Generování žádosti o následný certifikát Uživatelská příručka

Obsah

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 10
- Windows 11
- MacOS

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 PKIServicehost**

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

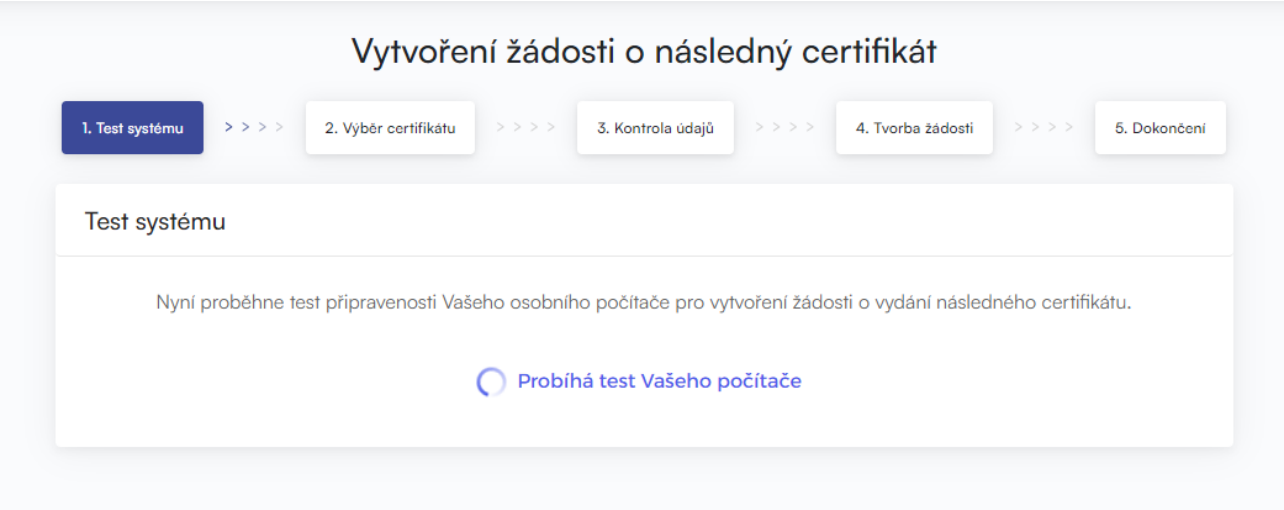
3. Proces generování žádosti o následný certifikát

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

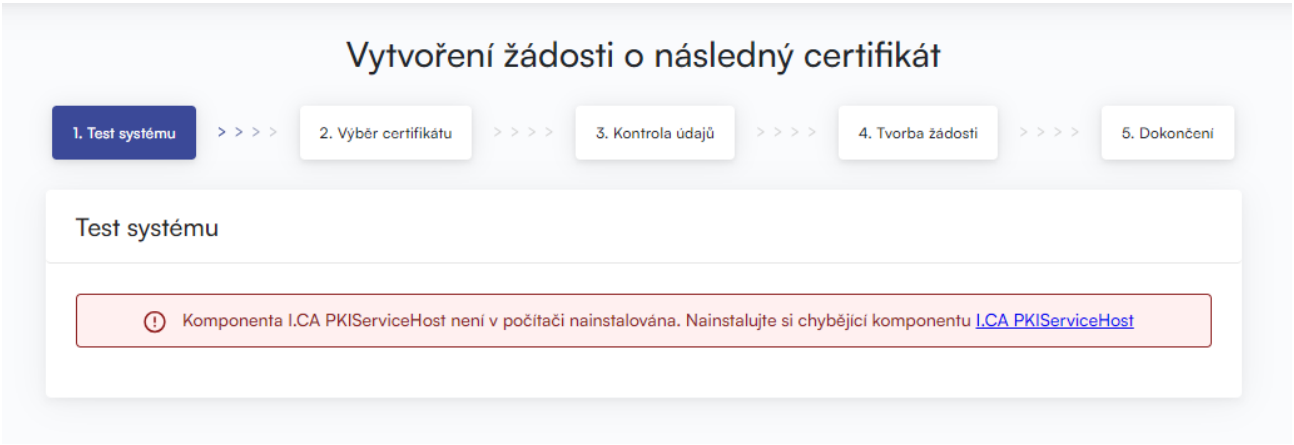
1. **Test systému**
2. **Výběr certifikátu**
3. **Kontrola údajů**
4. **Tvorba žádosti**
5. **Dokončení**

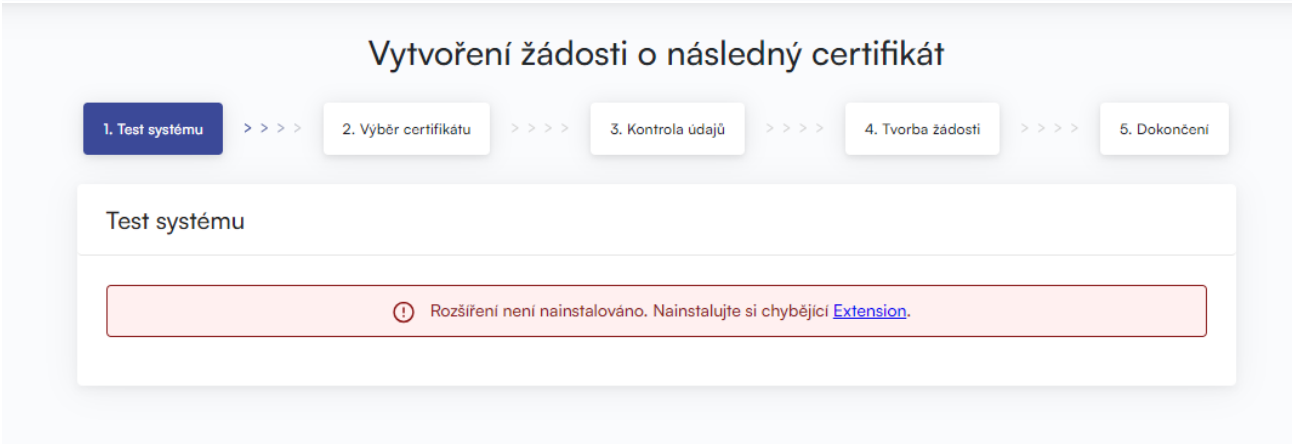
3.1. Kontrola softwarového vybavení

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 PKIServiceHost** se objeví chybová hláška viz. níže





Kliknutím na zvýrazněné **I.CA PKIServiceHost** a **Extension** stáhnete a poté nainstalujete do PC potřebné komponenty pro vygenerování žádosti. Po úspěšné instalaci restartujte prohlížeč.
Stránka otestuje počítač, pokud nejsou detekovány problémy, 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 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, 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**

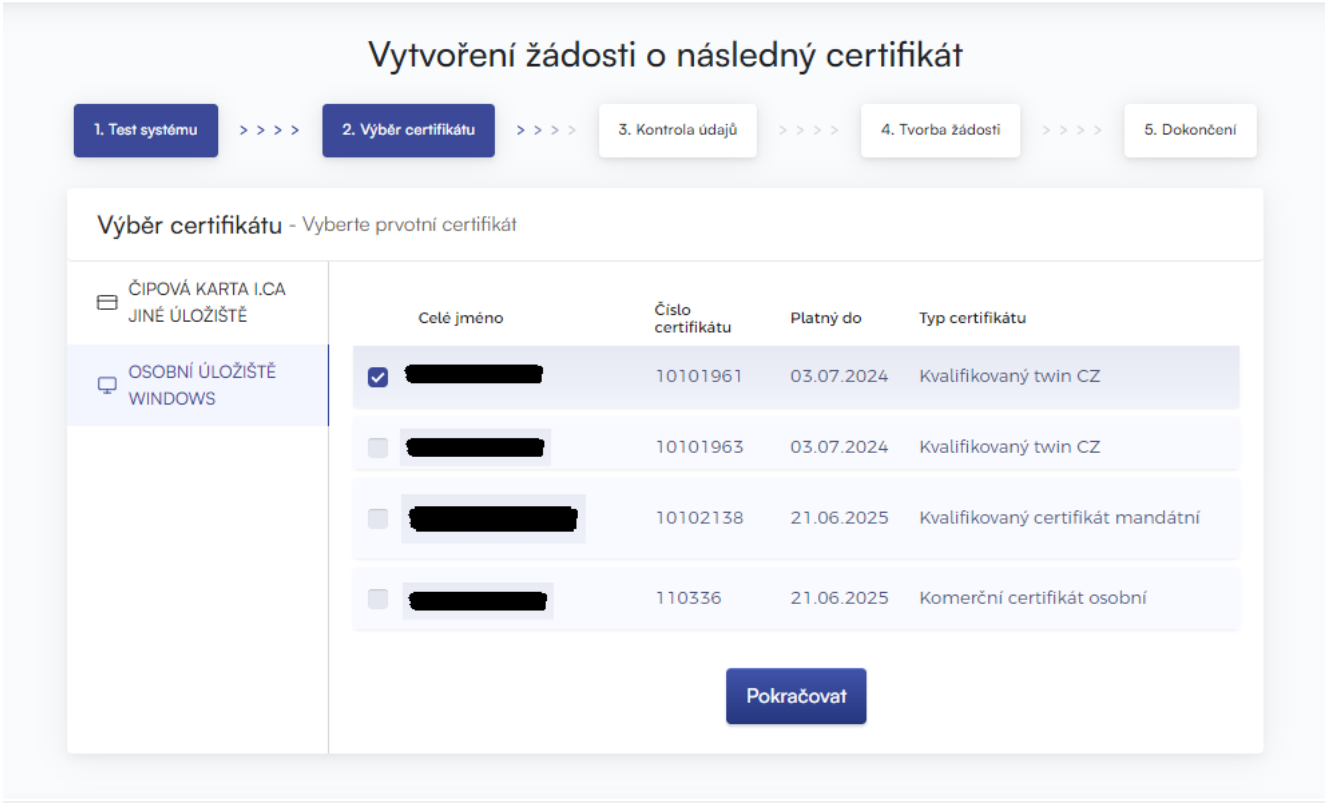
Dále je nutné mít nainstalované a povolené rozšíření v prohlížeči. Kliknutím na zvýrazněný název Extension Vás prohlížeč přesměruje do nastavení, kde rozšíření najdete a nainstalujete, po instalaci je nutno obnovit stránku.

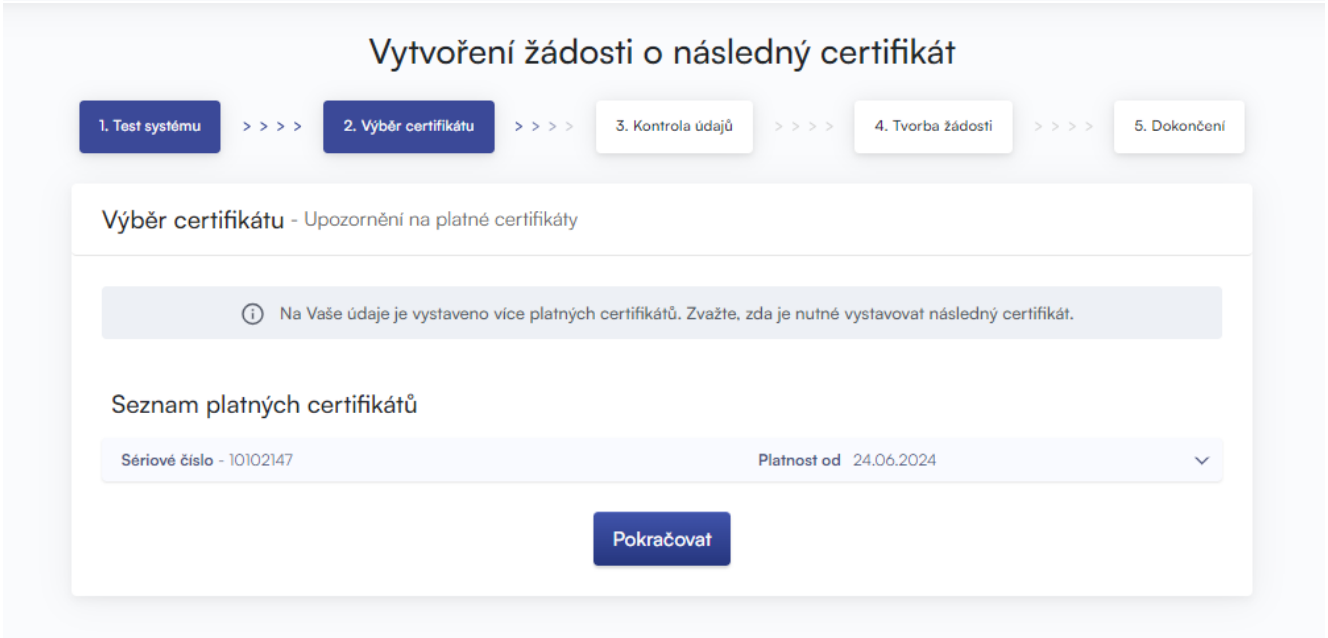
3.1.6. **Ukládání cookies**

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

3.2. Výběr certifikátu pro vytvoření žádosti o následný certifikát

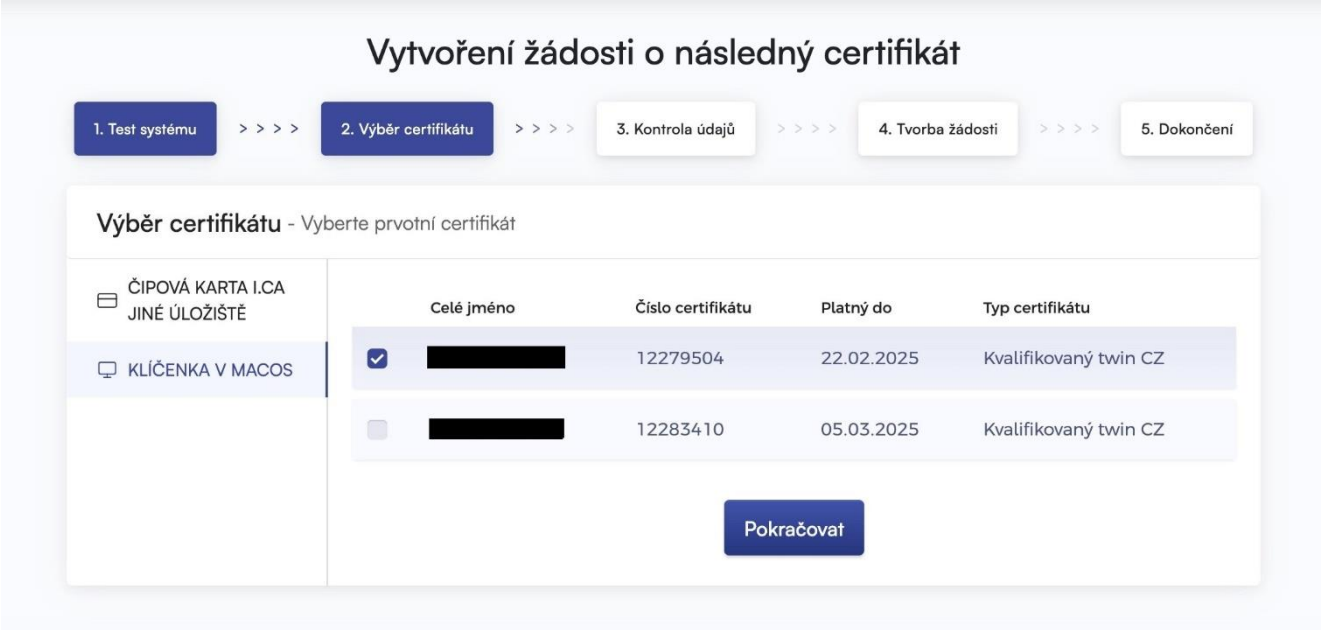
Pokud proces kontroly proběhl bez chyb, stránka zobrazí formulář, kde vyberete platný certifikát, ke kterému chcete vydat následný.





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

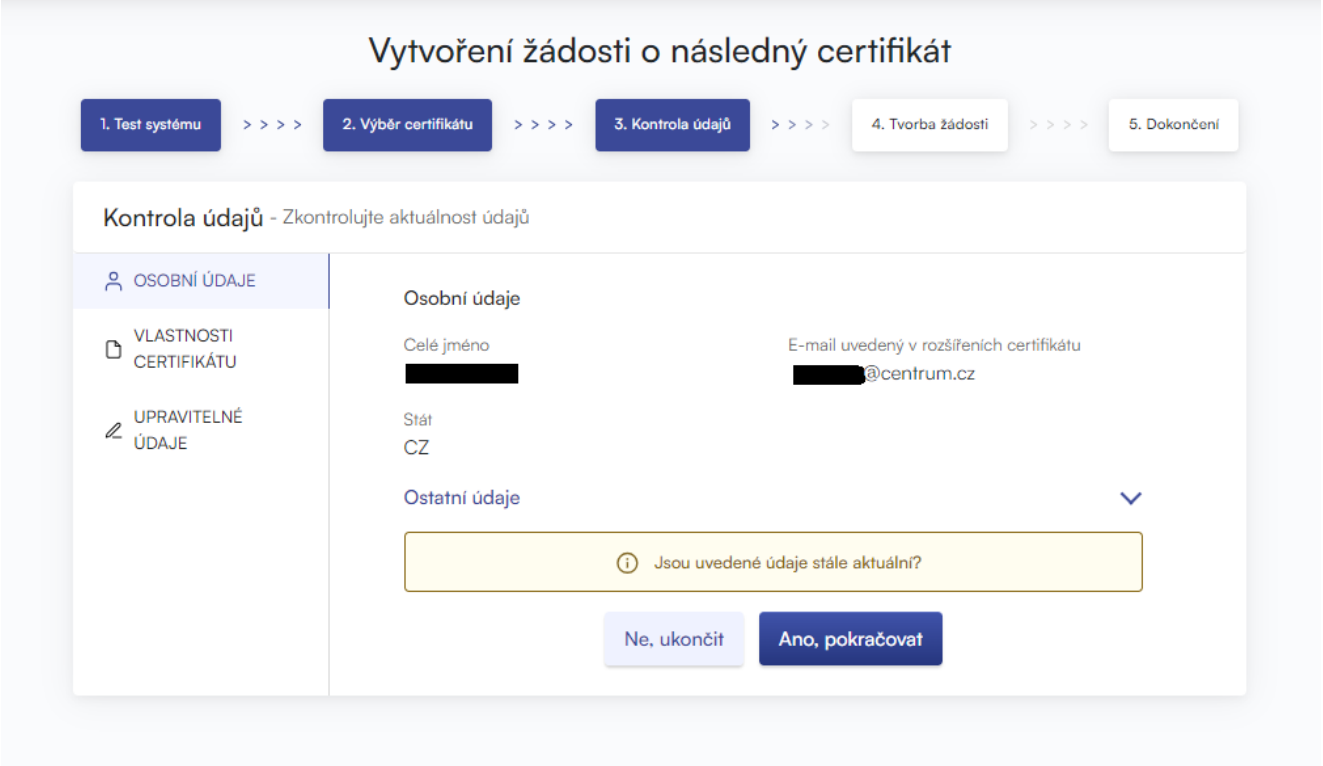
V případě certifikátu uloženého v uložišti MacOS**,** zvolte možnost **Klíčenka v MACOS**.



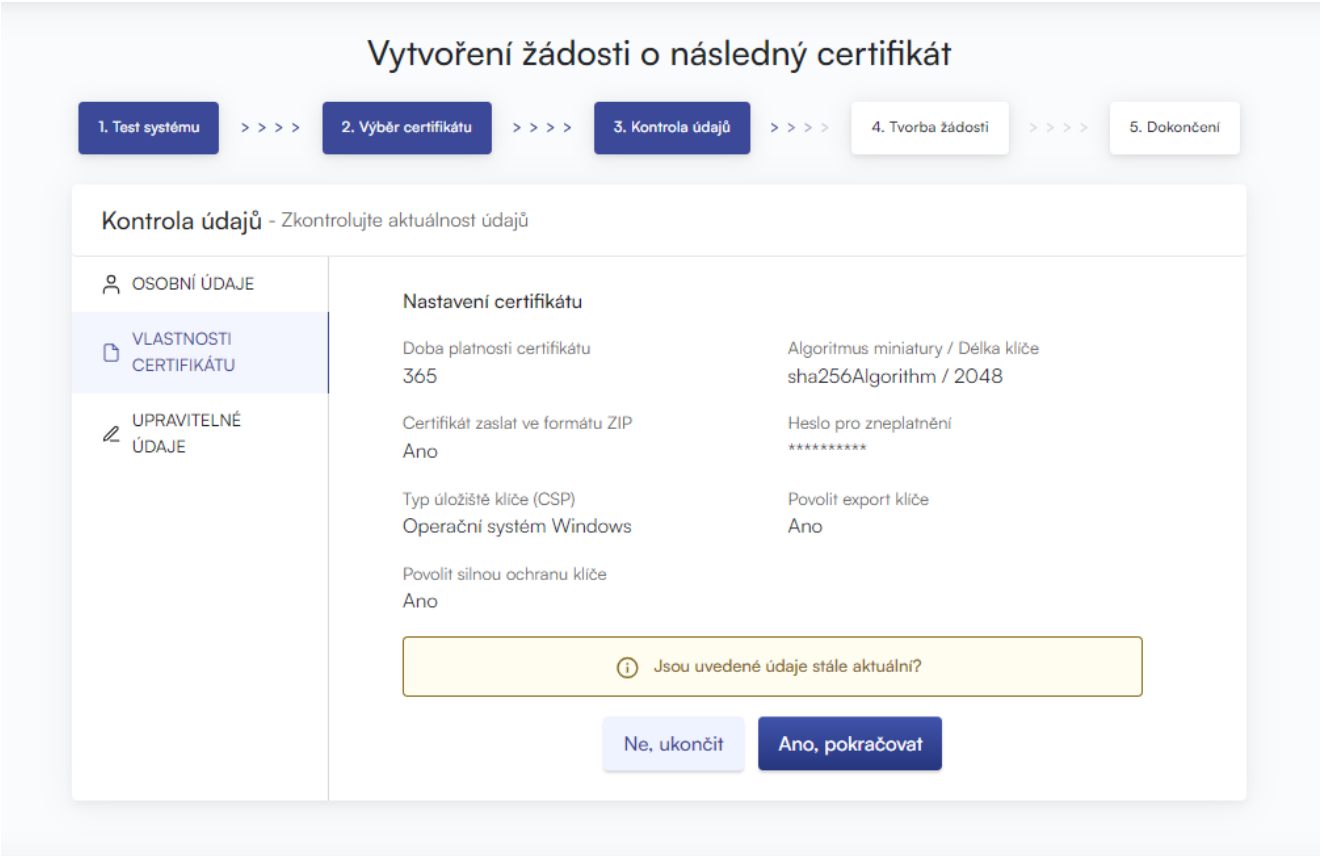
Podle Vaší předchozí volby je nabídnut seznam certifikátů, ke kterým lze vydat následný certifikát. Pokud jste zvolili možnost **Čipová karta I.CA**, musíte mít připojenou čtečku a vloženu čipovou kartu.
Vydat následný certifikát lze pouze u takových certifikátů, kterým ještě neskončila platnost, a které nejsou umístěny na CRL (seznam zneplatněných certifikátů)!

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. Kontrola údajů



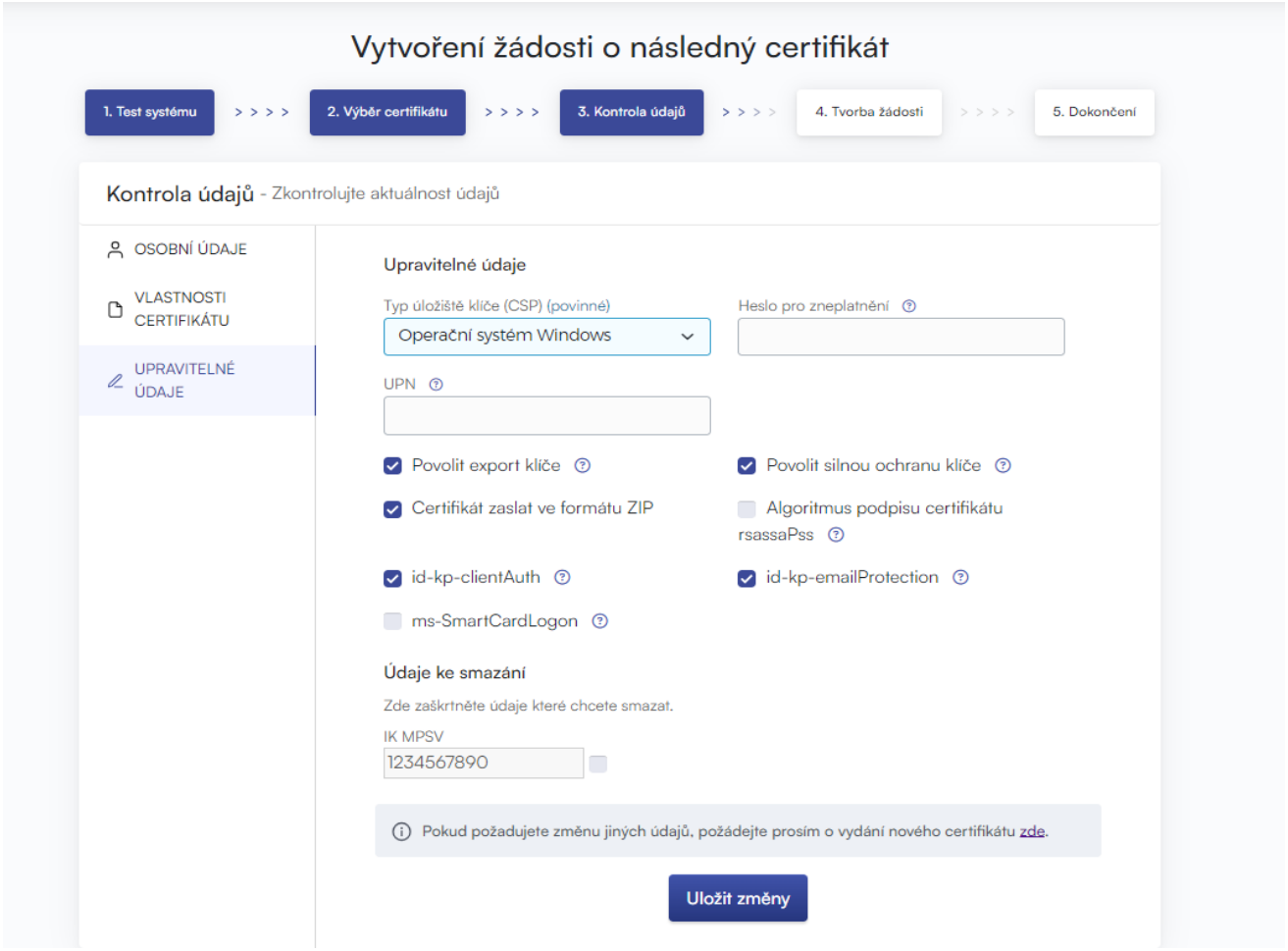
V případě, že jsou položky v certifikátu aktuální, pokračujte kliknutím na tlačítko **„ANO, pokračovat“** a zahájíte generování žádosti o certifikát. Podrobnější údaje si zobrazíte rozšířením možnosti **„Ostatní údaje“**.



V části **„VLASTNOSTI CERTIFIKÁTU“** je zobrazeno nastavení stávajícího certifikátu jako je například sériové číslo certifikátu nebo typ uložiště.
Pokud se některá položka v certifikátu změnila, pokračujte kliknutím na **„Upravitelné údaje“** a pokračujte v příručce na bod 3.4 Doplnění a změna některých údajů.

3.4. Doplnění a změna některých údajů

V části **„UPRAVITELNÉ ÚDAJE“** můžete ovlivnit některé údaje, které bude obsahovat Váš následný certifikát.



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 tato rozšíření před pokračováním odebrat.

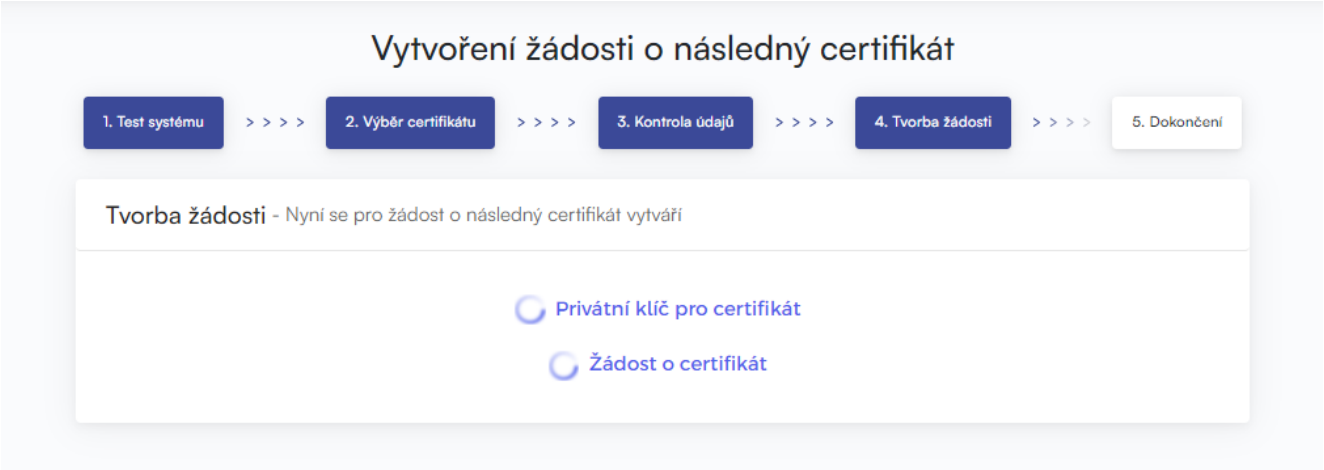
3.5. Generování žádosti o certifikát

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

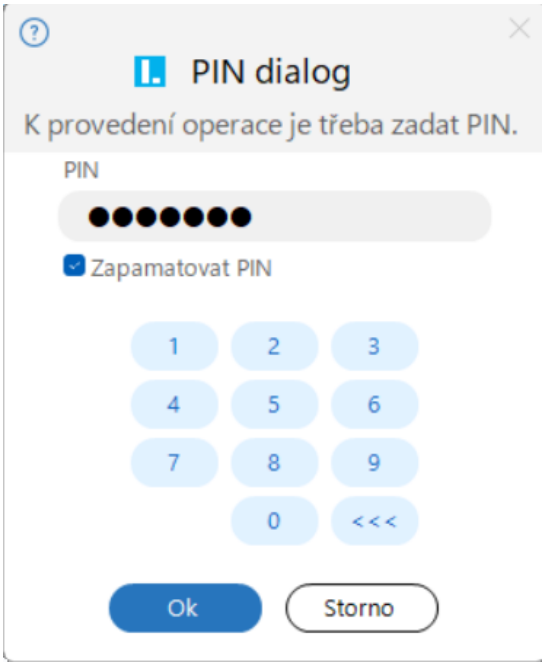
3.5.1. Čipová karta I.CA - Microsoft Smart Card Key Storage\ I.CA SecureStore PKCS11# Library

Pokud při vyplňování údajů o žadateli zvolíte jako typ úložiště klíče Microsoft Smart Card Key Storage, 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.



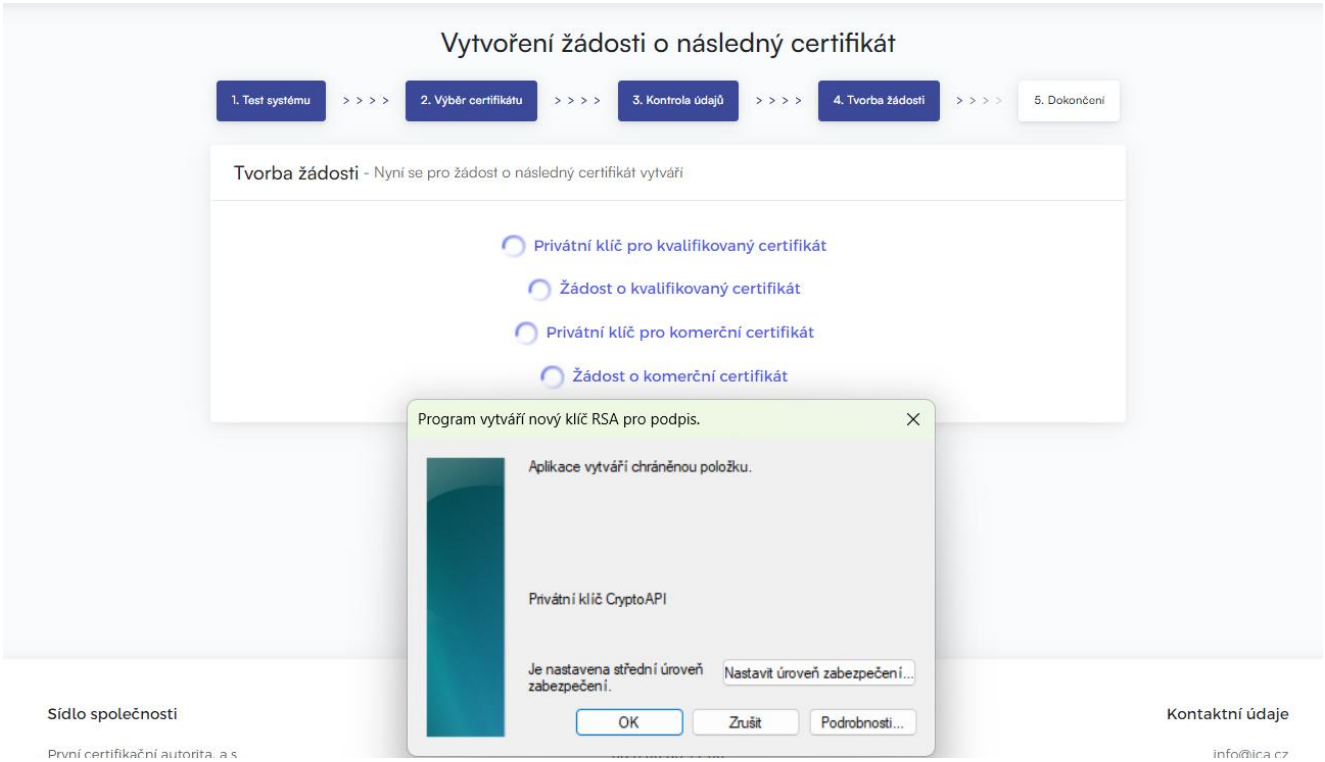
Poté co je privátní klíč vytvořen, jste vyzváni k zadání PINu k vaší kartě.



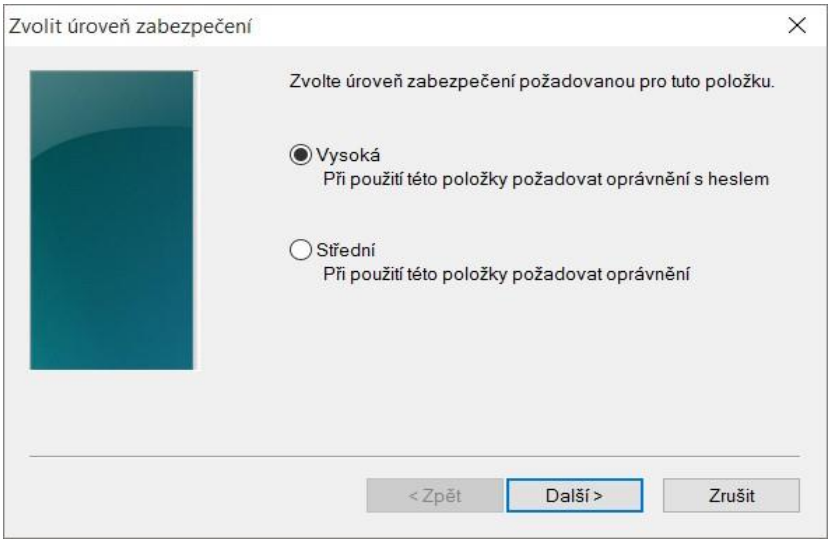
U čipové karty I.CA je možné použít i typ uložiště Microsoft Base Smart Card Crypto Provider. V případě tvoření žádosti na MacOS je zvolené uložiště I.CA SecureStore PKCS11# Library.

3.5.2. Microsoft Enhanced RSA and AES Cryptographic Provider (operační systém Windows) se silnou ochranou soukromého klíče

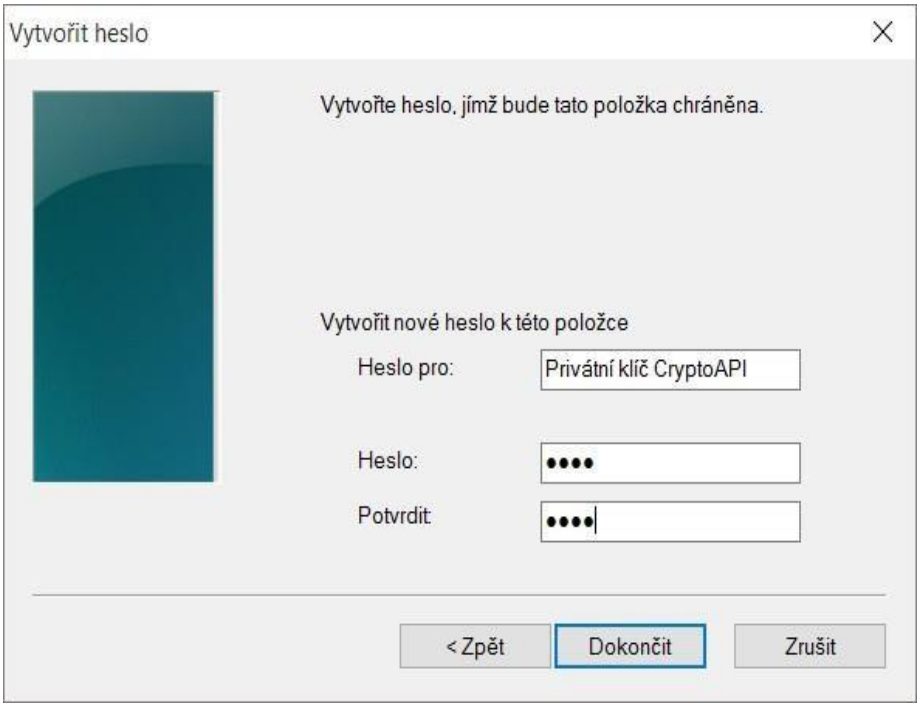
Pokud při vyplňování údajů o žadateli zvolíte jako typ úložiště klíče Microsoft Enhanced RSA and AES Cryptographic Provider (případně Microsoft Enhanced RSA and AES Cryptographic Provider /prototype/) a zatrhnete volbu Povolit silnou ochranu klíče, je postup generování žádosti následující:



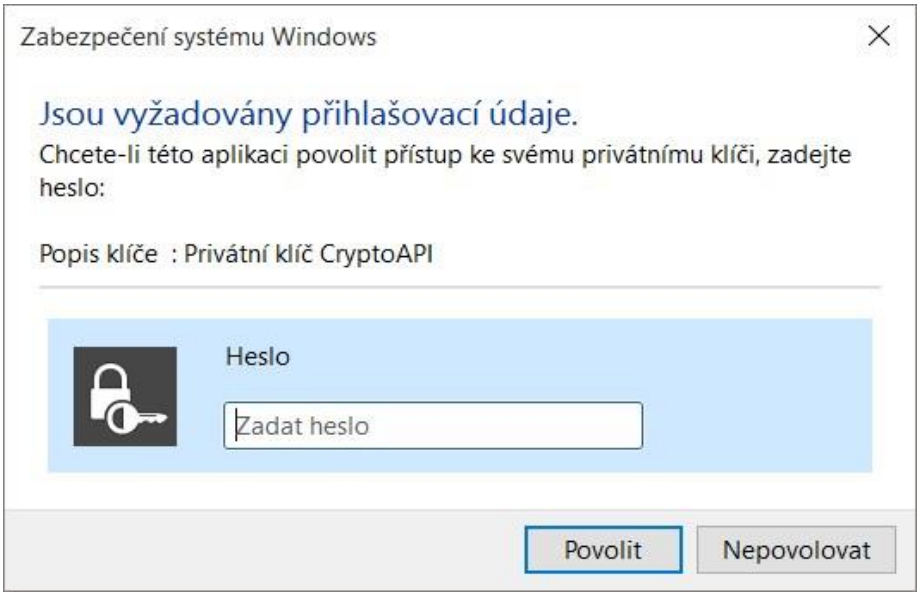
Pokud kliknete na **Nastavit úroveň zabezpečení**, budete moci změnit úroveň zabezpečení.



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

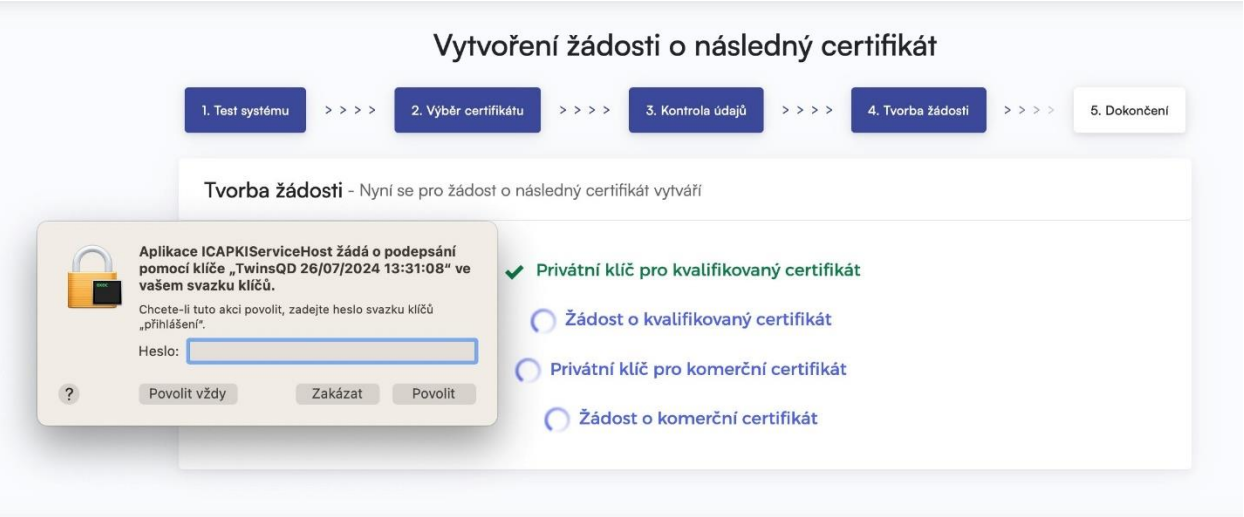


Po kliknutí na tlačítko **Dokončit** dojde ke změně úrovně zabezpečení. Nyní klikněte na tlačítko **OK**. V dalším dialogovém okně udělte oprávnění tlačítkem **Povolit**. Pokud jste zvolili **vysokou** úroveň zabezpečení, musíte zadat i heslo.



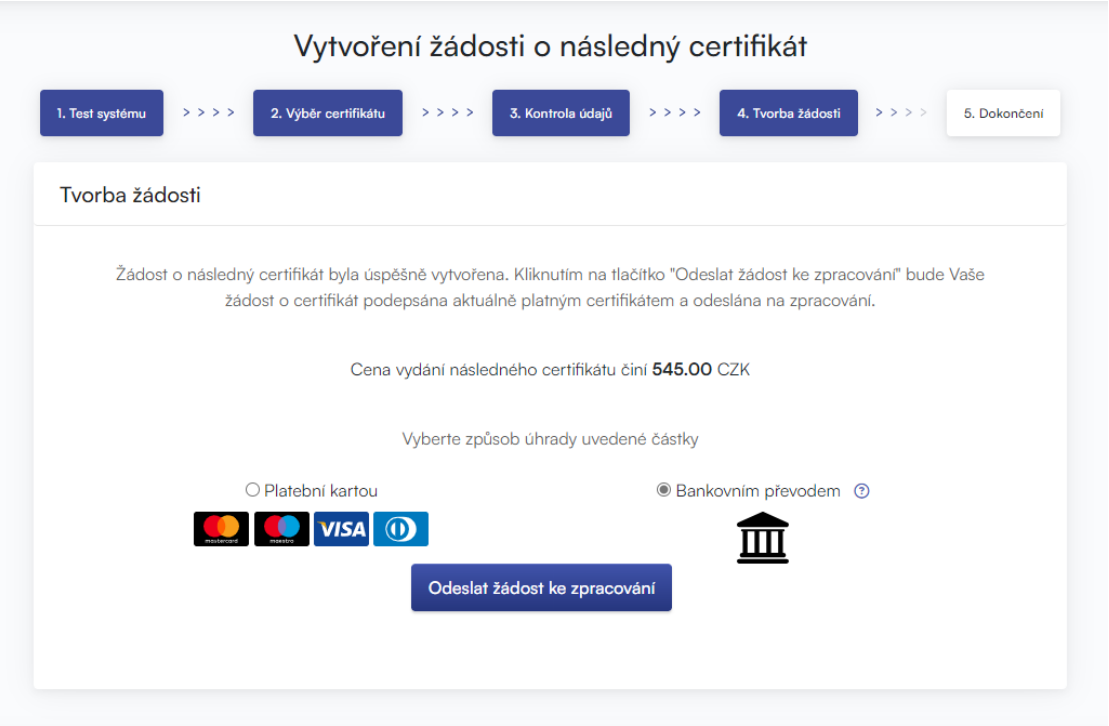
3.5.3. MacOS File-Based Keychain

Pokud tvoříme žádost na MacOS o certifikát, který je uložený v počítači, bude zvolený typ uložiště MacOS File-Based Keychain. Při generování klíče do klíčenky bude požadováno zadat heslo ke klíčence. Pokud nebude žádoucí, aby bylo heslo vyžadováno při každém použití certifikátu, je možné zvolit možnost povolit vždy.



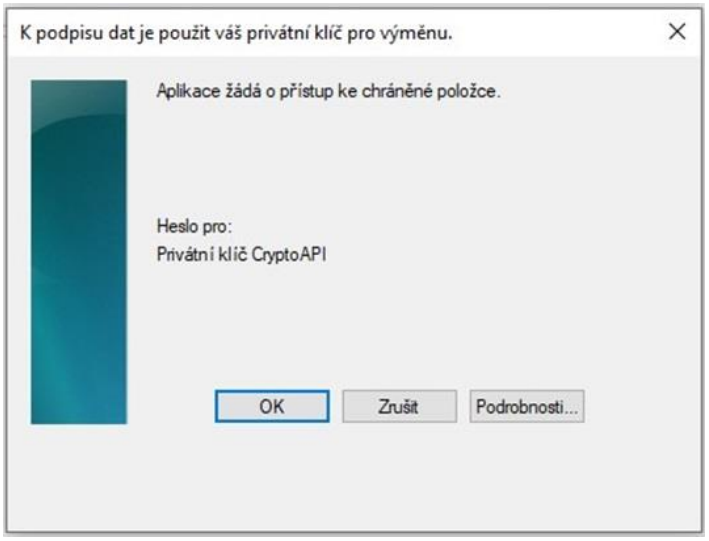
3.6. Podpis a odeslání žádosti o následný certifikát

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.

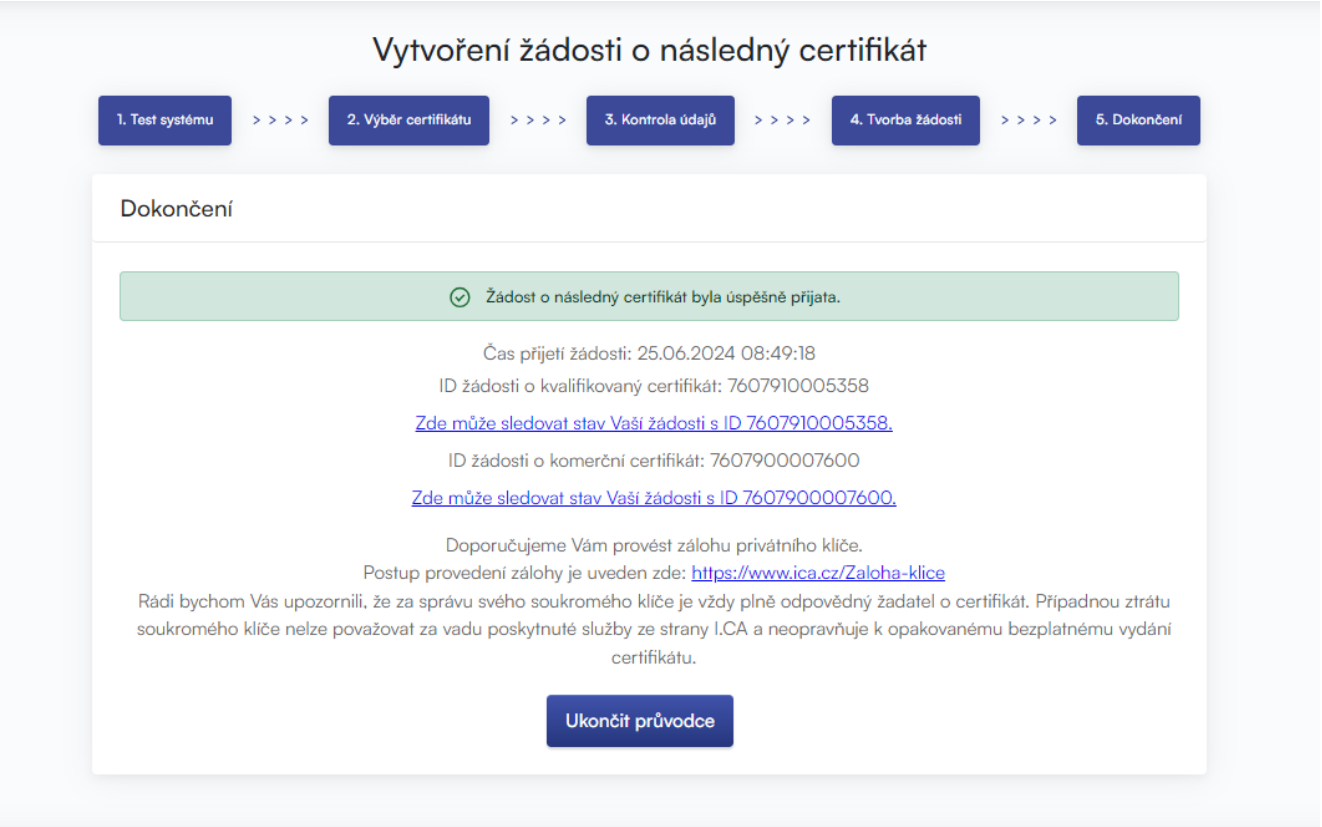


Žádost je potřeba podepsat kliknutím na tlačítko **„OK“**.
Pokud je žádost generována na čipovou kartu, je zapotřebí podepsat zadáním **PIN kódu** k čipové kartě.

V případě, že žádáte o následný certifikát TWINS, je nutné podepsat jak žádost o následný kvalifikovaný, tak i žádost o komerční certifikát.



Po úspěšném odeslání žádosti se Vám zobrazí následující stránka:



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.