

# Generování žádosti o následný certifikát

## Uživatelská příručka

### Obsah

1. Úvod .....	2
2. Požadavky na software .....	2
3. Proces generování žádosti o následný certifikát .....	2
3.1. Kontrola softwarového vybavení .....	3
3.2. Výběr certifikátu pro vytvoření žádosti o následný certifikát .....	5
3.3. Rekapitulace údajů .....	6
3.4. Doplnění a změna některých údajů .....	7
3.5. Generování žádosti o certifikát .....	9
3.6. Podpis a odeslání žádosti o následný certifikát .....	12
4. Řešení problémů .....	14

## 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:

### 2.1. nainstalovaný a spuštěný operační systém

- Windows 7 ServicePack 1
- Windows 8.1 (April 2014 update)
- Windows 10
- Windows 11

### 2.2. Podporované prohlížeče jsou:

- Microsoft Edge
- Chrome
- Firefox
- Opera

2.3. v internetovém prohlížeči zapnuta podpora skriptování Javascript, podpora ukládání cookies.

2.4. nainstalována komponenta a rozšíření **I.CA PKIService host**

2.5. **I.CA SecureStore Card Manager** (pouze v případě generování žádosti na čipovou kartu)

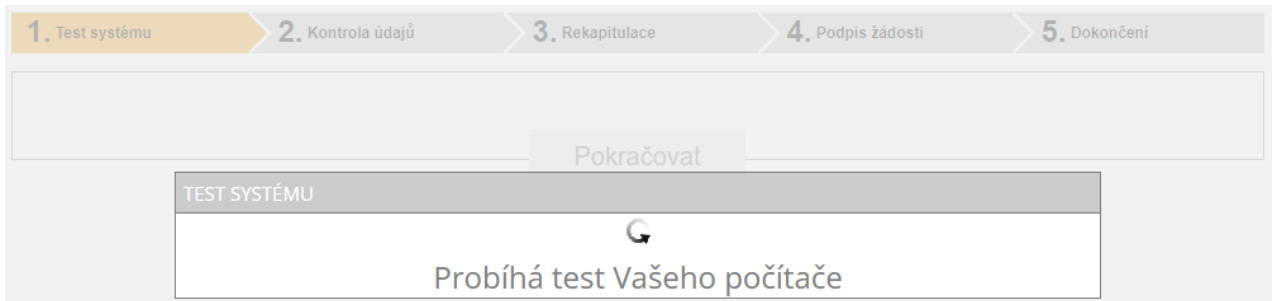
## 3. Proces generování žádosti o následný certifikát

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

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



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



Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.16.00



Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.16.00

Kliknutím na zvýrazněné „**I.CA PKIServiceHost**“ a „**Extension**“ nainstalujete do PC potřebné komponenty pro vygenerování žádosti. Po úspěšné instalaci restartujte prohlížeč.

Pokud máte uložený certifikát na čipové kartě, může se Vám zobrazit chyba aplikace **SecureStore**, kterou stáhnete a nainstalujete.

Stránka otestuje počítač, pokud nejsou detekovány problémy, automaticky 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 jazyce JavaScript. 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.

#### **3.1.4. I.CA PKIService Host**

Stránky vyžadují pro svou funkčnost nainstalovanou komponentu I.CA PKIService Host. Ujistěte se, 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 přeměruje 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.

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.

[2023-04-04] (I.CA Qualified 2 CA/RSA 02/2016) ▾

Pokračovat

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.16.00

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 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. Rekapitulace údajů

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 miniatury / 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	Celé jméno
Křestní jméno	Křestní jméno
Příjmení	Příjmení
Organizace	Organizace
E-mail uvedený v rozšířeních certifikátu	E-mail
IK MPSV	IK MPSV
Stát	Stát
Identifikátor právnické osoby	Identifikátor právnické osoby
SN ICA	SN ICA
SN ICA	SN ICA
Jsou uvedené údaje stále aktuální?	
<input type="button" value="ANO, údaje jsou aktuální"/> <input type="button" value="NE, údaje se změnilly"/>	

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.16.00

V případě, že jsou položky v certifikátu aktuální, pokračujte kliknutím na tlačítko „**ANO, údaje jsou aktuální**“ a zahájíte generování žádosti o certifikát.

Pokud se některá položka v certifikátu změnila, pokračujte kliknutím na tlačítko „**NE, údaje se změnilly**“ a pokračujte v příručce na bod 3.4 Doplnění a změna některých údajů.

### 3.4. 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

Heslo pro zneplatnění  ?

Typ úložiště klíče (CSP)  ▼

Certifikát zaslat ve formátu ZIP  Povolit export klíče ?  Povolit silnou ochranu klíče ?

Úprava e-mailu  Smazat  Změnit

Pro vydání certifikátu se správnými údaji kontaktujte prosím **technickou podporu I.CA.**

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Kontakty | 9.16.00

#### 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.

**Certifikát zaslat ve formátu ZIP**

Pokud budete chtít zasílat veřejnou část od nových certifikátů ve formátu ZIP, tak necháte zaškrtnuté pole.

**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 není možná, v tomto případě prosím požádejte o nový certifikát s opravenými údaji.

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



### 3.5. Generování žádosti o certifikát

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

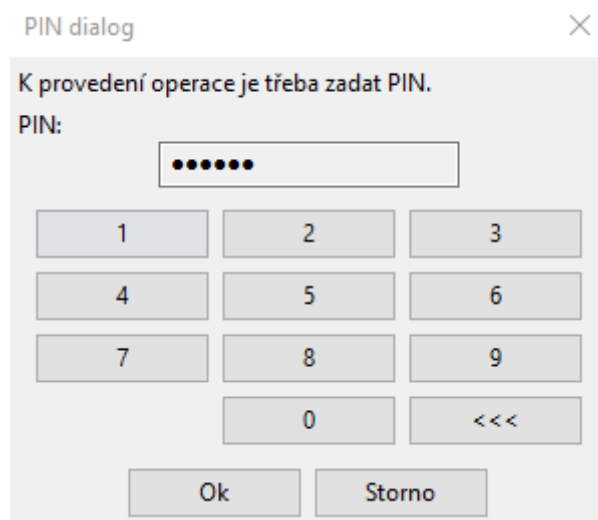
#### 3.5.1. SecureStoreCSP – čipová karta I.CA

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.



### 3.5.2. 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:

**SPOJENÍ S DŮVĚROU**

VYTVÁŘENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNĚHO CERTIFIKÁTU

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

**Rekapitulace údajů**

VYTVÁŘENÍ ŽÁDOSTI O NÁSLEDNÝ CERTIFIKÁT

Čekejte prosím, probíhá generování klíče a tvorba žádosti o následný certifikát.

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

Program vytváří nový klíč RSA pro podpis.

Aplikace vytváří chráněnou položku.

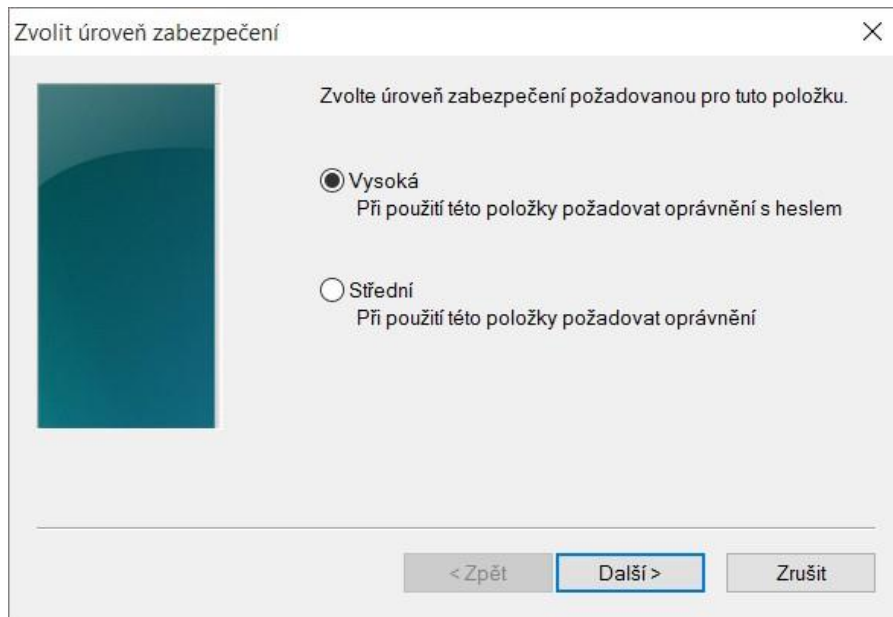
Privátní klíč CryptoAPI

Je nastavena střední úroveň zabezpečení. [Nastavit úroveň zabezpečení...](#)

SN ICA	10427375
SN ICA	951626

Jsou uvedené údaje stále aktuální?

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



Zvolit úroveň zabezpečení

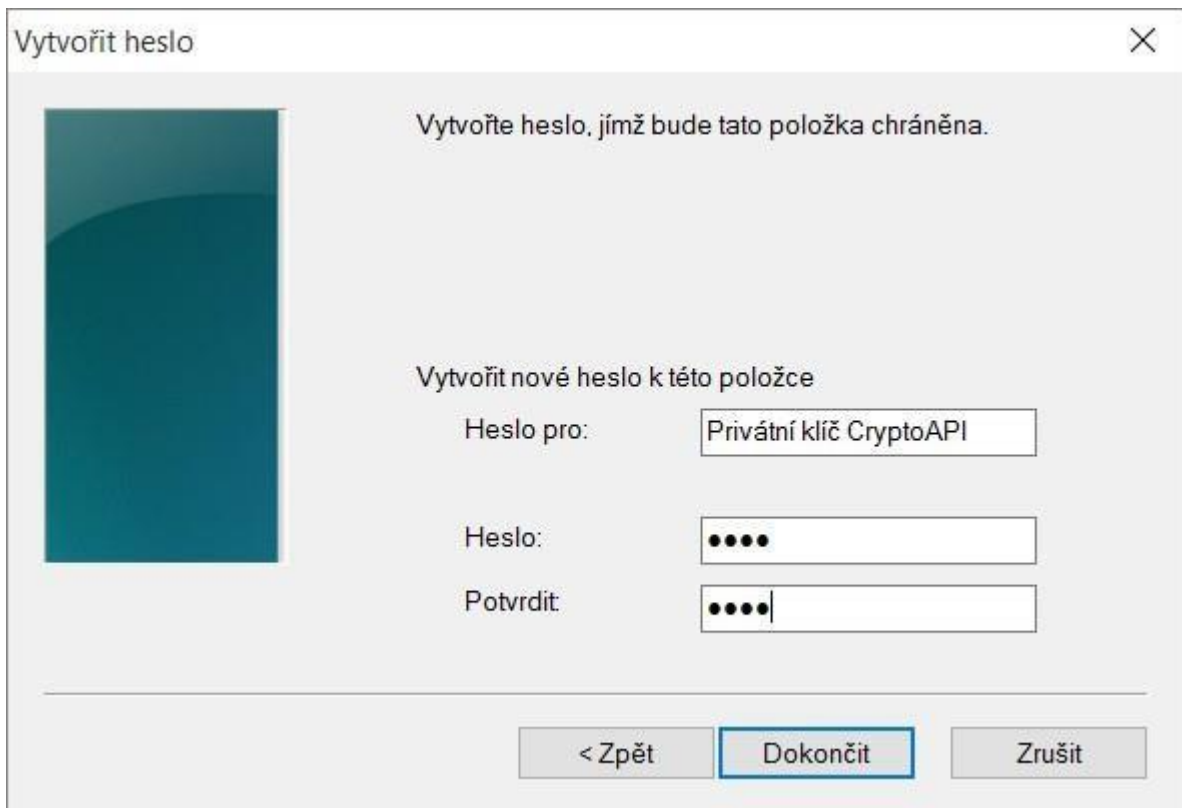
Zvolte úroveň zabezpečení požadovanou pro tuto položku.

Vysoká  
Při použití této položky požadovat oprávnění s heslem

Střední  
Při použití této položky požadovat oprávnění

< Zpět    **Další >**    Zrušit

Pokud zvolíte „**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

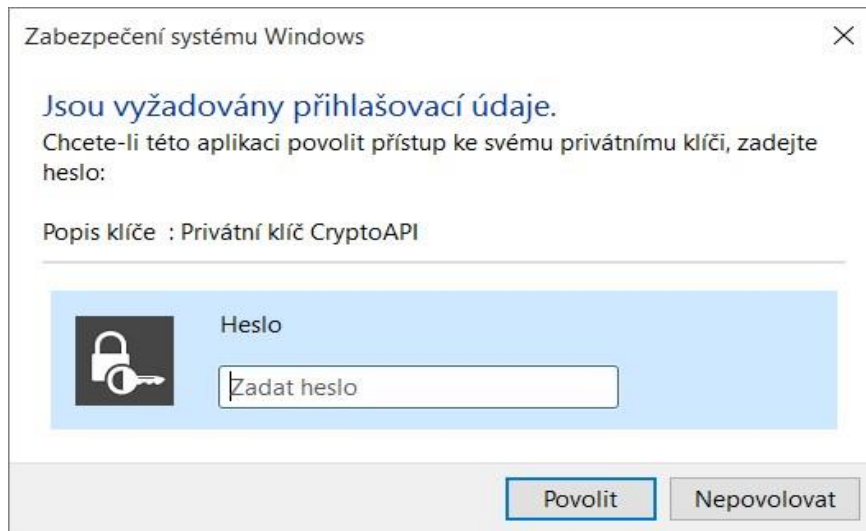
Heslo pro:    Privátní klíč CryptoAPI

Heslo:    ●●●●

Potvrdit:    ●●●●

< Zpět    **Dokončit**    Zrušit

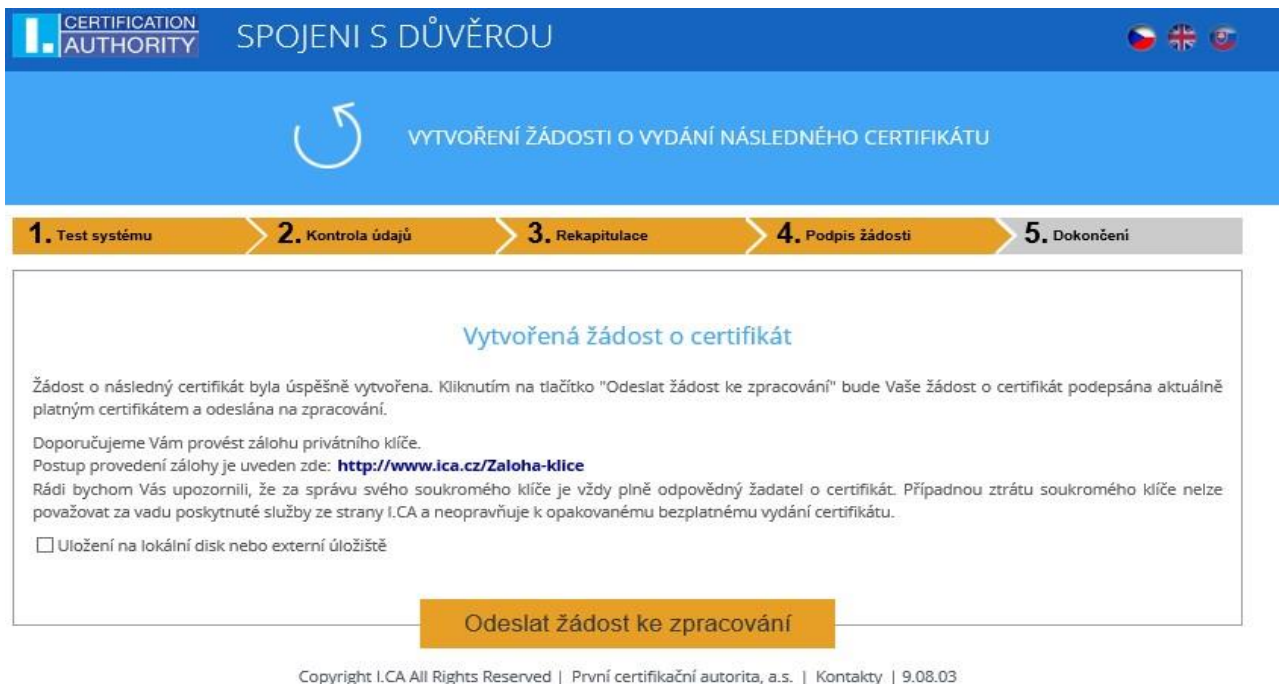
Po kliknutí na tlačítko „**Dokončit**“ dojde ke změně úrovně zabezpečení. Nyní klikněte na tlačítko „**OK**“. V dalším dialogovém okně udělte oprávnění tlačítkem „**Povolit**“. Pokud jste zvolili „**vysokou**“ úroveň zabezpečení, musíte zadat i heslo.



### 3.6. 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.



**CERTIFICATION AUTHORITY** SPOJENÍ S DŮVĚROU

VYTVORENÍ 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-klíce>

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

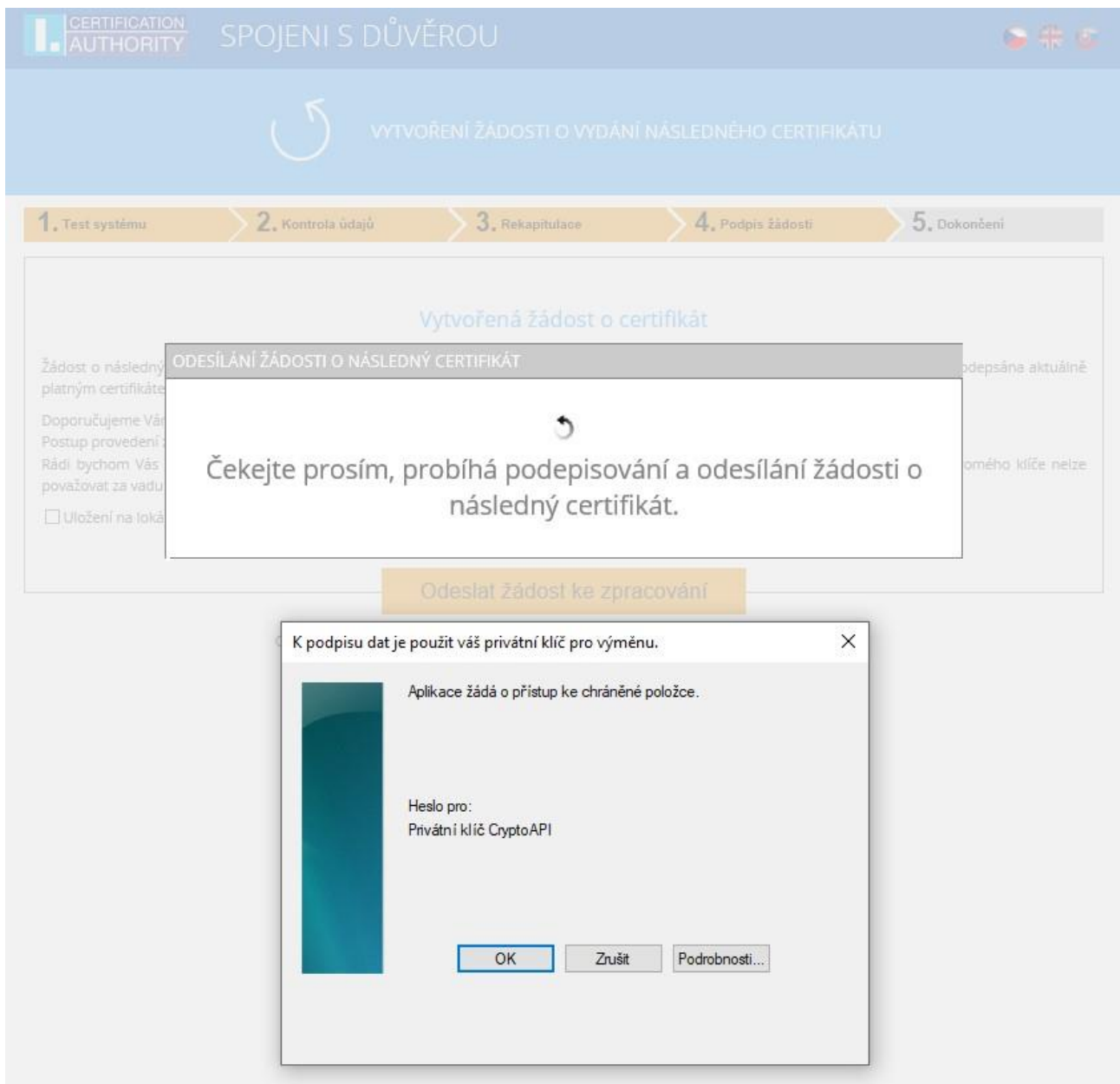
**Odeslat žádost ke zpracování**

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

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.



CERTIFICATION AUTHORITY SPOJENÍ S DŮVĚROU

VYTVORENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNĚHO 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

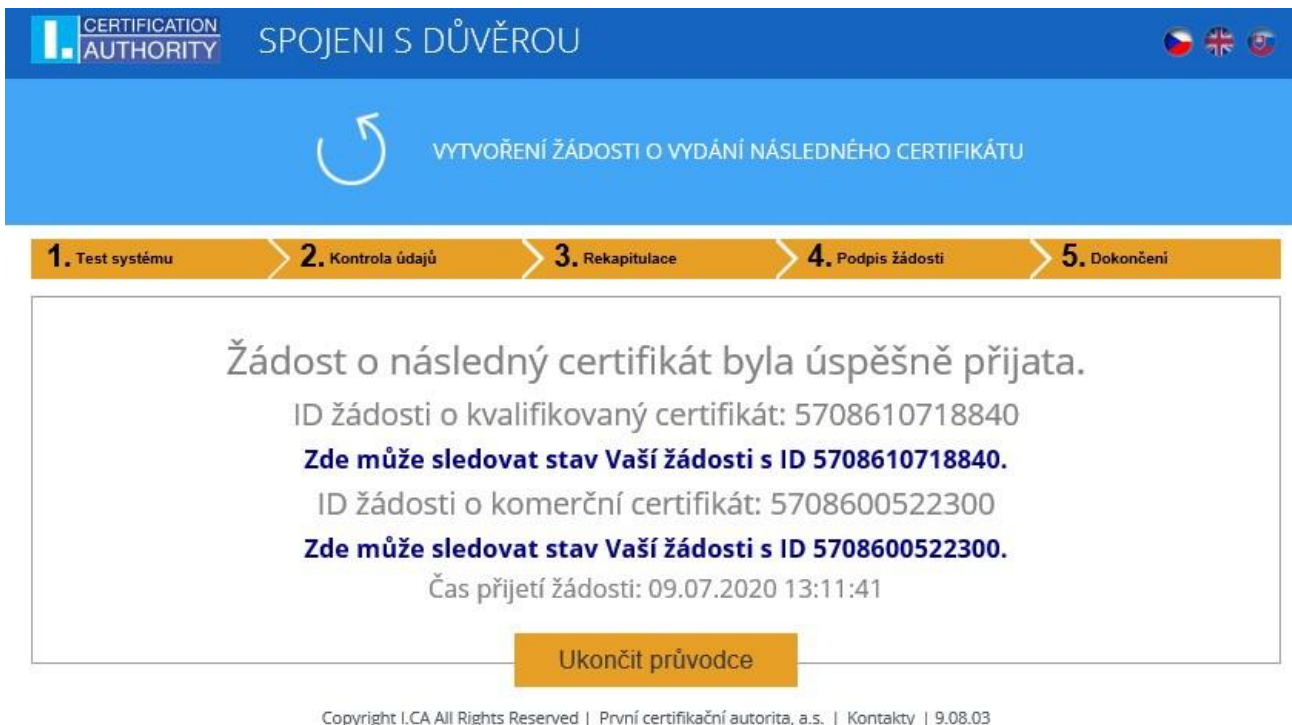
K podpisu dat je použit váš privátní klíč pro výměnu.

Aplikace žádá o přístup ke chráněné položce.

Heslo pro:  
Privátní klíč CryptoAPI

OK Zrušit Podrobnosti...

V případě úspěšného odeslání žádosti se Vám zobrazí následující stránka:



The screenshot shows a web page with a blue header containing the I.C.A. logo and the text "SPOJENÍ S DŮVĚROU". Below the header is a blue banner with a circular arrow icon and the text "VYTVOŘENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU". A progress bar below the banner shows five steps: 1. Test systému, 2. Kontrola údajů, 3. Rekapitulace, 4. Podpis žádosti, and 5. Dokončení. The main content area displays a confirmation message: "Žádost o následný certifikát byla úspěšně přijata." followed by two IDs and their corresponding tracking instructions, and the time of receipt. A yellow button labeled "Ukončit průvodce" is at the bottom.

CERTIFICATION AUTHORITY SPOJENÍ S DŮVĚROU

VYTVOŘENÍ 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.

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](#)