První certifikační autorita, a.s.

Obnova certifikátu

Uživatelská příručka pro prohlížeč Internet Explorer

První certifikační autorita, a.s.
1.8.2011
Verze 7.07

Obsah

1. Úvod 3
2. Požadavky na software 4
   2.1. Nastavení prohlížeče Internet Explorer 4
3. Instalace kořenového certifikátu I.CA 7
4. Proces obnovy certifikátu 11
   4.1. Kontrola softwarového vybavení 11
      4.1.1. Nepodporovaný operační systém 12
      4.1.2. Nepodporovaný internetový prohlížeč 12
      4.1.3. Podpora JavaScriptu 12
      4.1.4. Podpora Java Runtime Environment (JRE) 13
      4.1.5. Nainstalovaný Java Applet ICApki 13
      4.1.6. Ukládání cookies 14
   4.2. Výběr certifikátu pro obnovu (volitelné) 14
   4.3. Doplnění a změna některých údajů 15
   4.4. Kontrola zadaných údajů 16
   4.5. Generování žádosti o obnovu 17
      4.5.1. SecureStoreCSP 17
      4.5.2. Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou soukromého klíče. 18
   4.6. Podpis a odeslání žádosti o obnovu 20
5. Instalace Java Runtime Environment (JRE) 22
   5.1. Spuštění instalace JRE pod prohlížečem Internet Explorer 22
6. Instalační program JRE 22
7. Řešení problémů 24

První certifikační autorita, a.s.

1. Úvod

Tento dokument slouží jako návod, jak postupovat při obnově certifikátu přes webové stránky.

První certifikační autorita, a.s.

2. Požadavky na software

Počítač, na kterém se bude provádět generování žádosti o certifikát, musí splňovat následující požadavky:

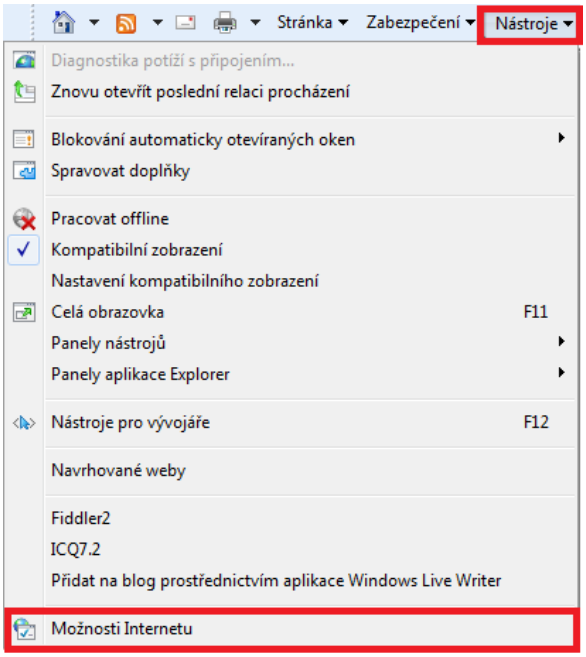
- Musí mít nainstalovaný a spuštěný operační systém
  - **Microsoft Windows XP**
  - **Windows Vista**
  - **Windows 7**
- Musí být nainstalován a použit některý z následujících prohlížečů (pro generování žádosti)
  - **Microsoft Internet Explorer** (verze 7 a výše).
  - **Mozilla Firefox** (verze 3 a výše)
  - **Google Chrome** (verze 2 a výše)
  - **Apple Safari** (verze 4 a výše)
  - **Opera** (verze 10 a výše)
- Musí mít nainstalovaný software **Java Runtime Environment** (dále **JRE**), alespoň verze **1.6.0_21**, který je potřebný pro správnou funkci webových stránek pro generování žádosti o certifikát.
  - Doporučujeme používat nejaktuálnější verzi JRE.
  - Přítomnost tohoto softwaru detekují stránky automaticky, pokud zjistí, že software přítomen není, vybídnou uživatele k jeho stažení/instalaci.
  - **V případě, že máte nainstalovanou starší verzi JRE, nežli je** uvedená v požadavcích, odinstalujte ji před zahájením generování žádosti o certifikát. Následně budete stránkami nasměrováni na stažení nejaktuálnější verze.
- Ve vašem internetovém prohlížeči musíte mít zapnutou podporu **skriptování Javascript , zapnutou podporu jazyku Java, podporu ukládání cookies.**

2.1.Nastavení prohlížeče Internet Explorer

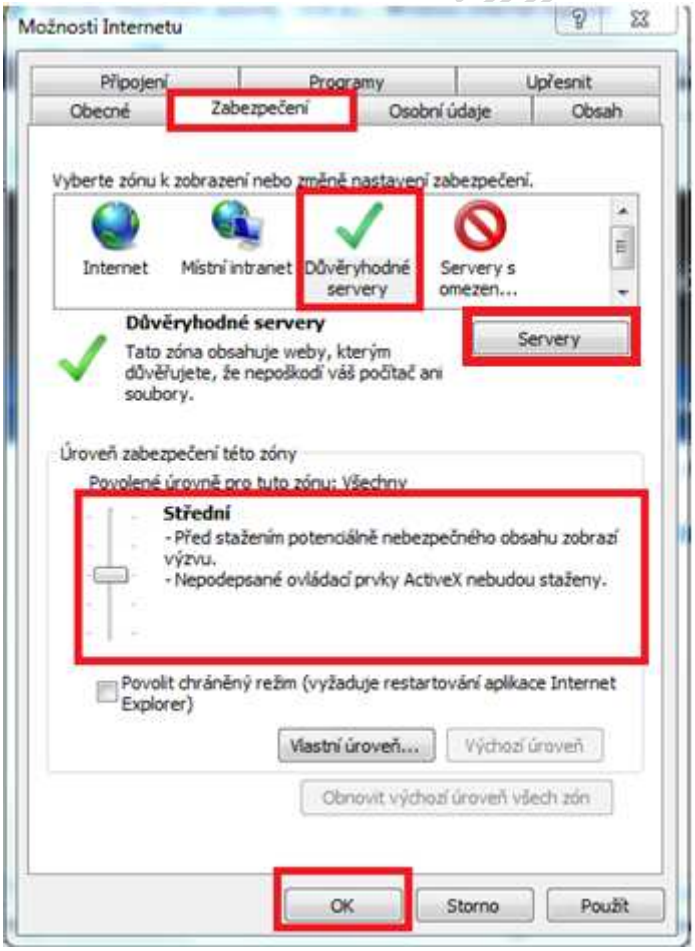
Pokud pro generování žádostí o certifikát používáte Internet Explorer, je nutné nastavit server s.ica.cz jako důvěryhodný.

Zvolte **Nástroje** a klikněte na nabídku **Možnosti Internetu**.

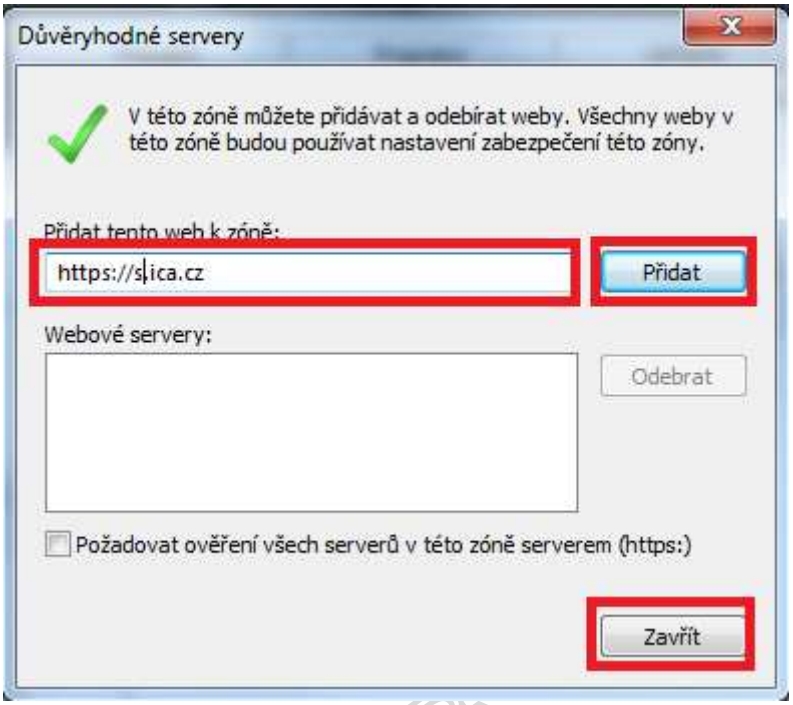
První certifikační autorita, a.s.



Klikněte na záložku **Zabezpečení** a zvolte **Důvěryhodné servery**. V nabídce **Úroveň zabezpečení této zóny** nastavte úroveň na **Střední**. Dále klikněte na tlačítko **Servery**.



Do pole **Přidat tento web k zóně** zadejte https://s.ica.cz. Klikněte na tlačítko **Přidat** a následně na tlačítko **Zavřít**.



Volbu potvrďte kliknutím na tlačítko **OK**.

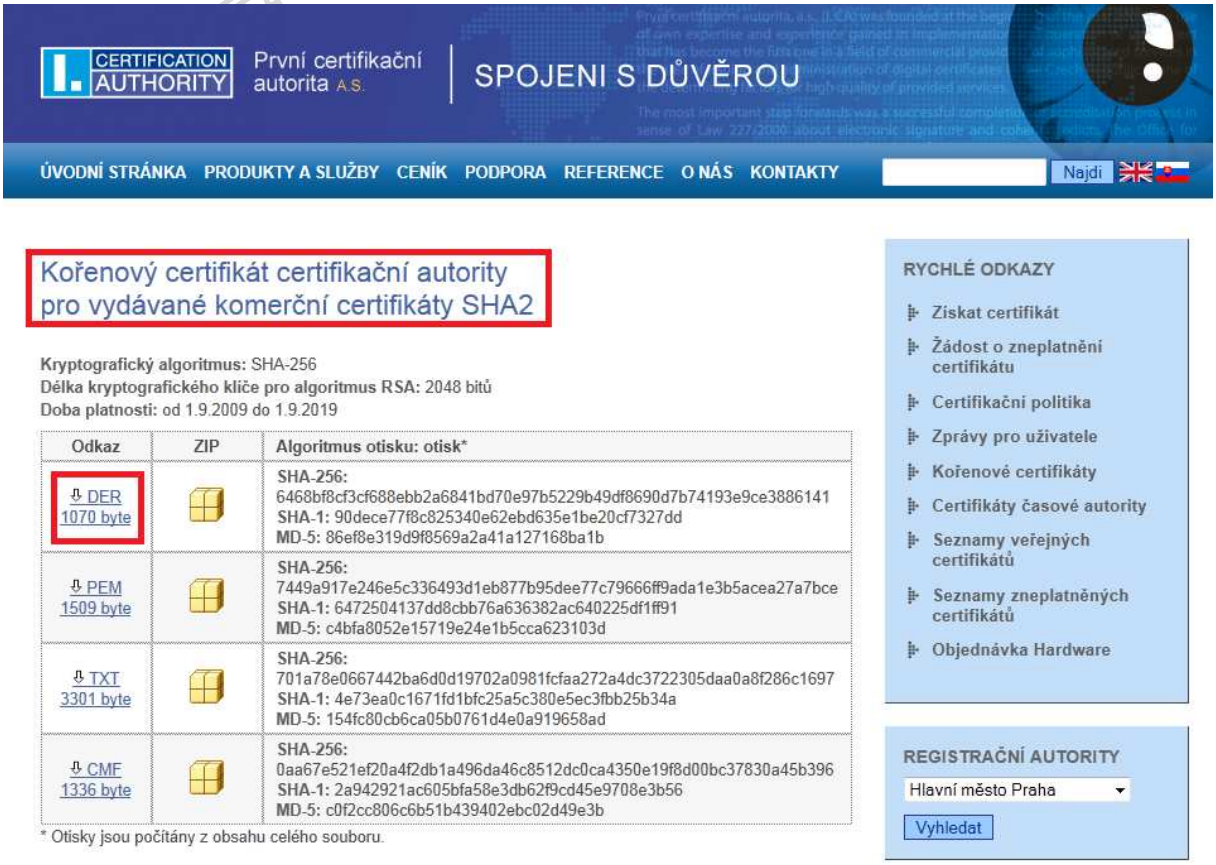
certifikační autorita, a.s.

3. Instalace kořenového certifikátu I.CA

Při spuštění stránky s žádostí o certifikát Vás může váš prohlížeč upozornit, že vstupujete na nedůvěryhodné stránky. Tento problém je způsoben tím, že nemáte uloženy v úložišti kořenové certifikáty I.CA.

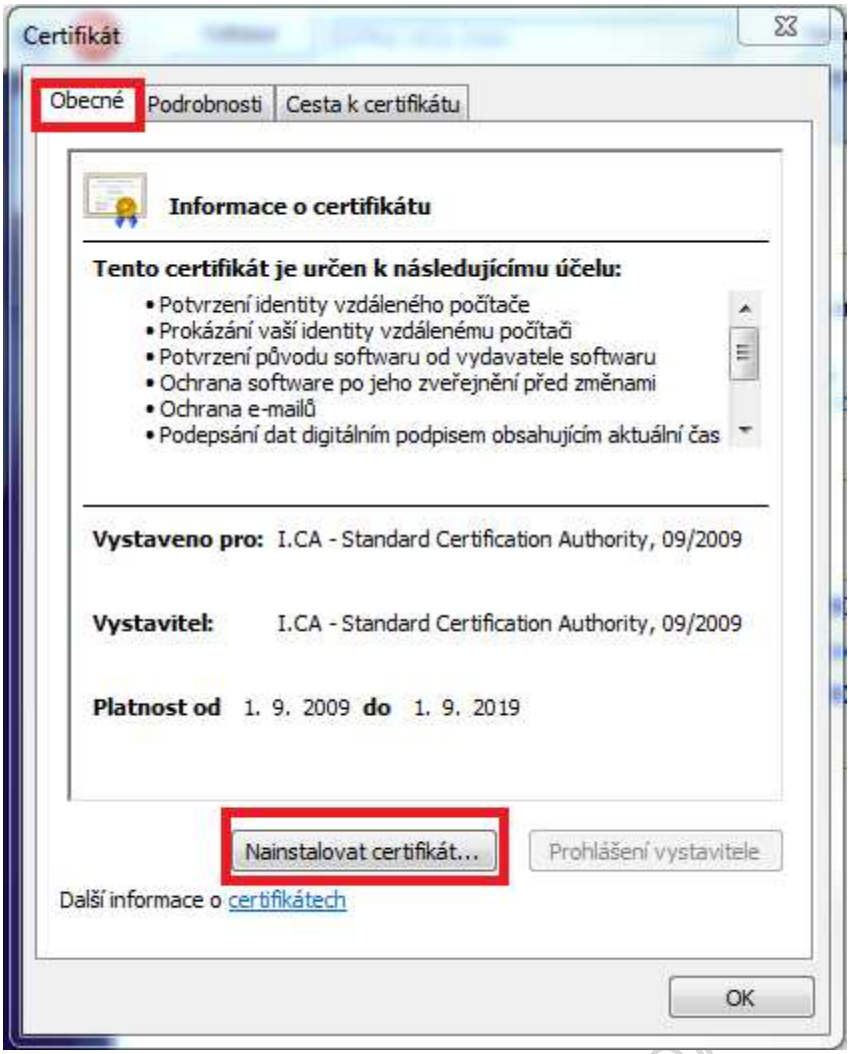
Zadejte do prohlížeče následující URL: http://www.ica.cz/SHA2-Komercni.aspx

Zobrazí se vám následující stránka:

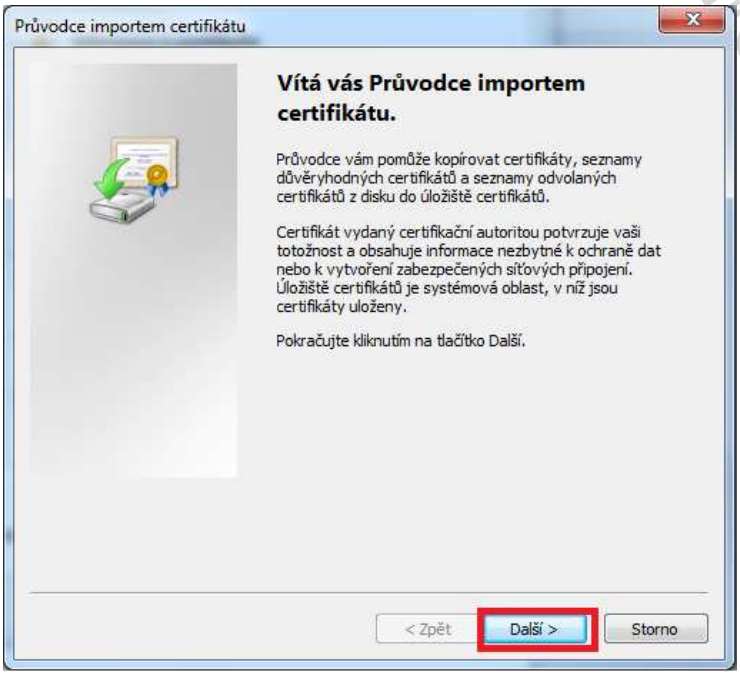


Pod nadpisem **Kořenový certifikát certifikační autority pro vydávané komerční certifikáty SHA2** klikněte na **DER**. Zobrazí se vám dialog pro stažení souboru. Soubor obsahující certifikát uložte na Váš pevný disk.

Dvojklikem otevřete soubor obsahující kořenový certifikát I.CA, který jste uložili na pevný disk. Tím dojde k zobrazení certifikátu. Na záložce **Obecné** klikněte na **Nainstalovat certifikát**.

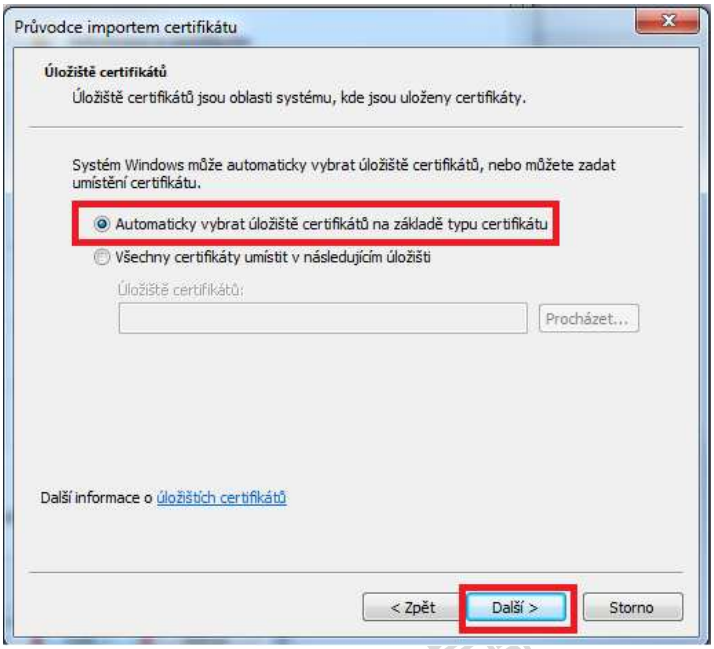


Spustí se průvodce instalací certifikátu. Klikněte na tlačítko **Další**.

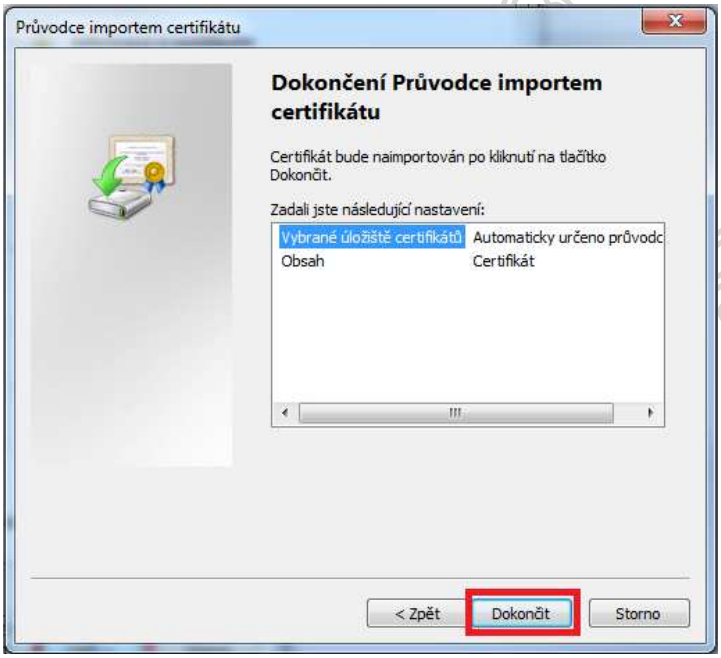


autorita, a.s.

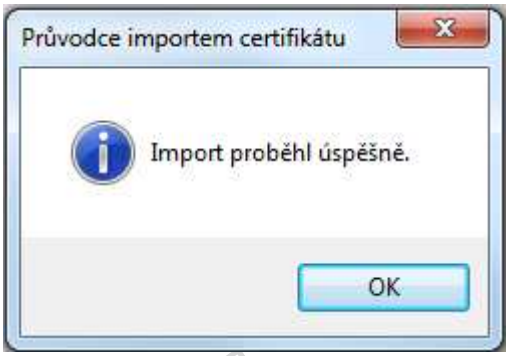
Zkontrolujte, že je zatržena volba **Automaticky vybrat úložiště certifikátů na základě typu certifikátu** a klikněte na tlačítko **Další**.



Klikněte na tlačítko **Dokončit**.



Průvodce by vás měl informovat o úspěšném importu.



První certifikační autorita, a.s.

4. Proces obnovy certifikátu

Postup generování žádosti o obnovu certifikátu je rozdělen do několika kroků:

- Kontrola softwarového vybavení
- Výběr certifikátu pro obnovu (volitelné)
- Doplnění a změna některých údajů
- Kontrola zadaných údajů
- Generování žádosti o obnovu
- Podpis a odeslání žádosti o obnovu

4.1.Kontrola softwarového vybavení

Pro usnadnění kontroly připravenosti Vašeho počítače pro obnovu certifikátu, je při zahájení obnovy zobrazena kontrolní stránka, která ověří přítomnost klíčových softwarových komponent.

Kliknutím na tlačítko **Zahájit test PC**, spustíte test Vašeho počítače.

První certifikační autorita, a.s.

Stránka otestuje počítač, test může trvat desítky sekund, a ohlásí, zdali je něco v nepořádku, případně vypíše chybové hlášení. Pokud nejsou detekovány problémy, kliknutím na tlačítko **Zahájit obnovu certifikátu** přejdete k samotné obnově certifikátu.

Pokud se při kontrole vyskytne chyba, nelze pokračovat v obnově certifikátu. Nejdříve je potřeba odstranit chybu, která znemožňuje obnovu. Význam chybových hlášení je uvedený v následujících kapitolách.

4.1.1. Nepodporovaný operační systém

Pro generování žádosti musíte použít jeden z operačních systémů uvedených v kapitole 2.

4.1.2. Nepodporovaný internetový prohlížeč

Pro generování žádosti musíte použít jeden z prohlížečů uvedených v kapitole 2.

4.1.3. Podpora JavaScriptu

Stránky pro generování žádosti o certifikát vyžadují podporu skriptování v jazyku JavaScript. Všechny podporované prohlížeče mají tuto podporu automaticky povolenu. Pokud by tato kontrola selhala, znamená to s největší pravděpodobností, že je v nastavení prohlížeče podpora scriptování vypnuta. Povolte podporu skriptování v jazyku JavaScript ve vašem prohlížeči.

autorita, a.s.

4.1.3.1.Povolení JavaScriptu v Internet Exploreru

Změňte nastavení podle návodu uvedeného v kapitole 2.1.

4.1.4.Podpora Java Runtime Environment (JRE)

Tyto stránky vyžadují pro svou funkčnost nainstalovanou podporu jazyka Java. Ujistěte se, že nemáte ve svém prohlížeči tuto podporu vypnutou. Pokud nemáte na svém počítači JRE nainstalováno, měl by vás prohlížeč vybídnout ke stažení a instalaci JRE. Pokud se tak nestalo, klikněte na odkaz uvedený na stránce a manuálně stáhněte a nainstalujte aktuální verzi JRE. V každém případě bude po instalaci JRE nutno zavřít a znovu spustit prohlížeč, aby se změny projevily.

Instalace JRE je popsána v **Kapitole5**.

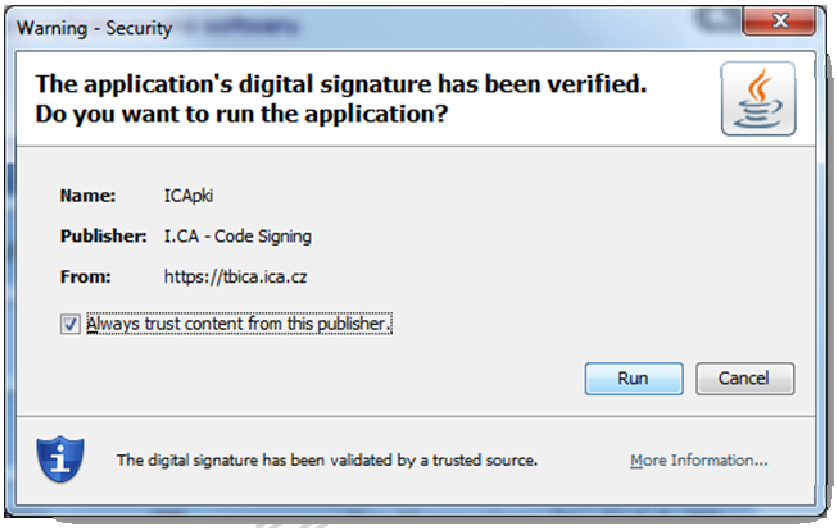
4.1.4.1.Povolení Java v Internet Exploreru

Změňte nastavení podle návodu uvedeného v kapitole 2.1.

4.1.5.Nainstalovaný Java Applet ICApki

V tomto místě se kontrolní stránka pokusí nainstalovat Java Applet ICApki, který je nutný pro funkčnost stránek pro generování žádosti o certifikát. Při první instalaci appletu na počítač, kde probíhá generování žádosti o certifikát, budete vyzváni k potvrzení důvěry vydavateli Java Appletu. Vydavatelem appletu je První certifikační autorita a.s. Důvěru appletu potvrdíte dialogem, který znázorňuje následující obrázek. V tomto dialogu je důležité zaškrtnout volbu **Always trust content from this publisher** a poté použít tlačítko **Yes**.

Následuje druhý dialog, kde se postupuje obdobně, a sice zaškrtne se volba **Always trust content from this publisher** a poté se použije tlačítko **Run**.



Při dalším spuštění stránek na počítači, kde tato instalace proběhla, již nebudete k opětovnému potvrzování Java Appletu ICApki vyzýváni.

V případě, že bude vydána nová verze Java Appletu ICApki, bude klientem v tomto místě okamžitě automaticky stažena a nainstalována. Tato instalace může chvíli trvat. Po jejím skončení budou stránky pokračovat v normální práci.

4.1.6.Ukládání cookies

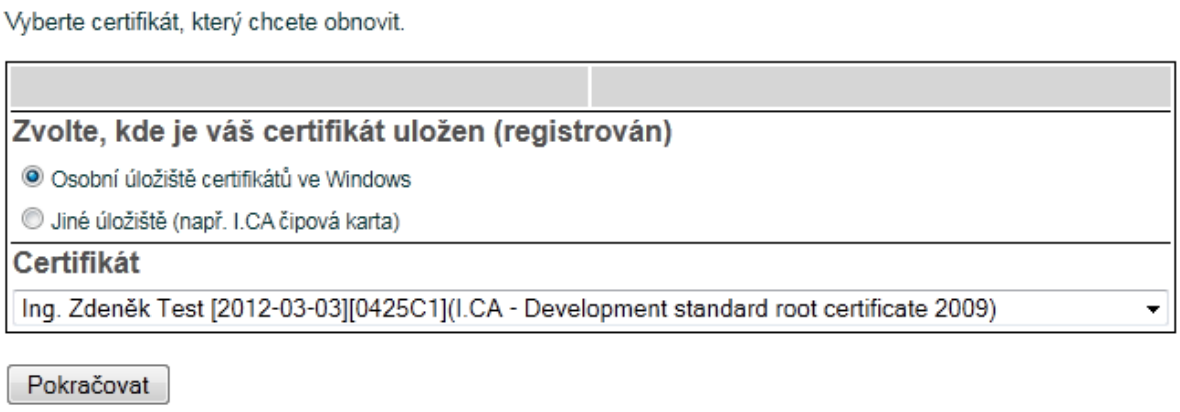
Pro správnou práci stránek pro generování žádostí je nutné, aby váš prohlížeč umožnil stránce ukládat cookies. Pokud máte zakázáno ukládání cookies, povolte jej.

4.1.6.1.Povolení cookis v Internet Exploreru

Změňte nastavení podle návodu uvedeného v kapitole 2.1.

4.2.Výběr certifikátu pro obnovu (volitelné)

Nejdříve je třeba vybrat certifikát, který chcete obnovovat.



Pokud je Váš certifikát registrován ve Windows, nechte zvoleno **Osobní úložiště** certifikátů Windows. Pokud se nachází Váš certifikát na příklad na čipové kartě I.CA a tento certifikát nebyl zaregistrován do Windows zvolte možnost **Jiné úložiště**.

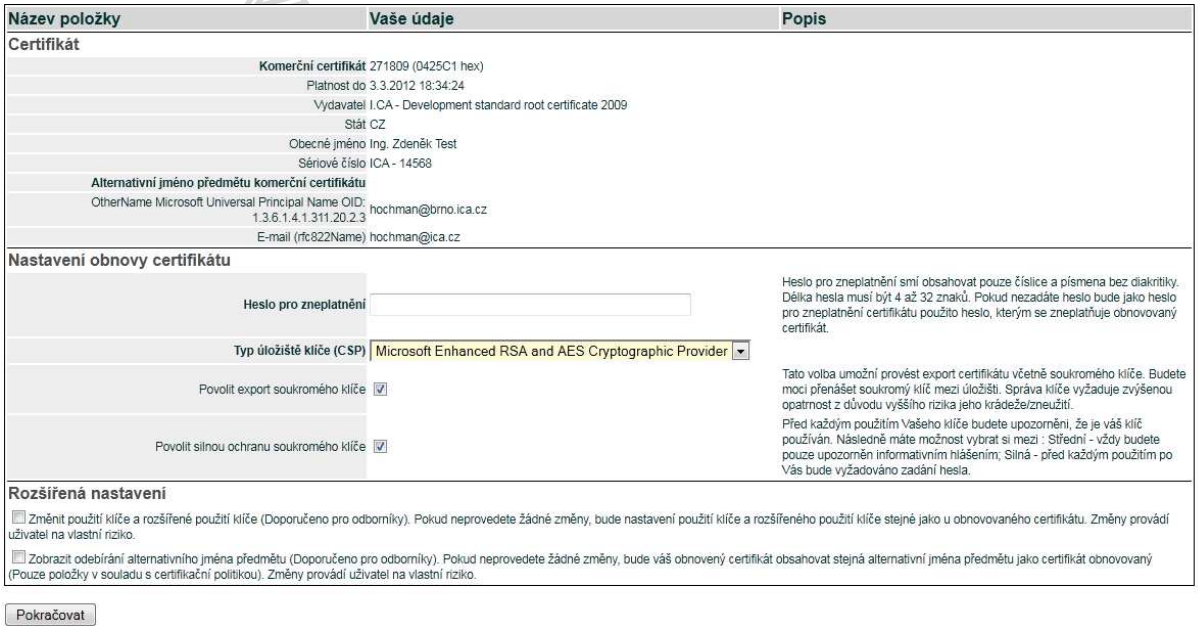
Podle Vaší předchozí volby je nabídnut seznam certifikátů, které můžete obnovit. Pokud jste zvolili možnost **Jiné úložiště**, musíte mít připojenu čtečku a vloženu čipovou kartu.

Obnovit lze pouze takové certifikáty, kterým ještě neskončila platnost a které nejsou umístěny na CRL!

Pokud obdržíte email s upozorněním na konec platnosti Vašeho certifikátu, je v tomto emailu uvedeno URL, na kterém můžete obnovit Váš certifikát. Součástí URL je i sériové číslo certifikátu. Pokud zadáte toto URL do vašeho prohlížeče, certifikát je pro obnovu vybrán automaticky.

4.3.Doplnění a změna některých údajů

V tomto kroku můžete ovlivnit některé údaje, které bude obsahovat Váš obnovený certifikát.



Název položky	Vaše údaje	Popis
Certifikát		
Komerční certifikát	271809 (0425C1 hex)	
Platnost do	3.3.2012 18:34:24	
Vydavatel	I.CA - Development standard root certificate 2009	
Stát	CZ	
Obecné jméno	Ing. Zdeněk Test	
Sériové číslo	ICA - 14568	
Alternativní jméno předmětu komerční certifikátu		
OtherName Microsoft Universal Principal Name OID: 1.3.6.1.4.1.311.20.2.3	hochman@brno.ica.cz	
E-mail (rfc822Name)	hochman@ica.cz	
Nastavení obnovy certifikátu		
Heslo pro zneplatnění		Heslo pro zneplatnění smí obsahovat pouze číslice a písmena bez diakritiky. Délka hesla musí být 4 až 32 znaků. Pokud nezadáte heslo bude jako heslo pro zneplatnění certifikátu použito heslo, kterým se zneplatňuje obnovovaný certifikát.
Typ úložiště klíče (CSP)	Microsoft Enhanced RSA and AES Cryptographic Provider	
Povolit export soukromého klíče	☑	Tato volba umožní provést export certifikátu včetně soukromého klíče. Budete moci přenášet soukromý klíč mezi úložišti. Správa klíče vyžaduje zvýšenou opatrnost z důvodu vyššího rizika jeho krádeže/zneužití.
Povolit silnou ochranu soukromého klíče	☑	Před každým použitím Vašeho klíče budete upozorněni, že je váš klíč používán. Následně máte možnost vybrat si mezi : Střední - vždy budete pouze upozorněn informativním hlášením; Silná - před každým použitím po Vás bude vyžadováno zadání hesla.
Rozšířená nastavení		
☐ Změnit použití klíče a rozšířené použití klíče (Doporučeno pro odborníky). Pokud neprovedete žádné změny, bude nastavení použití klíče a rozšířeného použití klíče stejné jako u obnovovaného certifikátu. Změny provádí uživatel na vlastní riziko.		
☐ Zobrazit odebírání alternativního jména předmětu (Doporučeno pro odborníky). Pokud neprovedete žádné změny, bude váš obnovený certifikát obsahovat stejná alternativní jména předmětu jako certifikát obnovovaný (Pouze položky v souladu s certifikační politikou). Změny provádí uživatel na vlastní riziko.		

Pokračovat

V části **Certifikát** jsou zobrazeny některé údaje z obnovovaného certifikátu. Zobrazeno je jeho sériové číslo, platnost, jméno vydavatele certifikátu, jednotlivé položky předmětu a všechna alternativní jména.

V části **Nastavení obnovy** se nachází údaje:

Heslo pro zneplatnění:

Pokud dojde během používání certifikátu ke kompromitaci privátního klíče, změně údajů (změna jména, bydliště…), nebo se vyskytnou další důvody, proč by neměl být certifikát dále používán, je Vaší zákonnou povinností certifikát zneplatnit. Certifikát lze zneplatnit přes webové rozhraní. Při zneplatnění budete vyzváni k zadání hesla pro zneplatnění.

Pokud nezadáte heslo, bude jako heslo pro zneplatnění certifikátu použito heslo, kterým se zneplatňuje obnovovaný certifikát.

Pokud se rozhodnete zadat jiné heslo, musí být délka hesla 4 až 32 znaků. Povoleny jsou pouze velká a malá písmena bez diakritiky a číslice.

Typ úložiště klíče (CSP):

U položky **Typ úložiště klíče (CSP)** zvolte z nabídky SW modul zajišťující kryptografické služby (CSP), který vygeneruje váš privátní klíč.

Export privátního klíče:

Pokud Vámi zvolený typ úložiště klíče (CSP) podporuje export privátního klíče, je Vám nabídnuta volba **Povolit export privátního klíče**. Tato volba umožní provést export certifikátu včetně soukromého klíče. Soukromý klíč tak budete moci přenášet mezi úložišti. Správa klíče vyžaduje v takovém případě zvýšenou opatrnost z důvodu vyššího rizika jeho krádeže/zneužití.

Silná ochrana privátního klíče:

Pokud Vámi zvolený typ úložiště klíče (CSP) podporuje silnou ochranu privátního klíče, je Vám nabídnuta volba **Povolit silnou ochranu privátního klíče**. Před každým použitím Vašeho klíče budete upozorněni, že je Váš klíč používán. Následně máte možnost vybrat si mezi: Střední - vždy budete pouze upozorněn informativním hlášením; Silná - před každým použitím po Vás bude vyžadováno zadání hesla.

Nepovolený obsah certifikátu

V některých výjimečných případech může Váš certifikát obsahovat rozšířená použití klíče a alternativní jména předmětu, která již nesmí být podle certifikační politiky přítomna v certifikátu. V takovém případě je zobrazeno upozornění:

Nebo

Abyste mohli pokračovat v obnově, musíte odsouhlasit odebrání nepovolených položek.

Po stisknutí tlačítka **Pokračovat** stránka provede kontrolu Vámi vyplněných údajů. Pokud některé zadané údaje nesplňují podmínky, budete vyzváni k jejich opravě. Údaje, vyžadující změnu nebo doplnění, jsou podbarveny červeně.

Pokud Vámi zadané údaje splňují podmínky, zobrazí se Vám stránka, rekapitulující Vámi zadané údaje.

4.4.Kontrola zadaných údajů

Na této stránce prosím zkontrolujte Vámi zadané údaje.

První certifikační autorita a.s.

Zkontrolujte si prosím níže uvedené údaje. Pokud jsou níže uvedené údaje v pořádku, je možné vytvořit žádost o obnovu certifikátu.

Rekapitulace údajů	
Název položky	**Zadaná hodnota**
Doba platnosti certifikátu	365
Typ úložiště klíče (CSP)	Microsoft Enhanced RSA and AES Cryptographic Provider
Algoritmus miniatury	sha256WithRSAEncryption
Povolit export soukromého klíče	Ano
Povolit silnou ochranu soukromého klíče	Ano
Délka klíče	2048
Položky předmětu	**Komerční certifikát**
Stát	CZ
Obecné jméno	Ing. Zdeněk Test
Sériové číslo	ICA - 14568
Rozšířené položky certifikátu	**Komerční certifikát**
OtherName Microsoft Universal Principal Name OID: 1.3.6.1.4.1.311.20.2.3	hochman@brno.ica.cz
E-mail (rfc822Name)	hochman@ica.cz
Použití klíče	**Komerční certifikát**
Non Repudiation	Ano
Digital Signature	Ano
Key Encipherment	Ano
Data Encipherment	Ano
Key Agreement	Ano
Rozšířené použití klíče	**Komerční certifikát**
TLS WWW client authentication OID: 1.3.6.1.5.5.7.3.2	Ano
E-mail protection OID: 1.3.6.1.5.5.7.3.4	Ano
Smartcard Logon OID: 1.3.6.1.4.1.311.20.2.2	Ano

Vystavený certifikát zaslat na e-mail: hochman@ica.cz

Certifikát zaslat ve formátu ZIP:

- ○ Ano
- ◉ Ne

Vytvořit žádost

Zadejte e-mailovou adresu, na kterou Vám bude certifikát zaslán (Položka **Vystavený certifikát zaslat na e-mail:**). Pozor: tato emailová adresa není součástí žádosti o certifikát, tudíž nebude uvedena ani v samotném certifikátu.

Kliknutím na tlačítko **Vytvořit žádost** spustíte generování žádosti o obnovu.

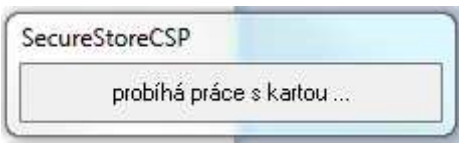
4.5.Generování žádosti o obnovu

Následující postup se pro jednotlivé typy úložiště klíče (CSP) mírně liší.

4.5.1.SecureStoreCSP

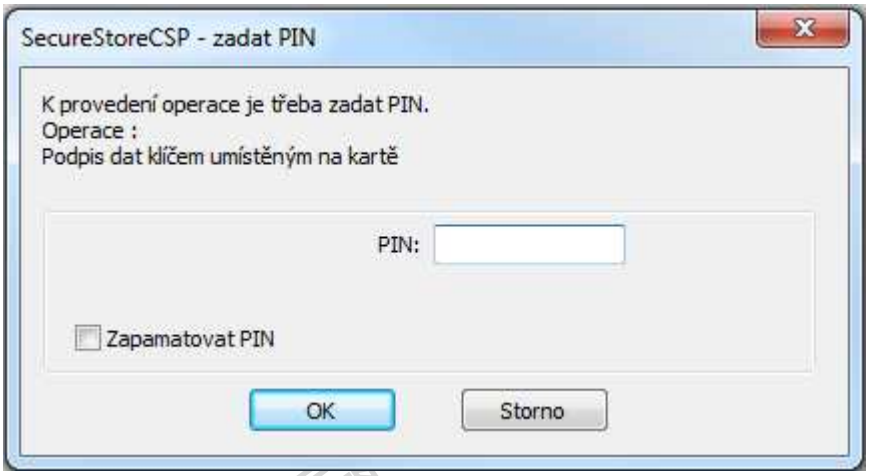
Pokud při vyplňování údajů o žadateli zvolíte jako typ úložiště klíče SecureStoreCSP, je postup generování žádosti následující:

Nejdříve se zobrazí následující dialog. V tomto okamžiku se generuje Váš privátní klíč. Tvorba privátního klíče může trvat několik desítek sekund.



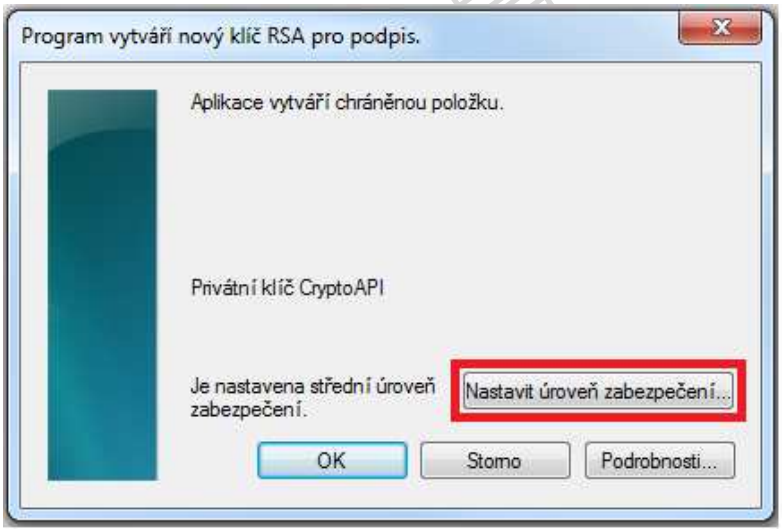
autorita, a.s.

Poté co je privátní klíč vytvořen, jste vyzváni k zadání PINu k Vaší kartě.

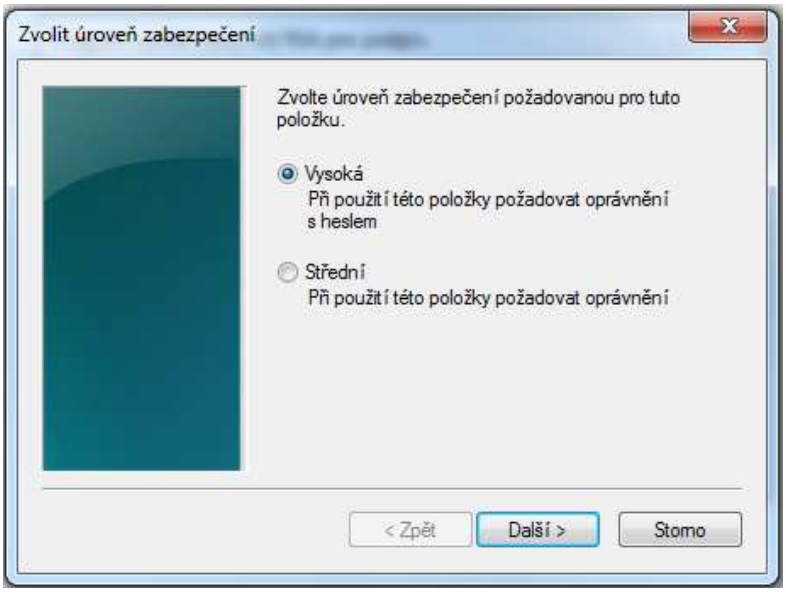


4.5.2. Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou soukromého klíče.

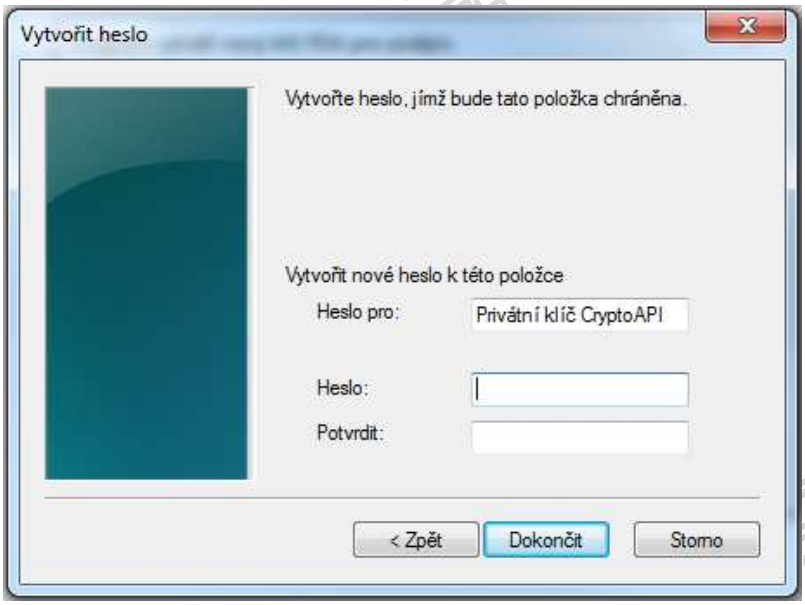
Pokud při vyplňování údajů o žadateli zvolíte jako typ úložiště klíče Microsoft Enhanced RSA and AES Cryptographic Provider (případně Microsoft Enhanced RSA and AES Cryptographic Provider /prototype/) a zatrhnete volbu **Povolit silnou ochranu klíče**, je postup generování žádosti následující:



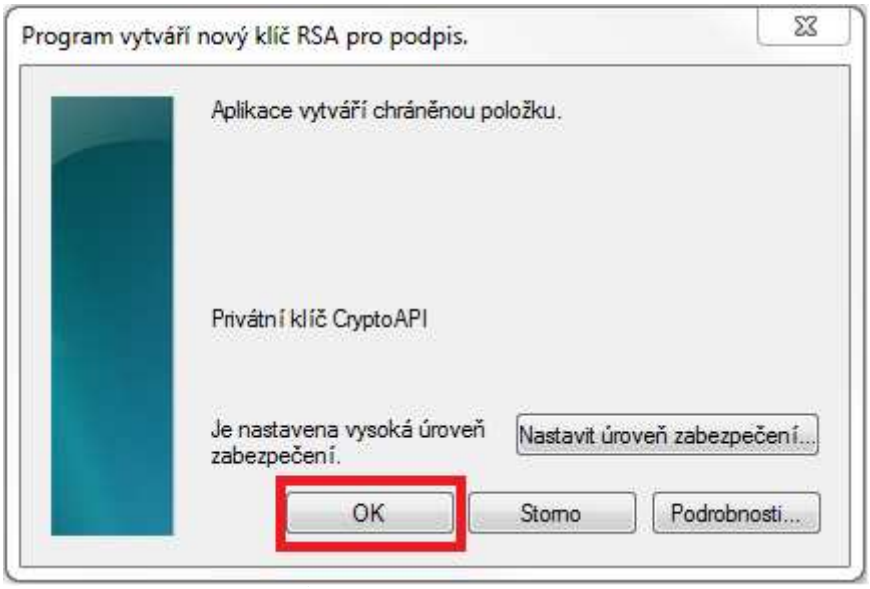
Pokud kliknete na **Nastavit úroveň zabezpečení…**, budete moci změnit úroveň zabezpečení.



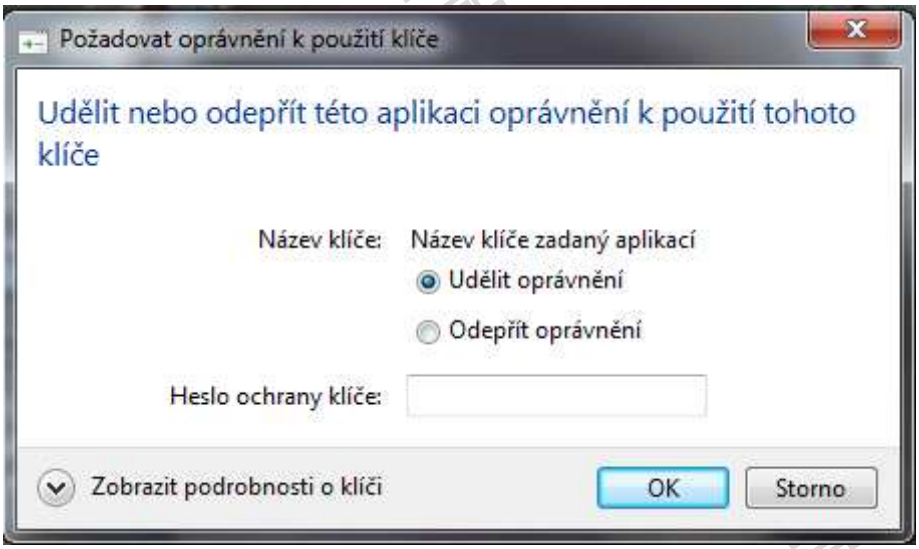
Pokud zvolíte vysokou úroveň zabezpečení, budete vyzváni k zadání hesla. Toto heslo bude potřeba zadat vždy, když budete používat soukromý klíč.



Po kliknutí na tlačítko **Dokončit** dojde ke změně úrovně zabezpečení. Nyní klikněte na tlačítko **OK**.



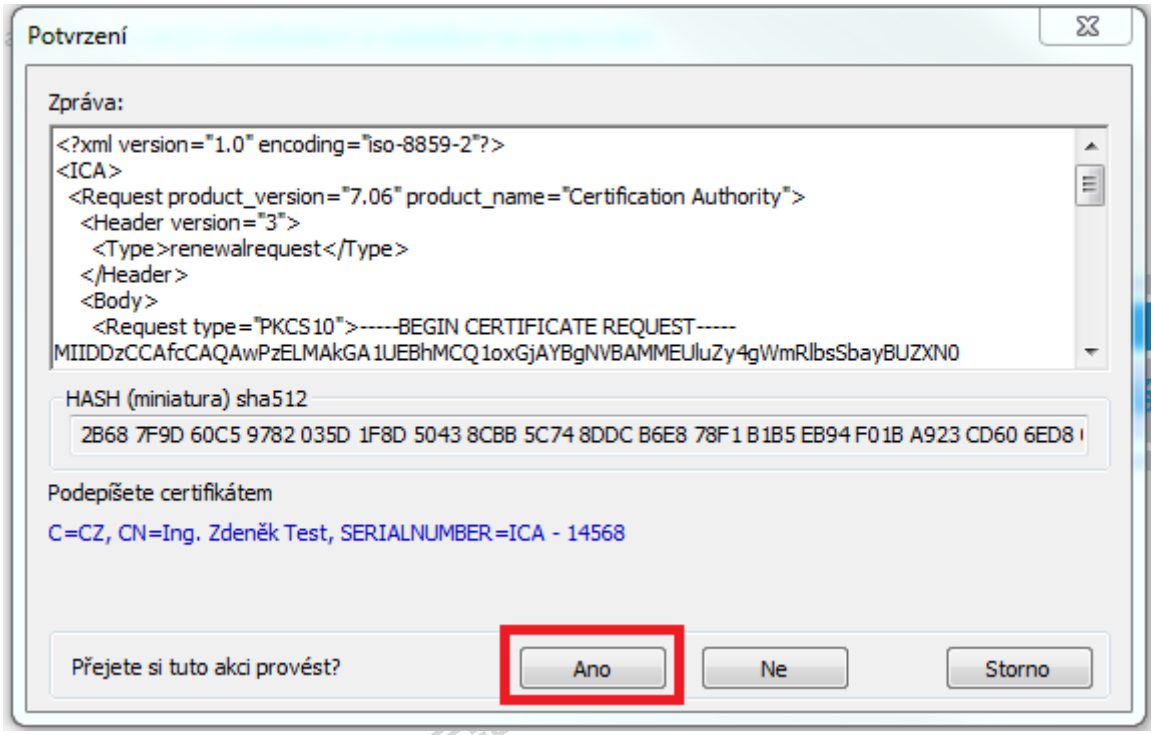
V dalším dialogovém okně zvolte **Udělit oprávnění**. Pokud jste zvolili vysokou úroveň zabezpečení, musíte zadat i heslo.



4.6.Podpis a odeslání žádosti o obnovu

Pokud nedošlo při generování žádosti k chybě, stránka Vám zobrazí vygenerovanou žádost ve formátu PKCS10.

Po kliknutí na tlačítko **Odeslat žádost ke zpracování**, se zobrazí dialog, obsahující Vaši žádost o obnovu certifikátu. Tuto žádost je nutné podepsat certifikátem, který obnovujete.



Podepište prosím žádost.

V některých případech budete požádáni o více podpisů. V případě, že obnovujete TWINS certifikát, je nutné podepsat jak žádost o obnovu kvalifikované, tak i komerční žádosti o obnovu.

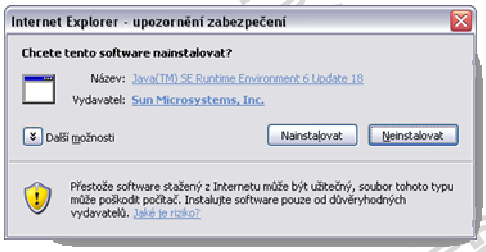
V případě úspěšného odeslání žádosti se Vám zobrazí následující stránka:

5. Instalace Java Runtime Environment (JRE)

Instalace JRE probíhá v rámci jednotlivých prohlížečů různými způsoby. Na jednom počítači není zapotřebí instalovat JRE v každém prohlížeči zvlášť, neboť po nainstalování funguje podpora JRE v rámci celého operačního systému, a tedy i v prohlížeči, ve kterém jste instalaci JRE neprováděli.

5.1. Spuštění instalace JRE pod prohlížečem Internet Explorer

Pokud nemáte nainstalovanou podporu Java Runtime Environment, budete při prvním přístupu na stránky pro generování žádosti o certifikát vyzváni k její instalaci. V prohlížeči Internet Explorer se zobrazí dialog:



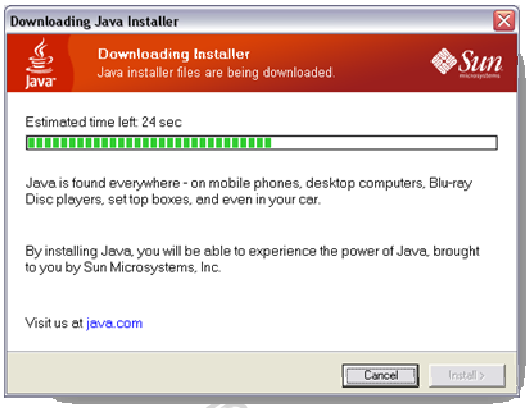
Zde kliknete na tlačítko **Nainstalovat**, čímž zahájíte proces instalace. Průběh instalačního programu je popsán v **Kapitole 6**.

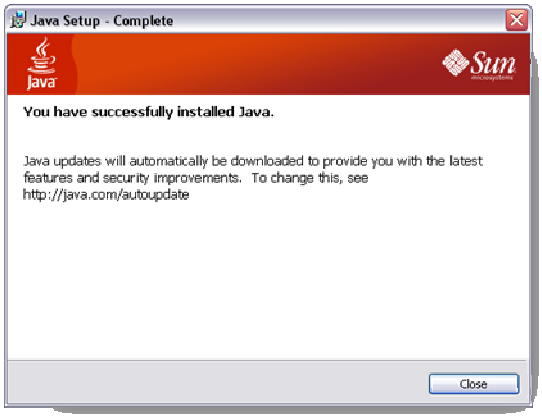
6. Instalační program JRE

Po spuštění instalačního programu JRE se zobrazí první okno instalačního programu.

Na úvodní obrazovce zvolte tlačítko **Install**. Dále je proces instalace až do konce automatický. Instalační program si následně stáhne z internetu dodatečné soubory, které potřebuje k zavedení JRE do Vašeho počítače.

První certifikační autorita, a.s.



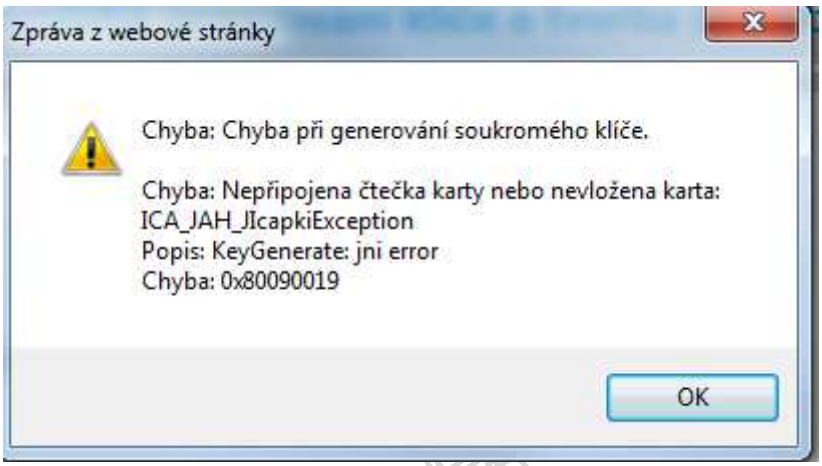


Kvalifikační autorita, a.s.

Na závěrečné obrazovce klikněte na tlačítko **Close**. V tuto chvíli doporučujeme prohlížeč vypnout a následně zapnout, aby se projevily změny.

7. Řešení problémů

V případě vzniku chyby během procesu obnovy certifikátu budete informováni chybovou hláškou.



Některé chyby mohou být závažnějšího technického rázu. Mohou souviset se stavem hardwarového či softwarového vybavení Vašeho počítače. Je důležité opsat, udělat screenshot, nebo jinak uchovat informace z podrobného výpisu chybového hlášení, neboť tyto informace jsou kritické pro rychlé vyřešení problémů s helpdeskem I.CA.

Certifikační autorita, a.s.