

Generování žádosti o prvotní certifikát

Obsah

1.	Úvod	2
2.	Požadavky na software.....	2
3.	Proces generování žádosti o následný certifikát.....	2
3.1	Výběr certifikátu.....	3
3.2	Test systému.....	4
3.3	Zadání údajů	5
3.4	Kontrola údajů.....	6
3.5	Uložení žádosti	7
3.6	Dokončení.....	7

1. Úvod

Tento dokument slouží jako návod, jak postupovat při generování žádosti o prvotní 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 PKIServiceHost**

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

2.6. **eObčanka – Správce karty** (pouze v případě generování žádosti na občanský průkaz)

3. Proces generování žádosti o následný certifikát

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

1. **Výběr certifikátu**
2. **Test systému**
3. **Zadání údajů**
4. **Kontrola údajů**
5. **Uložení žádosti**

2.1 Výběr certifikátu

Tvorbu žádosti zvolte po výběru typu certifikátu zde: <http://www.ica.cz/Certifikaty> nebo si certifikát vyberete zde: <https://ica.cz/produkty>.

Získání žádosti o certifikát

Krok 1: Pro koho je certifikát určen? Vyberte jednu z možností:

fyzická osoba

zaměstnanec nebo OSVČ

právní osoba nebo úřad

Fyzická osoba – pokud zvolíte tuto možnost, bude váš certifikát obsahovat Vaše jméno a příjmení, volitelně je možné uvést také bydliště a e-mailovou adresu.

Zaměstnanec nebo OSVČ – tato volba je určena pro ty, kdo v certifikátu potřebují uvést mimo jména a příjmení také název svého zaměstnavatele (organizace) nebo živnosti. Můžete ji také využít, pokud jste jednatelem společnosti.

Firma nebo státní instituce – pokud potřebujete certifikát pro vaši firmu, státní instituci nebo jiný právní subjekt, zvolte tuto možnost. Certifikát bude obsahovat název subjektu a volitelně také jeho sídlo.

- fyzická osoba – v certifikátu bude uvedeno **pouze jméno a příjmení** žadatele. Nikoliv organizace.
- zaměstnanec nebo OSVČ – v certifikátu bude uvedeno **jméno, příjmení a také organizace** za kterou žadatel vystupuje.
- právní osoba nebo úřad – zde se jedná především o elektronickou pečeť nebo komerční technologický certifikát. V certifikátu není uvedeno jméno a příjmení žadatele. Je zde uvedena **pouze organizace**.

V dalším kroku vyberete certifikát, o který žádáte (zde se jedná příkladně o Kvalifikovaný certifikát pro elektronický podpis) a zaškrtnete pole: „bude uložen ve vašem počítači“. Poté dole stisknete tlačítko „Získat“.

Pokud žádáte o certifikát s **uložením na čipové kartě**, je potřeba mít připojenou čipovou kartu k počítači. Pokud nemáte čipovou kartu je možnost navštívit pobočku registrační autority, která nabízí hardware, kde Vám následně vytvoří žádost a vystaví certifikát.

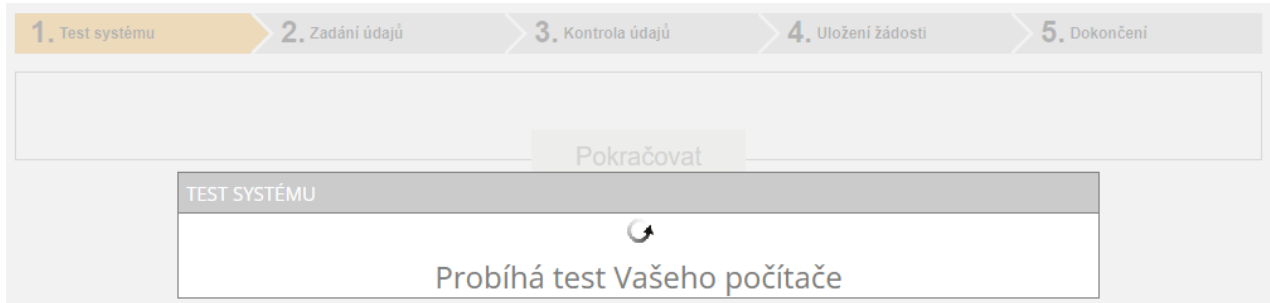
Pokud žádáte o certifikát s **uložením na občanském průkazu**, je potřebné mít nainstalovanou aplikaci eObčanka – Správce karty a připojený občanský průkaz k počítači, který má nastavený PIN a QPIN.

Krok 2: vyberte možnost, o kterou máte zájem ([zpátky ke kroku 1](#))

- Kvalifikovaný certifikát pro elektronický podpis**
používá se pro podepisování dokumentů. Využívá se tam, kde je vyžadován uznávaný elektronický podpis.
- bude uložen ve vašem počítači
- bude uložen na čipové kartě
- bude uložen na občanském průkazu

2.2 Test systému

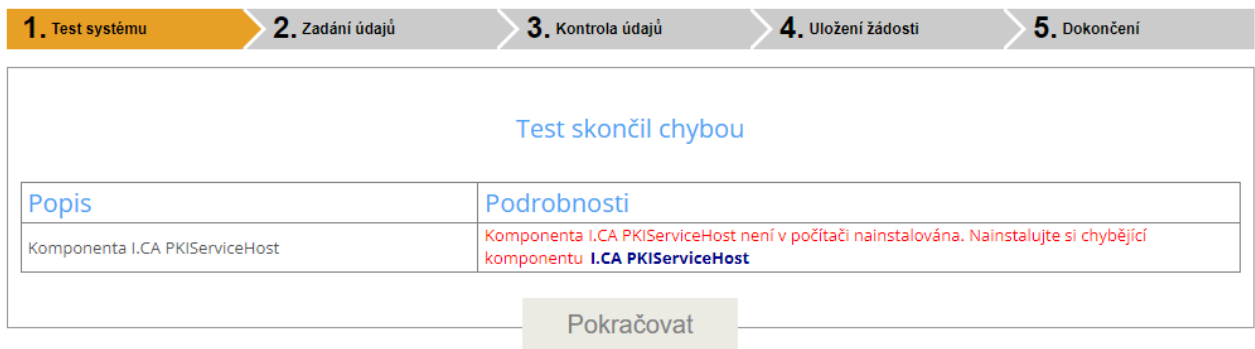
Pro usnadnění kontroly připravenosti Vašeho počítače na generování žádosti, je při zahájení generování žádosti zobrazena kontrolní stránka, která ověří přítomnost klíčových softwarových komponent.



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 certifikát.

2.3 Zadání údajů

Zde vyplníte údaje. Doporučujeme nechat zde nastavení zaškrtnutých polí, tak jak je nastaveno ve výchozím nastavení. Následně stiskněte tlačítko „**Pokračovat**“.

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

Údaje o žadateli Přidat volitelné položky >>

<input type="text" value="Titul (před jménem)"/>	<input type="text" value="Titul (za jménem)"/>	
<input type="text" value="Jméno"/>	<input type="text" value="Příjmení"/>	<input style="border: none; background-color: #e0f0ff; padding: 2px;" type="text" value="Česká republika"/> ?
<input type="text" value="E-mail uvedený v certifikátu"/> ?	<input type="text" value="E-mail pro komunikaci s I.CA"/> ?	
<input type="checkbox"/> Vložit volitelný identifikátor fyzické osoby		
Typ klíče	<input style="border: none; background-color: #e0f0ff; padding: 2px;" type="text" value="RSA 2048"/> ▾	
Heslo pro zneplatnění	<input type="text" value="Vaše heslo"/> ?	
Typ úložiště klíče (CSP)	<input style="border: none; background-color: #e0f0ff; padding: 2px;" type="text" value="Operační systém Windows"/> ▾	
<input checked="" type="checkbox"/> Certifikát obsahující IK MPSV pro komunikaci s orgány státu ?	<input checked="" type="checkbox"/> Povolit export klíče ?	
<input checked="" type="checkbox"/> Certifikát zaslat ve formátu ZIP	<input checked="" type="checkbox"/> Povolit silnou ochranu klíče ?	

Rozšířené možnosti certifikátu >>


2.4 Kontrola údajů

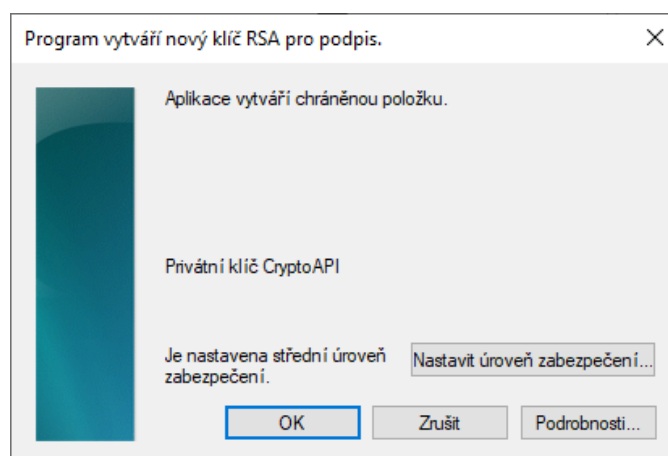
Na kartě kontrola údajů je potřeba zkontrolovat správnost Vámi zadaných údajů. Poté můžete stisknout tlačítko „Pokračovat“.

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

Údaje o žadateli	
Celé jméno	Celé jméno
Jméno	Jméno
Příjmení	Příjmení
Stát	Česká republika
Nastavení certifikátu	
Typ certifikátu	Kvalifikovaný certifikát
Typ žadatele	Běžný uživatel (fyzická osoba - nepodnikající)
Certifikát obsahující IK MPSV pro komunikaci s orgány státu	Ano
Heslo pro zneplatnění	
Certifikát zaslat ve formátu ZIP	Ano
Doba platnosti certifikátu	365 dní
Algoritmus podpisu certifikátu	pkcs#1 1v5
Typ úložiště klíče (CSP)	Operační systém Windows
Typ klíče / Algoritmus miniatury / Délka klíče	RSA / sha256Algorithm / 2048
Povolit export klíče	Ano
Povolit silnou ochranu klíče	Ano
Nastavení použití klíče	Non Repudiation / Digital Signature
Rozšířené nastavení použití klíče	id-kp-emailProtection
Typ kódování	UTF8_STRING

Pokračovat

Po stisknutí tlačítka „Pokračovat“ se do počítače začne generovat privátní klíč. Na Windows liště se zobrazí nová ikona  a po rozkliknutí této ikony se zobrazí okno, které je potřeba potvrdit tlačítkem „OK“. V případě generování certifikátu na čipovou kartu nebo občanský průkaz bude vyžadováno zadání PINu.



2.5 Uložení žádosti

Zde necháte zaškrtnuto „**Uložení na server I.CA**“ opišete kontrolní řetězec a vyplníte telefonní číslo (telefonní číslo je zde vyplněno pouze pro příjem SMS zprávy s číslem žádosti, které budete potřebovat na registrační autoritě). Poté stisknete tlačítko „**Pokračovat**“.

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 opišete kontrolní text uvedený na obrázku a stisknete 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 vyplnily e-mail pro zaslání certifikátu, bude identifikační kód rovněž zaslán na tento e-mail.



Pokračovat

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

2.6 Dokončení


V tomto kroku je žádost hotová a zbývá Vám už jen navštívit registrační autoritu pro ověření a vydání certifikátu.

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

Vaše žádost byla úspěšně uložena na server I.CA.

Identifikační kód Vaší žádosti je

145528



S tímto identifikačním kódem navštivte vybranou registrační autoritu, která dokončí vydání vašeho certifikátu.

Doporučujeme Vám provést zálohu privátního klíče.
Postup provedení zálohy je uveden zde: <https://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.

Vyhledat registrační autoritu

Ukončit průvodce

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