

Generování žádosti o certifikát

Uživatelská příručka

První certifikační autorita, a.s.
Verze 1.0

Obsah

1. Úvod.....	3
2. Požadavky na software.....	3
3. Kontrola softwarového vybavení.....	4
4. Vyplnění údajů o žadateli	6
5. Generování žádosti o certifikát.....	9
6. Uložení žádosti o certifikát	10
7. Vystavení certifikátu	10
8. Instalace certifikátu na občanský průkaz.....	10
9. Aplikace eObčanka	13

1. Úvod

Tento dokument slouží jako návod, jak postupovat při generování žádosti o certifikát přes webové stránky.

2. Požadavky na software

Počítač, na kterém se bude provádět generování žádosti o certifikát, musí splňovat následující požadavky:

- nainstalovaný a spuštěný operační systém
 - Windows 7
 - Windows 8 / 8.1
 - Windows 10
- nainstalován a použit Internet Explorer verze 10 – 11 nebo aktuální verze prohlížeče Google Chrome, Opera nebo Mozilla Firefox.
- nainstalována aktuální verze obslužné aplikace [eObčanka](#)
- nainstalovanou aktuální aplikaci I.CA PKIServiceHost
 - Přítomnost tohoto softwaru detekují testovací stránky automaticky, pokud zjistí, že software přítomen není, vybědnou uživatele k jeho stažení/instalaci.
- v internetovém prohlížeči zapnuta podpora skriptování Javascript, podpora ukládání cookies

3. 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. Kliknutím na tlačítko **Zahájit test** spustíte test Vašeho počítače.

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

Je Váš počítač připraven?

Nejdříve je nutné otestovat, zda Váš počítač splňuje minimální požadavky pro bezproblémový průběh generování žádosti. 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.C.A.](#)

Zahájit test

Čekám na spuštění testu

VÝSLEDEK	POPIS	PODROBNOSTI
	Verze operačního systému	
	Typ a verze prohlížeče	
	Podpora jazyka JavaScript	
	Podpora rozšíření nebo jazyka Java	
	Podpora Java Appletu I.C.A.	
	Podpora ukládání cookies	

Pokračovat

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

Je Váš počítač připraven?

Nejdříve je nutné otestovat, zda Váš počítač splňuje minimální požadavky pro bezproblémový průběh generování žádosti. 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	IE verze 11.0, tento webový prohlížeč je podporován.
✓	Podpora jazyka JavaScript	JavaScript povolen.
✓	Podpora rozšíření	Rozšíření jsou podporována
✓	Podpora ukládání cookies	Ukládání cookies je povoleno.

Pokračovat

Stránka otestuje počítač, pokud nejsou detekovány problémy, kliknutím na tlačítko **Pokračovat** přejdete k samotné tvorbě žádosti o certifikát.

Pokud se při kontrole vyskytne chyba, nelze pokračovat v tvorbě žádosti o certifikát. Nejdříve je potřeba odstranit chybu, která znemožňuje tvorbu žádosti o certifikát. Význam chybových hlášení je uveden v následujících bodech.

- Nepodporovaný operační systém pro generování žádosti musíte použít jeden z operačních systémů uvedených v kapitole 2.
- Nepodporovaný internetový prohlížeč pro generování žádosti musíte použít jeden z prohlížečů uvedených v kapitole 2.
- 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.

- Pokud není nainstalované rozšíření, je potřeba ho stáhnout a nainstalovat pomocí zobrazeného odkazu.
- 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.

4. Vyplnění údajů o žadateli

Pokud proces testu počítače proběhl bez chyb, stránka zobrazí formulář, do kterého vyplníte své osobní údaje.

1. Test systému	2. Zadání údajů	3. Kontrola údajů	4. Uložení žádosti	5. Dokončení
ÚDAJE O ŽADATELI		ZOBRAZIT DALŠÍ MOŽNOSTI >>		
<input checked="" type="radio"/> Běžný uživatel (fyzická osoba - nepodnikající)	Titul (před jménem)	Titul (za jménem)		
<input type="radio"/> Zaměstnanec (vč. členů statutárních orgánů)	<input type="text" value=""/>	<input type="text" value=""/>		
<input type="radio"/> Právnícká osoba (firma - OSVČ)	E-mail uvedený v certifikátu ?	E-mail pro komunikaci s I.CA ?		
<input type="radio"/> Pseudonym	Česká republika <input type="button" value="v"/>			
VOLITELNÝ IDENTIFIKÁTOR FYZICKÉ OSOBY				
<input type="checkbox"/> Vložit volitelný identifikátor fyzické osoby				
Heslo pro zneplatnění	<input type="text" value="mojeheslo"/> ?			
Typ úložiště klíče (CSP)	<input type="text" value="Microsoft Base Smart Card Crypto Provider"/> <input type="button" value="v"/>			
<input checked="" type="checkbox"/> Certifikát obsahující IK MPSV pro komunikaci s orgány státu ?				
<input checked="" type="checkbox"/> Certifikát zaslat ve formátu ZIP				
<input type="button" value="Pokračovat"/>				

Položky zdůrazněné modrým podbarvením jsou povinné. Například jméno a příjmení jsou povinné, tituly povinné nejsou.

E-mail uvedený v certifikátu: Tuto položku vyplňte v případě, kdy budete podpis používat pro podepisování emailových zpráv. E-mailová adresa uvedená v certifikátu musí být shodná s e-mailem odesílatele.

E-mail pro komunikaci s I. CA: Tento e-mail slouží pro zasílání certifikátů a zasílání upozornění na blížící se konec platnosti vašeho certifikátu.

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. Délka hesla pro zneplatnění certifikátu musí být 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) bude v případě generování na občanský průkaz automaticky zvoleno: **Microsoft Base Smart Card Crypto Provider**

Po stisknutí tlačítka pokračovat stránka provede kontrolu vámi vyplněných údajů. Pokud některé zadané údaje nesplňují podmínky, budete vyzváni k jejich opravě. Údaje vyžadující změnu nebo doplnění jsou podbarveny červeně.

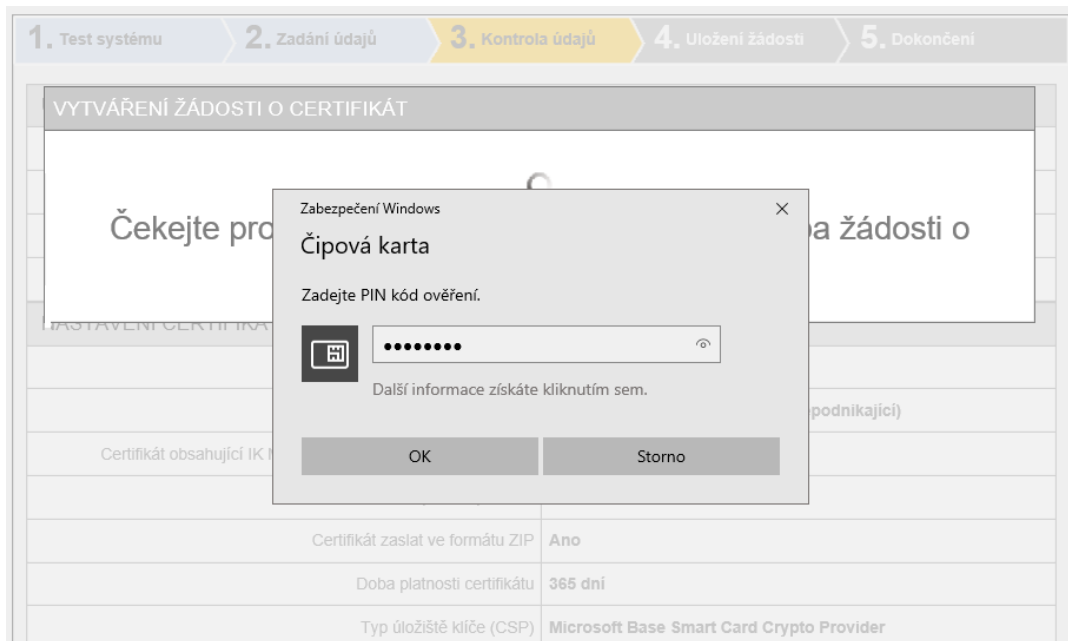
Pokud Vámi zadané údaje splňují podmínky, zobrazí se vám stránka rekapitulující vámi zadané údaje.

1. Test systému		2. Zadání údajů		3. Kontrola údajů		4. Uložení žádosti		5. Dokončení	
ÚDAJE O ŽADATELI									
Celé jméno				[REDACTED]					
Jméno				[REDACTED]					
Příjmení				[REDACTED]					
Stát				Česká republika					
NASTAVENÍ CERTIFIKÁTU									
Typ certifikátu				TWINS					
Typ žadatele				Běžný uživatel (fyzická osoba - nepodnikající)					
Certifikát obsahující IK MPSV pro komunikaci s orgány státu				Ano					
Heslo pro zneplatnění				TWINS					
Certifikát zaslat ve formátu ZIP				Ano					
Doba platnosti certifikátu				365 dní					
Typ úložiště klíče (CSP)				Microsoft Base Smart Card Crypto Provider					
Algoritmus miniatury / Délka klíče				sha256WithRSAEncryption / 2048					
Nastavení použití klíče kvalifikovaného certifikátu				Non Repudiation / Digital Signature					
Nastavení použití klíče komerčního certifikátu				Digital Signature / Key Encipherment					
Rozšířené nastavení použití klíče kvalifikovaného certifikátu				id-kp-emailProtection					
Rozšířené nastavení použití klíče komerčního certifikátu				id-kp-clientAuth / id-kp-emailProtection					
Typ kódování				UTF8_STRING					
Pokračovat									

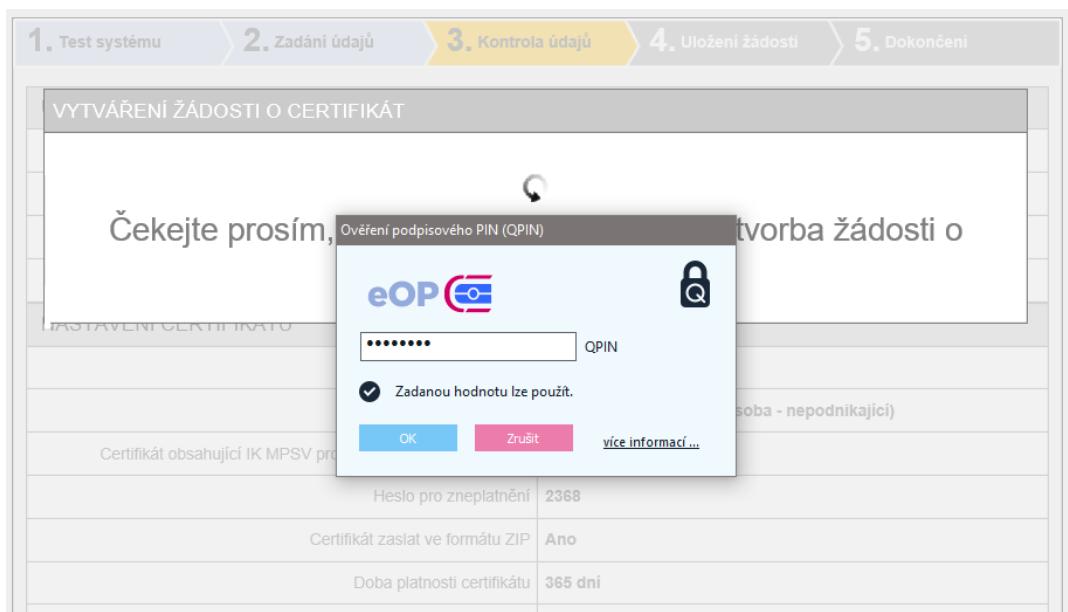
5. Generování žádosti o certifikát

Po kliknutí na tlačítko **Pokračovat** se zahájí generování privátních klíčů na občanský průkaz.

Nejdříve bude nutné zadat PIN.



Poté budete vyzváni k zadání QPINu.



6. Uložení žádosti o certifikát

Zvolením na **Uložit na lokální disk nebo externí úložiště** bude žádost uložena na váš pevný disk nebo jiné médium, které zvolíte.

Pokud chcete vaši žádost **uložit na server I.CA**, opište kód uvedený na obrázku do pole kontrolní řetězec a stiskněte tlačítko **Pokračovat**. Pokud bude vaše žádost úspěšně uložena na server I.CA, **obdržíte identifikátor**, který předložíte při návštěvě registrační autority. Registrační autorita pak bude moci získat vaši žádost o certifikát ze serveru. Identifikátor bude zaslán na e-mailovou adresu uvedenou v žádosti nebo na doplněné tel. číslo.

7. Vystavení certifikátu

Poté, co vytvoříte žádost o certifikát, je nutné navštívit některou registrační autoritu I.CA ([seznam zde](#)). S sebou na registrační autoritu I.CA přineste žádost, kterou jste vygenerovali (například na USB flash disku, uloženou na čipové kartě, identifikátor žádosti uložené na serveru I.CA), a dokumenty potřebné k vystavení certifikátu. Seznam potřebných dokumentů [naleznete zde](#).

8. Instalace certifikátu na občanský průkaz

Instalaci provedete pomocí odkazů v e-mailu. Instalaci stačí provést pomocí kliknutí na jedno z tlačítek, online skript nainstaluje oba certifikáty najednou.

Instalace kvalifikovaného
certifikátu

Instalace komerčního
certifikátu

Po kliknutí na tlačítko pro instalaci se zobrazí stránka, kde kliknete na **Instalovat certifikát na kartu**.

Instalace certifikátu na čipovou kartu Starcos

V případě, že máte privátní klíč k certifikátu uložen na čipové kartě STARCOS nebo v elektronickém občanském průkazu (eOP), klikněte na tlačítko "Instalovat certifikát na kartu".


Automaticky se vám vyhledají chybějící certifikáty, které se na kartu uloží a zaregistrují se také do Windows / MAC.

Instalovat certifikát na kartu

Instalace certifikátu do osobního počítače

V případě, že máte privátní klíč k certifikátu uložen na vašem osobním počítači (OS Windows), klikněte na tlačítko "Instalovat certifikát do PC".

Požadujete ze serveru I.CA certifikát číslo 11450474.

Kontrolní řetězec: 

Opište kontrolní řetězec z obrázku a klikněte na tlačítko "Instalovat certifikát do PC".

Instalovat certifikát do PC

Zde necháte zaškrtnuto **Registrovat certifikáty do MS Windows** a kliknete na **Instalovat**.

Zde si můžete provést instalaci certifikátů vydaných I.CA na čipovou kartu.

Stiskem tlačítka Instalovat zahájíte instalaci certifikátů na vaši čipovou kartu. Před zahájením instalace vložte kartu do čtečky a na vyzvání zadejte PIN. Po stisku tlačítka Instalovat vyčkejte dokončení instalace.

Registrovat certifikáty do MS Windows

Instalovat

Spustí se instalace, nejdříve zadáte PIN a poté QPIN k občanskému průkazu.

Po úspěšné instalaci na občanský průkaz se na stránce zobrazí, jaké certifikáty jsou nainstalovány.

Zde si můžete provést instalaci certifikátů vydaných I.CA na čipovou kartu.

Stiskem tlačítka Instalovat zahájíte instalaci certifikátů na vaši čipovou kartu. Před zahájením instalace vložte kartu do čtečky a na vyzvání zadejte PIN.
Po stisku tlačítka Instalovat vyčkejte dokončení instalace.

Registrovat certifikáty do MS Windows

Instalovat

Probíhá čtení obsahu čipové karty...

Název CSP: Microsoft Base Smart Card Crypto Provider (eOP CZE v2.1, Alcor Micro USB Smart Card Reader 0)

Čtení kontejneru "TwinsQD 19/10/2018 10:11:19": OK (identifikace klíče: 0BD0DC252D59C9B8E57A4CB7E7AEC85C7509BB0A)

Čtení kontejneru "TwinsSD 19/10/2018 10:11:19": OK (identifikace klíče: 3C4EF3B590122DE763F8F6EEA964E68F043A83F6)

Počet chybějících certifikátů: 2

Probíhá komunikace s certifikační autoritou...

Počet získaných platných certifikátů: 2

Probíhá zápis certifikátů na čipovou kartu...

Zápis certifikátu [REDACTED] OK (CN [REDACTED] C=CZ, G [REDACTED] SN [REDACTED] SERIALNUMBER=ICA - [REDACTED])

Zápis certifikátu [REDACTED] OK (CN [REDACTED] C=CZ, G [REDACTED] SN [REDACTED] SERIALNUMBER=ICA - [REDACTED])

Instalace certifikátů byla dokončena.

9. Aplikace eObčanka

Obslužnou aplikaci pro občanský průkaz můžete stáhnout na stránkách [Ministerstvo vnitra ČR](#).

Zde je vidět načtený občanský průkaz v aplikaci eObčanka a jsou zde vidět i vydané certifikáty.

