

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	6
3.4	Kontrola údajů.....	7
3.5	Uložení žádosti	9
3.6	Dokončení.....	9

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 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)

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

3. Proces generování žádosti o prvotní certifikát

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

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

1.1 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

právnícká 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.
- právnícká 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 například 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.

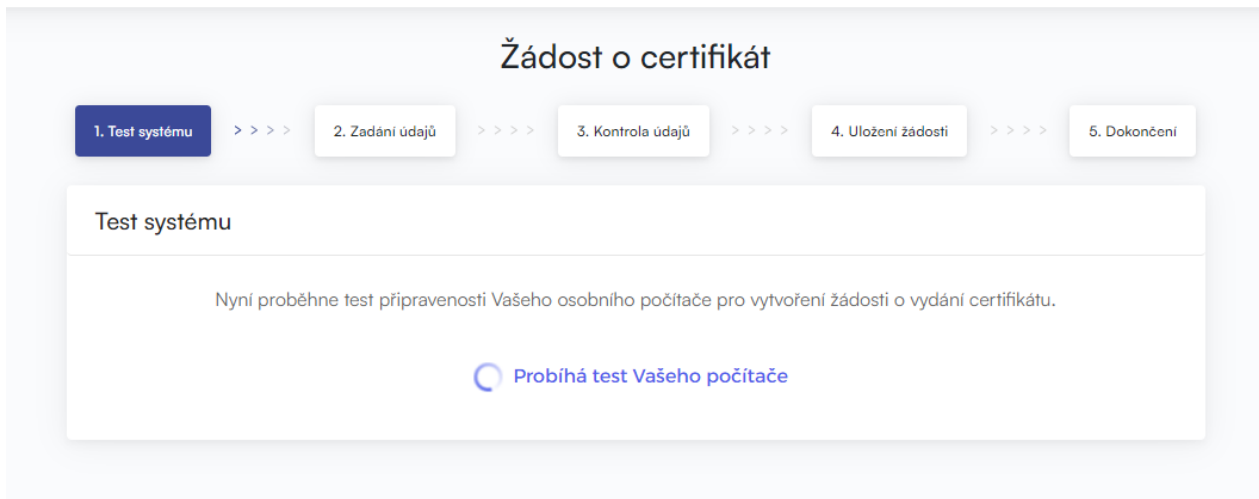
Pokud žádáte o certifikát s **uložením na občanském průkazu**, je potřebné mít nainstalovanou aplikaci eObčanka – Správce karty a připojený občanský průkaz k počítači, který má nastavený PIN a QPIN.

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

1.2 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.




Žádost o certifikát

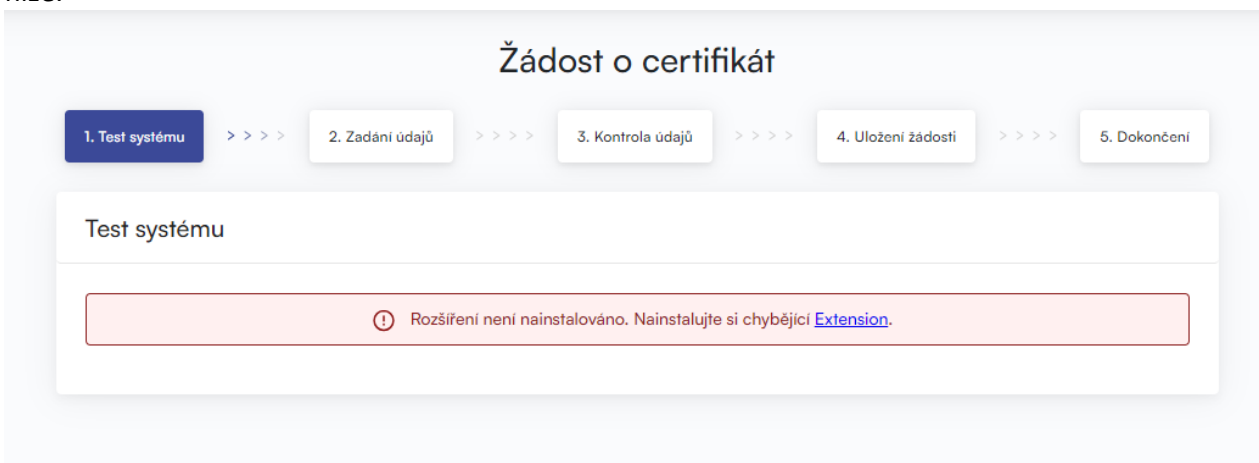
1. Test systému >>>> 2. Zadání údajů >>>> 3. Kontrola údajů >>>> 4. Uložení žádosti >>>> 5. Dokončení

Test systému

Nyní proběhne test připravenosti Vašeho osobního počítače pro vytvoření žádosti o vydání certifikátu.

 Probíhá test Vašeho počítače


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

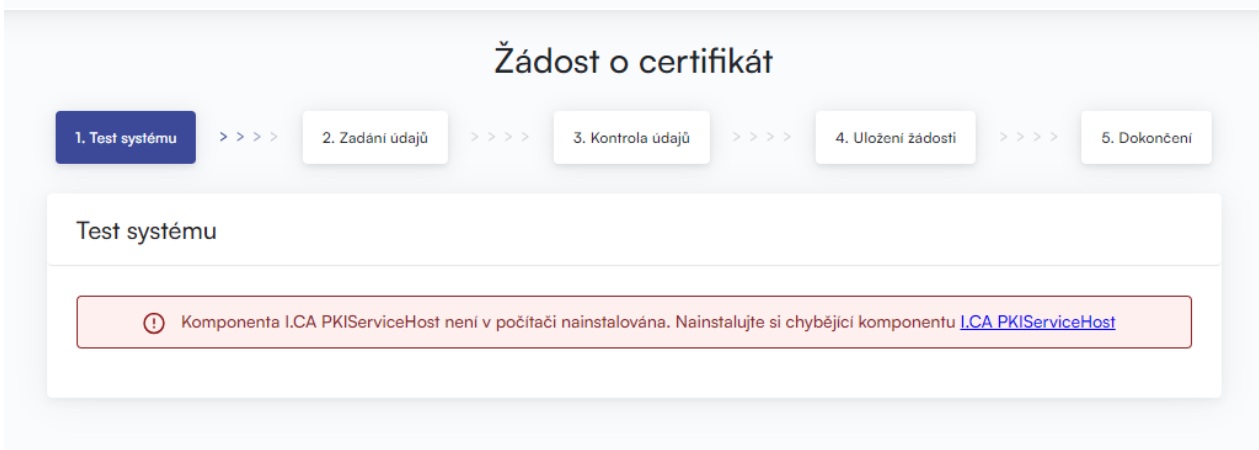


Žádost o certifikát

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

Test systému


 Rozšíření není nainstalováno. Nainstalujte si chybějící [Extension](#).



Žádost o certifikát

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

Test systému

 Komponenta I.CA PKIServiceHost není v počítači nainstalována. Nainstalujte si chybějící komponentu [I.CA PKIServiceHost](#)

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

Stránka otestuje počítač, pokud nejsou detekovány problémy, automaticky přejdete k samotné tvorbě žádosti o 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 je.

1.3 Zadání údajů

Zde vyplníte údaje. Doporučujeme nechat nastavení zaškrtnutých polí ve výchozím nastavení. Následně stiskněte tlačítko „**Pokračovat**“.

Žádost o certifikát

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

Údaje o žadateli

+ Zobrazit volitelné položky

Titul (před jménem)	Titul (za jménem)		
<input type="text"/>	<input type="text"/>		
Jméno (povinné)	Příjmení (povinné)	Stát (povinné) ⓘ	
<input type="text" value="Jan"/>	<input type="text" value="Novák"/>	<input type="text" value="Česká republika"/>	
E-mail uvedený v certifikátu ⓘ	E-mail pro komunikaci s I.CA ⓘ	Předčísli	Telefonní číslo
<input type="text" value="podpora@ica.cz"/>	<input type="text" value="podpora@ica.cz"/>	<input type="text" value="+420"/>	<input type="text"/>

Vložit volitelný identifikátor fyzické osoby

Nastavení certifikátu

Typ klíče (povinné)	Heslo pro zneplatnění (povinné) ⓘ	Typ úložiště klíče (CSP) (povinné)
<input type="text" value="RSA 2048"/>	<input type="text" value="Zneplatnění"/>	<input type="text" value="Operační systém Windows"/>

- Certifikát zaslat ve formátu ZIP
- Certifikát obsahující IK MPSV pro komunikaci s orgány státu ⓘ
- Povolit export klíče ⓘ
- Povolit silnou ochranu klíče ⓘ

Rozšířené možnosti

▼

Pokračovat




1.4 Kontrola údajů

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

Žádost o certifikát

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

Kontrola údajů - Zkontrolujte údaje




<p> OSOBNÍ ÚDAJE</p> <p> VLASTNOSTI CERTIFIKÁTU</p> <p> OSTATNÍ NASTAVENÍ</p>	<p>Osobní údaje</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Celé jméno Jan Novák</td> <td style="width: 50%;">Jméno Jan</td> </tr> <tr> <td>Příjmení Novák</td> <td>E-mail uvedený v certifikátu podpora@ica.cz</td> </tr> <tr> <td>Stát CZ</td> <td></td> </tr> </table>	Celé jméno Jan Novák	Jméno Jan	Příjmení Novák	E-mail uvedený v certifikátu podpora@ica.cz	Stát CZ	
Celé jméno Jan Novák	Jméno Jan						
Příjmení Novák	E-mail uvedený v certifikátu podpora@ica.cz						
Stát CZ							

Pokračovat

Žádost o certifikát

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

Kontrola údajů - Zkontrolujte údaje

<p> OSOBNÍ ÚDAJE</p> <p style="background-color: #e6f2ff; padding: 2px;">  VLASTNOSTI CERTIFIKÁTU </p> <p> OSTATNÍ NASTAVENÍ</p>	<p>Nastavení certifikátu</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Typ certifikátu Kvalifikovaný certifikát</td> <td style="width: 50%;">Typ žadatele Běžný uživatel (fyzická osoba - nepodnikající)</td> </tr> <tr> <td>Certifikát obsahující IK MPSV pro komunikaci s orgány státu Ano</td> <td>Heslo pro zneplatnění Zneplatnění</td> </tr> <tr> <td>E-mail pro komunikaci s I.CA podpora@ica.cz</td> <td>Certifikát zaslat ve formátu ZIP Ano</td> </tr> <tr> <td>Doba platnosti certifikátu 365 dní</td> <td></td> </tr> </table>	Typ certifikátu Kvalifikovaný certifikát	Typ žadatele Běžný uživatel (fyzická osoba - nepodnikající)	Certifikát obsahující IK MPSV pro komunikaci s orgány státu Ano	Heslo pro zneplatnění Zneplatnění	E-mail pro komunikaci s I.CA podpora@ica.cz	Certifikát zaslat ve formátu ZIP Ano	Doba platnosti certifikátu 365 dní	
Typ certifikátu Kvalifikovaný certifikát	Typ žadatele Běžný uživatel (fyzická osoba - nepodnikající)								
Certifikát obsahující IK MPSV pro komunikaci s orgány státu Ano	Heslo pro zneplatnění Zneplatnění								
E-mail pro komunikaci s I.CA podpora@ica.cz	Certifikát zaslat ve formátu ZIP Ano								
Doba platnosti certifikátu 365 dní									

Pokračovat

Žádost o certifikát

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


Kontrola údajů - Zkontrolujte údaje

- OSOBNÍ ÚDAJE
- VLASTNOSTI CERTIFIKÁTU
- OSTATNÍ NASTAVENÍ

Ostatní nastavení

Algoritmus podpisu certifikátu pkcs#1 lv5	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 vyžádáno zadání PINu.

Žádost o certifikát

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

Kontrola údajů - Nyní se pro žádost o certifikát vytváří

○ Privátní klíč pro certifikát
○ Žádost o certifikát

Program vytváří nový klíč RSA pro podpis.
✕

Applikace vytváří chráněnou položku.

Privátní klíč CryptoAPI

Je nastavena střední úroveň zabezpečení. Nastavit úroveň zabezpečení...

OK
Zrušit
Podrobnosti...

1.5 Uložení žádosti

Zde necháte zaškrtnuto „Uložení na server I.CA“ opíšete 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“.

Žádost o certifikát


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

Uložení žádosti

Uložení na server I.CA

Pro uložení žádosti na server I.CA opište kontrolní text uvedený na obrázku a stiskněte 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.

Kontrolní řetězec (povinné)



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.

Předčíslí Telefonní číslo

Uložení na lokální disk nebo externí úložiště

Pokračovat

1.6 Dokončení

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

Žádost o certifikát

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

Uložení žádosti

✔ Vaše žádost byla úspěšně uložena na server I.CA.

Identifikační kód Vaší žádosti byl odeslán na e-mail uvedený v žádosti o certifikát.

Identifikátor byl úspěšně odeslán na Váš e-mail podpora@ica.cz

Doporučujeme Vám provést zálohu privátního klíče.

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

Vyhledat registrační autoritu
Ukončit průvodce