

Generovanie žiadosti o následný certifikát Užívateľská príručka pre Mozilla Firefox

První certifikační autorita, a.s.

Verzia 8.16

1. Úvod

Tento dokument slúži ako návod, ako postupovať pri generovaní žiadosti o následný certifikát cez webové stránky.

2. Požiadavky na software

Počítač, na ktorom sa bude vykonávať generovanie žiadosti o certifikát, musí spĺňať nasledujúce požiadavky:

- nainštalovaný a spustený operačný systém
 - **Windows 7 ServicePack 1**
 - **Windows 8.1 (April 2014 update)**
 - **Windows 10**
- nainštalovaná a použitá **Mozilla Firefox** verzia 52 a vyššia
- v internetovom prehliadači zapnutá podpora skriptovania Javascript, zapnutá podpora jazyka Java, podpora ukladania cookies.
- nainštalovaný komponent a rozšírenie **I.CA PKIService host**
- **I.CA SecureStore Card Manager** (iba v prípade generovania žiadosti na čipovú kartu)

3. Proces generovania žiadosti o následný certifikát

Postup generovania žiadosti o následný certifikát je rozdelený do niekoľko

krokov: Test systému

Kontrola údajov

Rekapitulácia


Podpis žiadosti




Dokončenie


3.1. Kontrola softwarového vybavenia

Pre uľahčenie kontroly pripravenosti Vášho počítača na generovanie žiadosti, je pri začatí generovania žiadosti zobrazená kontrolná stránka, ktorá overí prítomnosť kľúčových softwarových komponentov.

Kliknutím na tlačidlo **Začať test** spustíte test Vášho počítača.


SPOJENÍ S DŮVĚROU


VYTVORENÍ 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 prípade neprítomnosti komponentu a rozšírenia **I.CA PKIService Host** sa objaví chybová hláška, vid' nižšie


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	Opera verze 70, tento webový prohlížeč je podporován.
✓	Podpora jazyka JavaScript	JavaScript povolen.
✗	Podpora rozšíření	Rozšíření nejsou nainstalovaná. Nainstalujte si chybějící komponenty I.CA PKIServiceHost a Extension
	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 zvýraznené **I.CA PKIServiceHost** a **Extension** nainštalujete do PC potrebné komponenty pre vygenerovanie žiadosti. Po úspešnej inštalácii reštartujte prehliadač a kliknite na tlačidlo **Začať test**



VYTVORENÍ 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	Opera verze 70, 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 a pokiaľ nie sú detekované problémy, kliknutím na tlačidlo **Pokračovať** prejdete k samotnej tvorbe žiadosti o následný certifikát.

Pokiaľ sa pri kontrole vyskytne chyba, nedá sa pokračovať v tvorbe žiadosti o následný certifikát. Najskôr je potrebné odstrániť chybu, ktorá znemožňuje tvorbu žiadosti o certifikát. Význam chybových hlásení je uvedený v nasledujúcich kapitolách.

3.1.1. Nepodporovaný operačný systém

Pre generovanie žiadosti musíte použiť jeden z operačných systémov uvedených v kapitole 2.

3.1.2. Nepodporovaný internetový prehliadač

Pre generovanie žiadosti musíte použiť jednu z verzií prehliadača uvedených v kapitole 2.

3.1.3. Podpora JavaScriptu

Stránky pre generovanie žiadosti o certifikát vyžadujú podporu skriptovania v jazyku JavaScript. Pokiaľ by táto kontrola zlyhala, znamená to s najväčšou pravdepodobnosťou, že je v nastavení prehliadača podpora skriptovania vypnutá. Povoľte podporu skriptovania v jazyku JavaScript vo Vašom prehliadači.

3.1.4. I.CA PKIService Host

Stránky vyžadujú pre svoju funkčnosť nainštalovaný komponent I.CA PKIService Host. Uistite sa, že ho máte nainštalovaný. Pokiaľ nemáte na svojom počítači komponent nainštalovaný, k stiahnutiu použite zvýraznený názov I.CA PKIService Host, po inštalácii je nutné reštartovať prehliadač.

3.1.5. Rozšírenie (doplnok) I.CA PKIService Host


Ďalej je nutné mať nainštalované a povolené rozšírenie v prehliadači. Kliknutím na zvýraznený názov Extension Vás prehliadač presmeruje do nastavení, kde rozšírenie nájdete a nainštalujete, po inštalácii je nutné obnoviť stránku.




3.1.6. Ukladanie cookies


Pre správnu prácu stránok pre generovanie žiadosti je nutné, aby Váš prehliadač umožnil stránke ukladať cookies. Pokiaľ máte zakázané ukladanie cookies, povoľte ho.

3.2. Výber certifikátu pre vytvorenie žiadosti o následný certifikát

Pokiaľ proces kontroly prebehol bez chýb, stránka zobrazí formulár, kde vyberiete platný certifikát, ku ktorému chcete vydať následný.


SPOJENÍ S DŮVĚROU


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.

XXXXXXXXXX 2020-08-21][00B0598A](I.CA Qualified 2 CA/RSA 02/2016) ▼

Pokračovat

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

Pokiaľ je Váš certifikát uložený v úložisku systému Windows, nechajte zvolené **Osobné úložisko certifikátov Windows**. Pokiaľ sa nachádza Váš certifikát na čipovej karte I.CA, zvolte možnosť **Iné úložisko (napr. I.CA čipová karta)**.

Podľa Vašej predchádzajúcej voľby je ponúknutý zoznam certifikátov, ku ktorým je možné vydať následný certifikát. Pokiaľ ste zvolili možnosť **Iné úložisko**, musíte mať pripojenú čítačku a vloženú čipovú kartu.

Vydať následný certifikát je možné iba pri takých certifikátoch, ktorým ešte neskončila platnosť, a ktoré nie sú umiestnené na CRL!

Pokiaľ dostanete e-mail s upozornením na koniec platnosti Vášho certifikátu, je v tomto e-maili uvedené URL, na ktorom môžete vytvoriť žiadosť o následný certifikát. Súčasťou URL je i sériové číslo certifikátu.

Pokiaľ zadáte toto URL do Vášho prehliadača, certifikát je vybraný automaticky.

3.3. Doplnenie a zmena niektorých údajov

V tomto kroku môžete ovplyvniť niektoré údaje, ktoré bude obsahovať 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 rozšířeních certifikátu	[redacted]	
SN ICA	[redacted]	
IK MPSV	[redacted]	
SN ICA	[redacted]	

Heslo pro zneplatnění ?

Typ úložiště klíče (CSP) ▼

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

id-kp-clientAuth ? id-kp-emailProtection ? ms-SmardCardLogon ?

Úprava e-mailu Smazat Změnit

Přidání UPN (Microsoft Universal Principal Name)

TWIN kvalifikovaný

IK MPSV ? Smazat Změnit

Pokračovat

V časti Certifikát sú zobrazené niektoré údaje zo súčasného certifikátu. Zobrazené je jeho sériové číslo, platnosť a jednotlivé položky predmetu.

Po kliknutí na Povolené úpravy následného certifikátu v hornej časti, sa zobrazia

nasledujúce možnosti:

Heslo pre zneplatnenie:

Pokiaľ dôjde počas používania certifikátu ku kompromitácii privátneho kľúča, zmene údajov (zmena mena, bydliska...) alebo sa vyskytnú ďalšie dôvody, prečo by nemal byť certifikát ďalej používaný, je nutné certifikát zneplatniť.

Certifikát je možné zneplatniť cez webové rozhranie. Pri zneplatnení certifikátu budete vyzvaný k zadaniu hesla pre zneplatnenie.

Pokiaľ nezadáte heslo, bude ako heslo pre zneplatnenie certifikátu použité heslo nastavené pri súčasnom certifikáte.

Pokiaľ sa rozhodnete zadať iné heslo, musí byť jeho dĺžka 4 až 32 znakov. Povolené sú iba veľké a malé písmená bez diakritiky a číslice.

Typ úložiska kľúča (CSP):

Pri položke **Typ úložiska kľúča (CSP)** zvolte z ponuky modul zaisťujúci kryptografické služby (CSP), ktorý vygeneruje Váš privátny kľúč. Všetky tu zobrazené CSP sú nainštalované vo Vašom počítači.

Export privátneho kľúča:

Pokiaľ Vami zvolený typ úložiska kľúča (CSP) podporuje export privátneho kľúča, je Vám ponúknutá voľba povoliť export privátneho kľúča. Táto voľba umožní vykonať export certifikátu vrátane súkromného kľúča. Súkromný kľúč tak budete môcť prenášať medzi úložiskami. Správa kľúča vyžaduje v takom prípade zvýšenú opatrnosť z dôvodu vyššieho rizika jeho krádeže/zneužitia.

Silná ochrana privátneho kľúča:

Pokiaľ Vami zvolený typ úložiska kľúča (CSP) podporuje silnú ochranu privátneho kľúča, je Vám ponúknutá voľba povoliť silnú ochranu privátneho kľúča. Pred každým použitím Vášho kľúča budete upozornený, že je Váš kľúč používaný.

Následne máte možnosť si vybrať medzi:

Stredná - vždy budete iba upozornený informatívnym hlásením

Silná - pred každým použitím bude po Vás vyžadované zadanie hesla

Úprava e-mailu:

Pokiaľ je v súčasnom certifikáte uvedený e-mail, tu máte možnosť ho z následného certifikátu odobrať. Zmena vo väčšine prípadov nie je možná, v tomto prípade prosím požiadajte o nový certifikát s opravenými údajmi.

Nepovolený obsah certifikátu

V niektorých výnimočných prípadoch môže Váš certifikát obsahovať rozšírené použitie kľúča a alternatívne mená predmetu, ktoré už nesmú byť podľa certifikačnej politiky prítomné v certifikáte.

V takom prípade je zobrazené upozornenie a je nutné tieto rozšírenia pred pokračovaním odobrať.

Po stlačení tlačidla **Pokračovať** sa zobrazí rekapitulácia údajov a nastavení následného certifikátu.



VYTVOŘENÍ ŽÁDOSTI 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?

ANO, údaje jsou aktuální

NE, údaje se změnily

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

V případě, že sú položky v certifikáte aktuálne, pokračujeme kliknutím na tlačidlo „ANO, údaje sú aktuálne“ a začneme proces vytvorenia privátneho kľúča.

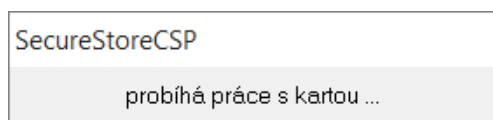
3.4. Generovanie žiadosti o certifikát

Nasledujúci postup sa pre jednotlivé typy úložiska kľúča (CSP) mierne líši:

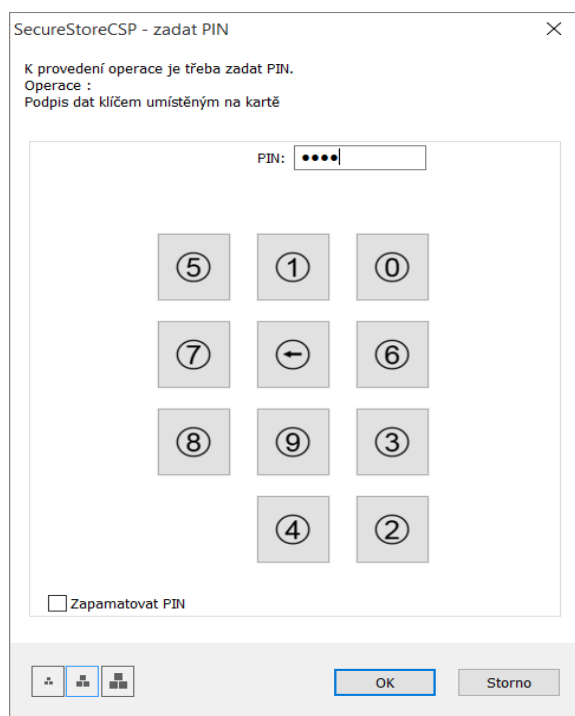
3.4.1. SecureStoreCSP – čipová karta I.CA

Pokiaľ pri vyplňovaní údajov o žiadateľovi zvolíte ako typ úložiska kľúča SecureStoreCSP, je postup generovania žiadosti nasledujúci:

Najskôr sa Vám zobrazí nasledujúci dialóg. V tomto okamihu sa generuje Váš privátny kľúč. Tvorba privátneho kľúča môže trvať niekoľko desiatok sekúnd.

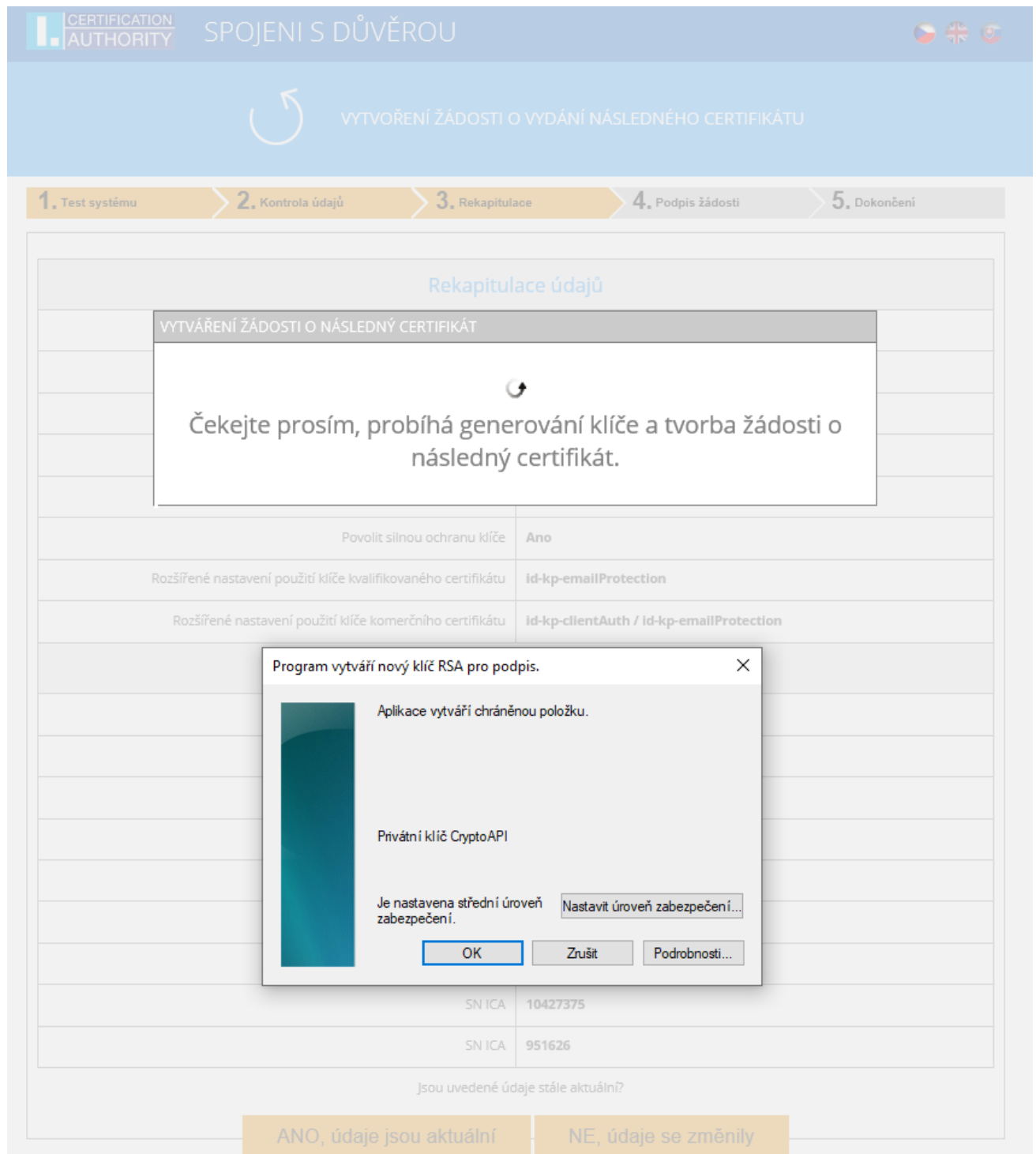


Potom čo je privátny kľúč vytvorený, ste vyzvaný k zadaniu PINu na Vašej karte.



3.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider so silnou ochranou súkromného kľúča

Pokiaľ pri vyplňovaní údajov o žiadateľovi zvolíte ako typ úložiska kľúča Microsoft Enhanced RSA and AES Cryptographic Provider (prípadne Microsoft Enhanced RSA and AES Cryptographic Provider /prototype/) a zatrhnete voľbu Povolit silnú ochranu kľúča, je postup generovania žiadosti nasledujúci:



The screenshot shows a web interface for creating a certificate request. The main window is titled "VYTVÁŘENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU" and is in the "3. Rekapitulace" (Summary) step. A central message box says "Čekejte prosím, probíhá generování klíče a tvorba žádosti o následný certifikát." (Please wait, key generation and request creation is in progress).

Below the message box, there is a table of settings:

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

A dialog box titled "Program vytváří nový klíč RSA pro podpis." (Program is creating a new RSA key for signing) is overlaid on the screen. It contains the following text:

Aplikace vytváří chráněnou položku.

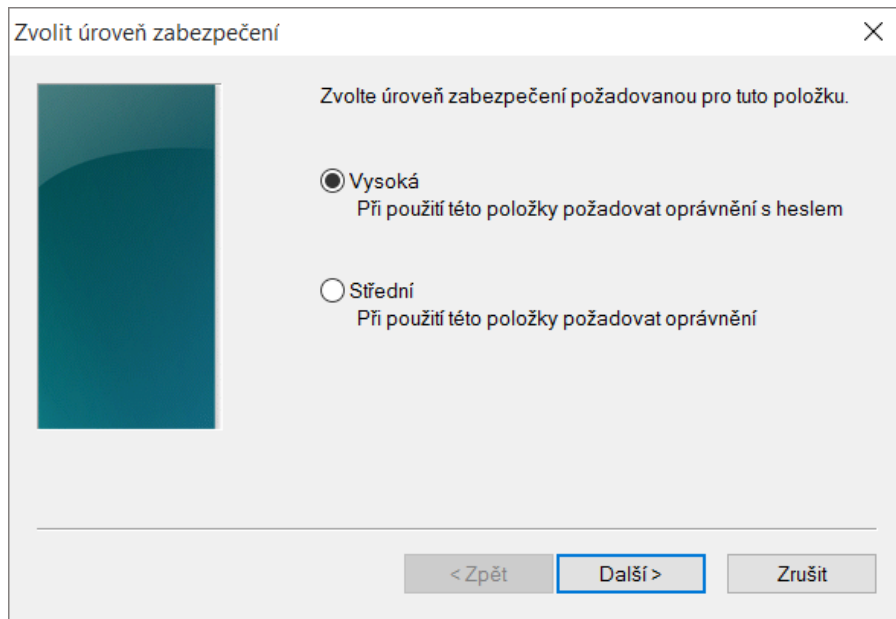
Privátní klíč CryptoAPI

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

Buttons: OK, Zrušit, Podrobnosti...

At the bottom of the main window, there is a question "Jsou uvedené údaje stále aktuální?" (Are the entered data still current?) with two buttons: "ANO, údaje jsou aktuální" and "NE, údaje se změnilly".

Pokiaľ kliknete na **Nastaviť úroveň zabezpečenia**, budete môcť zmeniť úroveň zabezpečenia.



Zvolit úroveň zabezpečení

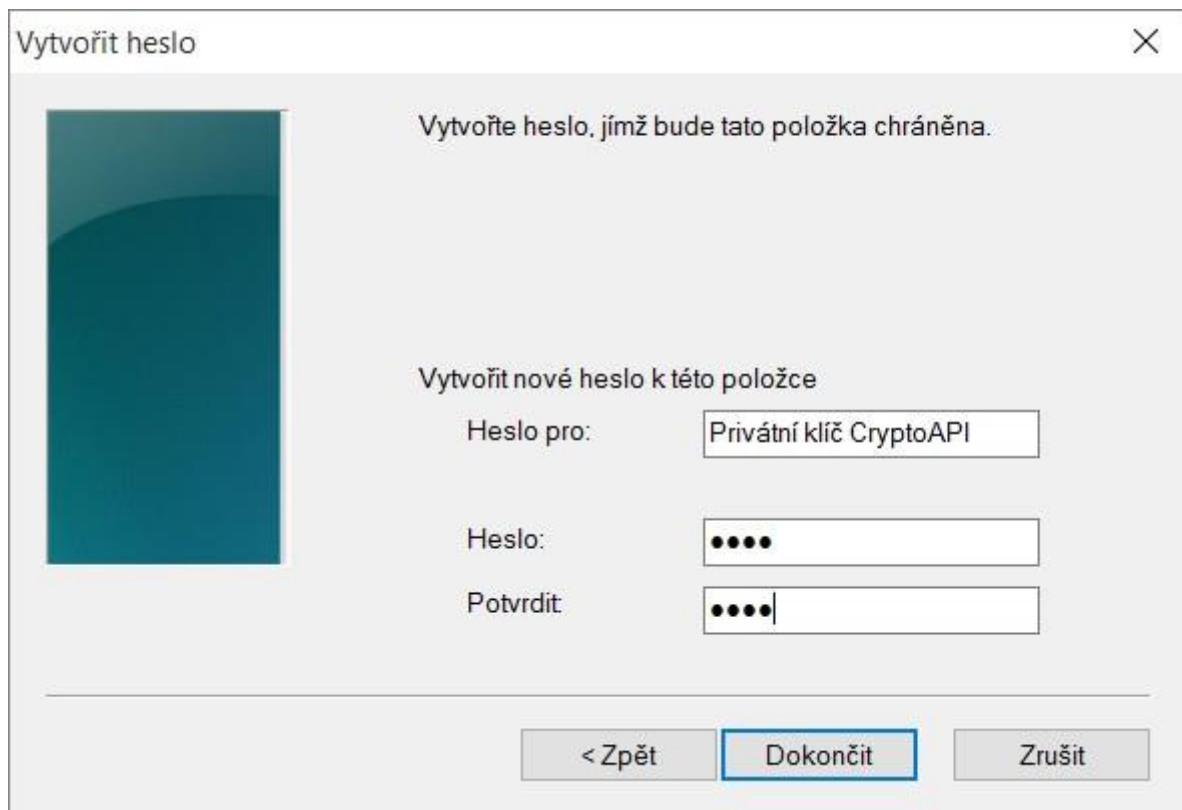
Zvolte úroveň zabezpečení požadovanou pro tuto položku.

Vysoká
Při použití této položky požadovat oprávnění s heslem

Střední
Při použití této položky požadovat oprávnění

< Zpět **Další >** Zrušit

Pokiaľ zvolíte **vyšokú** úroveň zabezpečenia, budete vyzvaný k zadaniu hesla. (Toto heslo bude potrebné zadať vždy, keď budete používať Váš vydaný certifikát).



Vytvořit heslo

Vytvořte heslo, jímž bude tato položka chráněna.

Vytvořit nové heslo k této položce

Heslo pro:

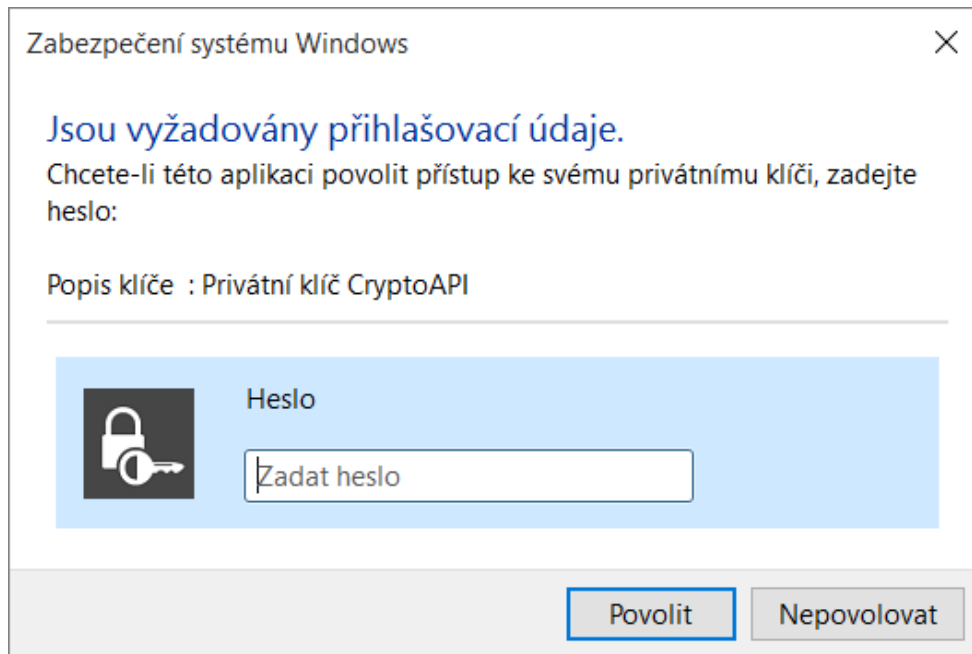
Heslo:

Potvrdit:

< Zpět **Dokončit** Zrušit

Po kliknutí na tlačidlo **Dokončit** nastane zmena úrovne zabezpečenia. Teraz kliknite na tlačidlo **OK**.

V ďalšom dialógovom okne udeľte oprávnenie tlačidlom **Povolit**. Pokiaľ ste zvolili **vysokú** úroveň zabezpečenia, musíte zadať aj heslo.



3.5. Podpis a odoslanie žiadosti o následný certifikát

Pokiaľ nedošlo pri generovaní žiadosti k chybe, stránka Vám zobrazí vygenerovanú žiadosť vo formáte PKCS10.

Po kliknutí na tlačidlo **Odoslať žiadosť na spracovanie**, sa zobrazí dialóg, obsahujúci Vašu žiadosť o následný certifikát. Túto žiadosť je nutné podpísať certifikátom, ku ktorému žiadate následný.



VYTVORENÍ ŽÁDOSTI O VYDÁNÍ NÁSLEDNÉHO 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.

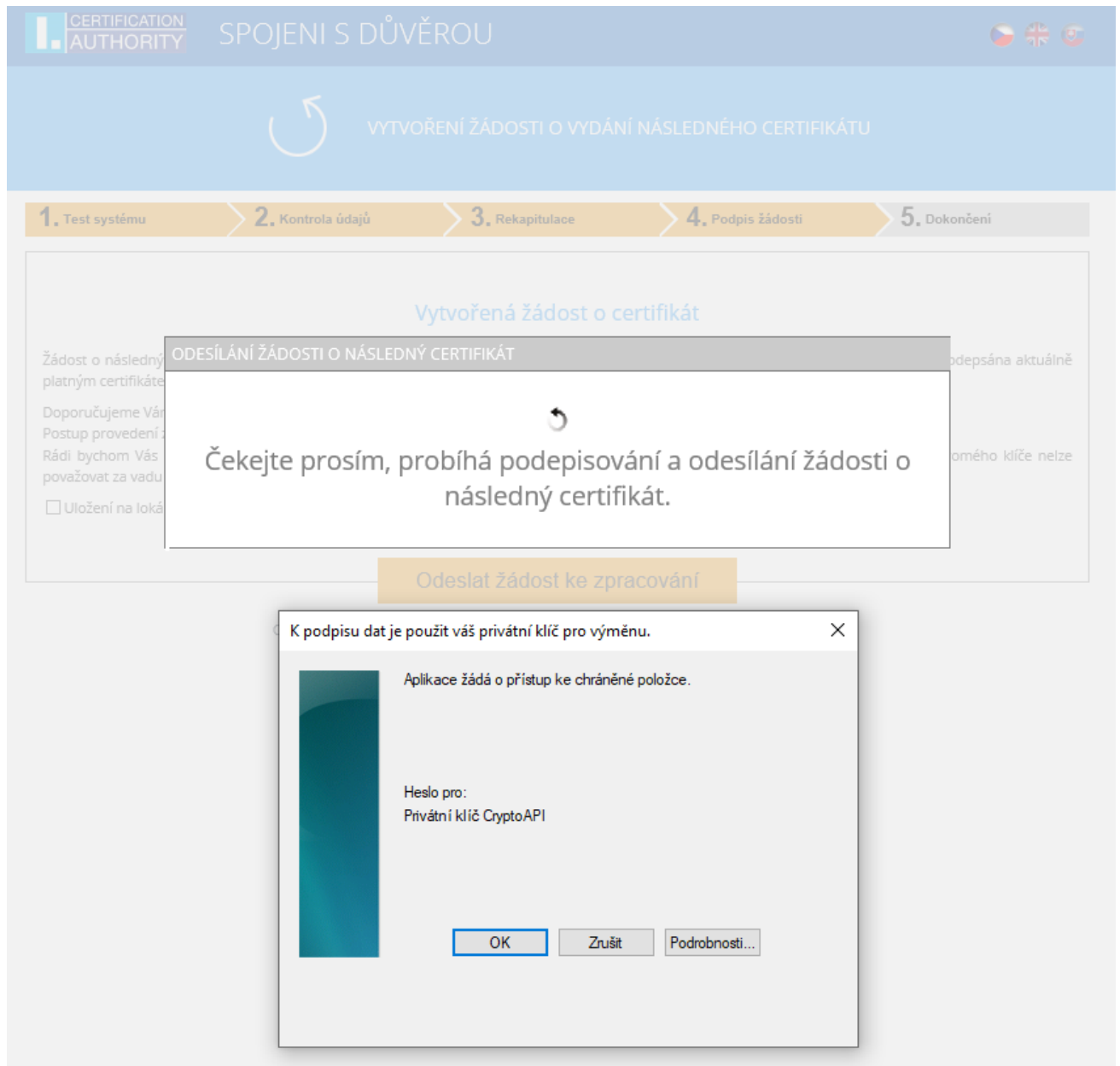
Doporučujeme Vám provést zálohu privátního klíče.

Postup provedení zálohy je uveden zde: <http://www.ica.cz/Zaloha-kllice>

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



Žiadosť je potrebné podpísať kliknutím na tlačidlo „OK“

Pokiaľ je žiadosť generovaná na čipovú kartu, je potrebné ju podpísať zadaním **PIN kódu** na čipovej karte.

V prípade, že žiadate o následný certifikát DUÁL, je nutné podpísať žiadosť o následný kvalifikovaný, aj žiadosť o komerčný certifikát.

V prípade úspešného odoslania žiadosti sa Vám zobrazí nasledujúca stránka:



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.

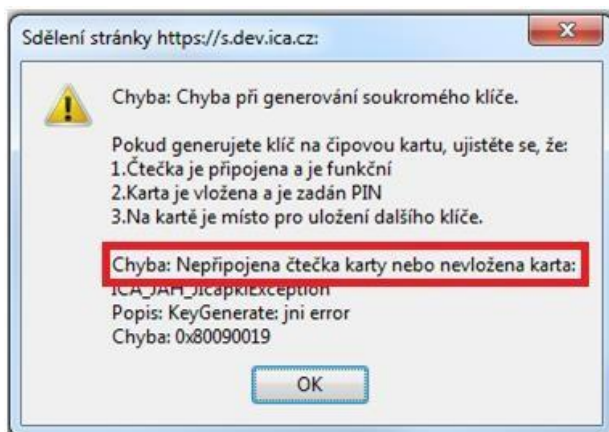
Čas přijetí žádosti: 09.07.2020 13:11:41

Ukončit průvodce

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

4. Riešenie problémov

V prípade vzniku chyby behom procesu generovania žiadosti budete informovaný chybovou hláškou.



V treťom odstavci nájdete popis chyby.

Niektoré chyby môžu byť závažnejšieho technického rázu. Môžu súvisieť so stavom hardwarového či softwarového vybavenia Vášho počítača. V tomto prípade doporučujeme kontaktovať [technickú podporu I.CA](#)