

Generování žádosti o následný certifikát

Uživatelská příručka pro Mozilla Firefox

První certifikační autorita, a.s.

Verze 8.15

Obsah

1.	Úvod	3
2.	Požadavky na software.....	3
3.	Proces generování žádosti o následný certifikát.....	3
3.1.	Kontrola softwarového vybavení	4
3.1.1.	Nepodporovaný operační systém	6
3.1.2.	Nepodporovaný internetový prohlížeč	6
3.1.3.	Podpora JavaScriptu	6
3.1.4.	Podpora Java Runtime Environment (JRE)	6
3.1.5.	Ukládání cookies.....	6
3.2.	Výběr certifikátu pro vytvoření žádosti o následný certifikát	6
3.3.	Doplnění a změna některých údajů.....	7
3.4.	Generování žádosti o certifikát	9
3.4.1.	SecureStoreCSP – čipová karta I.CA	9
3.4.2.	Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou soukromého klíče	10
3.5.	Podpis a odeslání žádosti o následný certifikát.....	12
4.	Instalace Java Runtime Environment (JRE).....	13
5.	Řešení problémů	15

1. Úvod

Tento dokument slouží jako návod, jak postupovat při generování žádosti o následný certifikát přes webové stránky.

2. Požadavky na software

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

- nainstalovaný a spuštěný operační systém
 - **Microsoft Windows XP Service Pack 3**
 - **Windows Vista**
 - **Windows 7**
 - **Windows 8 / 8.1**
 - **Windows 10**
- nainstalován a použit **Mozilla Firefox** verze 13.0 – 39.0
- nainstalován aktuální software **Java Runtime Environment** (dále **JRE**).
 - Přítomnost tohoto softwaru detekují testovací stránky automaticky, pokud zjistí, že software přítomen není, vybědnou uživatele k jeho stažení/instalaci.
- v internetovém prohlížeči zapnuta podporaskriptování Javascript, zapnuta podpora jazyku Java, podpora ukládání cookies.

3. Proces generování žádosti o následný certifikát

Postup generování žádosti o následný certifikát je rozdělen do několika kroků:

Kontrola softwarového vybavení

Kontrola údajů

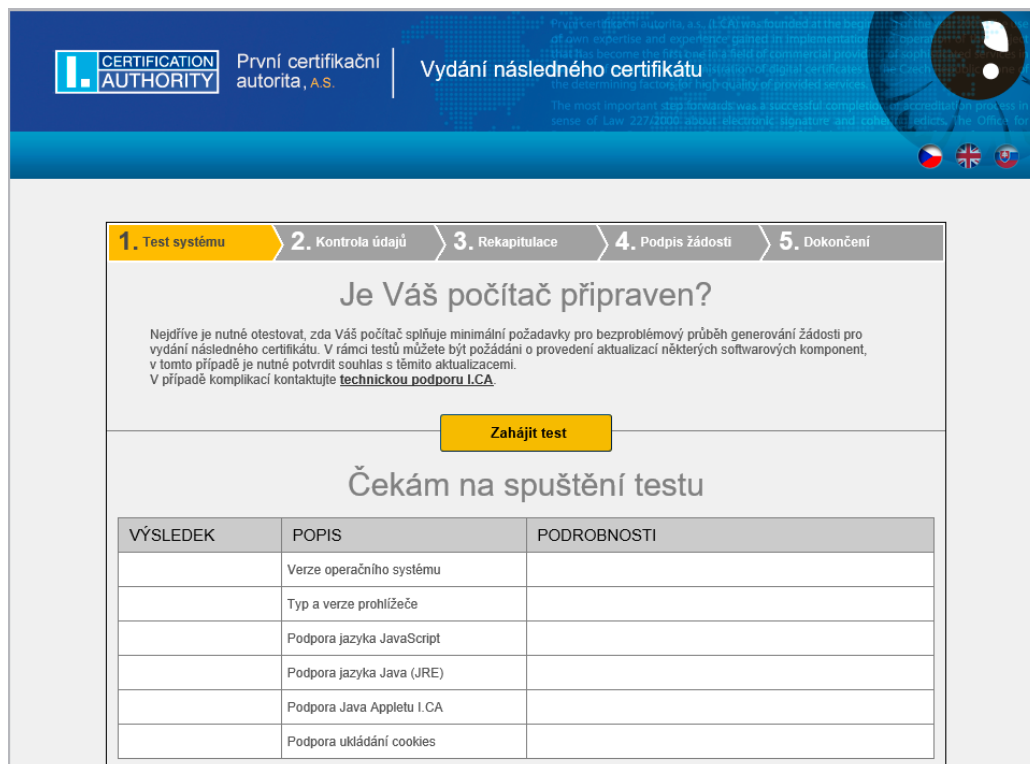
Generování žádosti

Odeslání žádosti

3.1. Kontrola softwarového vybavení

Pro usnadnění kontroly připravenosti vašeho počítače na generování žádosti, je při zahájení generování žádosti zobrazena kontrolní stránka, která ověří přítomnost klíčových softwarových komponent.

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



1. Test systému > 2. Kontrola údajů > 3. Rekapitulace > 4. Podpis žádosti > 5. Dokončení

Je Váš počítač připraven?

Nejdříve je nutné otestovat, zda Váš počítač splňuje minimální požadavky pro bezproblémový průběh generování žádosti pro vydání následného certifikátu. V rámci testů můžete být požádáni o provedení aktualizací některých softwarových komponent, v tomto případě je nutné potvrdit souhlas s těmito aktualizacemi.
V případě komplikací kontaktujte [technickou podporu I.CA](#).

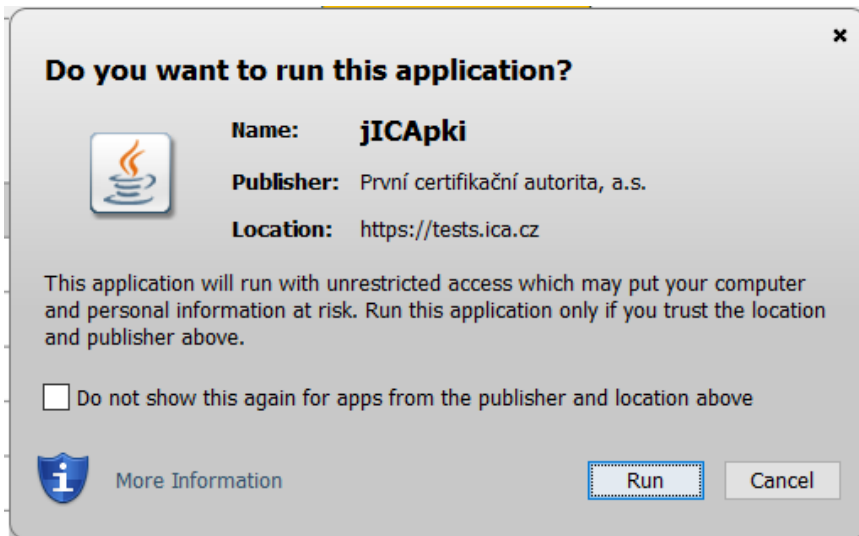
Zahájit test

Čekám na spuštění testu

VÝSLEDEK	POPIS	PODROBNOSTI
	Verze operačního systému	
	Typ a verze prohlížeče	
	Podpora jazyka JavaScript	
	Podpora jazyka Java (JRE)	
	Podpora Java Appletu I.CA	
	Podpora ukládání cookies	

Zobrazí-li se v průběhu testu okno s upozorněním od JRE, zvolte **Run**.

Tímto dojde k instalaci a spuštění appletu ICApki, který je nezbytný pro funkčnost stránek pro generování žádosti o certifikát. Tato instalace může chvíli trvat.



Zahájit test

Test úspěšně dokončen

VÝSLEDEK	POPIS	PODROBNOSTI
✓	Verze operačního systému	Windows 10, tento operační systém je podporován.
✓	Typ a verze prohlížeče	Firefox verze 39.0, tento webový prohlížeč je podporován.
✓	Podpora jazyka JavaScript	JavaScript povolen.
✓	Podpora jazyka Java (JRE)	Nainstalována Java JRE (Runtime Environment) od výrobce: Oracle Corporation (Verze: 1.8.0_51).
✓	Podpora Java Appletu I.CA	Java Applet jICApki je spuštěn.
✓	Podpora ukládání cookies	Ukládání cookies je povoleno.

Pokračovat

Stránka otestuje počítač, pokud nejsou detekovány problémy, kliknutím na tlačítko **Pokračovat** přejdete k samotné tvorbě žádosti o následný certifikát.

Pokud se při kontrole vyskytne chyba, nelze pokračovat v tvorbě žádosti o následný certifikát. Nejdříve je potřeba odstranit chybu, která znemožňuje tvorbu žádosti o certifikát. Význam chybových hlášení je uvedený v následujících kapitolách.

3.1.1. Nepodporovaný operační systém

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

3.1.2. Nepodporovaný internetový prohlížeč

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

3.1.3. Podpora JavaScriptu

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

3.1.4. Podpora Java Runtime Environment (JRE)

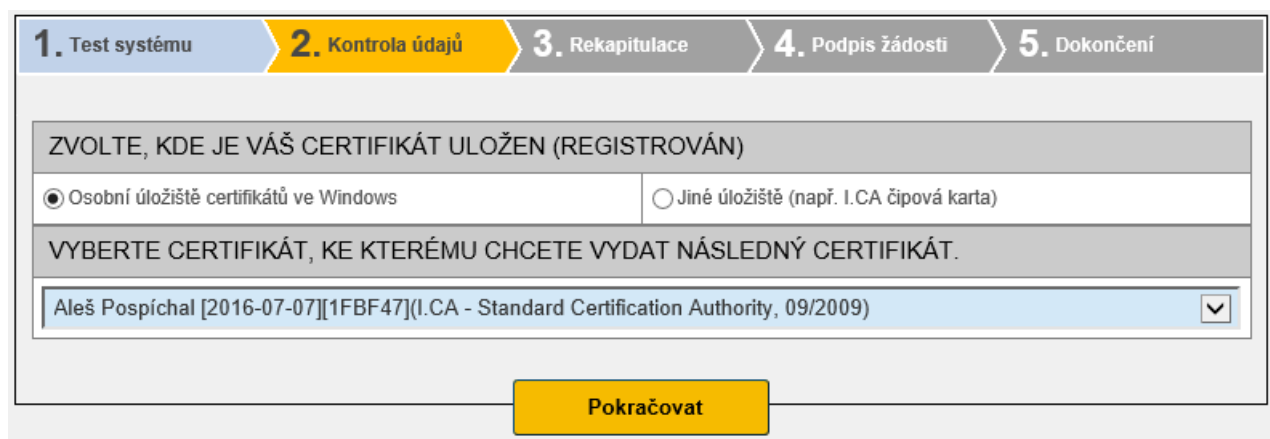
Stránky vyžadují pro svou funkčnost **nainstalovanou podporu jazyka Java**. Ujistěte se, že nemáte ve svém prohlížeči tuto podporu vypnutou. Pokud nemáte na svém počítači JRE nainstalováno, ke stažení použijte uvedený odkaz na stránky JRE, po instalaci JRE nutno obnovit prohlížeč

3.1.5. 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.

3.2. Výběr certifikátu pro vytvoření žádosti o následný certifikát

Pokud proces kontroly proběhl bez chyb, stránka zobrazí formulář, kde vyberete platný certifikát, ke kterému chcete vydat následný.



Pokud je Váš certifikát uložen v úložišti systému Windows, nechte zvoleno **Osobní úložiště** certifikátů Windows. Pokud se nachází Váš certifikát například na čipové kartě I.CA, zvolte možnost **Jiné úložiště**.

Podle Vaší předchozí volby je nabídnut seznam certifikátů, ke kterým lze vydat následný certifikát. Pokud jste zvolili možnost **Jiné úložiště**, musíte mít připojenu čtečku a vloženu čipovou kartu.

Vydat následný certifikát lze pouze u takových certifikátů, kterým ještě neskončila platnost, a které nejsou umístěny na CRL!

Pokud obdržíte e-mail s upozorněním na konec platnosti Vašeho certifikátu, je v tomto e-mailu uvedeno URL, na kterém můžete vytvořit žádost o následný certifikát. Součástí URL je i sériové číslo certifikátu.

Pokud zadáte toto URL do Vašeho prohlížeče, certifikát je vybrán automaticky.

3.3. Doplnění a změna některých údajů

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

1. Test systému		2. Kontrola údajů		3. Rekapitulace		4. Podpis žádosti		5. Dokončení	
CERTIFIKÁT						SKRÝT POVOLENÉ ÚPRAVY >>			
Komerční	2080583 (1FBF47 hex)								
Platnost do	7. 7. 2016 13:20:56								
Stát	CZ								
Celé jméno	Aleš Pospíchal								
Organizace	První certifikační autorita, a.s.								
E-mail uvedený v certifikátu	pospichal@ica.cz								
Heslo pro zneplatnění	<input type="password" value="Heslo pro zneplatnění"/> ?								
Typ úložiště klíče (CSP)	SecureStoreCSP ▾								
<input checked="" type="checkbox"/> Certifikát zaslat ve formátu ZIP	<input checked="" type="checkbox"/> Povolit export klíče ?								<input checked="" type="checkbox"/> Povolit silnou ochranu klíče ?
Úprava e-mailu	<input type="checkbox"/> Smazat	<input type="checkbox"/> Změnit	<input type="text" value="pospichal@ica.cz"/>						
Pokračovat									

V části Certifikát jsou zobrazeny některé údaje ze stávajícího certifikátu. Zobrazeno je jeho sériové číslo, platnost a jednotlivé položky předmětu.

Po kliknutí na Povolené úpravy následného certifikátu v horní části, se zobrazí následující možnosti:

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 nutné certifikát zneplatnit.

Certifikát lze zneplatnit přes webové rozhraní. Při zneplatnění certifikátu budete vyzváni k zadání hesla pro zneplatnění.

Pokud nezadáte heslo, bude jako heslo pro zneplatnění certifikátu použito heslo nastavené u stávajícího certifikátu.

Pokud se rozhodnete zadat jiné heslo, musí být jeho délka 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 modul zajišťující kryptografické služby (CSP), který vygeneruje váš privátní klíč. Všechny zde zobrazené CSP jsou nainstalovány ve vašem počítači.

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

Úprava e-mailu:

Pokud je ve stávajícím certifikátu uveden e-mail, zde máte možnost ho z následného certifikátů odebrat. Změna ve většině případů není možná, v tomto případě prosím požádejte o nový certifikát s opravenými údaji.

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 a je nutné tuto rozšíření před pokračováním odebrat.

Po stisknutí tlačítka **Pokračovat** se zobrazí rekapitulace údajů a nastavení následného certifikátu.

REKAPITULACE ÚDAJŮ	
Certifikát zaslat ve formátu ZIP	Ano
Doba platnosti certifikátu	365
Typ úložiště klíče (CSP)	Operační systém Windows
Algoritmus miniatury / Délka klíče	sha256WithRSAEncryption / 2048
Povolit export klíče	Ano
Povolit silnou ochranu klíče	Ano
NASTAVENÍ CERTIFIKÁTU	
Celé jméno	Pavel Novák
Organizace	První certifikační autorita, a.s.
E-mail uvedený v certifikátu	pospichal@ica.cz
IK MPSV	1234567890
Stát	CZ
<div style="border: 1px solid black; background-color: yellow; padding: 5px; display: inline-block; margin-top: 10px;"> Vytvořit žádost </div>	

Kliknutím na tlačítko **Vytvořit žádost** se zahájí vytvoření privátního klíče.

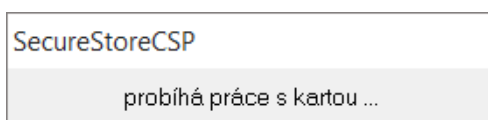
3.4. Generování žádosti o certifikát

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

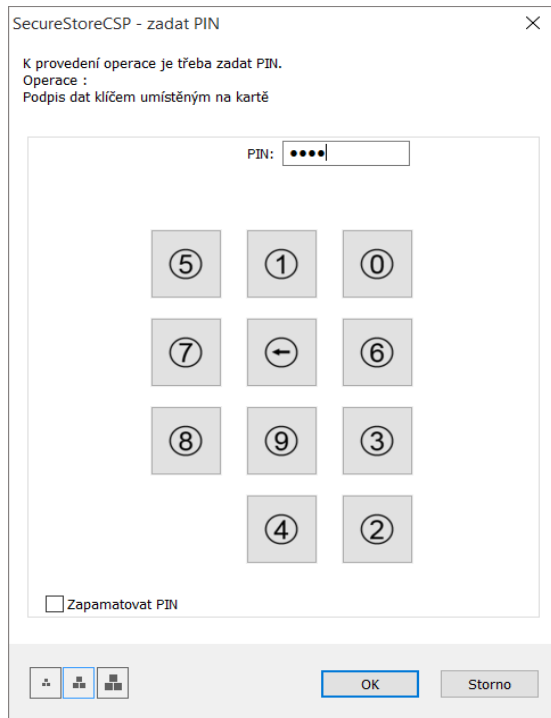
3.4.1. SecureStoreCSP – čipová karta I.CA

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

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

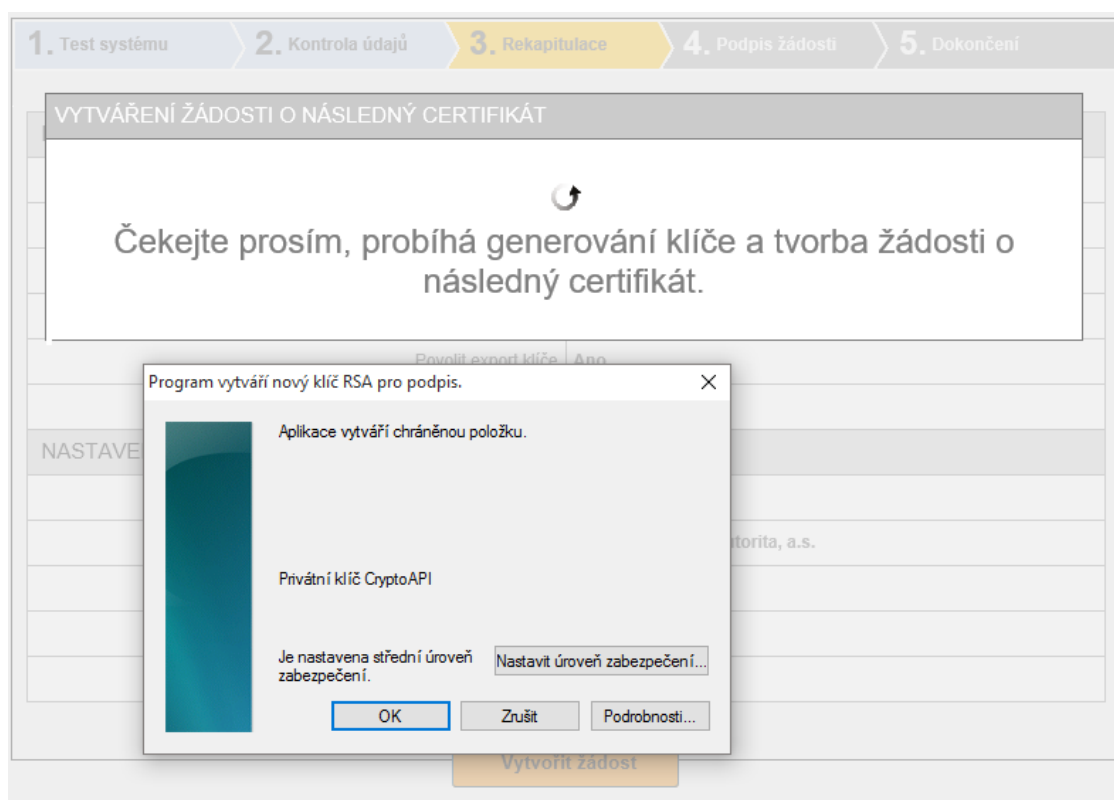


Poté co je privátní klíč vytvořen, jste vyzváni k zadání PINu k vaší kartě.

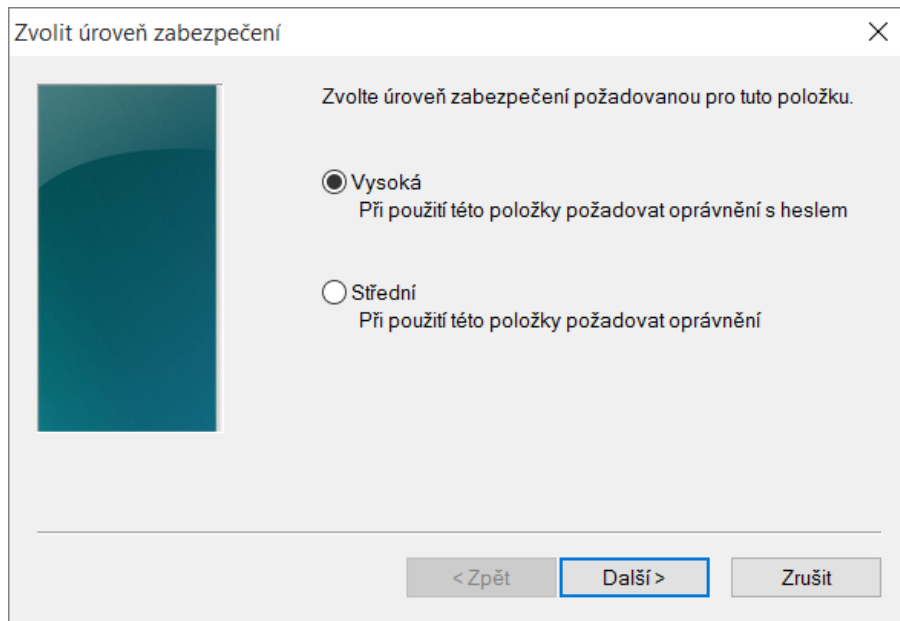


3.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou soukromého klíče

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.



Zvolit úroveň zabezpečení

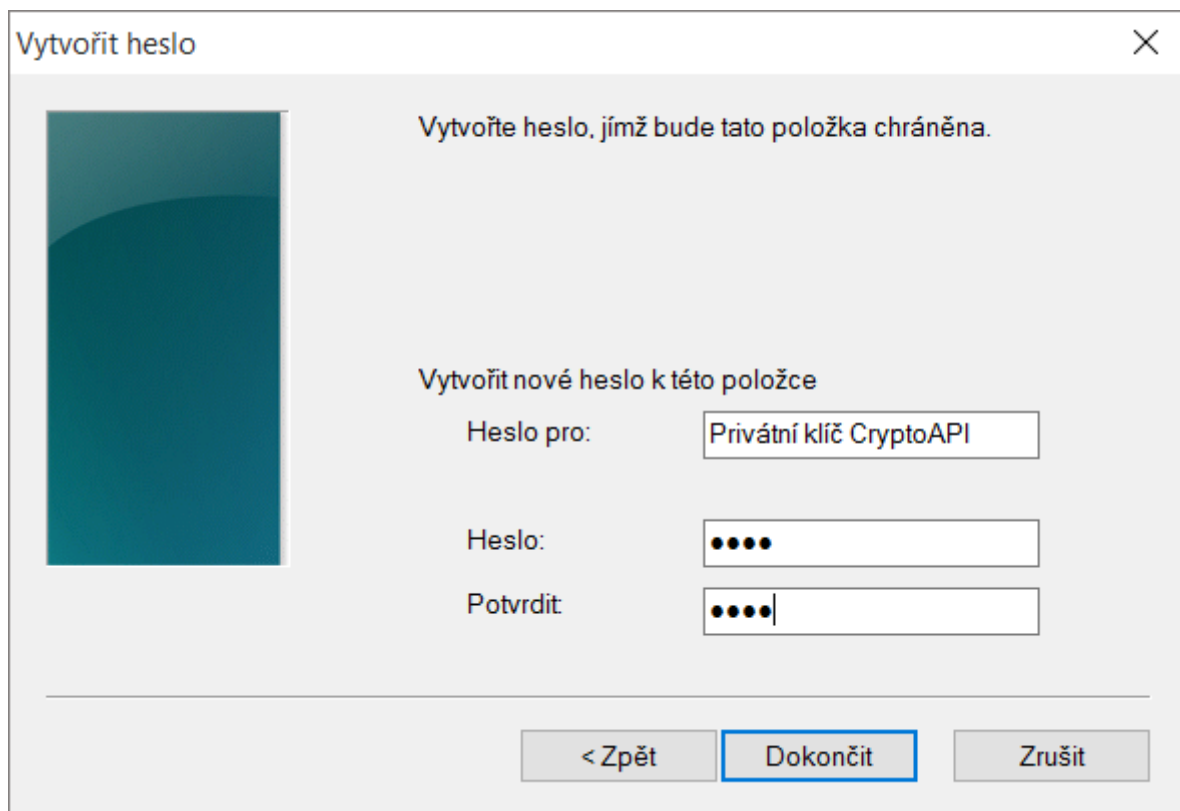
Zvolte úroveň zabezpečení požadovanou pro tuto položku.

Vysoká
Při použití této položky požadovat oprávnění s heslem

Střední
Při použití této položky požadovat oprávnění

< Zpět **Další >** Zrušit

Pokud zvolíte **vyšokou** úroveň zabezpečení, budete vyzváni k zadání hesla. (Toto heslo bude potřeba zadat vždy, když budete používat Váš vydaný certifikát).



Vytvořit heslo

Vytvořte heslo, jímž bude tato položka chráněna.

Vytvořit nové heslo k této položce

Heslo pro: Privátní klíč CryptoAPI

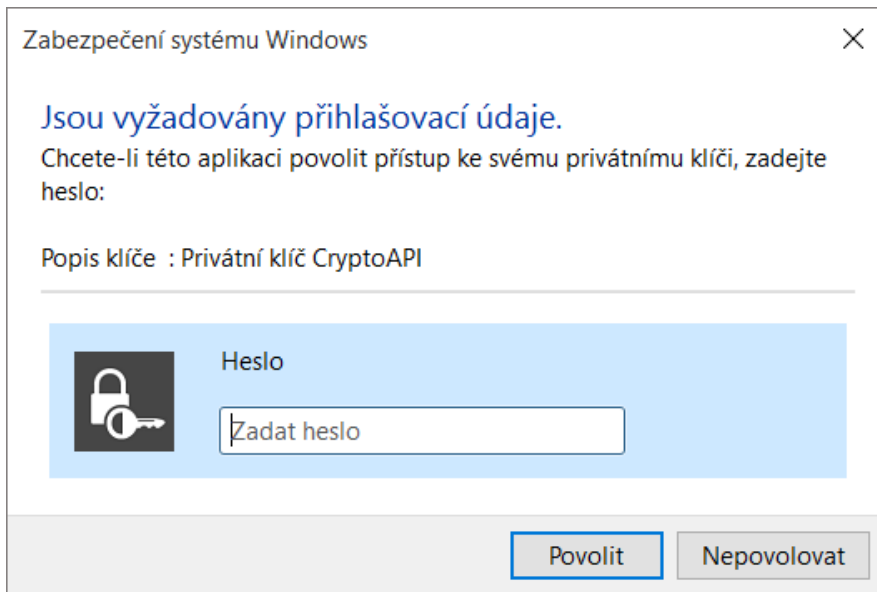
Heslo: ●●●●

Potvrdit: ●●●●

< Zpět **Dokončit** Zrušit

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

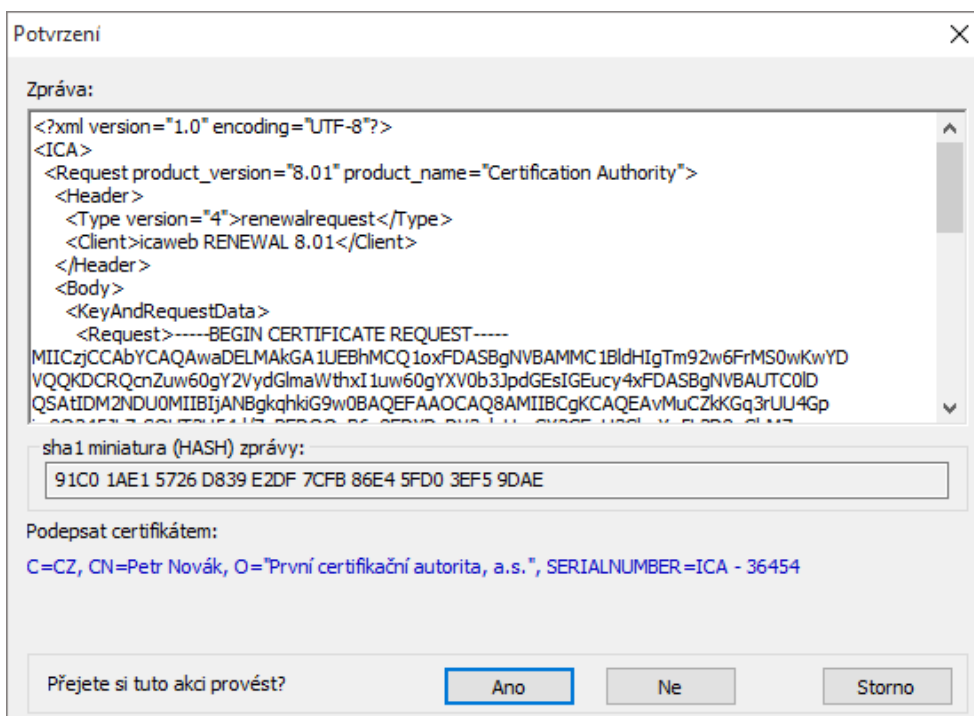
V dalším dialogovém okně udělte oprávnění tlačítkem **Povolit**. Pokud jste zvolili **vysokou** úroveň zabezpečení, musíte zadat i heslo.



3.5. Podpis a odeslání žádosti o následný certifikát

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 následný certifikát. Tuto žádost je nutné podepsat certifikátem, ke kterému žádáte následný.



Podepište prosím žádost.

V některých případech budete požádáni o více podpisů. V případě, že žádáte o následný certifikát TWINS, je nutné podepsat jak žádost o následný kvalifikovaný, tak i žádost o komerční certifikát.

V případě úspěšného odeslání žádosti se Vám zobrazí následující stránka:

1. Test systému
2. Kontrola údajů
3. Rekapitulace
4. Podpis žádosti
5. Dokončení

Žádost o následný certifikát byla úspěšně přijata.

ID žádosti o komerční certifikát: 7607900002709

Zde může sledovat stav Vaší žádosti s ID 7607900002709.

Čas přijetí žádosti: 17.08.2015 13:42:20

Ukončit průvodce

4. Instalace Java Runtime Environment (JRE)

Pokud nemáte nainstalovanou podporu Java Runtime Environment, budete při prvním přístupu na stránku pro generování žádosti o certifikát vyzváni k její instalaci.

VÝSLEDEK	POPIS	PODROBNOSTI
✓	Verze operačního systému	Windows 10, tento operační systém je podporován.
✓	Typ a verze prohlížeče	Firefox verze 39.0, tento webový prohlížeč je podporován.
✓	Podpora jazyka JavaScript	JavaScript povolen.
✗	Podpora jazyka Java (JRE)	Nepovedlo se úspěšně detekovat instalaci Java Runtime Environment (JRE). Buď není nainstalováno, nebo Váš prohlížeč blokuje plugin z našeho webu. Ověření funkčnosti JRE či jeho instalaci můžete provést na stránkách výrobce . Po instalaci zavřete a znovu spustte prohlížeč, aby se změny projevíly.
	Podpora Java Appletu I.CA	
	Podpora ukládání cookies	

Instalaci je možné zahájit na stránce: <https://java.com/en/download/index.jsp>, případně využitím odkazu uvedeného u chyby při testování počítače. Po otevření stránek výrobce kliknete na tlačítko **Free Java Download** a následně **Agree and Start Free Download**.

Zobrazí se dialog s možnostmi stažení. Zvolte spustit, případně soubor uložte na disk a následně jej spustíte.

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 zavedení JRE do vašeho počítače.

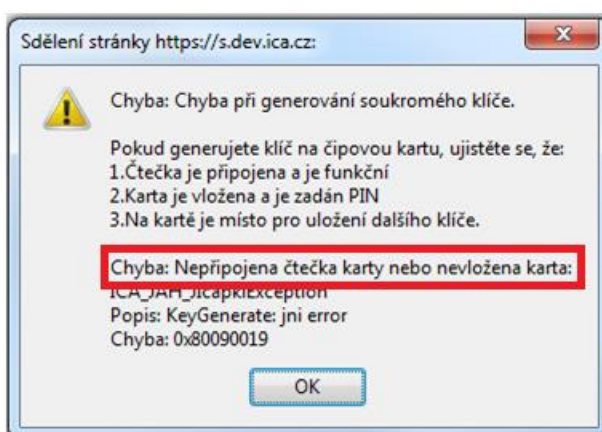


Na závěrečné obrazovce klikněte na tlačítko **Close**. V tuto chvíli doporučujeme prohlížeč obnovit, aby se projevil změny.



5. Řešení problémů

V případě vzniku chyby během procesu generování žádosti budete informováni chybovou hláškou.



Ve třetím odstavci naleznete popis chyby.

Některé chyby mohou být závažnějšího technického rázu. Mohou souviset se stavem hardwarového či softwarového vybavení vašeho počítače. V tomto případě doporučujeme kontaktovat [technickou podporu I.CA](#)