

# **Generování žádosti o následný certifikát**

## **Uživatelská příručka pro Mozilla Firefox**

**První certifikační autorita, a.s.**

**Verze 8.16**

## 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
  - **Windows 7 ServicePack 1**
  - **Windows 8.1 (April 2014 update)**
  - **Windows 10**
- nainstalován a použit **Mozilla Firefox** verze 52 a vyšší
- v internetovém prohlížeči zapnuta podpora skriptování Javascript, zapnuta podpora jazyku Java, podpora ukládání cookies.
- nainstalována komponenta a rozšíření **I.CA PKIService host**
- **I.CA SecureStore Card Manager** (pouze v případě generování žádosti na čipovou kartu)

## 3. Proces generování žádosti o následný certifikát

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

Test systému

Kontrola údajů

Rekapitulace


Podpis žádosti


Dokončení


### 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.


SPOJENÍ S DŮVĚROU




VYTVOŘENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU

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 rozšíření	
	Podpora čipových karet I.CA / aplikace I.CA SecureStore	
	Podpora ukládání cookies	

Pokračovat

V případě nepřítomnosti komponenty a rozšíření **I.CA PKIService Host** se objeví chybová hláška viz. níže


SPOJENÍ S DŮVĚROU




VYTVOŘENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU

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

---

Test skončil chybou

Výsledek	Popis	Podrobnosti
✓	Verze operačního systému	Windows 10, tento operační systém je podporován.
✓	Typ a verze prohlížeče	Firefox verze 79.0, tento webový prohlížeč je podporován.
✓	Podpora jazyka JavaScript	JavaScript povolen.
✗	Podpora rozšíření	Rozšíření nejsou nainstalovaná. Nainstalujte si chybějící komponenty <b>I.CA PKIServiceHost</b> a <b>Extension</b>
	Podpora čipových karet I.CA / aplikace I.CA SecureStore	Čekám na test ...
	Podpora ukládání cookies	

Pokračovat

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.08.03

Kliknutím na zvýrazněné **I.CA PKIServiceHost** a **Extension** nainstalujete do PC potřebné komponenty pro vygenerování žádosti. Po úspěšné instalaci restartujte prohlížeč a klikněte na tlačítko **Zahájit test**



## VYTVOŘENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU

**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

## Test úspěšně dokončen

Výsledek	Popis	Podrobnosti
✓	Verze operačního systému	Windows 10, tento operační systém je podporován.
✓	Typ a verze prohlížeče	Firefox verze 79.0, tento webový prohlížeč je podporován.
✓	Podpora jazyka JavaScript	JavaScript povolen.
✓	Podpora rozšíření	Rozšíření jsou podporována
✓	Podpora čipových karet I.CA / aplikace I.CA SecureStore	Karty I.CA jsou podporovány, aplikace I.CA SecureStore je instalována.
✓	Podpora ukládání cookies	Ukládání cookies je povoleno.

Pokračovat

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.08.03

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 jednu z verzí prohlížeče uvedeného 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. I.CA PKIService Host**

Stránky vyžadují pro svou funkčnost nainstalovanou komponentu I.CA PKIService Host. Ujistěte, že jí máte nainstalovanou. Pokud nemáte na svém počítači komponentu nainstalovanou, ke stažení použijte zvýrazněný název I.CA PKIService Host, po instalaci je nutno restartovat prohlížeč.

### **3.1.5. Rozšíření (doplněk) I.CA PKIService Host**

Dále je nutné mít nainstalované a povolené rozšíření v prohlížeči. Kliknutím na zvýrazněný název Extension Vás prohlížeč přesměruje do nastavení, kde rozšíření najdete a nainstalujete, po instalaci je nutno obnovit stránku.

### **3.1.6. 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.

## **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.



VYTVOŘENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU

1. Test systému

2. Kontrola údajů

3. Rekapitulace

4. Podpis žádosti

5. Dokončení

Zvolte, kde je Váš certifikát uložen (registrován)

 Osobní úložiště certifikátů ve Windows
  Jiné úložiště (např. I.CA čipová karta)

Vyberte certifikát, ke kterému chcete vydat následný certifikát.

Pokračovat

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.08.03

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

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 vloženou 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.

Certifikát		Skrýt povolené úpravy >>
TWIN	[redacted]	
Celé jméno	[redacted]	
Stát	[redacted]	
Organizace	[redacted]	
Křestní jméno	[redacted]	
Příjmení	[redacted]	
E-mail uvedený v rozšířených certifikátu	[redacted]	
SN ICA	[redacted]	
IK MPSV	[redacted]	
SN ICA	[redacted]	

Heslo pro zneplatnění

Typ úložiště klíče (CSP)

Certifikát zaslat ve formátu ZIP

id-kp-clientAuth

Úprava e-mailu

Přidání UPN (Microsoft Universal Principal Name)

**TWIN kvalifikovaný**

IK MPSV

Heslo pro zneplatnění ?

Operační systém Windows v

Povolit export klíče ?

id-kp-emailProtection ?

Povolit silnou ochranu klíče ?

ms-SmardCardLogon ?

Smazat  Změnit

Smazat  Změnit

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 ne zadáte 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 tato rozšíření před pokračováním odebrat.

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



VYTVOŘENÍ ŽADOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU

1. Test systému

2. Kontrola údajů

3. Rekapitulace

4. Podpis žádosti

5. Dokončení

Rekapitulace údajů	
Certifikát zaslat ve formátu ZIP	Ano
Doba platnosti certifikátu	365
Typ úložiště klíče (CSP)	Operační systém Windows
Algoritmus miniaturní / Délka klíče	sha256Algorithm / 2048
Povolit export klíče	Ano
Povolit silnou ochranu klíče	Ano
Rozšířené nastavení použití klíče kvalifikovaného certifikátu	id-kp-emailProtection
Rozšířené nastavení použití klíče komerčního certifikátu	id-kp-clientAuth / id-kp-emailProtection
Nastavení certifikátu	
Celé jméno	██████████
Křestní jméno	████
Příjmení	██████
Organizace	████████████████████
E-mail uvedený v rozšířených certifikátu	██████████
IK MPSV	██████████
Stát	██
SN ICA	██████
SN ICA	██████
Jsou uvedené údaje stále aktuální?	
<input type="button" value="ANO, údaje jsou aktuální"/> <input type="button" value="NE, údaje se změnily"/>	

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.08.03

V případě, že jsou položky v certifikátu aktuální, pokračujeme kliknutím na tlačítko „ANO, údaje jsou aktuální“ a zahájíme vytvoření privátního klíče.

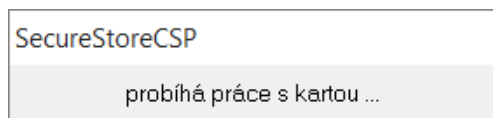
### 3.4. Generování žádosti o certifikát

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

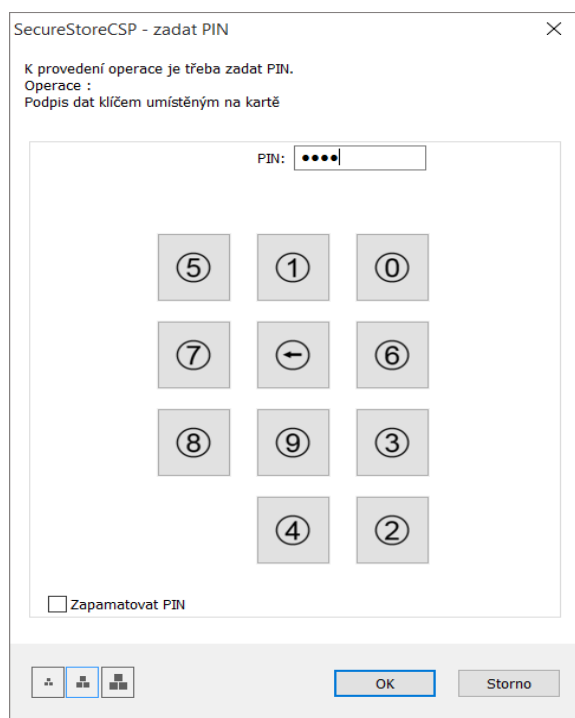
### 3.4.1. SecureStoreCSP – čipová karta I.CA

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.

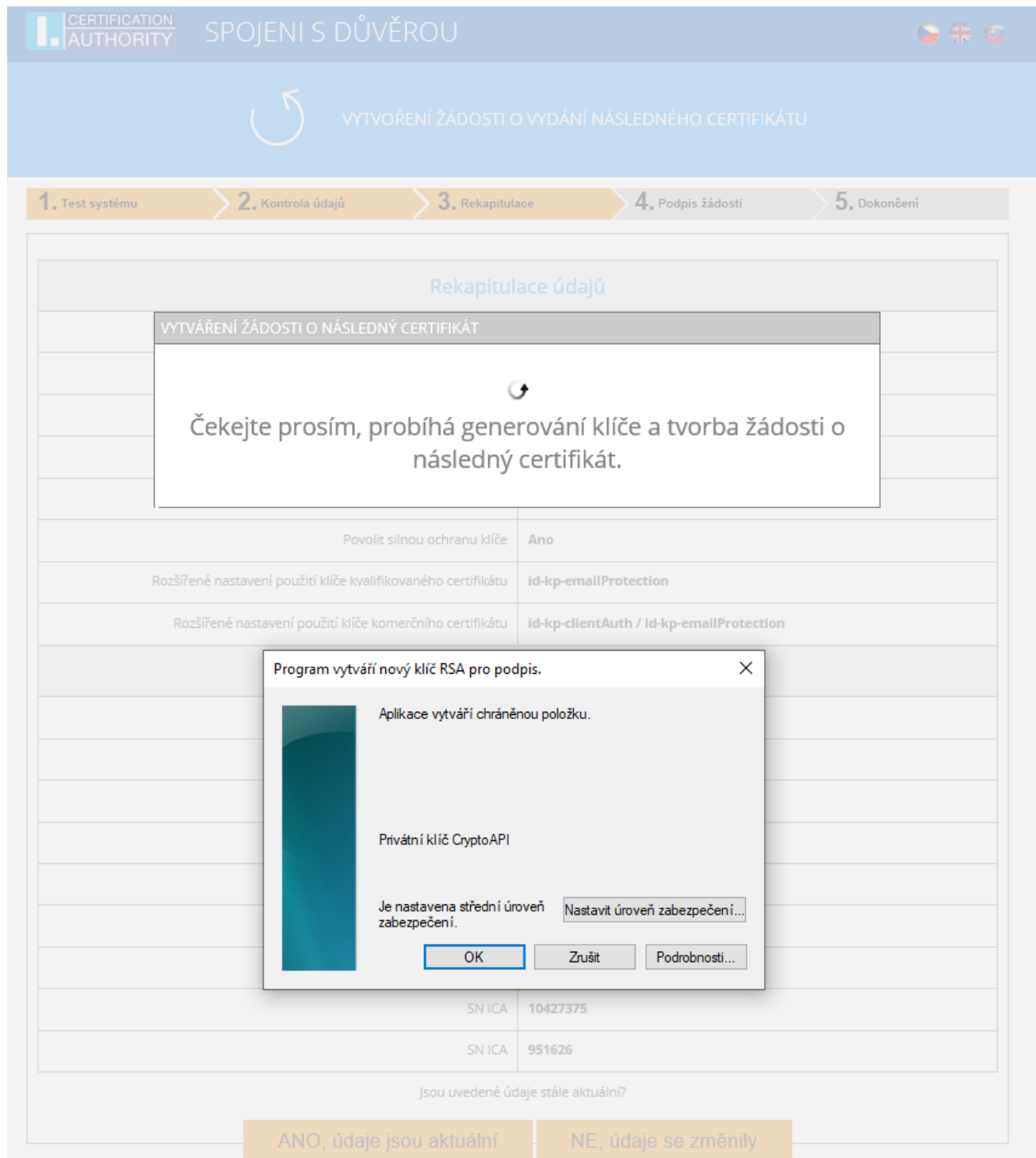


Poté co je privátní klíč vytvořen, jste vyzváni k zadání PINu k vaší kartě.



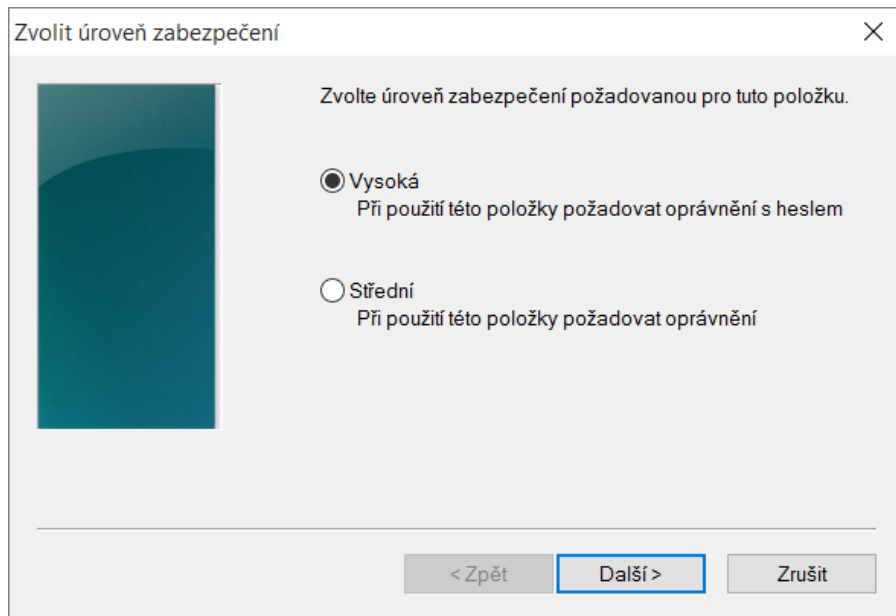
### 3.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider se silnou ochranou soukromého klíče

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:

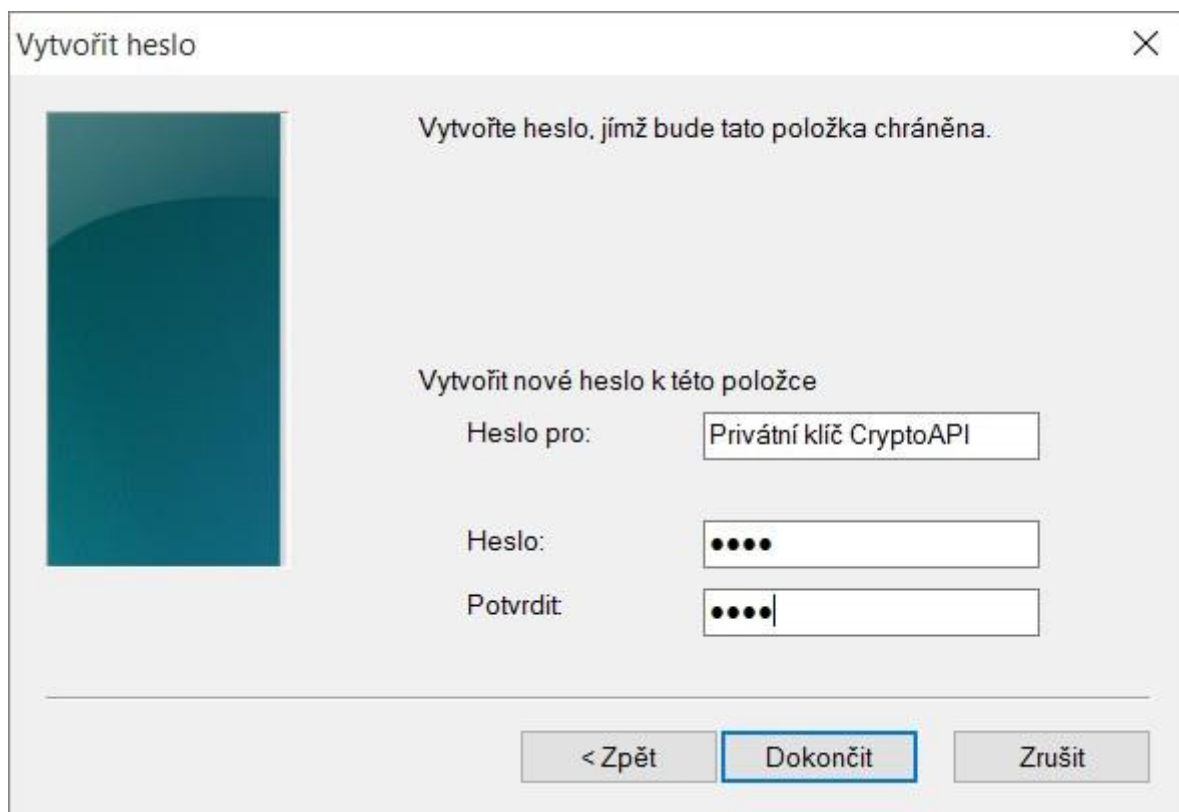


The screenshot shows the 'SPOJENÍ S DŮVĚROU' web interface. The main content area is titled 'Rekapitulace údajů' and 'VYTVÁŘENÍ ŽÁDOSTI O NÁSLEDNÝ CERTIFIKÁT'. A progress bar at the top indicates the current step is '3. Rekapitulace'. A modal dialog box is open, titled 'Program vytváří nový klíč RSA pro podpis.' It contains a progress bar and the text 'Aplikace vytváří chráněnou položku.' Below this, it says 'Privátní klíč CryptoAPI' and 'Je nastavena střední úroveň zabezpečení.' There is a button 'Nastavit úroveň zabezpečení...' and three buttons at the bottom: 'OK', 'Zrušit', and 'Podrobnosti...'. Below the dialog box, there are two rows of data: 'SN ICA 10427375' and 'SN ICA 951626'. At the bottom, there are two buttons: 'ANO, údaje jsou aktuální' and 'NE, údaje se změnily'.

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

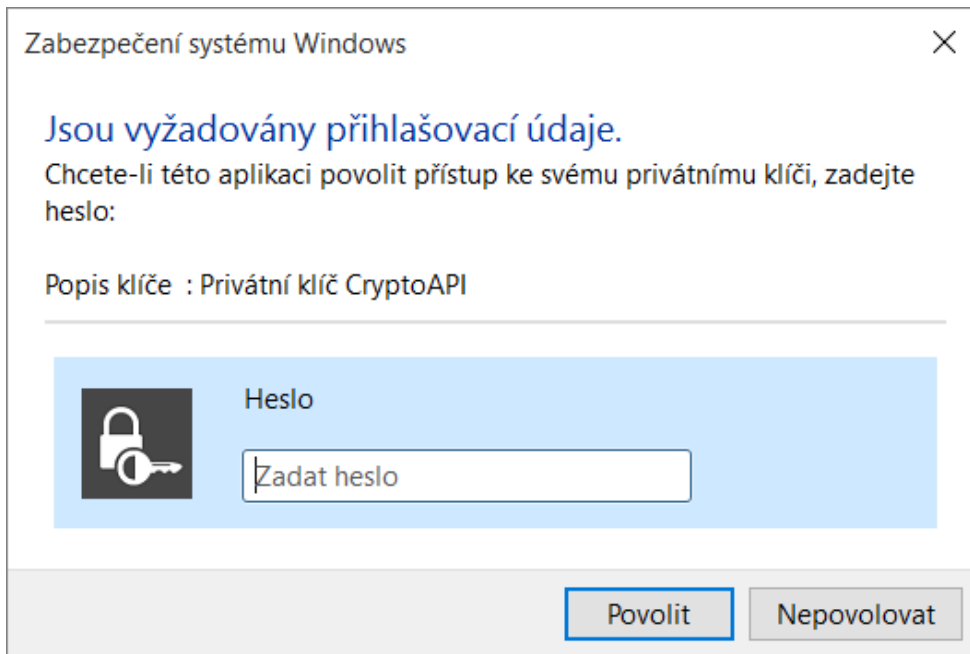


Pokud zvolíte **vysokou** úroveň zabezpečení, budete vyzváni k zadání hesla. (Toto heslo bude potřeba zadat vždy, když budete používat Váš vydaný certifikát).



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.


SPOJENÍ S DŮVĚROU




VYTVOŘENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNĚHO CERTIFIKÁTU

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

### Vytvořená žádost o certifikát

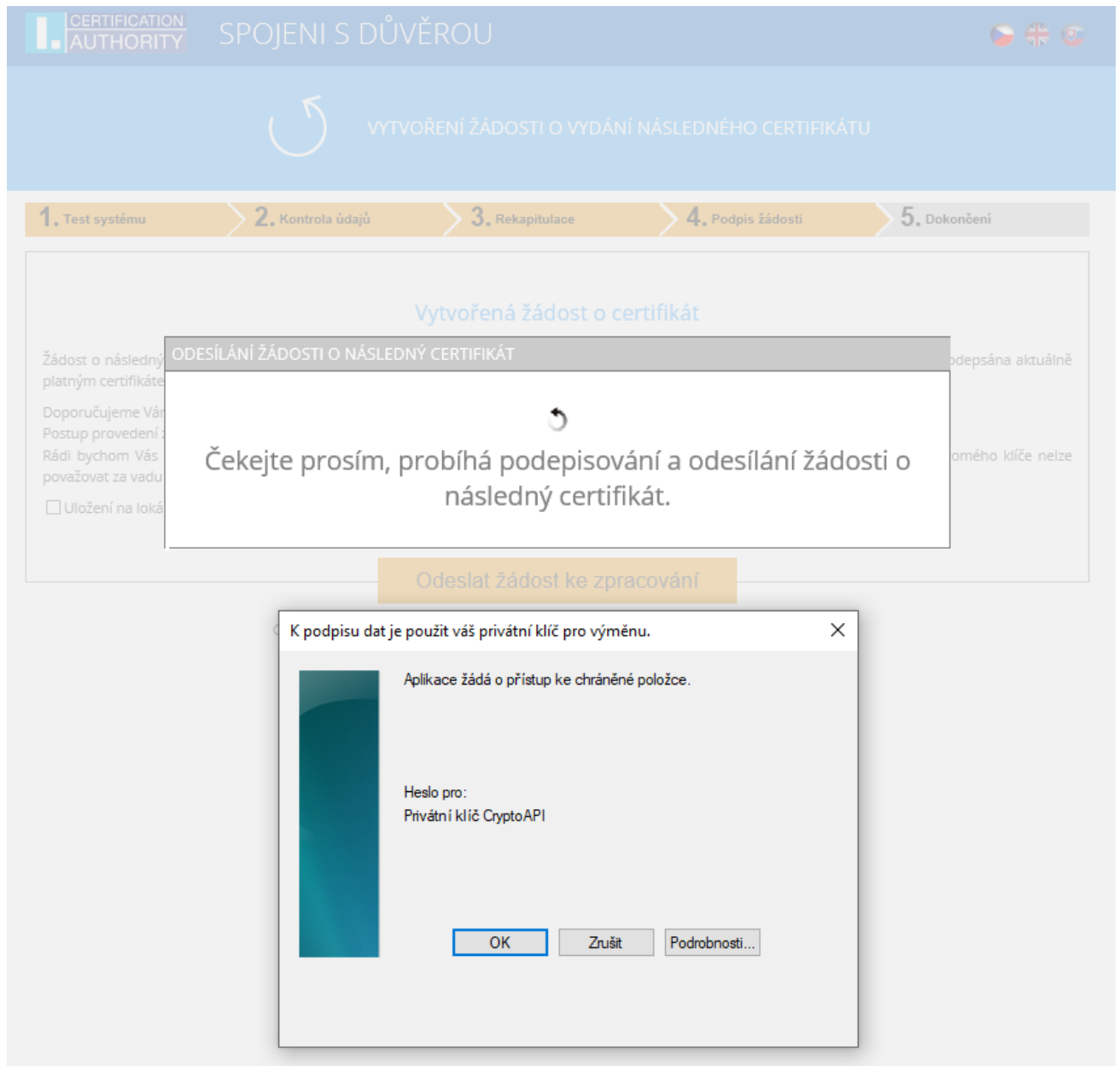
Žádost o následný certifikát byla úspěšně vytvořena. Kliknutím na tlačítko "Odeslat žádost ke zpracování" bude Vaše žádost o certifikát podepsána aktuálně platným certifikátem a odeslána na zpracování.

Doporučujeme Vám provést zálohu privátního klíče.  
Postup provedení zálohy je uveden zde: <http://www.ica.cz/Zaloha-klisce>

Rádi bychom Vás upozornili, že za správu svého soukromého klíče je vždy plně odpovědný žadatel o certifikát. Případnou ztrátu soukromého klíče nelze považovat za vadu poskytnuté služby ze strany I.CA a neopravňuje k opakovanému bezplatnému vydání certifikátu.

Uložení na lokální disk nebo externí úložiště

Odeslat žádost ke zpracování



CERTIFICATION AUTHORITY SPOJENÍ S DŮVĚROU

VYTVORENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU

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

Vytvořená žádost o certifikát

ODESÍLÁNÍ ŽÁDOSTI O NÁSLEDNÝ CERTIFIKÁT

Čekejte prosím, probíhá podepisování a odesílání žádosti o následný certifikát.

Odeslat žádost ke zpracování

K podpisu dat je použit váš privátní klíč pro výměnu.

Aplikace žádá o přístup ke chráněné položce.

Heslo pro:  
Privátní klíč CryptoAPI

OK Zrušit Podrobnosti...


Žádost je potřeba podepsat kliknutím na tlačítko „OK“




Pokud je žádost generována na čipovou kartu, je zapotřebí podepsat zadáním **PIN kódu** k čipové kartě.


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:




SPOJENÍ S DŮVĚROU


VYTVORENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU

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

Žádost o následný certifikát byla úspěšně přijata.

ID žádosti o kvalifikovaný certifikát: 5708610718840  
**Zde může sledovat stav Vaší žádosti s ID 5708610718840.**

ID žádosti o komerční certifikát: 5708600522300  
**Zde může sledovat stav Vaší žádosti s ID 5708600522300.**

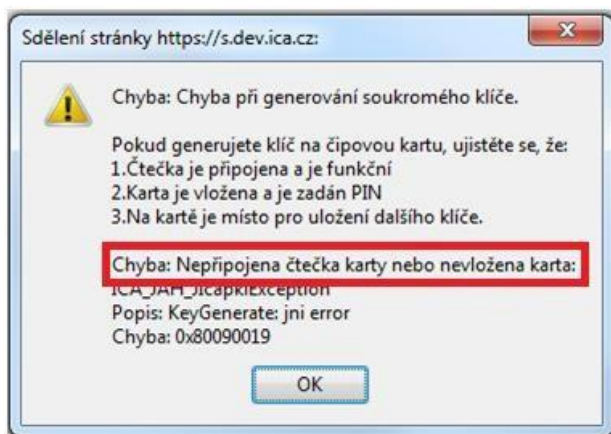
Čas přijetí žádosti: 09.07.2020 13:11:41

Ukončit průvodce

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.08.03

## 4. 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](#)