

Generování žádosti o certifikát

Uživatelská příručka pro Mozilla Firefox

První certifikační autorita, a.s.

Verze 8.15

Obsah

1. Úvod	3
2. Požadavky na software	3
3. Instalace kořenového certifikátu I. CA	3
4. Proces generování žádosti o certifikát	6
4.1. Kontrola softwarového vybavení	6
4.1.1. Nepodporovaný operační systém	8
4.1.2. Nepodporovaný internetový prohlížeč	8
4.1.3. Podpora JavaScriptu	8
4.1.4. Podpora Java Runtime Environment (JRE)	8
4.1.5. Ukládání cookies.....	8
4.2. Vyplnění údajů o žadateli	9
4.3. Kontrola zadaných údajů	11
4.4. Generování žádosti o certifikát	11
4.4.1. SecureStoreCSP – čipová karta I.CA	11
4.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou soukromého klíče	12
4.5. Uložení žádosti o certifikát	15
5. Vystavení certifikátu.....	15
6. Instalace Java Runtime Environment (JRE).....	15
7. Řešení problémů	18

1. Úvod

Tento dokument slouží jako návod, jak postupovat při generování žádosti o 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, vybídnu uživatele k jeho stažení/instalaci.
- v internetovém prohlížeči zapnuta podpora skriptování Javascript, zapnuta podpora jazyku Java, podpora ukládání cookies.

3. Instalace kořenového certifikátu I. CA

Při spuštění stránky s žádostí o certifikát vás může prohlížeč upozornit, že vstupujete na nedůvěryhodné stránky. Tento problém je způsoben tím, že nemáte uloženy v úložišti kořenové certifikáty I.CA, stažení je možné zde: <http://www.ica.cz/Korenove-certifikaty>

Zobrazí se vám následující stránka:



CERTIFICATION AUTHORITY První certifikační autorita, a.s. | **SPOJENÍ S DŮVĚROU**

O NÁS | REGISTRAČNÍ AUTORITY | PRODUKTY A SLUŽBY | CENÍK | PODPORA | KONTAKTY

Hledej...

> O nás > Rychlé odkazy > Kořenové certifikáty I.CA

Kořenové certifikáty I.CA

Kořenové certifikáty jsou vydávány samotnou Certifikační autoritou I.CA. Po instalaci do PC je kořenový certifikát zařazen mezi Důvěryhodné kořenové certifikační úřady a umožňuje následné automatizované ověření klientských certifikátů vydávaných I.CA v systému.

Instalaci všech aktuálních kořenových certifikátů I.CA provedete spuštěním aplikace [ICARootMan](#).

Postup pro instalaci kořenových certifikátů I.CA do prohlížeče Mozilla Firefox naleznete [zde](#) >>>.

Níže je možné vybrat si instalaci konkrétního kořenového certifikátu.

Kořenový certifikát pro vydávané komerční certifikáty SHA2

Kořenový certifikát pro vydávané kvalifikované certifikáty SHA2

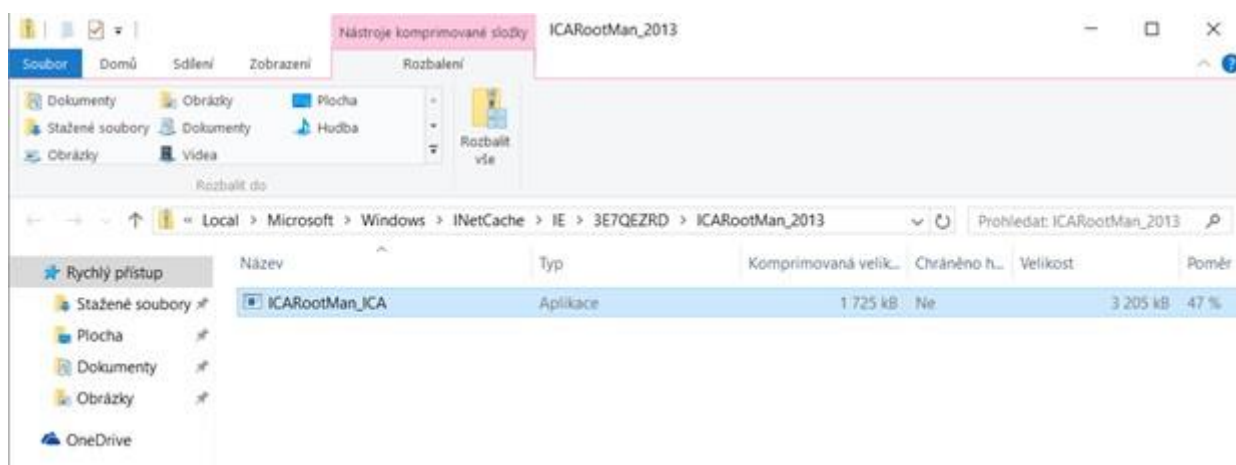
Kořenový certifikát pro vydávané komerční certifikáty SHA1

Kořenový certifikát pro vydávané kvalifikované certifikáty SHA1

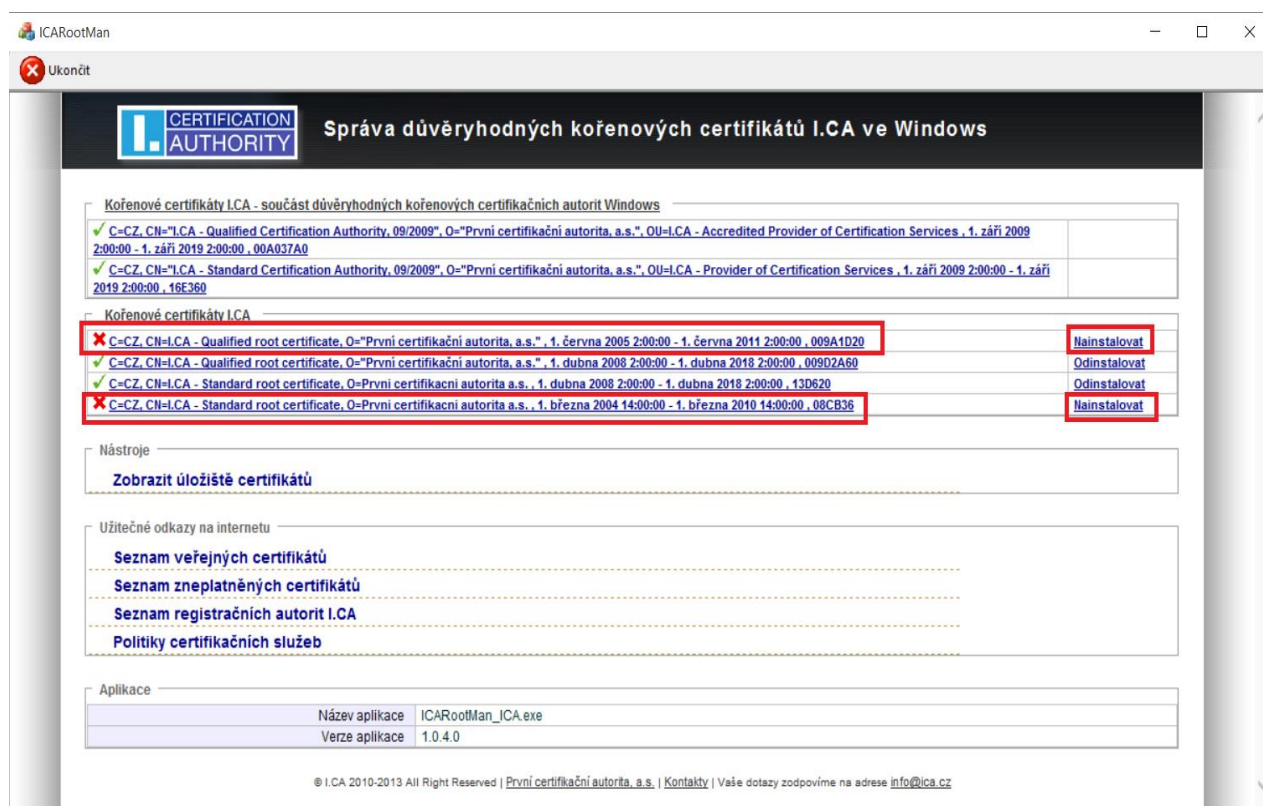
Rychlé odkazy

- Objednávky produktů a služeb
- Získat elektronický podpis
- Dokumenty k získání certifikátu
- Žádost o zneplatnění certifikátu
- Certifikační politika
- Zprávy pro uživatele el. podpisu
- Kořenové certifikáty I.CA
- Certifikáty časové autority
- Seznamy veřejných certifikátů
- Seznamy zneplatněných certifikátů

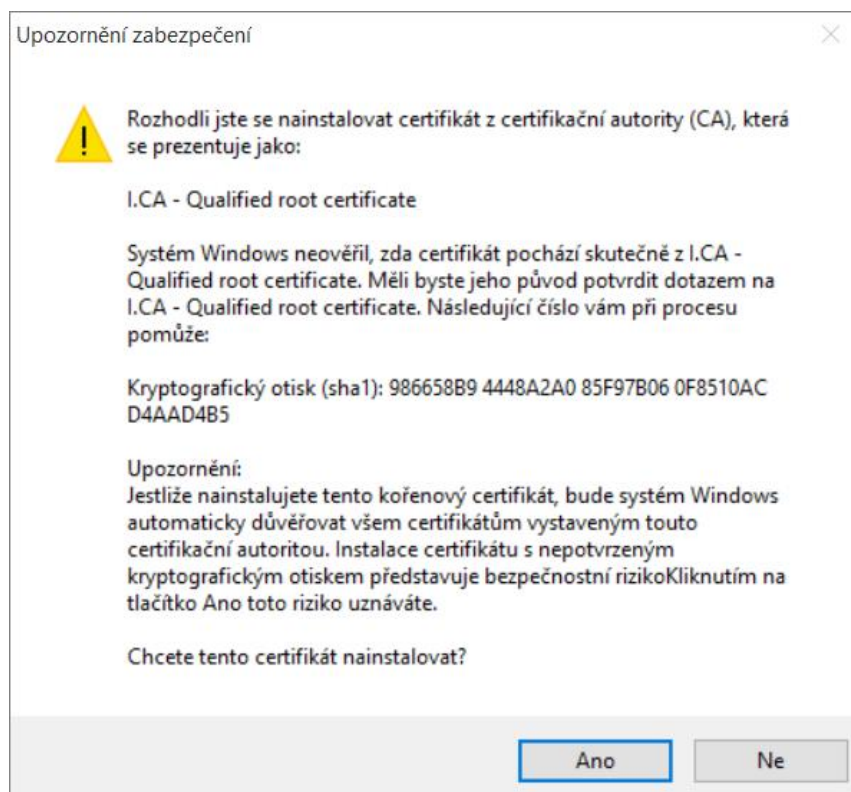
Klikněte na **ICARootMan**, zobrazí se Vám dialog pro stažení souboru. Soubor uložte na Váš pevný disk a spusťte **ICARootMan_ICA.exe**

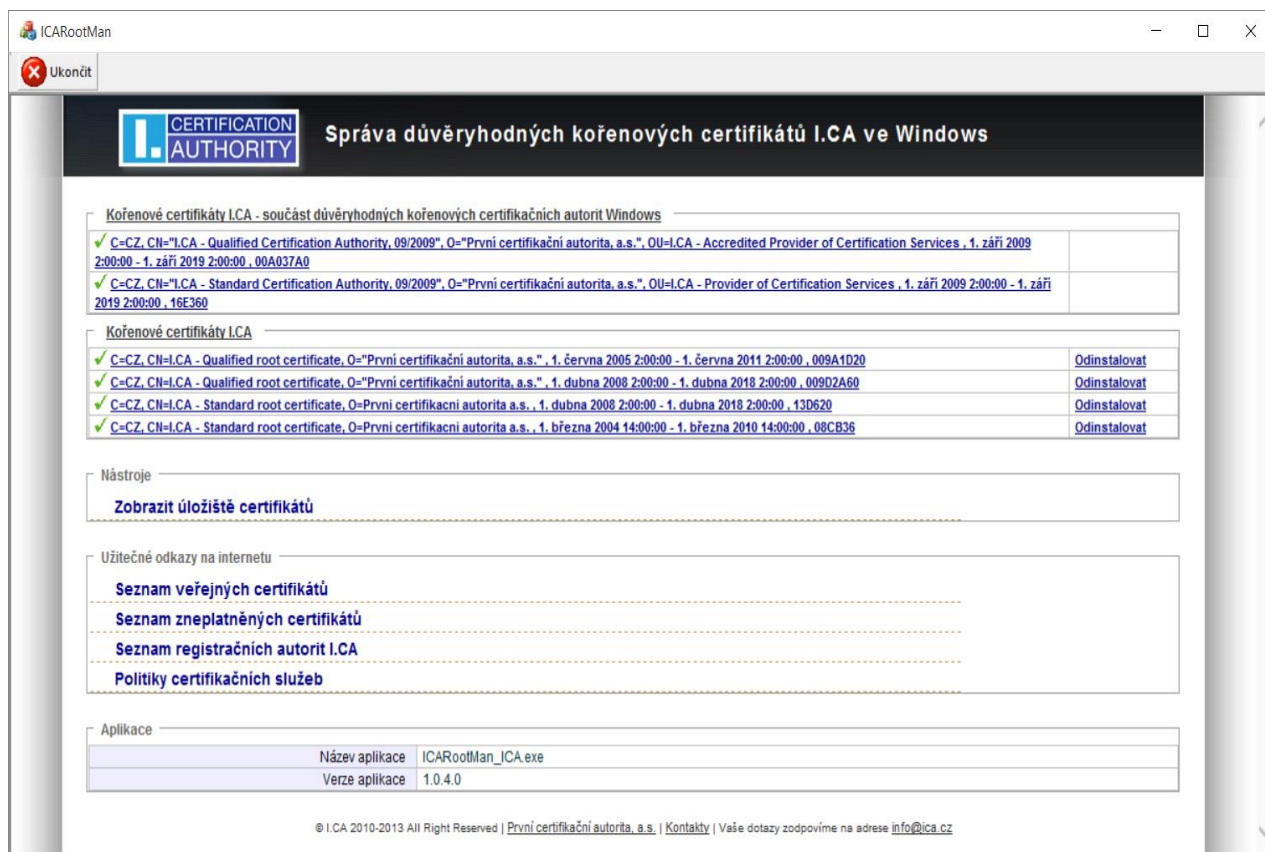


Dojde ke spuštění aplikace. Vidíte-li pod sekci Kořenové certifikáty I. CA symbol červeného křížku, klikněte v pravé části na odkaz **Nainstalovat**.



Zobrazí se dialog s instalací certifikátu. Zvolte **Ano**, kořenový certifikát se nainstaluje.





4. Proces generování žádosti o certifikát

Tvorbu žádosti zvolte po výběru typu certifikátu zde: <http://www.ica.cz/Certifikaty>

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

Kontrola softwarového vybavení

Vyplnění údajů žadatele

Kontrola vyplněných údajů

Generování žádosti o certifikát

Uložení žádosti o certifikát

4.1. 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.



První certifikační
autorita, a.s.

Žádost o certifikát

1. Test systému
2. Zadání údajů
3. Kontrola údajů
4. Uložení žádosti
5. Dokončení

Je Váš počítač připraven?

Nejdříve je nutné otestovat, zda Váš počítač splňuje minimální požadavky pro bezproblémový průběh generování žádosti. 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](#).

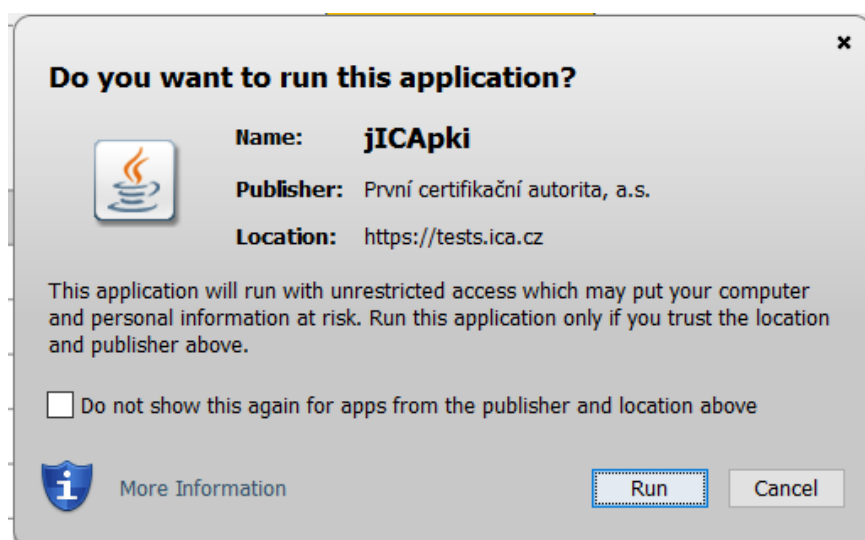
Zahájit test

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.



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

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

Pokud se při kontrole vyskytne chyba, nelze pokračovat v tvorbě žádosti certifikátu. Nejdříve je potřeba odstranit chybu, která znemožňuje tvorbu žádosti o certifikát. 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. 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.

4.1.4. 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

Instalace JRE je popsána v **Kapitole 6**.

4.1.5. 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.

4.2. Vyplnění údajů o žadateli

Pokud proces kontroly proběhl bez chyb, stránka zobrazí formulář, do kterého vyplníte své osobní údaje.

1. Test systému

2. Zadání údajů

3. Kontrola údajů

4. Uložení žádosti

5. Dokončení

ÚDAJE O ŽADATELI

SKRÝT DALŠÍ MOŽNOSTI >>

☒ **Běžný uživatel**
(fyzická osoba - nepodnikající)

Jméno

Příjmení

☐ Zaměstnanec
(vč. členů statutárních orgánů)

E-mail uvedený v certifikátu ?

E-mail pro komunikaci s I.CA ?

☐ Právníká osoba
(firma - OSVČ)

Česká republika

☐ Pseudonym

Česká republika

PODROBNÉ ÚDAJE O ŽADATELI

ADRESA TRVALÉHO BYDLIŠTĚ

Titul (před jménem)

Titul (za jménem)

Generační rozlišení

Ulice

Číslo popisné / orientační

Město / obec

PSČ

Kraj

Heslo pro zneplatnění

Vaše heslo ?

Typ úložiště klíče (CSP)

Operační systém Windows

☒ Certifikát splňující podmínky pro komunikaci s orgány veřejné moci ČR ?
 ☒ Certifikát určený pro podpis
 ☐ Certifikát určený pro šifrování
 ☒ Povolit export klíče ?
 ☒ Povolit silnou ochranu klíče ?
 ☒ Certifikát zaslat ve formátu ZIP

ROZŠÍŘENÉ MOŽNOSTI CERTIFIKÁTU >>

Pokračovat

Položky zdůrazněné modrým podbarvením jsou povinné. Například jméno a příjmení jsou povinné, tituly povinné nejsou.

E-mail uvedený v certifikátu:

Tuto položku vyplňte zejména v případě, kdy budete podpis používat pro podepisování e-mailových zpráv. E-mailová adresa uvedená v certifikátu musí být shodná s e-mailem odesílatele.

E-mail pro komunikaci s I. CA:

Tento e-mail slouží pro zasílání certifikátů a zasílání upozornění na blížící se konec platnosti vašeho certifikátu.

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. Délka hesla pro zneplatnění certifikátu musí být 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

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.

ÚDAJE O ŽADATELI		SKRÝT DALŠÍ MOŽNOSTI >>	
☒ Běžný uživatel (fyzická osoba - nepodnikající)	Jméno ✗ Příjmení ✗	☐ Zaměstnanec (vč. členů statutárních orgánů)	E-mail uvedený v certifikátu ? E-mail pro komunikaci s I.CA ?
☐ Právnícká osoba (firma - OSVČ)	Česká republika ▼	☐ Pseudonym	

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

4.3. Kontrola zadaných údajů

Na této stránce zkontrolujete vámi zadané údaje.

ÚDAJE O ŽADATELI	
Celé jméno	Petr Pavel
Stát	Česká republika
NASTAVENÍ CERTIFIKÁTU	
Typ certifikátu	Kvalifikovaný certifikát
Typ žadatele	Běžný uživatel (fyzická osoba - nepodnikající)
Certifikát splňující podmínky pro komunikaci s orgány veřejné moci ČR	Ano
Heslo pro zneplatnění	12341234
Certifikát zaslat ve formátu ZIP	Ano
Doba platnosti certifikátu	365 dní
Typ úložiště klíče (CSP)	Operační systém Windows
Algoritmus miniatury / Délka klíče	sha256WithRSAEncryption / 2048
Povolit export klíče	Ano
Povolit silnou ochranu klíče	Ano
Nastavení použití klíče	Certifikát určený pro podpis
Typ kódování	UTF8_STRING

V případě špatného zadání se v krokové liště vraťte zpět na **Zadání údajů**

Kliknutím na tlačítko **Pokračovat** se zahájí vytvoření privátního klíče.

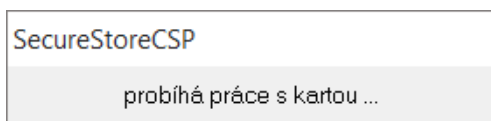
4.4. Generování žádosti o certifikát

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

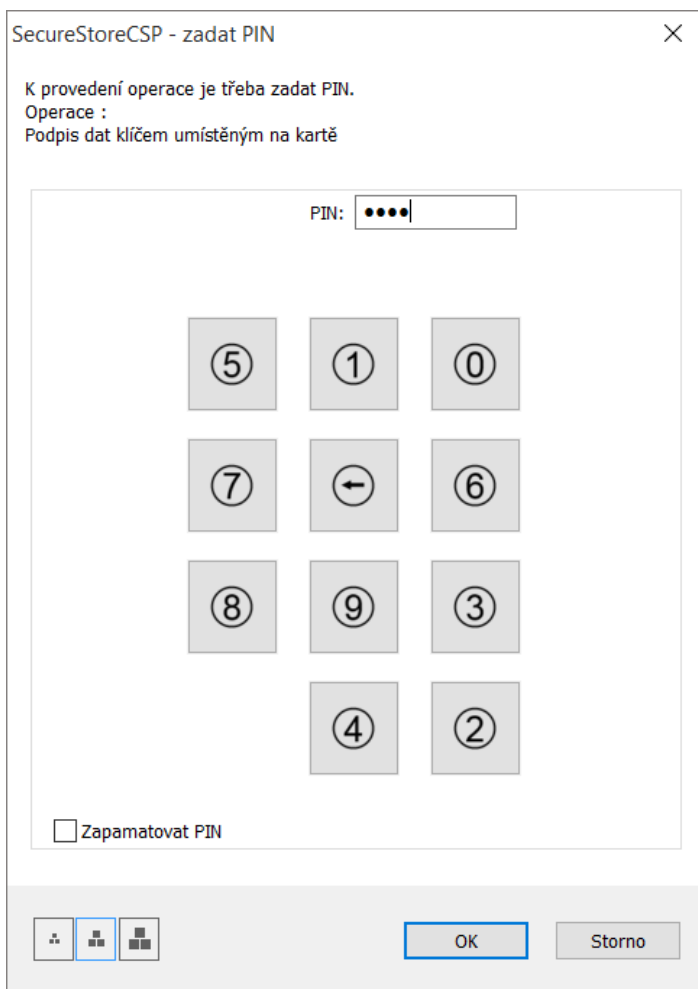
4.4.1. SecureStoreCSP – čipová karta I.CA

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.

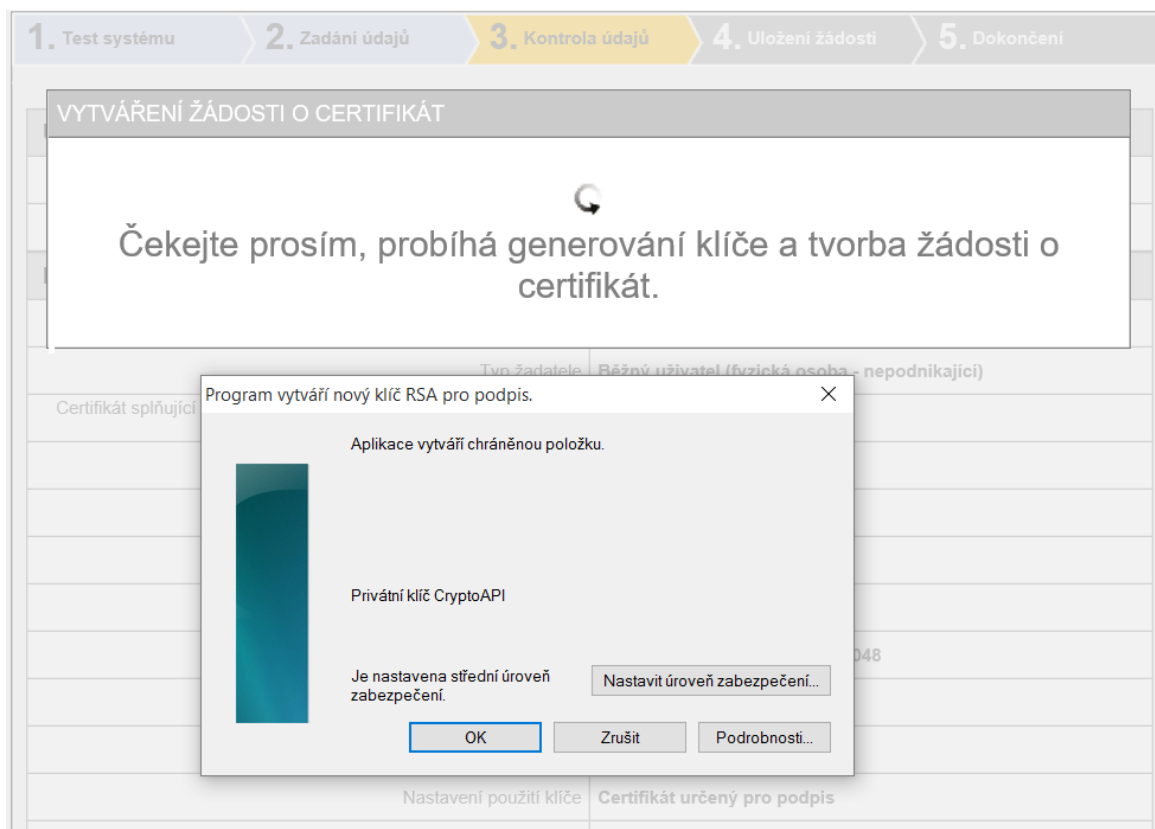


Poté co je privátní klíč vytvořen, jste vyzváni k zadání PINu k vaší kartě.

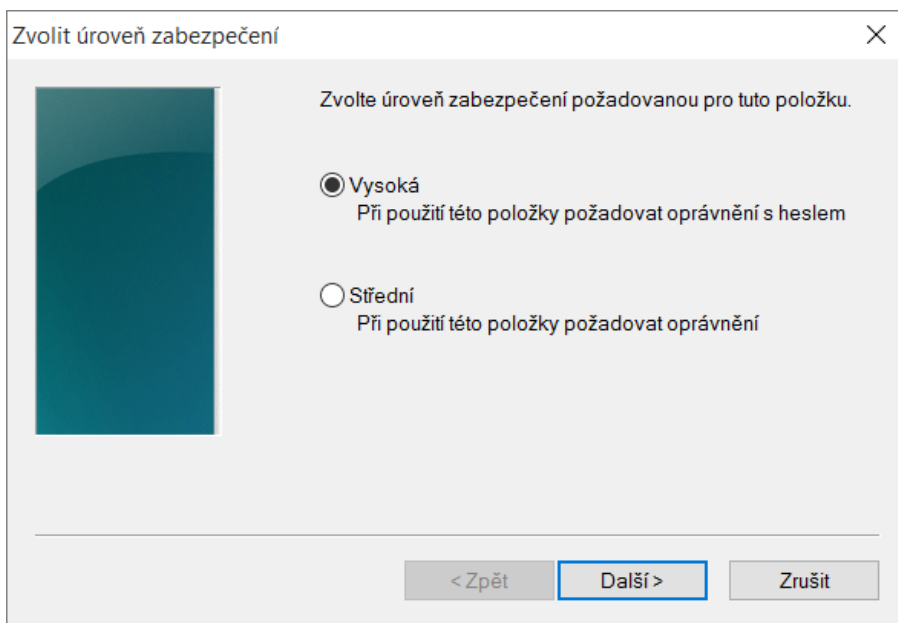


4.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou soukromého klíče

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.



Pokud zvolíte vysokou 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:

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.

Zabezpečení systému Windows

Jsou vyžadovány přihlašovací údaje.

Chcete-li této aplikaci povolit přístup ke svému privátnímu klíči, zadejte heslo:

Popis klíče : Privátní klíč CryptoAPI



Heslo

Povolit

Nepovolovat

4.5. Uložení žádosti o certifikát

Zvolením na **Uložit na lokální disk nebo externí úložiště** bude žádost uložena na váš pevný disk nebo jiné médium, které zvolíte.

Pokud chcete vaši žádost **uložit na server I.CA**, opište kód uvedený na obrázku do pole Kontrolní řetězec a stiskněte tlačítko **Pokračovat**. Pokud bude vaše žádost úspěšně uložena na server I.CA, **obdržíte identifikátor**, který předložíte při návštěvě registrační autority. Registrační autorita pak bude moci získat vaši žádost o certifikát ze serveru.

Identifikátor bude zaslán na e-mailovou adresu uvedenou v žádosti nebo na doplněné tel. číslo.

1. Test systému	2. Zadání údajů	3. Kontrola údajů	4. Uložení žádosti	5. Dokončení
-----------------	-----------------	-------------------	--------------------	--------------

VYBERTE ZPŮSOB ULOŽENÍ VAŠÍ ŽÁDOSTI O CERTIFIKÁT

☒ Uložení na server I.CA

☐ Uložení na lokální disk nebo externí úložiště

ULOŽENÍ NA SERVER I.CA

Pro uložení žádosti na server I.CA opište kontrolní text uvedený na obrázku a stiskněte tlačítko Pokračovat. Vaše žádost bude uložena po dobu 30 dní. Po uložení na server se Vám zobrazí identifikační kód žádosti, který předložíte při návštěvě registrační autority.

Na zadané telefonní číslo Vám bude zaslán identifikační kód žádosti SMS zprávou. Pokud jste vyplnili e-mail pro zaslání certifikátu, bude identifikační kód rovněž zaslán na tento e-mail.



Pokračovat

5. Vystavení certifikátu

Poté, co vytvoříte žádost o certifikát, je nutné navštívit některou registrační autoritu I.CA ([seznam zde](#)). S sebou na registrační autoritu I.CA přineste žádost, kterou jste vygenerovali (například na USB flash disku, uloženou na čipové kartě, identifikátor žádosti uložený na serveru I.CA), a dokumenty potřebné k vystavení certifikátu. Seznam potřebných dokumentů [naleznete zde](#).

6. Instalace Java Runtime Environment (JRE)

Pokud nemáte nainstalovanou podporu Java Runtime Environment, budete při prvním přístupu na stránky 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 spustíte 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**.

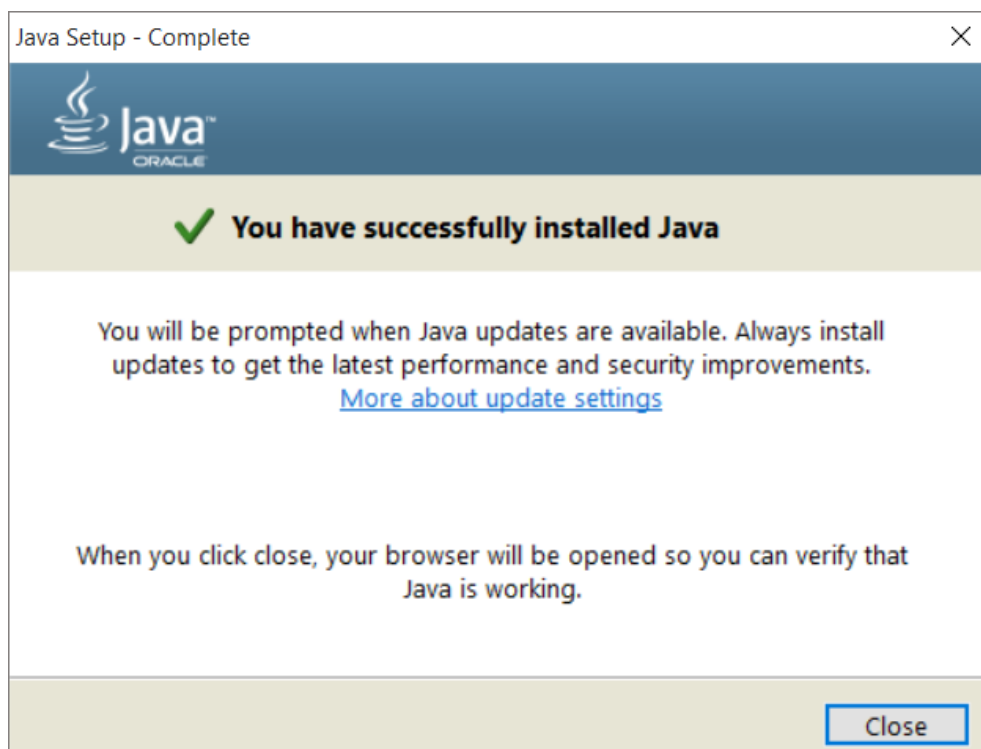
Zobrazí se dialog s možnostmi stažení. Zvolte spustit, případně soubor uložte na disk a následně jej spustíte.

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.



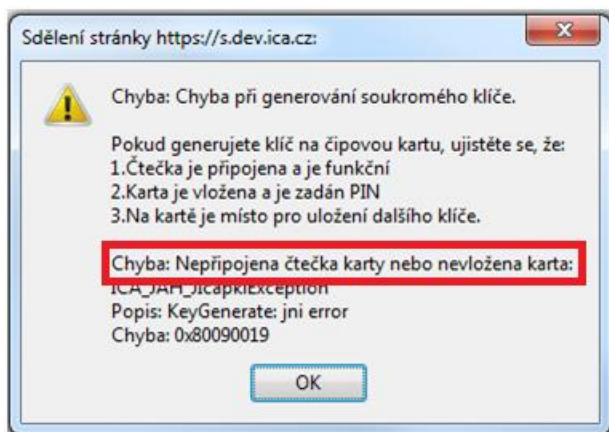


Na závěrečné obrazovce klikněte na tlačítko **Close**. V tuto chvíli doporučujeme prohlížeč obnovit, aby se projevil změny.



7. 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](#)