia** a kliknite na **Povoliť JavaScript**.



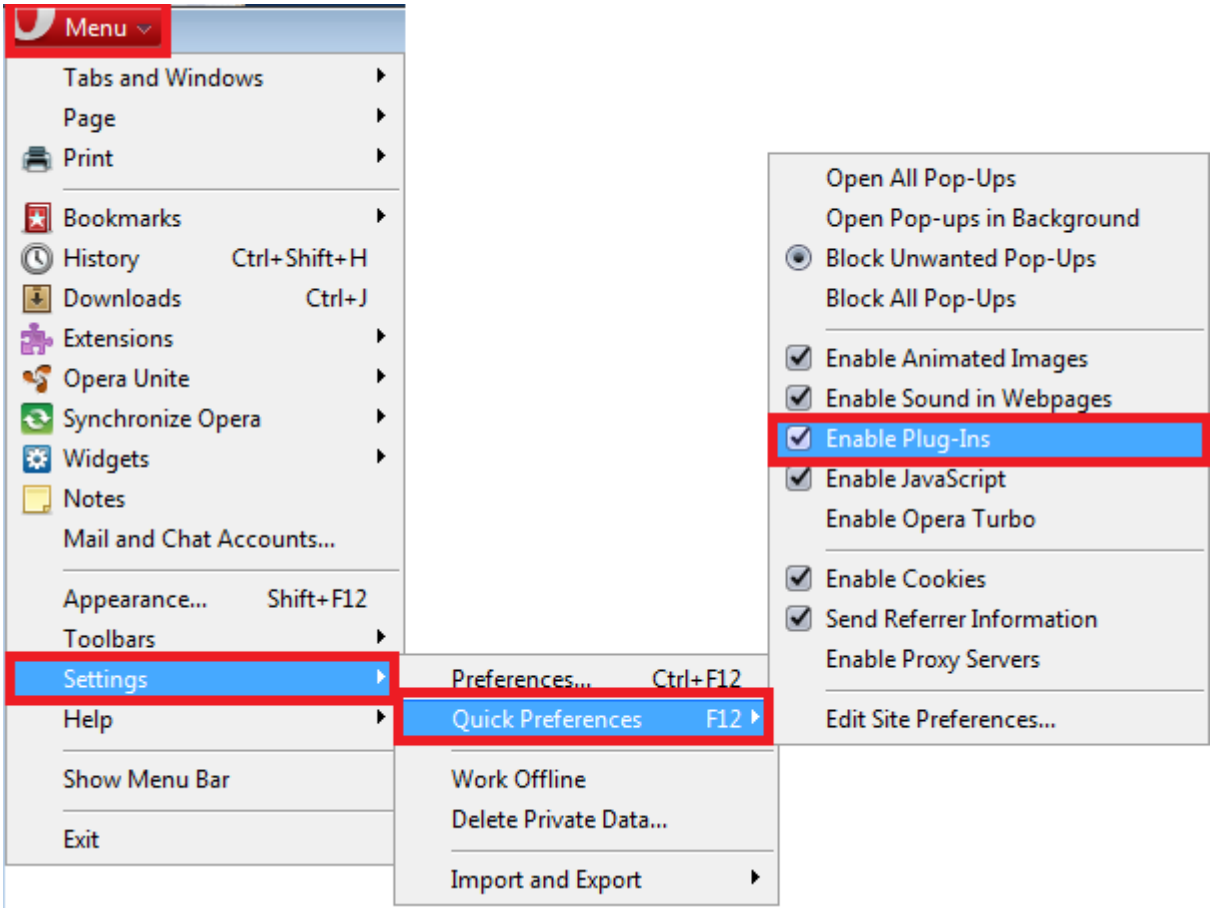
4.1.4.Podpora Java Runtime Environment (JRE)

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 nastránke 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.**

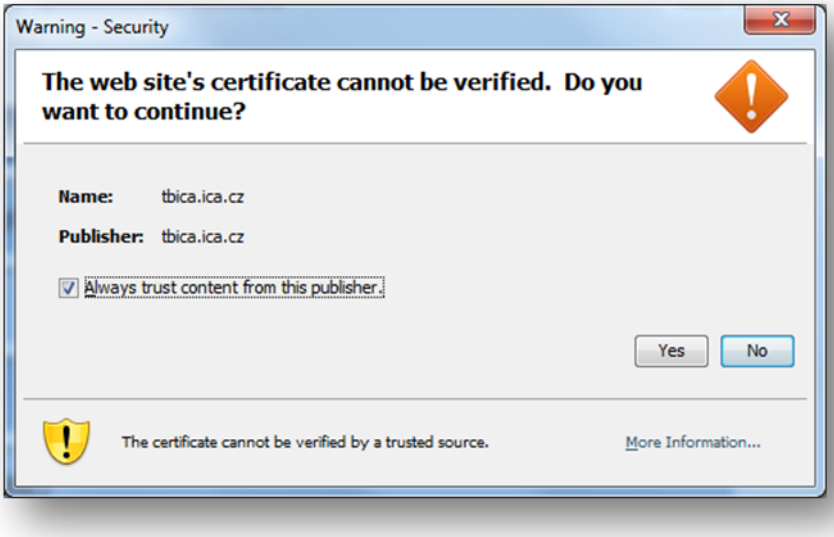
4.1.4.1.Povolenie Java v Opera

Kliknite na **Menu**, v ponuke vyberte **Nastavenia**, objaví sa ďalšia ponuka, z ktorej vyberte **Rýchle nastavenia** a následne kliknite na **Povoliť zásuvné moduly.**

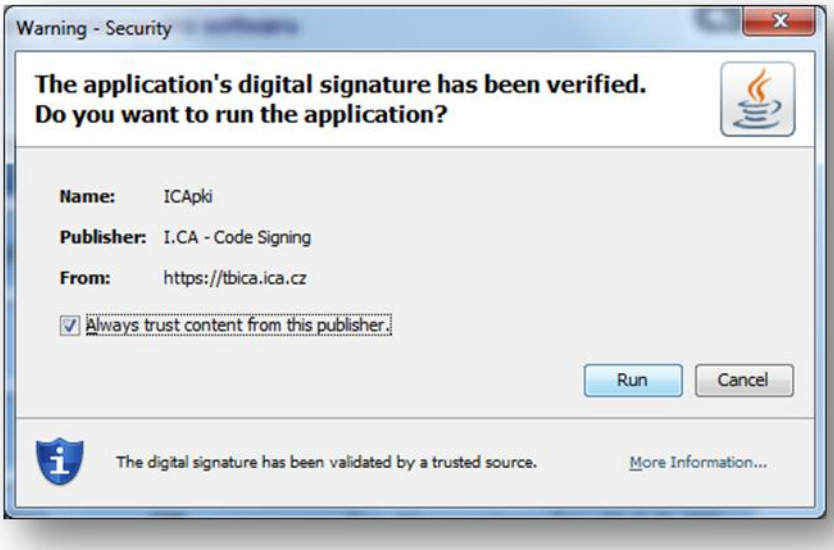


4.1.5.Nainštalovaný Java Applet ICApki

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 dôležitézaškrtnúť voľbu **Always trust content from this publisher** a potom použiť tlačidlo **Yes**.



Nasleduje druhý dialóg, kde sa postupuje obdobne, a síce zaškrtne 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 vyzývaný.

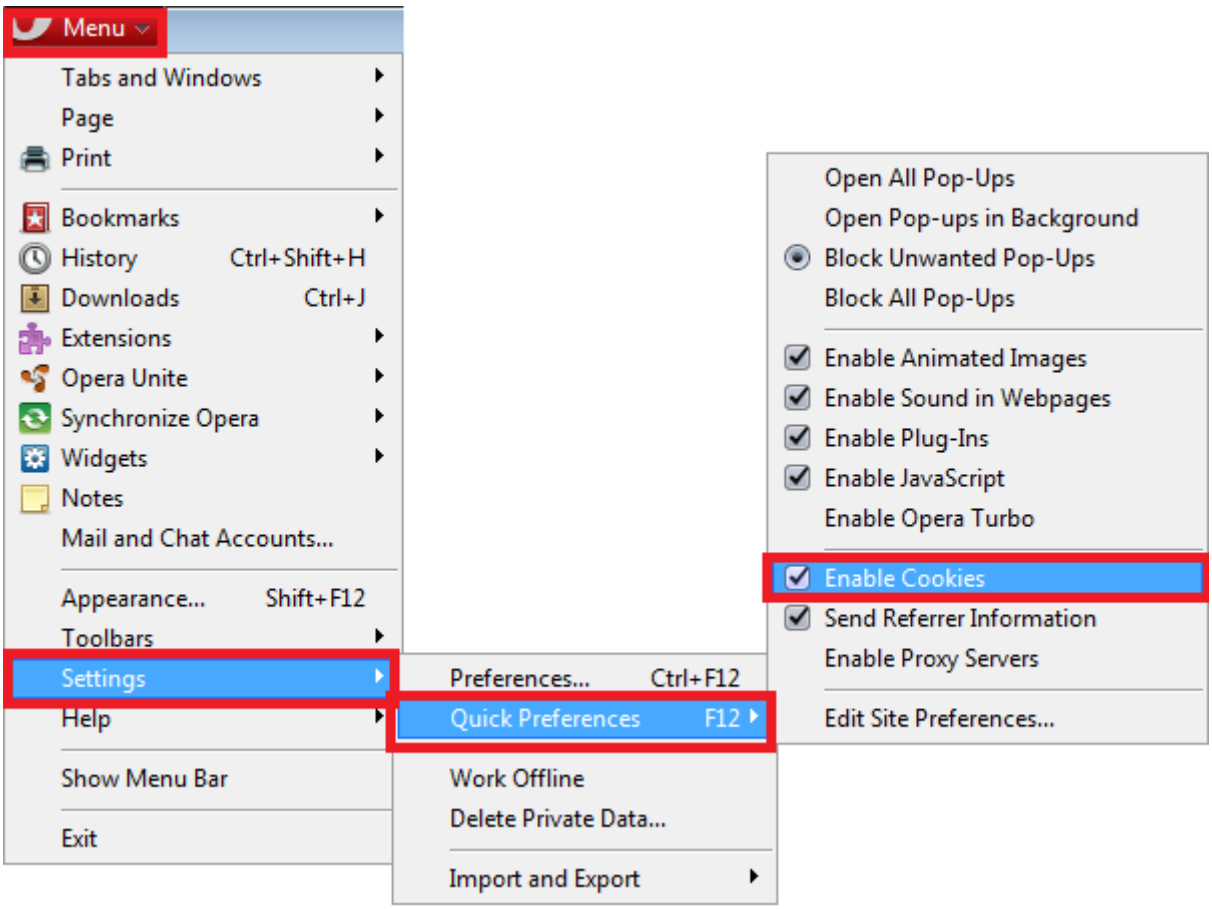
V prípade, že bude vydaná nová verzia Java Applet ICApki, bude klientom v tomto mieste okamžite automaticky stiahnutá a nainštalovaná. Táto inštalácia môže chvíľu trvať. Po jej skončení budú stránky pokračovať v normálnej práci.

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.

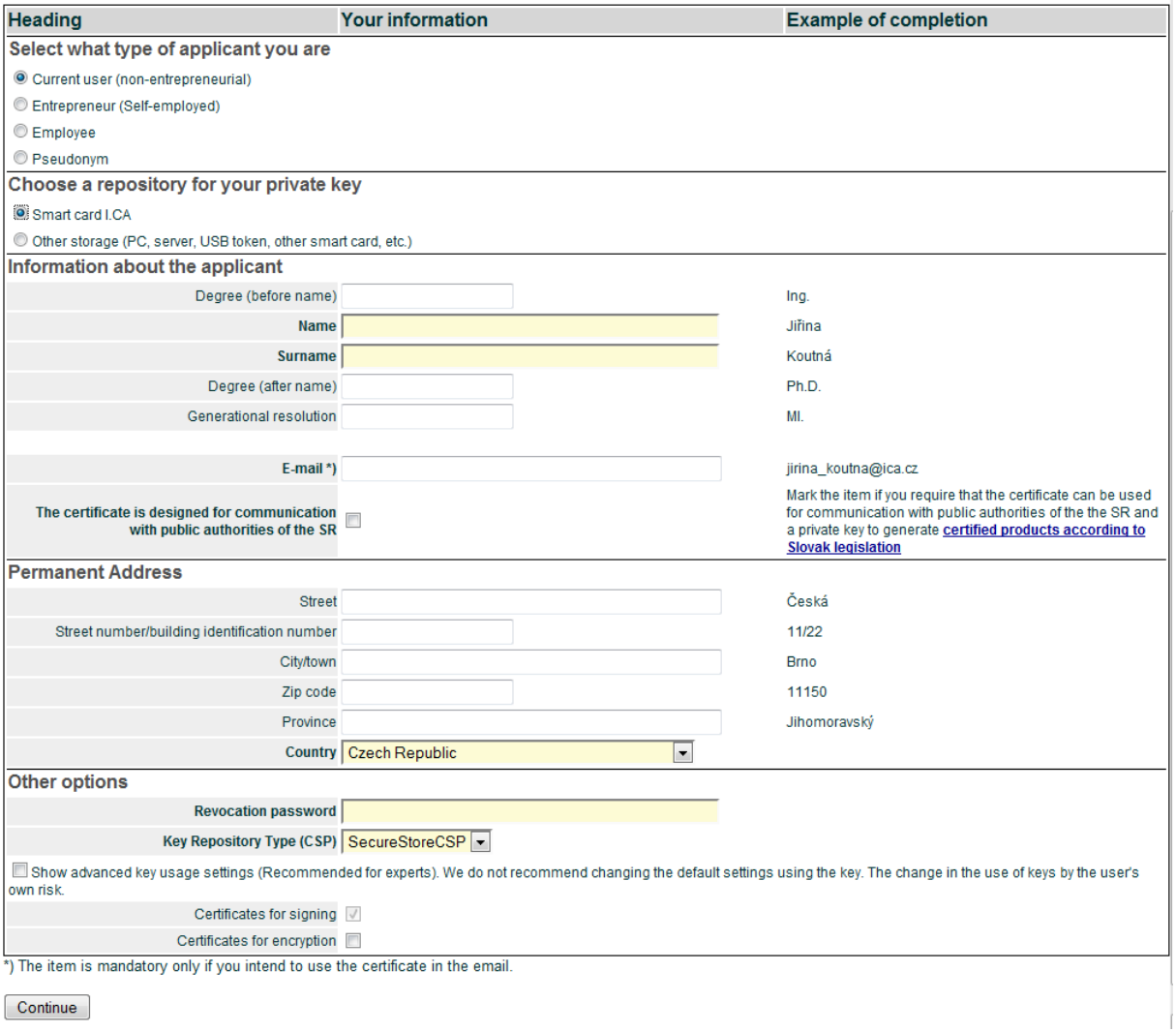
4.1.6.1.Povolenie cookies v Opera

Kliknite na **Menu**, v ponuke vyberte **Nastavenia**, objaví sa ďalšia ponuka, z ktorej vyberte **Rýchle nastavenia** a následne kliknite na **Povoliť cookies.**



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		
(•) Current user (non-entrepreneurial)		
( ) Entrepreneur (Self-employed)		
( ) Employee		
( ) Pseudonym		
Choose a repository for your private key		
(•) Smart card I.CA		
( ) Other storage (PC, server, USB token, other smart card, etc.)		
Information about the applicant		
Degree (before name)		Ing.
Name		Jiřina
Surname		Koutná
Degree (after name)		Ph.D.
Generational resolution		MI.
E-mail *)		jirina_koutna@ica.cz
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		Česká
Street number/building identification number		11/22
City/town		Brno
Zip code		11150
Province		Jihomoravský
Country	Czech Republic	
Other options		
Revocation password		
Key Repository Type (CSP)	SecureStoreCSP	
[ ] 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	[x]	
Certificates for encryption	[ ]	

*) The item is mandatory only if you intend to use the certificate in the email.

Continue

Položky zdôraznené tučným písmom a žltým podfarbením vstupného polia 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 zneplatnit. Certifikát je možné zneplatnit cez webové rozhranie. Pri zneplatnenie budete vyzvaní na zadanie hesla pre zneplatnenie. Toto heslo pre zrušenie určujete pri generovaní žiadosti o certifikát.

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

Typ úložiska kľúča (CSP):

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

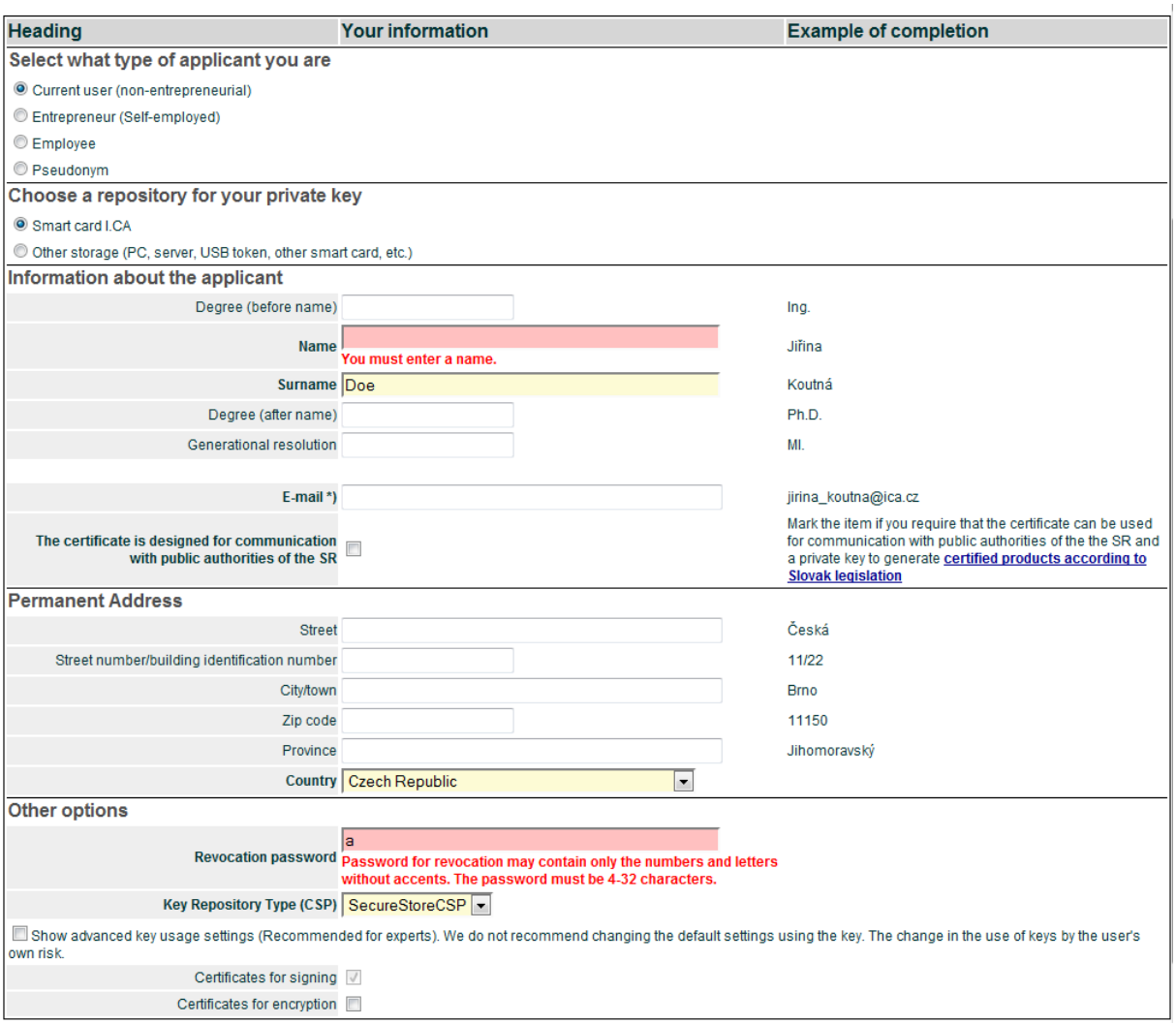
Export privátneho kľúča:

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

Silná ochrana privátneho kľúča:

Ak vami zvolený typ úložiska kľúča (CSP) podporuje silnú ochranu privátneho kľúča, je vám ponúknutá voľba **povoliť silnú ochranu privátneho kľúča**. Pred každým použitím vášho kľúča budete upozornení, že je váš kľúč používaný.Následne máte možnosť vybrať si medzi: Stredná - vždy budete len upozornený 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.



Ak Vami zadané údaje spĺňajú podmienky, zobrazí sa vám stránka rekapitulujúca vami zadané údaje.

4.3.Kontrola zadaných údajov

Na tejto stránke prosím skontrolujte vami zadané 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

Ak si prajete zaslať vydaný certifikát na e-mail, zadajte e-mailovú adresu, na ktorú vám bude certifikát zaslaný (položka **Vystavený certifikát zaslať 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 autority 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.

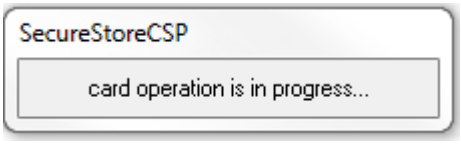
4.4.Generovanie žiadostí o certifikát

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

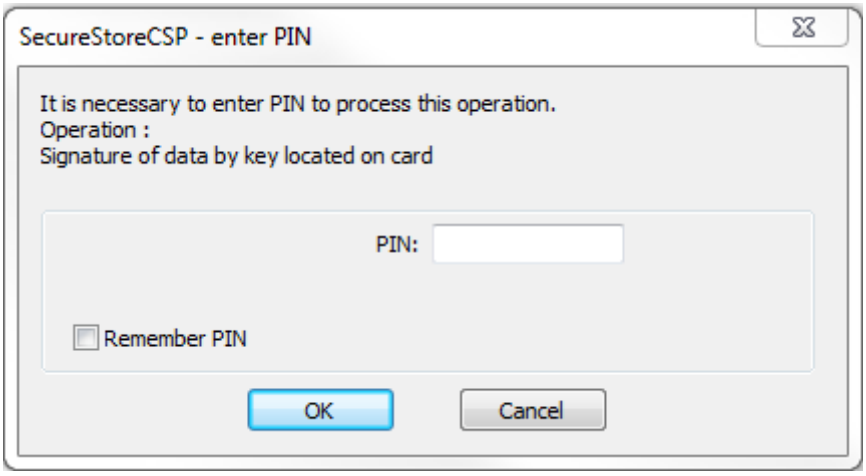
4.4.1.SecureStoreCSP

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

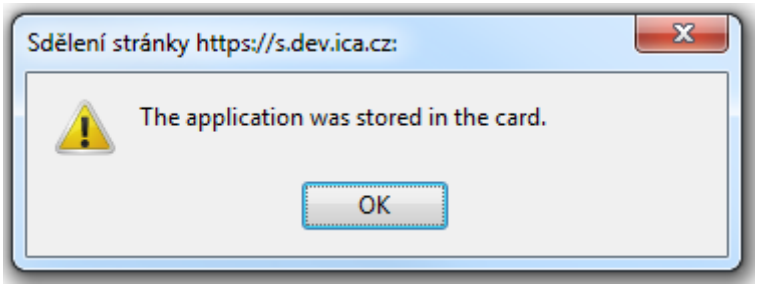
Najskôr sa vám zobrazí nasledujúci dialóg. V tomto momente sa generuje váš privátny kľúč. Tvorba privátneho kľúča môže trvať niekoľko desiatok sekúnd.



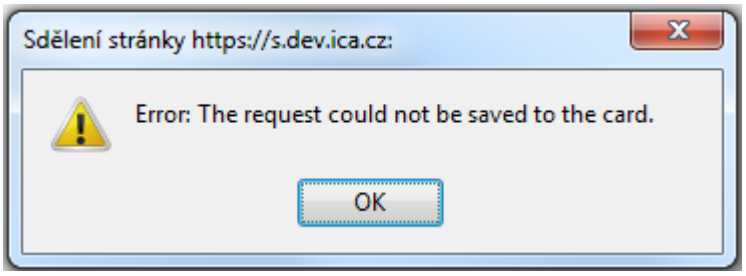
Potom čo je privátny kľúč vytvorený, ste vyzvaný na zadanie PINu k vašej karte.



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):



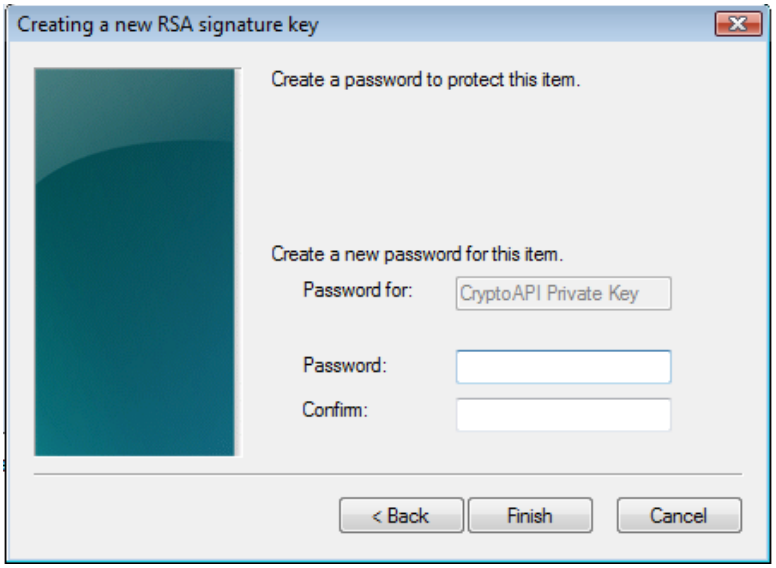
V takom prípade sa žiadosť na karte nenachádza. Musíte žiadosť uložiť na USB flash disk alebo iné médium, ktoré predložíte na registračnej autorite I.CA.

4.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider so silnou ochranou súkromného kľúča.

Ak pri vyplňovaní údajov o žiadateľovi zvolíte ako typ úložisko kľúča Microsoft Enhanced RSA and AES Cryptographic Provider (prípadne Microsoft Enhanced RSA and AES Cryptographic Provider / prototype /) a zaškrtnite voľbu Povoliť silnú ochranu kľúča, je postup generovania žiadosti nasledovný:

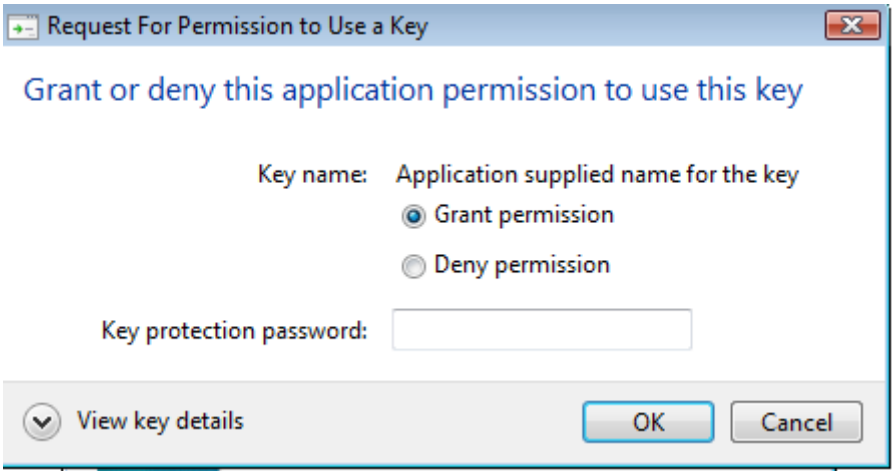
Ak kliknete na **Nastaviť úroveň zabezpečenia** ..., budete môcť zmeniť úroveň zabezpečenia.

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



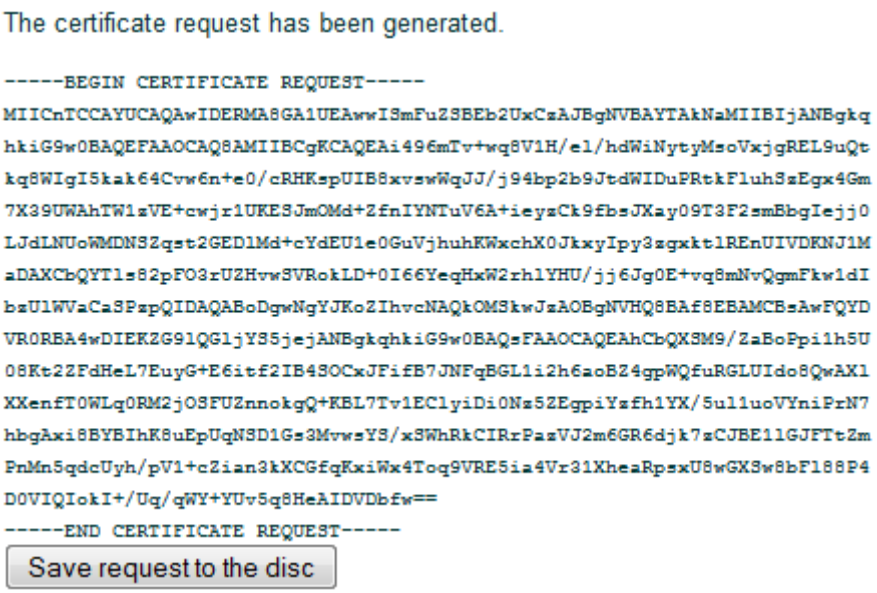
Po kliknutí na tlačidlo **Dokončiť** dôjde k zmene úrovne zabezpečenia. Teraz kliknite na tlačidlo **OK**.

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.



5. Vystavenie certifikátu

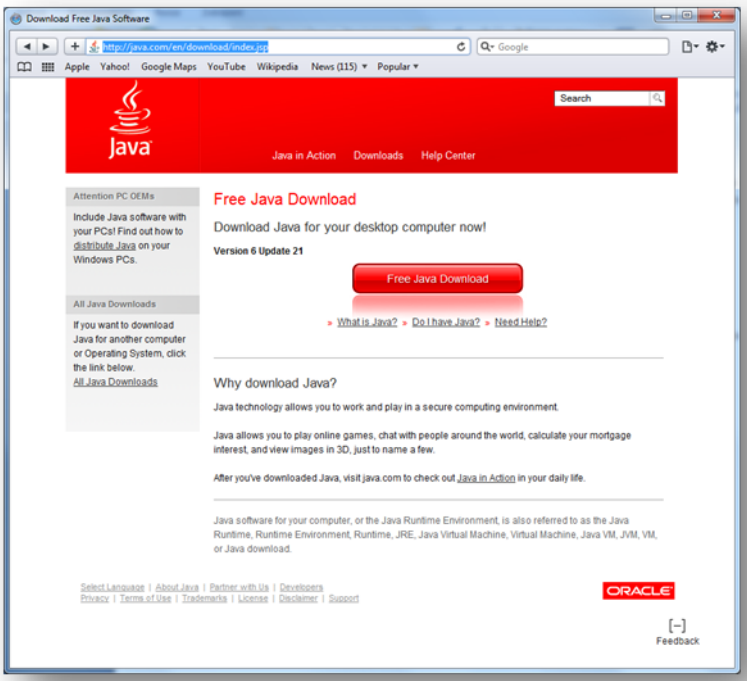
Potom, čo vytvoríte žiadosť o certifikát, je nutné navštíviť niektorú registračnú autoritu I. CA (zoznam tu). So sebou na registračnú autoritu I. CA prineste žiadosť, ktorú ste vygenerovali (napríklad na USB flash disku, uloženú na čipovej karte), a dokumenty potrebné na vystavenie certifikátu. Zoznam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

6. Inštalácia Java Runtime Environment (JRE)

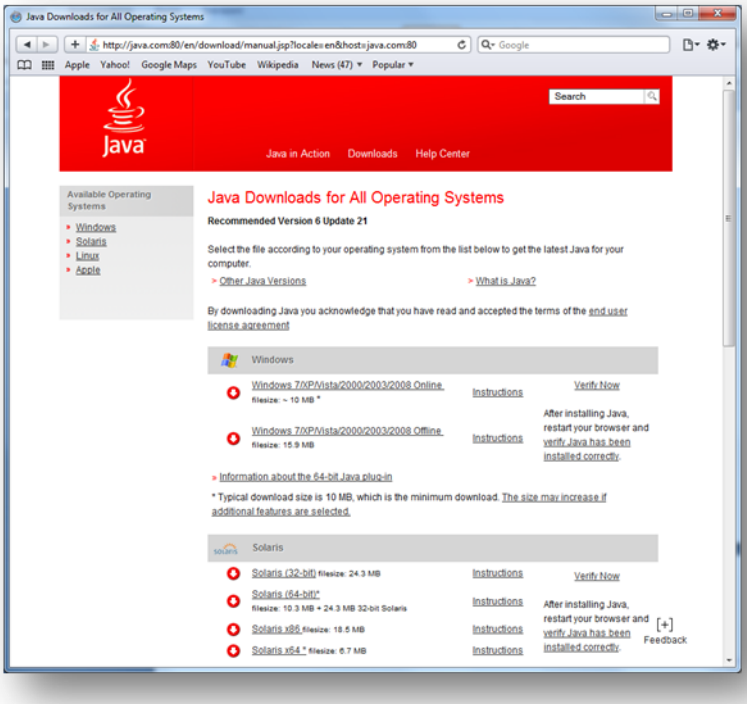
Inštalácia JRE prebieha v rámci jednotlivých prehliadačov rôznymi spôsobmi. Na jednom počítači nie je potrebné inštalovať JRE v každom prehliadači zvlášť, lebo po nainštalovaní funguje podpora JRE v rámci celého operačného systému a teda aj v prehliadači, v ktorom ste inštaláciu JRE nevykonávali.

6.1. Spustenie inštalácie JRE pod prehliadačom Opera

Prehliadač Opera neponúkne automatickú možnosť stiahnutia JRE, preto zadajte do prehliadača adresu http://java.com/en/download/index.jsp. Zobrazí sa úvodná stránka podobná tejto:



Na tejto stránke kliknite na červené tlačidlo **Free Java Download**, čím budete presmerovaný na nasledujúcu stránku

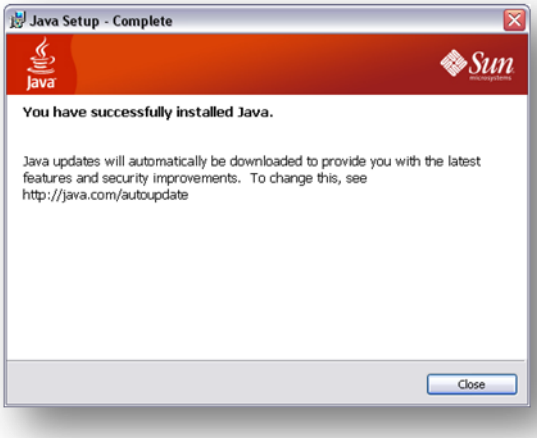


Na tejto stránke zvoľte **Offline** verziu instalačného programu pre Windows**,** čím zahájite sťahovanie inštalačného programu. Po dokončení sťahovania ho spustite; priebeh inštalačného programu je popísaný v **Kapitole 7**.

7. Inštalačný program JRE

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

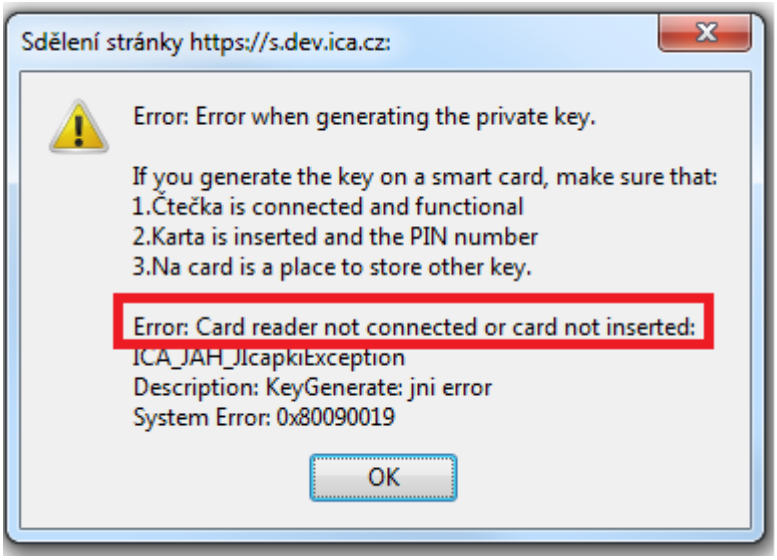
Na úvodnej obrazovke zvoľte tlačidlo **Install**. Ďalej je proces inštalácie až do konca automatický. Inštalačný program si následne stiahne z internetu dodatočné súbory, ktoré potrebuje zavedenie JRE do vášho počítača.



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.