Generování žádosti o certifikát

Uživatelská příručka

První certifikační autorita, a.s.
Verze 1.0

První certifikační autorita, a.s., se sídlem Podvinný mlýn 2178/6, 190 00 Praha 9 - Libeň, zapsaná dne 12. 3. 2001v Obchodním rejstříku, vedeném u Městského soudu v Praze, spisová značka: oddíl B, vložka 7136. IČ: 26439395, DIČ: CZ26439395. Tel.: +420 284 081 940, fax: +420 284 081 965, e-mail: info@ica.cz, www.ica.cz

Obsah

1. Úvod

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

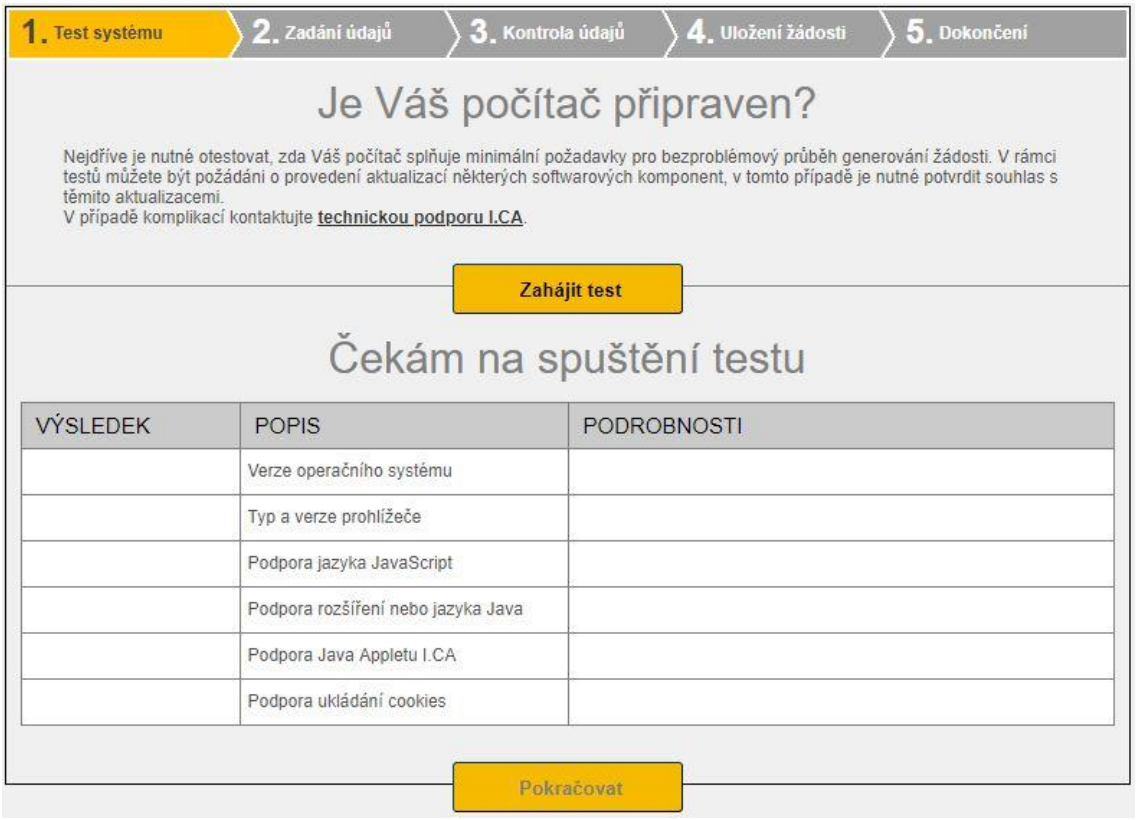
2. Požadavky na software

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, vybídnou 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.



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 certifikátu. Nejdříve je potřeba odstranit chybu, která znemožňuje tvorbu žádosti o certifikát. Význam chybových hlášení je uvedený 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.

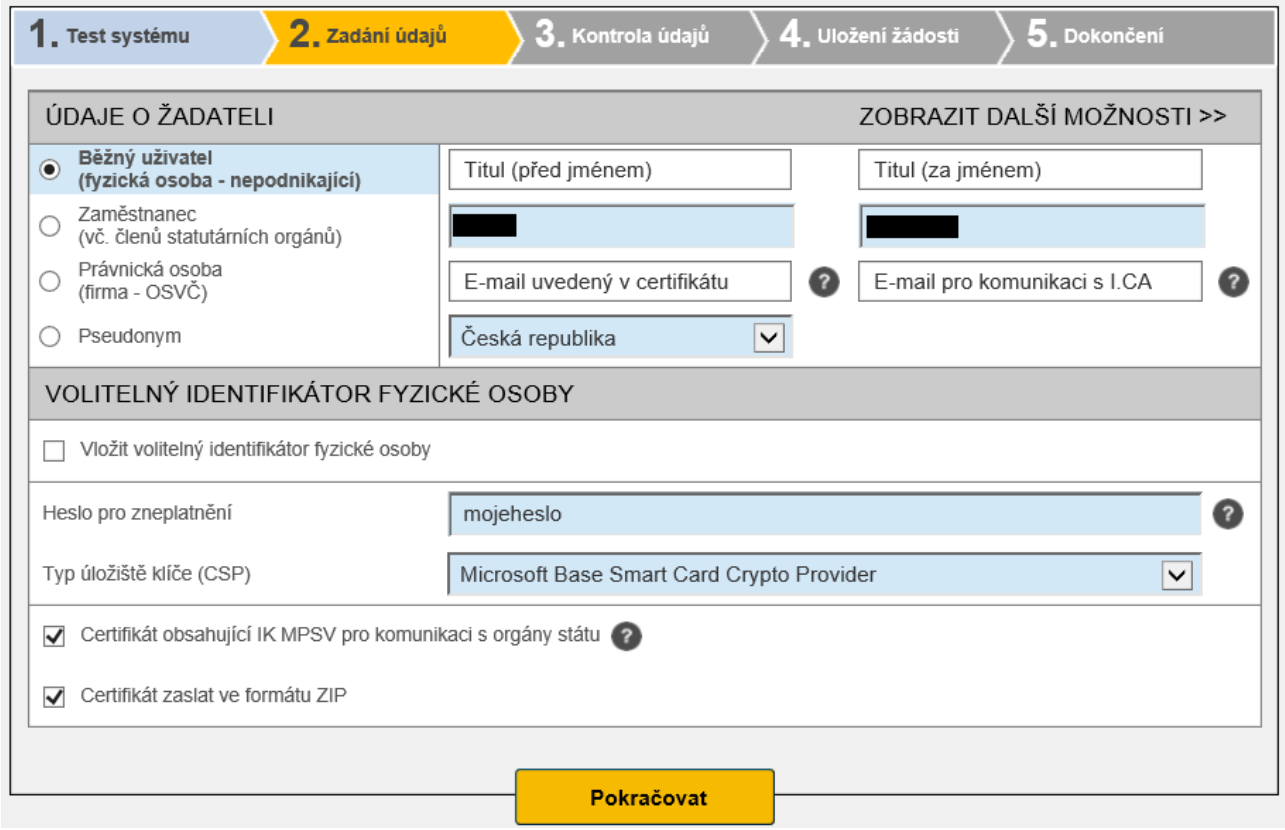
- Podpora JavaScriptu Stránky pro generování žádosti o certifikát vyžadují podporu skriptování v jazyku JavaScript. Pokud by tato kontrola selhala, znamená to s největší pravděpodobností, že je v nastavení prohlížeče podpora scriptování vypnuta. Povolte podporu skriptování v jazyku JavaScript ve vašem 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.



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.

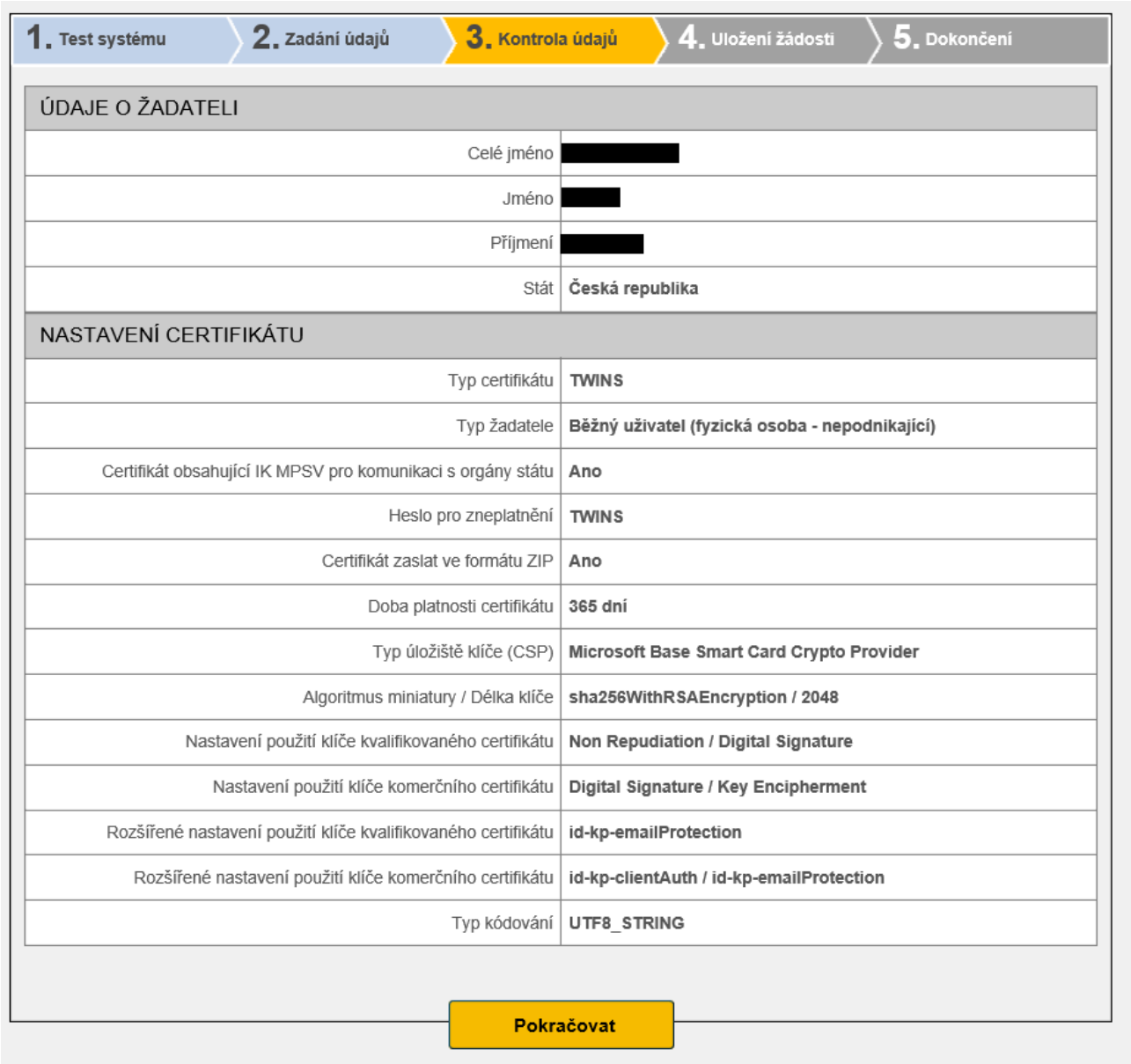
E-mail pro komunikaci s I. CA: Tento e-mail slouží pro zasílání certifikátů a zasílání upozornění na blížící se konec platnosti vašeho certifikátu.

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.

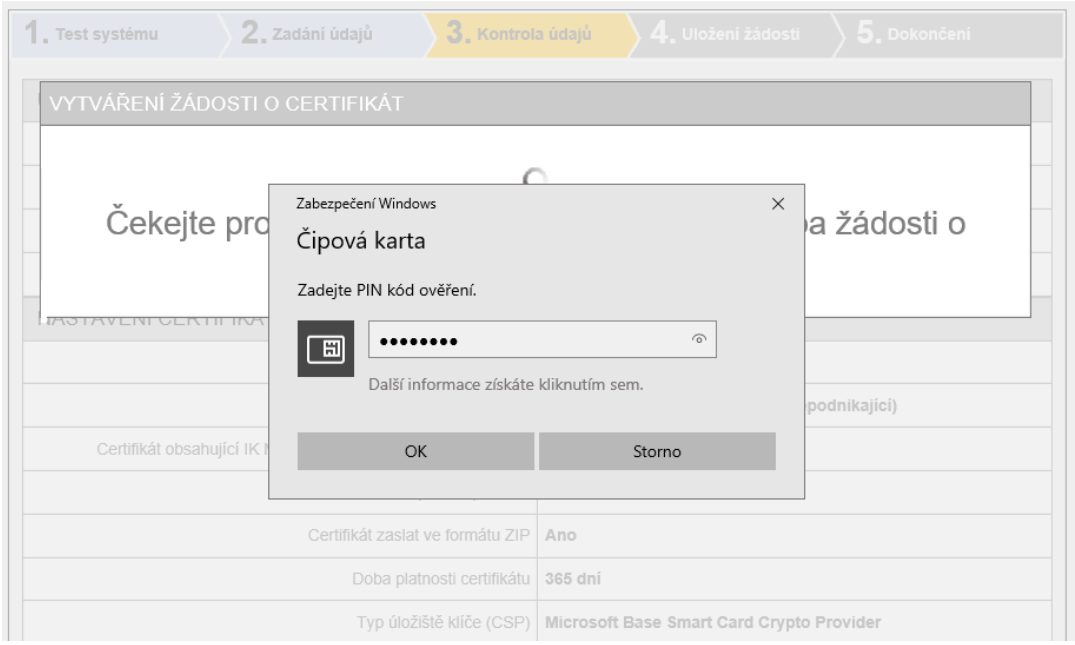
Pokud Vámi zadané údaje splňují podmínky, zobrazí se vám stránka rekapitulující vámi zadané údaje.



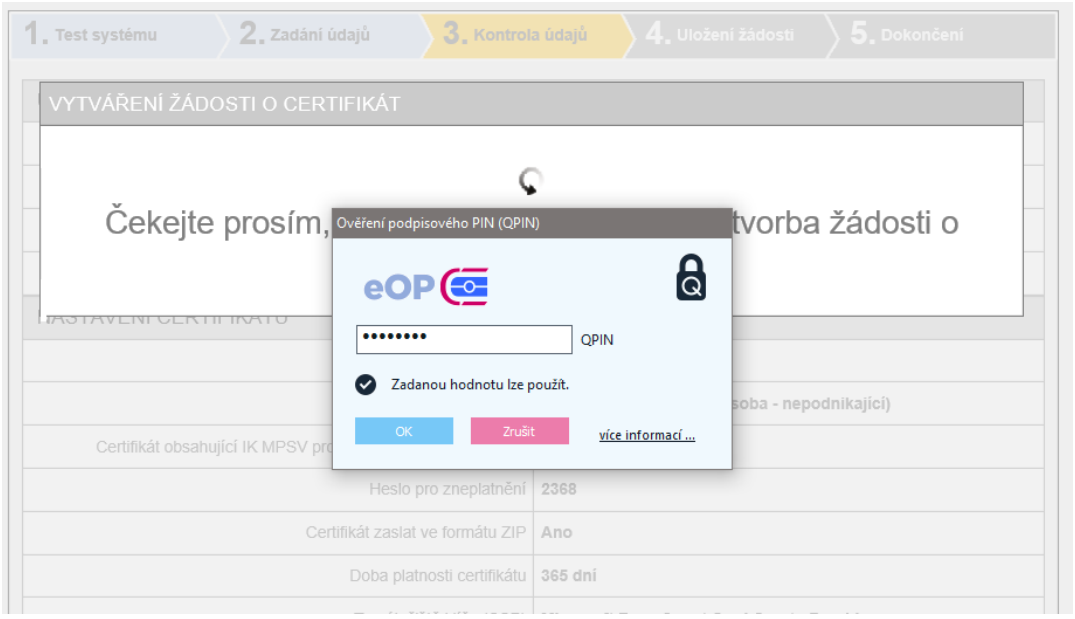
5. Generování žádosti o certifikát

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

Nejdříve bude nutné zadat PIN.



Poté budete vyzvání 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.

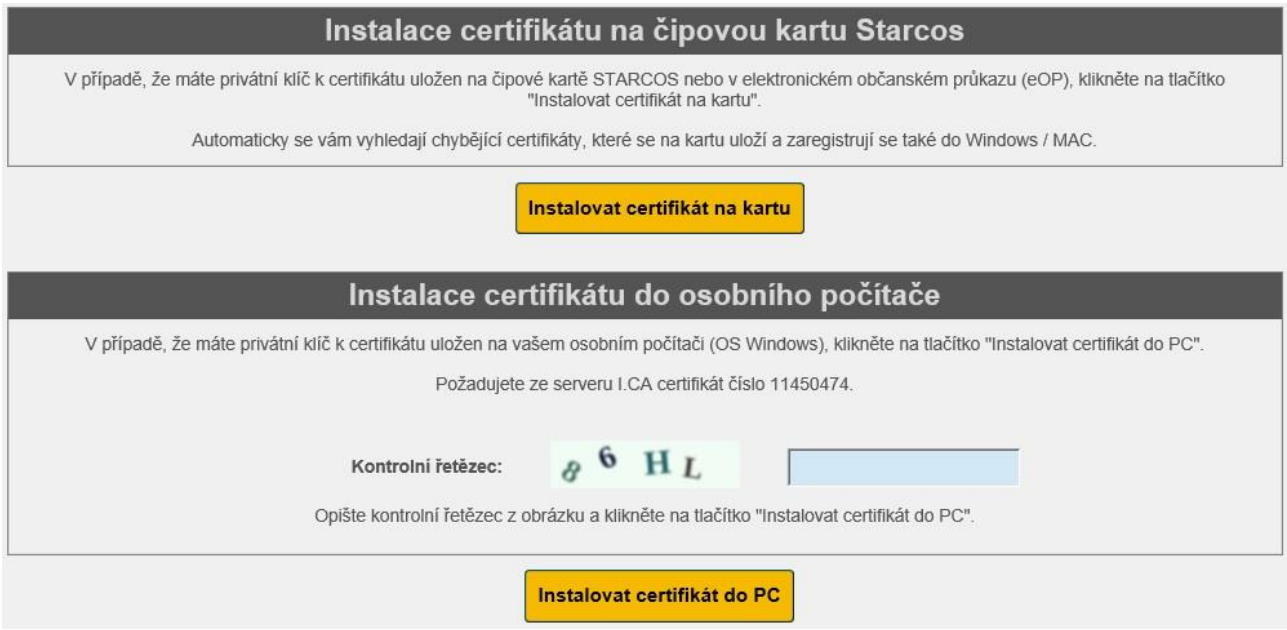
7. Vystavení certifikátu

Poté, co vytvoříte žádost o certifikát, je nutné navštívit některou registrační autoritu I.CA (seznam zde). S sebou na registrační autoritu I.CA přinesete 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.

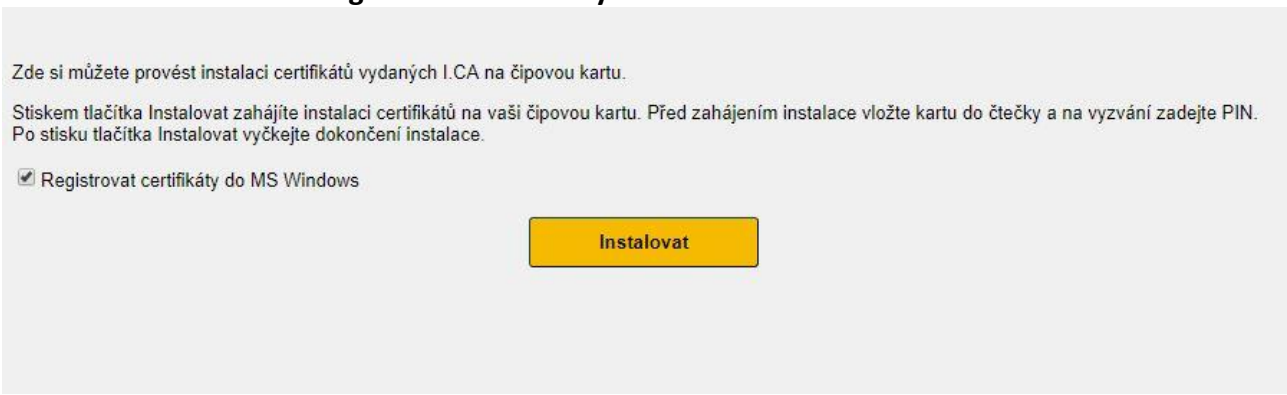
8. Instalace certifikátu na občanský průkaz

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

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



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

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.