MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Instalace software eObčanka pro macOS

instalační příručka

verze 1.90 ze dne 19. 2. 2025

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

1 OBSAH

Seznam obrázků

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

2 ÚVOD

Čip občanského průkazu poskytuje podporu pro:

- **Elektronickou identifikaci vůči online službám kvalifikovaných poskytovatelů** dle zák. č. 250/2017 Sb.
  Držitel se může pomocí svého občanského průkazu přihlašovat k internetovým službám a portálům, zejména veřejné správy. Na základě úspěšného prokázání své totožnosti může občan bezpečně využívat služby, které daný úřad nabízí k vyřízení elektronickou cestou.
- **Vytváření kvalifikovaných elektronických podpisů**.
  Držitel si do čipu může uložit kvalifikované certifikáty pro vytváření elektronických podpisů. Pomocí těchto certifikátů (a příslušných kryptografických klíčů) pak může elektronicky podepisovat dokumenty, e-maily, smlouvy, apod…
- **Autentizaci** držitelů občanských průkazů vůči informačním systémům **prostřednictvím autentizačního certifikátu** vydaného kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Uvedené funkce může držitel využívat z osobního počítače - z domova či z práce.

Pro používání elektronických funkcí občanského průkazu v prostředí macOS je třeba na počítač instalovat software *eObčanka*.

Tento dokument popisuje způsob instalace software *eObčanka* do počítače s operačním systémem macOS.

Software se instaluje pomocí instalačního balíčku typu PKG, který slouží jako grafický průvodce instalací.

2.1 Instalovaný SW

Softwarový balíček eObčanka v sobě obsahuje kompletní podporu elektronických funkcí občanského průkazu pro macOS. Po úspěšné instalaci budou mít uživatelé počítače dostupné všechny softwarové aplikace, které se pro občanský průkaz na macOS nabízí.

Součástí instalovaného balíčku *eObčanka* je několik samostatných softwarových aplikací, které pracují s čipem občanského průkazu. Jedná se o:

- Aplikaci *eObčanka - Identifikace,* pro elektronickou identifikaci občanským průkazem k webovým stránkám na internetu.
- Ovladače čipu občanského průkazu, pro práci s certifikáty a vytváření elektronických podpisů.
- Aplikaci *eObčanka - Správce karty*, pro správu certifikátů a přístupových kódů občanského průkazu.

V následujících podkapitolách je stručně popsána charakteristika jednotlivých instalovaných aplikací. Více informací o těchto aplikacích lze nalézt v samostatných uživatelských příručkách anebo na webových stránkách pro podporu občanských průkazů.

2.1.1 eObčanka - Identifikace

Občan pomocí svého občanského průkazu s čipem může prokázat svou identitu vůči online službám a portálům veřejné správy. *eObčanka - Identifikace* zpřístupňuje identifikační funkci občanského průkazu.

eObčanka - Identifikace je aplikace, umožňující držiteli občanského průkazu s čipem provést **elektronickou identifikaci vůči online službám kvalifikovaných poskytovatelů dle zákona č. 250/2017 Sb. o elektronické identifikaci**. *eObčanka - Identifikace* se využívá pro **přihlášení občanským průkazem** vůči webovým stránkám, zejména veřejné správy.

eObčanka - Identifikace má také **diagnostickou** funkci - umožňuje uživateli najít problémy s využíváním elektronických funkcí občanského průkazu a navrhuje řešení nalezených problémů.

2.1.2 eObčanka - Správce karty

eObčanka - Správce karty je aplikace pro **správu uživatelských certifikátů a přístupových kódů občanského průkazu**.

Pomocí *Správce karty* uživatel může např.:

- Zobrazit seznam kryptografických klíčů v čipu.
- Zobrazit informace o certifikátech v čipu.
- Importovat či smazat certifikát.
- Nastavit, odblokovat či změnit některý z přístupových kódů (IOK, PIN,…).
- Diagnostikovat potíže se čtečkou, čipem, certifikáty, …

2.1.3 Ovladače čipu občanského průkazu

Pro práci s elektronickými certifikáty je nutno do operačního systému instalovat kryptografické ovladače.

Ovladače občanského průkazu umožní aplikacím pracovat s certifikáty, uloženými v čipu občanského průkazu. Prostřednictvím ovladačů se dají certifikáty (a klíče) používat pro:

- **elektronické podpisování** (dokumentů, e-mailů, apod…);
- **přihlašování** (např. do webových stránek).

Ovladače ale slouží také pro **správu certifikátů** v čipu občanského průkazu:

- Čtení informací o uložených certifikátech.
- Vytváření či zápis nových certifikátů a kryptografických klíčů.
- Mazání nepotřebných certifikátů a klíčů.

Další důležitou funkcí ovladačů je práce s **přístupovými kódy** občanského průkazu:

- zobrazování okna pro zadání kódu;
- kontrola hodnot kódu oproti čipu občanského průkazu;
- změna hodnoty kódu;
- zablokování kódu po opakovaném chybném zadání;
- atd.

Ovladače občanského průkazu dodržují uznávané technické standardy pro integraci čipových karet do operačních systémů macOS:

- **CryptoTokenKit -** Tento ovladač používají nativní aplikace (např.: Mail, Safari apod…) na novějších verzích macOS.
  Ovladač CryptoTokenKit je automaticky instalován na macOS 10.14 nebo novější.
- **tokenD** – Tento ovladač používají nativní aplikace (např.: Klíčenka, Mail, Safari apod…) na starších verzích macOS.
  Ovladač tokenD je určen pro macOS 10.13.6 nebo starší. Na tyto verze macOS je tokenD automaticky instalován. Na novějších verzích macOS je tokenD nahrazen ovladačem CryptoTokenKit.
- **PKCS#11** - Tuto verzi ovladače mohou použít aplikace, které se nespoléhají na kryptografické funkce macOS, ale implementují vlastní kryptografii (např. Firefox, Thunderbird, apod…).

Více o ovladačích občanského průkazu viz kapitola 7.

2.2 Podpora starší verze občanského průkazu s čipem

Software *eObčanka* je primárně určena pro podporu občanských průkazů, vydávaných od 1. 7. 2018. Instalační balíček *eObčanka* v sobě ale **obsahuje i podporu starší verze občanského průkazu s čipem**. Software *eObčanka* tedy nahrazuje předchozí instalační balíček, určený pouze pro starší verzi občanských průkazů.

Instalací software *eObčanka* se pro starší verzi občanských průkazů neaktivuje podpora identifikačních funkcí. Podpora elektronického podepisování také zůstane na úrovni, která platila před 1. 7. 2018.

Software *eObčanka* nepřináší pro starší verzi občanských průkazů žádné nové funkce, pouze obsahuje původní podporu starší verze občanských průkazů:

- ovladače pro starší verzi občanských průkazů;
- Správce karty - jedna verze Správce karty podporuje obě verze občanských průkazů.

3 PŘED ZAPOČETÍM INSTALACE

Instalaci software *eObčanka* je třeba provést v těchto krocích:

1. **Stáhnout instalační balíček**
   - viz kapitola 3.3
2. **Spustit instalační balíček**
   - pod účtem správce operačního systému
   - viz kapitola 4.1
3. **Provést všechny kroky instalace**
   - grafický instalační průvodce uživatele průběžně instruuje
   - viz kapitola 4
4. **Zkontrolovat úspěšnost instalace**
   - nepovinný krok
   - viz kapitola 5

3.1 Podporované operační systémy

Software *eObčanka* je určen pro počítače s operačním systémem macOS a s přístupem do internetu. Seznam podporovaných verzí operačního systému je uveden na webových stránkách pro podporu občanských průkazů.

3.2 Stav počítače před započetím instalace

Operační systém nemusí být k provedení instalace speciálně upravován. Vše potřebné zajistí instalační průvodce software *eObčanka*.

Pro samotnou instalaci software *eObčanka* není nezbytné připojení k internetu. Připojení k internetu je třeba jen ke stažení instalačního balíčku.

Pro instalaci software *eObčanka* není nutné mít k počítači připojenou čtečku a instalované ovladače čteček. Instalaci čtečky karet lze provést až po instalaci software *eObčanka*. Přesto lze doporučit, aby byla **čtečka instalována před instalací software *eObčanka***. Po dokončení instalace umožňuje aplikace *eObčanka* spustit diagnostiku, která umí prověřit dostupnost a funkčnost čtečky – viz kapitola 5.

Instalaci software *eObčanka* je třeba spouštět pod uživatelským účtem, který má **oprávnění správce** operačního systému. Pokud uživatel nemá k dispozici uvedená oprávnění, měl by se obrátit na správce operačního systému a požádat jej o provedení instalace.

Před spuštěním instalace je doporučeno uložit rozdělanou práci a ukončit běžící aplikace.

3.3 Stažení instalačního balíčku

Instalace aplikací *eObčanka* se provádí pomocí instalačního balíčku. **Soubor s instalačním programem je uložen ve formě diskového obrazu (DMG) a je třeba ho stáhnout z internetu**, z webových stránek pro podporu občanského průkazu.

V samotném obrazu disku (DMG) je uložen grafický instalační balíček ve formátu PKG, který provede uživatele samotným procesem instalace.

Při stahování instalačního balíčku by si uživatel měl všímat, do kterého adresáře se stažený soubor uloží - aby pak z tohoto adresáře mohl instalační program spustit.

Pomocí instalačního balíčku lze provést jak *prvotní* instalaci, tak *upgrade* software *eObčanka*. Uživatel, který má instalovánu starší verzi si může stáhnout aktuální verzi a spustit instalaci - dojde k upgrade na novější verzi.

3.4 Ověření původu instalačního balíčku

Uživatel by si před instalací software měl vždy ověřit, že daný software pochází z důvěryhodného zdroje a že s obsahem balíčku nikdo nemanipuloval. Instalací nedůvěryhodného či modifikovaného software hrozí riziko, že se do počítače dostane např. počítačový virus či jiný škodlivý software.

Instalační balíček eObčanky je elektronicky podepsán pomocí certifikátu Ministerstva vnitra ČR. Operační systém macOS před instalací automaticky ověřuje elektronický podpis instalačního balíčku. Pokud by instalační balíček nebyl podepsán důvěryhodným certifikátem (resp. příslušným klíčem), operační systém neumožní instalaci provést.

Po ověření elektronického podpisu instalačního balíčku může uživatel důvěřovat tomu, že používá originální balíček eObčanka, který neobsahuje škodlivý software.

Více o ověření integrity a původu instalačního balíčku v kapitole 10.

4 SPUŠTĚNÍ A PROVEDENÍ INSTALACE

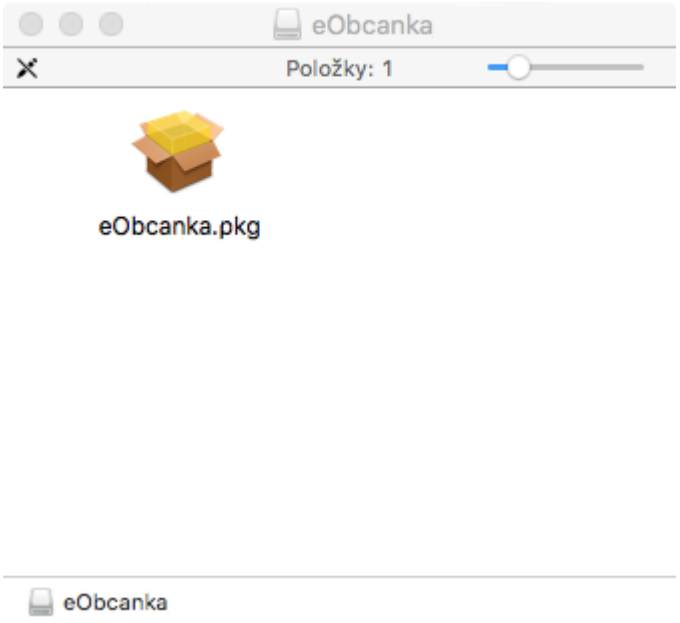
Instalace ovládacího software *eObčanka* se provádí pomocí **grafického instalačního průvodce**, uloženého ve staženém diskovém obrazu.
Grafický instalační průvodce řídí průběh instalace a je koncipován tak, aby co nejvíce usnadnil práci běžného uživatele.

4.1 Spuštění instalace

Instalace se odstartuje spuštěním instalačního programu, staženého z internetových stránek podpory občanského průkazu. Uživatel stáhne obraz disku ve formátu DMG a z něj spustí instalační program uložený v souboru *eObcanka.pkg*

4.2 Připojení obrazu disku

Po spuštění DMG obrazu disku dojde automaticky k připojení obrazu. Operační systém následně automaticky zobrazí jeho obsah.

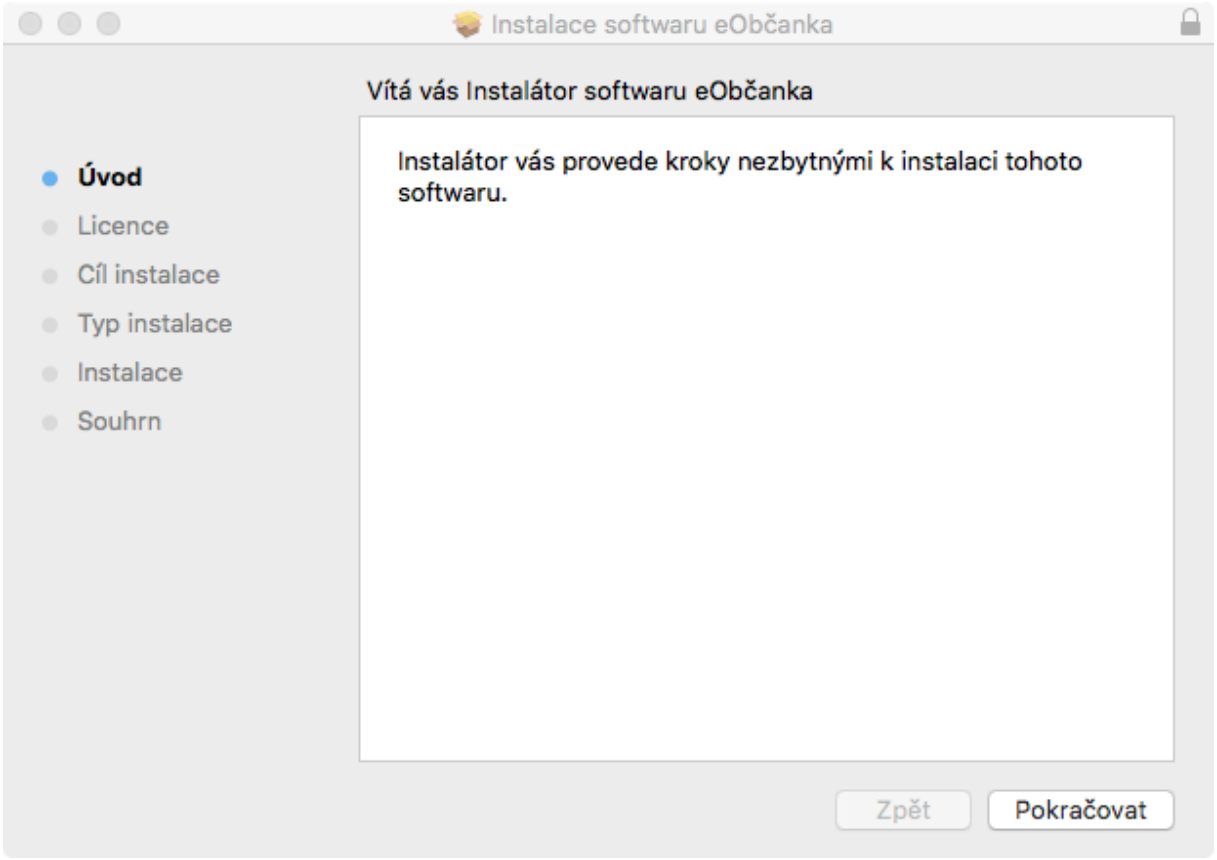


Obrázek 1: Připojení obrazu disku eObčanka

Uživatel musí v obrazu disku vybrat instalační soubor *eObcanka.pkg* a spustit jej.

4.3 Uvítací okno

Jako další krok se zobrazí okno instalačního průvodce software *eObčanka*:

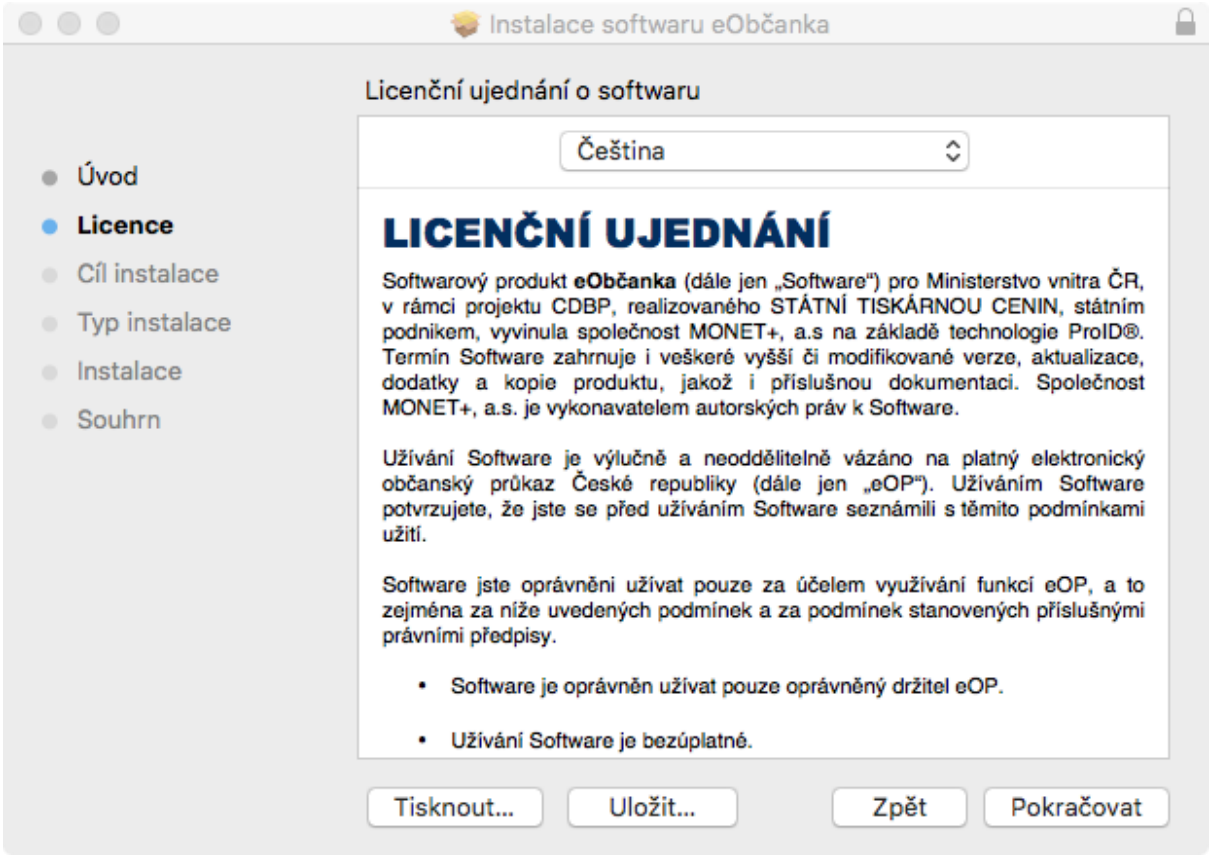


Obrázek 2: Uvítací okno instalačního průvodce eObčanka

Pro pokračování procesu instalace je třeba stisknout tlačítko *Pokračovat*.

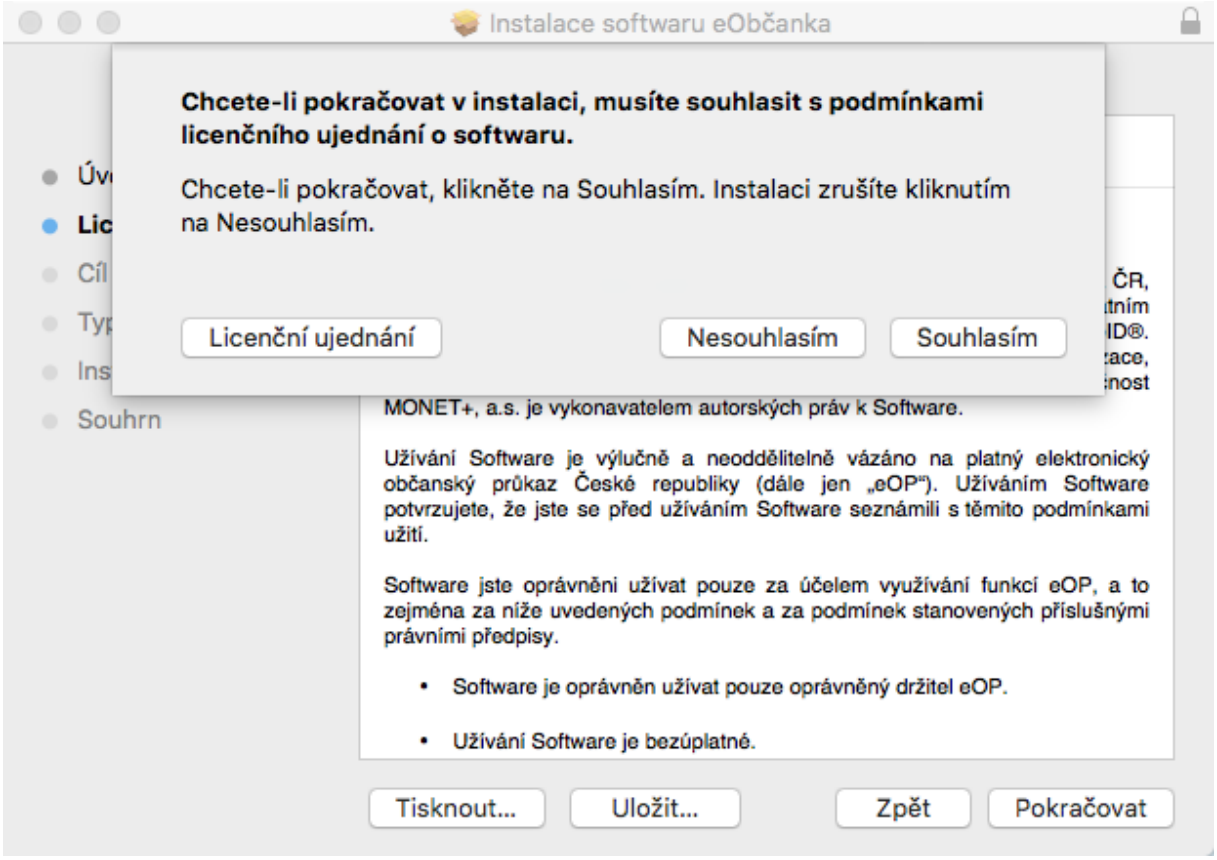
4.4 Licenční ujednání

V dalším okně se zobrazí text licenčního ujednání:



Obrázek 3: Okno s licenčním ujednání eObčanka

Text je třeba přečíst a pro pokračování procesu instalace stisknout tlačítko *Pokračovat*. Uživatel je vyzván k odsouhlasení licenčního ujednání. V případě souhlasu stiskne tlačítko *Souhlasím*, v opačném případě lze předčasně ukončit instalaci tlačítkem *Nesouhlasím.*



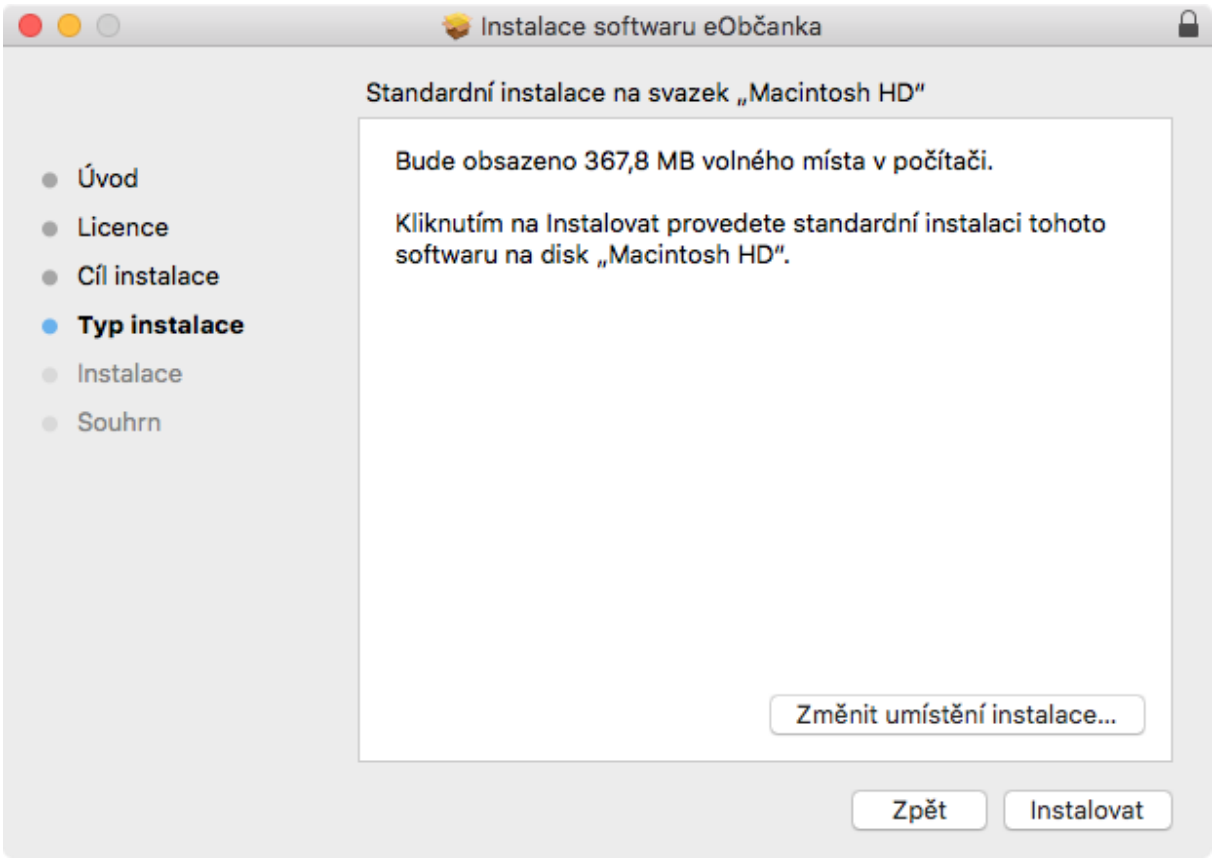
Obrázek 4: Souhlas s licenčním ujednáním software eObčanka

Pro **pokračování instalace** je třeba:

- **Stisknout** tlačítko *Pokračovat.*
- Udělit souhlas se zněním licenčního ujednání – **stisknutím tlačítka** *Souhlasím.*

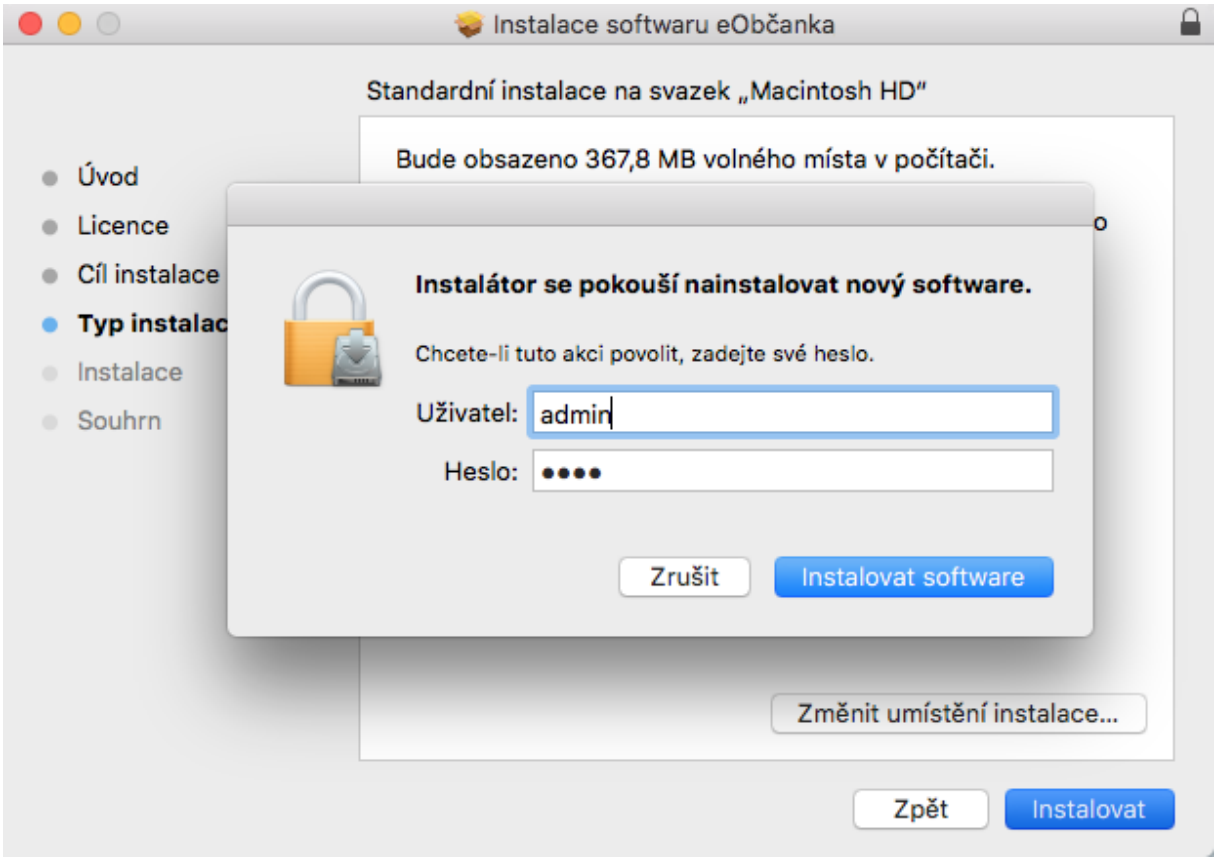
4.5 Průběh instalace

V dalším kroku spustí uživatel instalaci tlačítkem *Instalovat*:



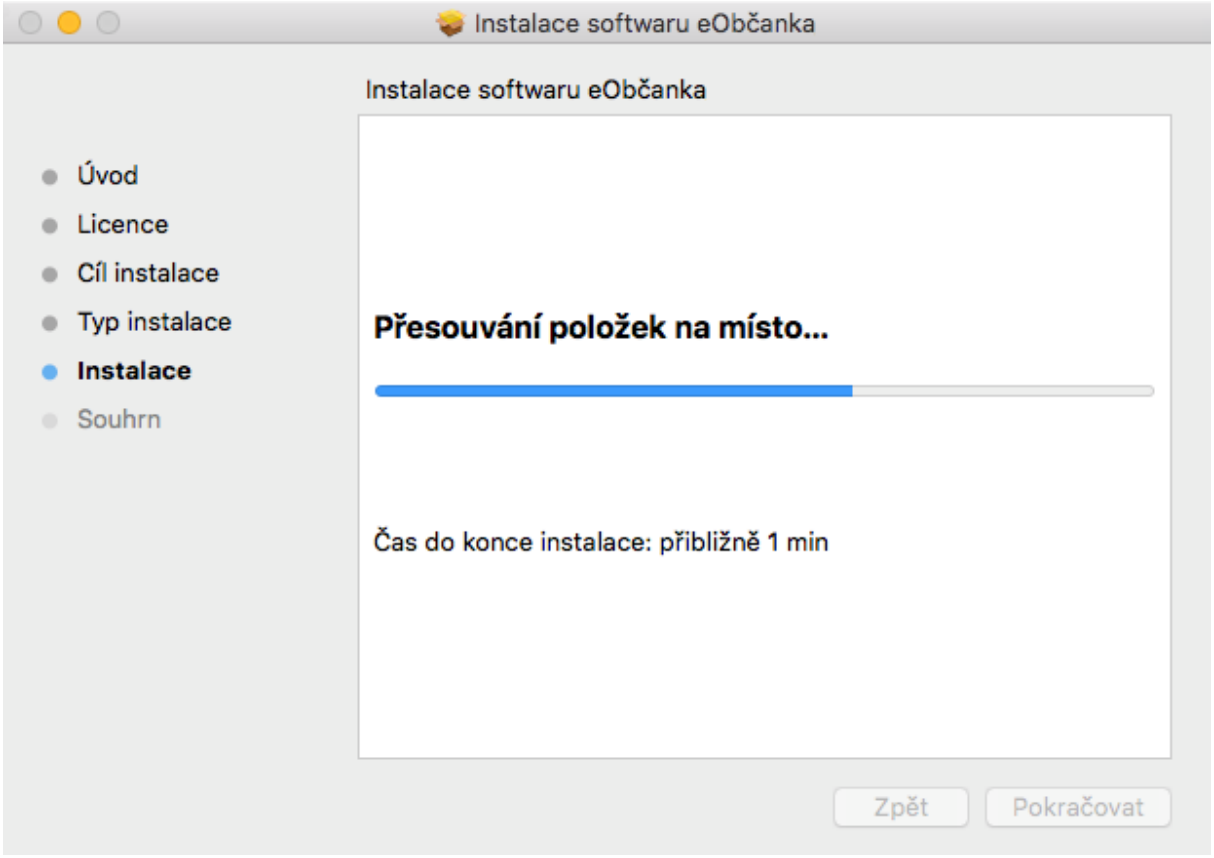
Obrázek 5: Okno pro spuštění procesu instalace

Upozornění: Instalační program musí být spuštěn pod uživatelským účtem s **oprávněním správce** operačního systému. Pokud je instalace spuštěna pod uživatelským účtem, který nemá správcovská oprávnění, zobrazí instalační průvodce okno operačního systému pro zvýšení (elevaci) uživatelských oprávnění. Neprivilegovaný uživatel může v tomto okně zadat jméno a heslo účtu správce a autorizovat tím následný proces instalace. Po dokončení instalace bude software *eObčanka* dostupný všem uživatelům počítače.



Obrázek 6: Okno elevace práv, pro schválení instalace účtem správce

Po spuštění se provede instalace souborů a konfigurace operačního systému. Proces instalace probíhá automaticky; je třeba počkat na dokončení procesu:



Obrázek 7: Průběh instalace software eObčanka

Instalační balíček automaticky provádí všechny potřebné kroky:

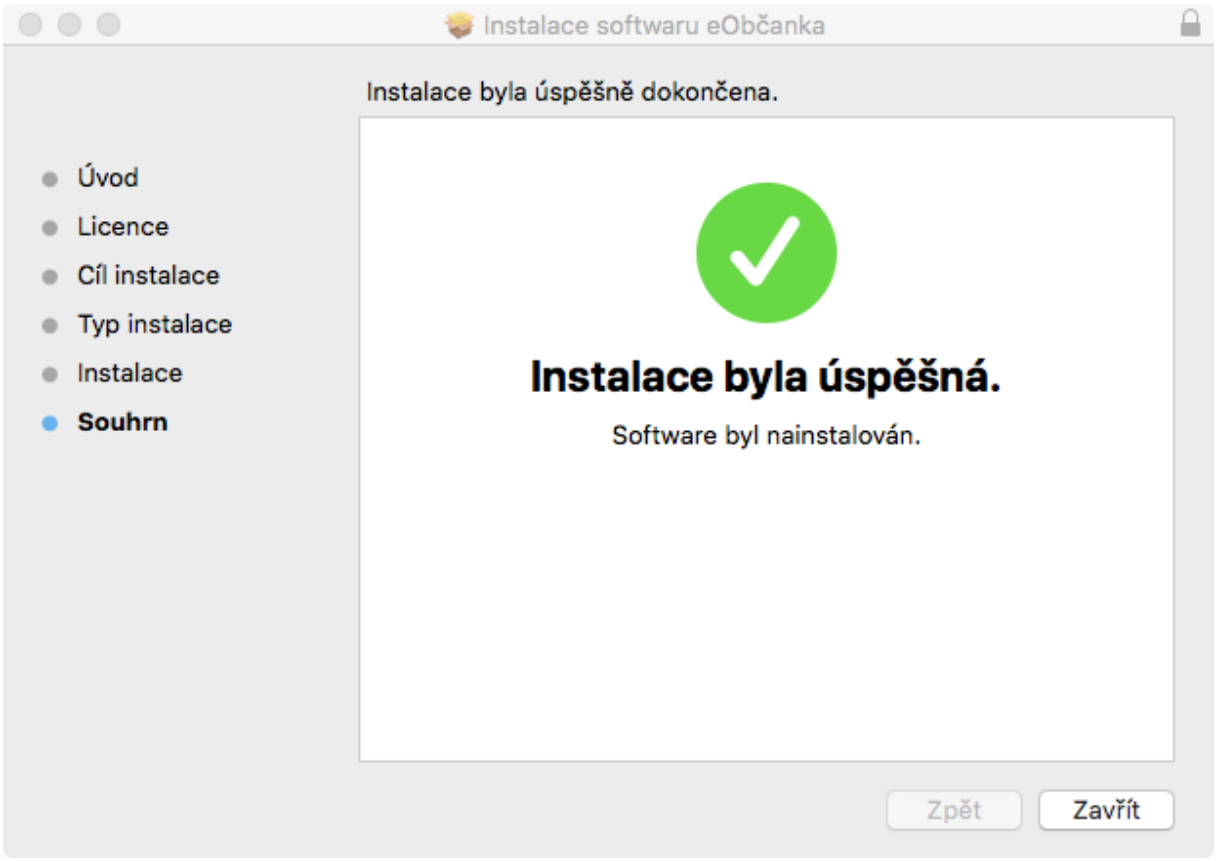
- Instaluje aplikační a konfigurační soubory.
- Provádí registraci aplikace.
- Instaluje aplikace do složky *Aplikace* (*/Applications*).

Během instalace může instalační průvodce vyžadovat povolení ke správě počítače, v takovém případě je potřeba povolení udělit. Instalační průvodce v tomto kroku registruje ovladače občanského průkazu (rozhraní CryptoTokenKit, případně tokenD – viz kapitola 7.1).

Obrázek 8: Průběh instalace software eObčanka - povolení ke správě

4.6 Dokončení instalace

Po dokončení instalace zobrazí instalační průvodce informaci o výsledku:



Obrázek 9: Okno s informací o dokončení instalace software eObčanka

Uvedeným krokem je **instalace** software *eObčanka* **dokončena**.

Spustitelné aplikace jsou po instalaci dostupné v obvyklé složce Aplikace (/Applications):

- *eObčanka – Identifikace*,
- *eObčanka - Správce karty*.

Okno instalačního průvodce lze zavřít tlačítkem *Zavřít*.

4.7 Po dokončení instalace

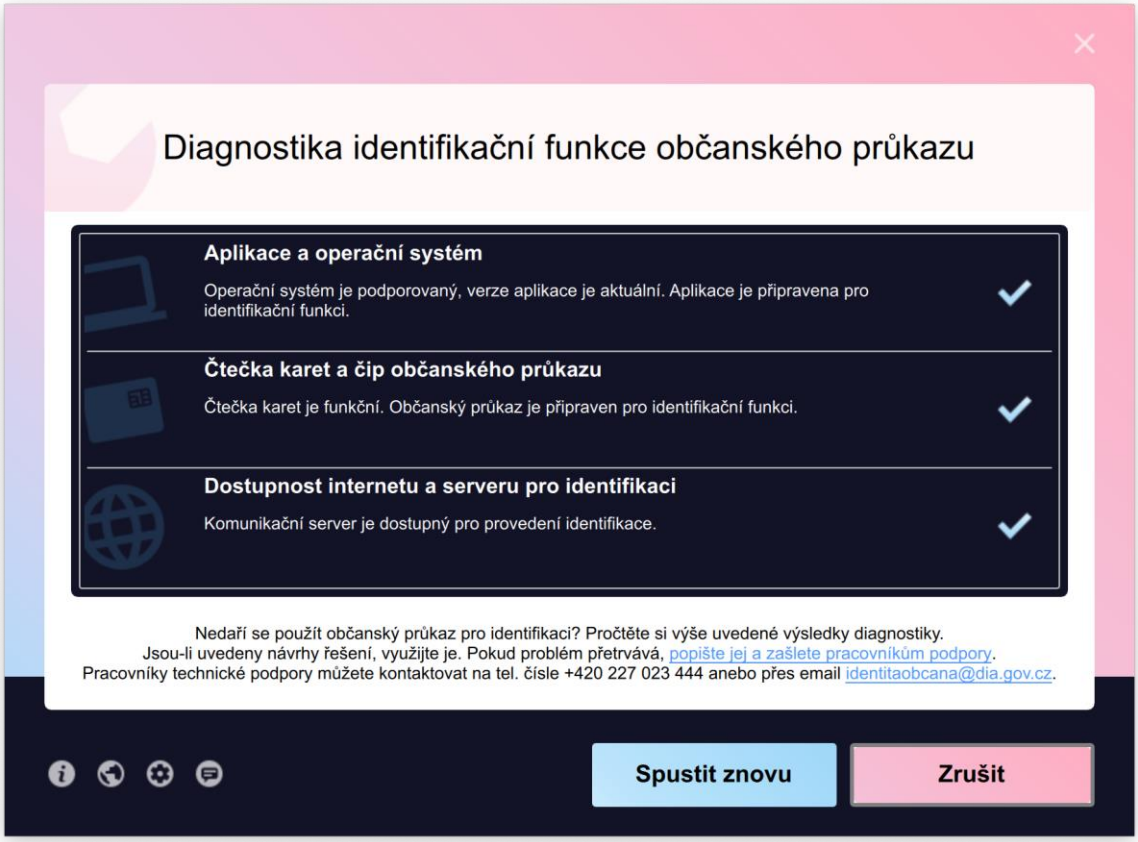
Po dokončení instalace je doporučeno provést kontrolu instalace pomocí aplikace *eObčanka - Identifikace* viz. kapitola 5.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

5 OVĚŘENÍ INSTALACE

Úspěšnost instalace se nejsnáze ověří spuštěním aplikace *eObčanka - Identifikace*. Pro spuštění je třeba ve složce *Aplikace* (*/Applications*) vyhledat aplikaci *eObčanka – Identifikace* a spustit ji.

Po spuštění aplikace *eObčanka - Identifikace* započne aplikace automaticky shromažďovat diagnostické informace; jejich výsledky pak zobrazí do okna:



Obrázek 10: Okno diagnostiky aplikace eObčanka - Identifikace

Pokud jsou všechny **tři položky označeny jako úspěšné**, pak **instalace** software *eObčanka* **proběhla správně** a uživatelé PC mohou používat elektronické funkce občanského průkazu.

Pokud k počítači není připojena čtečka, nebo do ní není vložen občanský průkaz, skončí prostřední položka upozorněním. V takovém případě se doporučuje připojit k počítači čtečku, vložit občanský průkaz a spustit diagnostiku znovu - tlačítkem *Spustit znovu*.

Pokud diagnostika nalezne potíže, měl by si uživatel **přečíst nabízené návrhy řešení a pokusit se pomocí nich odstranit problém**. Pokud se problém nepodaří vyřešit, může se uživatel obrátit na pracovníky technické podpory. Pro kontakt s pracovníky podpory je nejvhodnější využít formulář, integrovaný do aplikace *eObčanka - Identifikace*.

Podrobněji jsou diagnostické funkce popsány v uživatelské příručce aplikace *eObčanka - Identifikace*.

6 ČTEČKY

Software *eObčanka* komunikuje s čipem občanského průkazu prostřednictvím čtečky čipových karet. Bez čtečky čipových karet není možné používat elektronické funkce občanského průkazu. Uživatel tedy musí:

- získat vhodnou čtečku karet,
- připojit čtečku k počítači,
- popř. instalovat ovladače čtečky.

6.1 Výběr čtečky

K počítači s operačním systémem macOS je třeba pořídit a připojit čtečku, která je v souladu se standardem CCID a spolupracuje s PC/SC subsystémem operačního systému.

Software *eObčanka* umí spolupracovat:

- jak s běžnými čtečkami (bez integrované klávesnice);
- tak i se čtečkami, které mají vlastní klávesnici, popř. i displej.

Informace, podle kterých kritérií lze vybrat vhodnou čtečku pro PC, jsou uvedeny na webové stránce podpory občanských průkazů.

6.2 Ovladač čtečky

Čtečka karet, jako každé zařízení připojené k PC, musí mít v operačním systému instalován příslušný ovladač. Pokud správný ovladač instalován není, operační systém se čtečkou neumí komunikovat a čtečka pak nefunguje.

Upozornění: **Ovladače čteček nejsou součástí instalačního balíčku *eObčanka*.** Zprovoznění čtečky (včetně případné instalace ovladačů) je třeba provést samostatně - mimo instalaci software *eObčanka*.

Některé čtečky (Plug&Play) *nevyžadují* instalaci ovladačů, resp. si operační systém nalezne a instaluje potřebné ovladače sám. U jiných čteček je třeba ovladač instalovat samostatně. Pro instalaci ovladačů se vyžaduje privilegované oprávnění - ovladače může instalovat jen uživatel s oprávněním správce operačního systému.

Prodejce či dodavatel čtečky by měl uživatele informovat, zda je třeba (do daného operačního systému) ovladače instalovat. Pokud je instalace nutná, měl by prodejce či dodavatel dát k dispozici instalační balíček s ovladači čtečky. Uživatel pak musí zajistit instalaci ovladačů.

6.2.1 Ověření funkčnosti ovladače čtečky

V operačním systému macOS je funkčnost čteček závislá na službě *PC/SC Lite*. Tato služba je standardní součástí operačního systému.

Funkčnost čtečky lze ověřit například příkazem *pcsctest*, spuštěným z terminálu příkazové řádky. Program vypíše všechny připojené čtečky a vyzve uživatele k výběru čtečky, která bude testována. Následně je uživatel vyzván k vložení karty do požadované čtečky. Proběhne první část testu a uživatel je znovu vyzván k výběru testované čtečky. Po skončení testu aplikace

zobrazí výsledný status. Uživatel by měl během testu vidět ATR karty (*Current Reader ATR Value*) a název čtečky (*Current Reader Name*).

```
MUSCLE PC/SC Lite Test Program

Testing SCardEstablishContext    : Command successful.
Testing SCardGetStatusChange
Please insert a working reader   : Command successful.
Testing SCardListReaders         : Command successful.
Reader 01: Gemalto PC Twin Reader
Enter the reader number          : 1
Waiting for card insertion
                                 : Command successful.
Testing SCardConnect             : Command successful.
Testing SCardStatus              : Command successful.
Current Reader Name              : Gemalto PC Twin Reader
Current Reader State             : 0x54
Current Reader Protocol          : 0x0
Current Reader ATR Size          : 19 (0x13)
Current Reader ATR Value         : 3B 7E 94 00 00 80 25 D2 03 10 01 00 56 00 00 00 02 02 00
Testing SCardDisconnect          : Command successful.
Testing SCardReleaseContext      : Command successful.
Testing SCardEstablishContext    : Command successful.
Testing SCardGetStatusChange
Please insert a working reader   : Command successful.
Testing SCardListReaders         : Command successful.
Reader 01: Gemalto PC Twin Reader
Enter the reader number          : 1
Waiting for card insertion
                                 : Command successful.
Testing SCardConnect             : Command successful.
Testing SCardStatus              : Command successful.
Current Reader Name              : Gemalto PC Twin Reader
Current Reader State             : 0x54
Current Reader Protocol          : 0x0
Current Reader ATR Size          : 19 (0x13)
Current Reader ATR Value         : 3B 7E 94 00 00 80 25 D2 03 10 01 00 56 00 00 00 02 02 00
Testing SCardDisconnect          : Command successful.
Testing SCardReleaseContext      : Command successful.

PC/SC Test Completed Successfully !
```

Obrázek 11: Ověření funkčnosti čtečky pomocí pcsctest

Po úspěšném dokončení testu by se měla vypsat informace: *PC/SC Test Completed Sucessfully!*

6.3 Připojení čtečky

Čtečku je nutno připojit k počítači prostřednictvím konektoru daného typu čtečky. Nejběžnější čtečky se dodávají s USB kabelem. Tyto čtečky je třeba připojit do volného USB portu počítače. USB čtečky jsou napájeny přímo pomocí USB portu počítače a tak je lze po instalaci ovladačů ihned používat.

USB kabel čtečky není vhodné prodlužovat pomocí prodlužovacích USB kabelů, z důvodu poklesu napájení.

7 INTEGRACE INSTALOVANÉHO SOFTWARE

Identifikační aplikace je po dokončení instalace software eObčanka **plně funkční** a není třeba je dále nijak konfigurovat. Při identifikační operaci je třeba jen povolit spuštění aplikace z webového prohlížeče – viz kapitola 7.5.

Naproti tomu, pro práci s **elektronickými certifikáty** je třeba do operačního systému, resp. do používaných aplikací, **nutno integrovat ovladače** občanského průkazu. Ovladače jsou součástí instalace – je třeba je propojit s aplikacemi. Postup integrace ovladačů do operačního systému a do aplikací je popsán v následujících podkapitolách.

7.1 Typy ovladačů občanského průkazu

Součástí instalace eObčanky jsou i ovladače čipu občanského průkazu pro práci s certifikáty. Jsou instalovány ovladače:

- **CryptoTokenKit -** ovladač je určen pro práci s certifikáty v nativních aplikacích macOS (např.: Mail, Safari apod…). Tento ovladač je automaticky instalován na novější verze macOS (od verze 10.14).
- **tokenD** – starší verze ovladače, používaná nativními aplikace macOS (např.: Klíčenka, Mail, Safari apod…). Tento ovladač je automaticky instalován na starší verze macOS (do verze 10.13.6).
- **PKCS#11** - ovladač pro aplikace, které se nespoléhají na kryptografické funkce macOS, ale implementují vlastní kryptografii (např. Firefox, Thunderbird, apod…).

7.1.1 CryptoTokenKit

Ovladač CryptoTokenKit je možné (v závislosti na typu certifikátu) využít ke třem základním operacím:

- Přihlášení / autentizace (Safari, LoginWindow, PKINIT, SSH, Screensaver)
- Podpis (Mail)
- Šifrování (Mail, Keychain Access)

Přihlášení (autentizace)

Operační systém podporuje ověřování pomocí čipových karet, vč. přihlášení certifikátem na webové stránky pomocí Safari.
macOS také podporuje ověřování pomocí protokolu Kerberos.

Digitální podpis a šifrování v aplikaci Mail

V aplikaci Mail (Pošta) může uživatel odesílat zprávy, které jsou digitálně podepsány a šifrovány. E-mailová adresa odesílatele se musí shodovat s e-mailem, uvedeným v certifikátu.

Ochrana dat Klíčenky

Hesla v Klíčence lze chránit pomocí kryptografických klíčů, uložených s certifikáty v občanském průkazu. Občanský průkaz lze využít k zabezpečení použití hesel z Klíčenky.

Hesla z Klíčenky lze použít po vložení občanského průkazu do čtečky a zadání PIN. Více o ochraně dat Klíčenky viz kapitola 7.2.

7.1.2 PKCS#11

Aplikace, které **nevyužívají kryptografické rozhraní operačního systému**, **komunikují přímo s knihovnou PKCS#11**. Aby tyto aplikace uměly pracovat s certifikáty v občanském průkazu, musí do nich uživatel konfigurovat správnou knihovnu PKCS#11 (někdy nazývanou též *Cryptoki*). Způsob konfigurace knihovny se pro jednotlivé aplikace liší, uživatel by měl najít správný způsob v technické dokumentaci dané aplikace.

Pro každou verzi občanského průkazu je určena jiná knihovna PKCS#11:

- Pro práci s občanským průkazem vydaným před 1. 7. 2018 slouží PKCS#11 knihovna uložená v souboru *libeopczep11.dylib*
- Pro práci s občanským průkazem vydaným po 1. 7. 2018 slouží PKCS#11 knihovna uložená v souboru *libeop2v1czep11.dylib*

Knihovny jsou umístěny v adresáři */usr/local/lib/eOPCZE/*

Aby byla konfigurace aplikací, které využívají rozhraní PKCS#11 maximálně zjednodušena, je součástí instalace i knihovna *libeopproxyp11.dylib*, která zajišťuje komunikaci s oběma verzemi občanských průkazů. Tento soubor se nachází stejně jako knihovny PKCS#11 v adresáři */usr/local/lib/eOPCZE/*

Postup konfigurace ovladače PKCS#11 do Firefox a dalších aplikací je popsán v kapitolách 7.3 a 7.4.

7.1.3 tokenD

Starší verze ovladače. V novějších verzích macOS je *tokenD* nahrazen ovladačem *CryptoTokenKit*.

Aplikace, které využívají ovladače přes tokenD, není třeba nijak konfigurovat. Operační systém sám zajistí, aby tyto aplikace uměly s občanským průkazem pracovat.

Certifikáty z občanského průkazu lze pomocí tokenD zobrazit v aplikaci Klíčenka (*Keychain Access*).

7.2 Integrace ovladače CryptoTokenKit

Operační systém macOS od verze 10.14 již nepodporuje rozhraní tokenD. Software eObčanka reaguje na změnu podporovaných ovladačů karet v macOS. V novějších verzích proto eObčanka instaluje ovladač CryptoTokenKit. Pomocí rozhraní CryptoTokenKit lze používat certifikáty z občanského průkazu v nativních aplikacích, jako jsou Mail, Safari, apod…

Z pohledu uživatele znamená přechod na CryptoTokenKit nové možnosti, ale také některá omezení:

- Pomocí kryptografického klíče z certifikátu lze zašifrovat data Klíčenky (*Keychain Access*). Po zašifrování lze občanským průkazem schválit bezpečné použití dat Klíčenky – např. pro přihlášení do operačního systému. Více o ochraně Klíčenky v kapitole 7.2.1.

Pro aktivaci ochrany Klíčenky je třeba spárovat občanský průkaz s operačním systémem – viz kapitola 7.2.2.

- Uživatel nemůže zvolit, který certifikát má být použit v nativních aplikacích, např. pro elektronický podpis e-mailu.
  (Původní ovladač tokenD umožňoval volbu certifikátu v Klíčence.)
- V Klíčence nelze zobrazit seznam certifikátů, uložených v čipové kartě. (Klíčenka takovou možnost nabízela pro starší ovladač tokenD.)
  Obsah čipu občanského průkazu lze zobrazit pomocí aplikace *eObčanka – Správce karty*, viz také kapitola 2.1.2. Pro technické zobrazení obsahu čipu lze použít také terminálový příkaz: *system_profiler SPSmartCardsDataType:*
  `$ system_profiler SPSmartCardsDataType`

7.2.1 Ochrana dat Klíčenky pomocí občanského průkazu

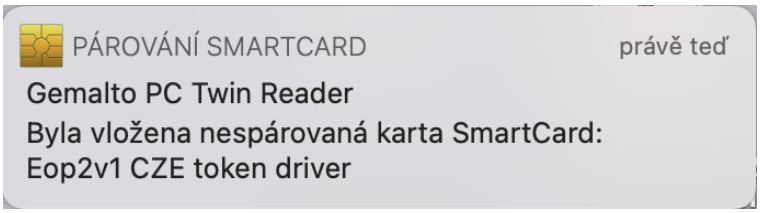
Uživatel, který má v občanském průkazu uložen *komerční* certifikát, může použít občanský průkaz k zabezpečení dat Klíčenky. Klíčem komerčního certifikátu může zašifrovat hesla v Klíčence. Následně může občanský průkaz využít pro schválení použití hesel z Klíčenky. Občanský průkaz pak uživatel může použít např. pro přihlášení do operačního systému nebo na webové stránky v Safari. Použití občanského průkazu pro přihlášení musí uživatel potvrdit zadáním PIN.

Technicky se data v Klíčence zašifrují veřejným klíčem zvoleného certifikátu. Před použitím dat z Klíčenky je třeba použít soukromý klíč (chráněný v čipu) pro dešifrování dat. Operaci se soukromým klíčem musí uživatel schválit pomocí PIN.

Pokud operační systém zjistí, že je v čipu občanského průkazu uložen vhodný certifikát s klíčem, automaticky nabídne možnost použití klíče pro ochranu dat Klíčenky. Po vložení občanského průkazu do čtečky se spustí proces párování občanského průkazu. V průběhu párování se zvolí klíč, jímž mají být chráněna data Klíčenky. Postup párování je popsán v kapitole 7.2.2.

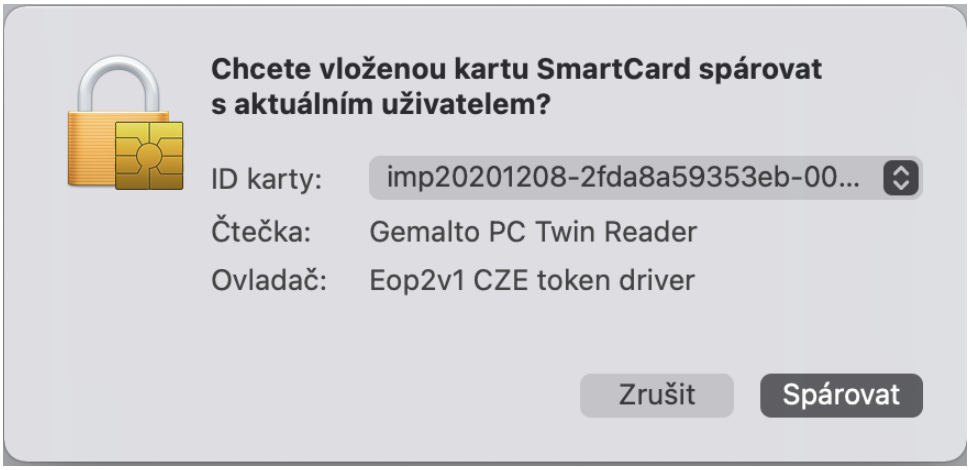
7.2.2 Párování občanského průkazu

Po vložení nespárovaného občanského průkazu do čtečky spustí operační systém automaticky proces párování:



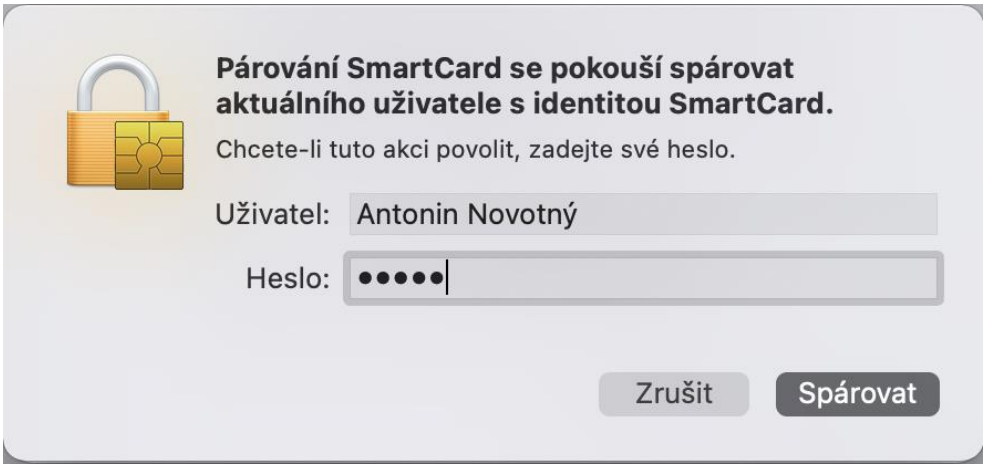
Obrázek 12: Okno s výzvou k párování občanského průkazu s účtem uživatele

Uživatel vybere v seznamu *ID karty* identifikátor klíče certifikátu, který si přeje spárovat se svým uživatelským účtem. Párování se potvrdí tlačítkem *Spárovat*:



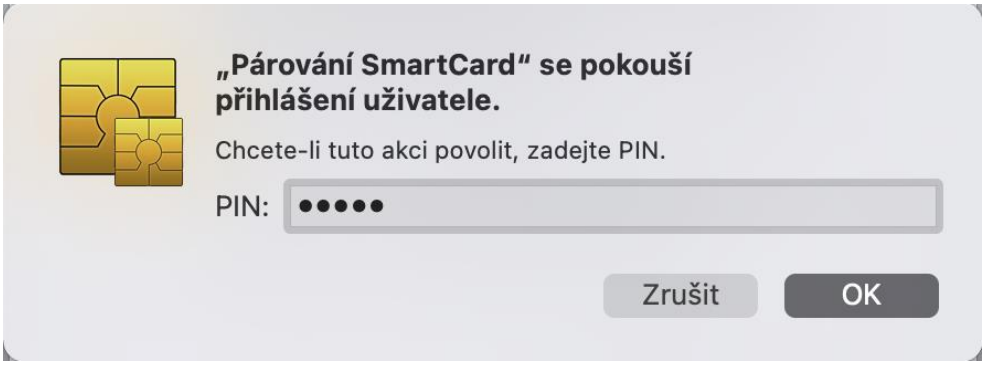
Obrázek 13: Potvrzení párování občanského průkazu s účtem uživatele

Kliknutím na *Spárovat* se páruje zvolený certifikát k účtu uživatele. Uživatel je vyzván k zadání hesla k uživatelskému účtu:



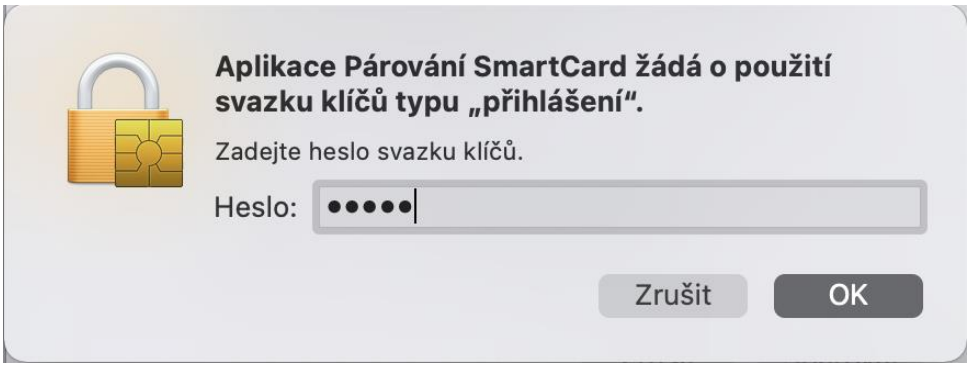
Obrázek 14: Zadání hesla pro schválení párování občanského průkazu

Po zadání hesla je uživatel vyzván k zadání hodnoty PIN občanského průkazu:



Obrázek 15: Potvrzení párování občanského průkazu s účtem uživatele

Po zadání platné hodnoty PIN je uživatel ještě jednou vyzván k zadání hesla k uživatelskému účtu:



Obrázek 16: Zadání hesla pro schválení párování občanského průkazu

Párování certifikátu na občanském průkazu je tímto krokem dokončeno. Párování neověřuje platnost certifikátu a je tak platné až do doby než jej uživatel nezruší.

Úspěšné spárování certifikátu lze ověřit příkazem *sc_auth list,* který se spustí v okně terminálu. Příkazem se zobrazí otisk (hash) identifikátoru klíče spárovaného certifikátu. Pokud je spárováno více certifikátů (z různých čipových karet), jsou zobrazeny všechny.

Příklad výpisu spárovaných certifikátů:

```
$ sc_auth list

Hash: 0B2BEA714EE563AAD60C33D5C7F82572AB26C2C7
```

Pokud chce uživatel zrušit spárování certifikátu, může použít příkaz *sc_auth unpair hash.* Zrušit párování je vhodné například v okamžiku, kdy dojde k expiraci spárovaného certifikátu a je potřeba spárovat certifikát nový.

```
$ sc_auth unpair 0B2BEA714EE563AAD60C33D5C7F82572AB26C2C7
```

7.2.3 Další informace k párování občanského průkazu

Spárováním občanského průkazu nevzniká *povinnost* používat občanský průkaz při každém přístupu k datům Klíčenky. Pokud není občanský průkaz vložen do čtečky, použijí se hesla z Klíčenky stejně, jako když uživatel vůbec žádnou kartu nespároval. Také do operačního systému se lze vždy přihlásit heslem.

Párování se nabízí pouze v případě, že je v čipu uložen *komerční* certifikát s klíčem. Klíče *komerčního* certifikátu lze použít pro šifrovací operace. Pokud je v čipu nalezen pouze certifikát pro *elektronický podpis*, pak se párování ani ochrana dat Klíčenky nenabízejí. Klíč podpisového certifikátu nelze používat pro šifrování.

Uživatel může párování občanského průkazu odmítnout. V takovém případě operační systém opakovaně vyzývá k párování při každém vložení občanského průkazu.

Operační systém nekontroluje platnost certifikátu, jehož klíčem jsou chráněna data Klíčenky. Ochrana dat Klíčenky funguje i po vypršení platnosti certifikátu.

S uživatelským účtem je možné spárovat vždy jen jeden certifikát, resp. klíč z občanského průkazu. Pokud je v čipu uloženo více použitelných certifikátů, musí uživatel při párování zvolit, který má být použit pro ochranu dat Klíčenky. Po úspěšném spárování již operační systém neupozorňuje na možnost párování.

Uživatel má možnost vypnout výzvu k párování, pomocí příkazu *sc_auth pairing_ui -s disable*:

```
$ sc_auth pairing_ui -s disable
```

Tento příkaz trvale vypne výzvu k párování pro všechny čipové karty (nejen pro občanský průkaz).

Aktivaci/deaktivaci párování lze ověřit příkazem *sc_auth pairing_ui -s status*:

```
$ sc_auth pairing_ui -s status
```

Deaktivované párování lze znovu aktivovat příkazem *sc_auth pairing_ui -s enable:*

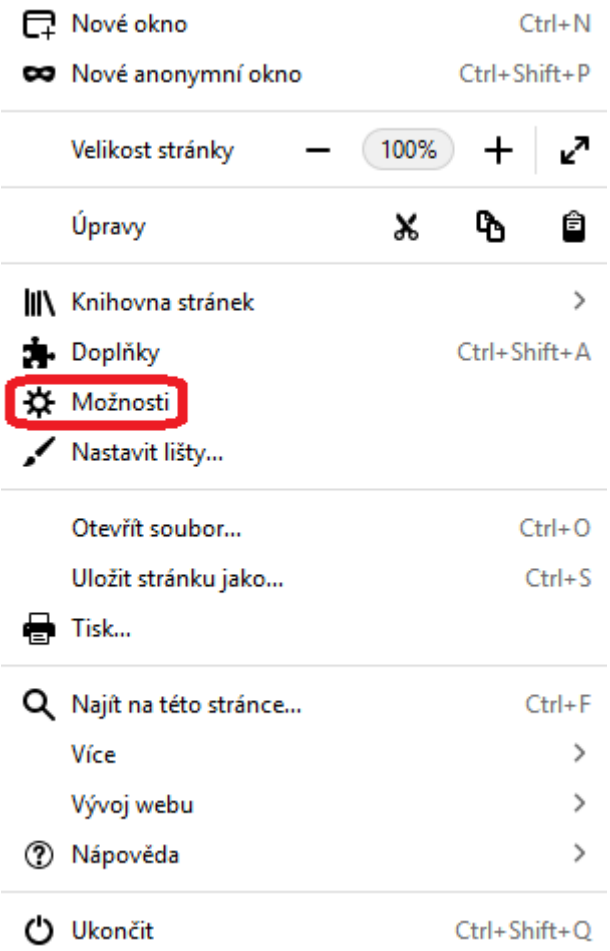
```
$ sc_auth pairing_ui -s enable
```

Data Klíčenky lze zašifrovat pomocí několika klíčů - z různých čipových karet. Před použitím dat z Klíčenky pak operační systém detekuje vloženou kartu a použije dostupný klíč pro zpřístupnění dat Klíčenky.

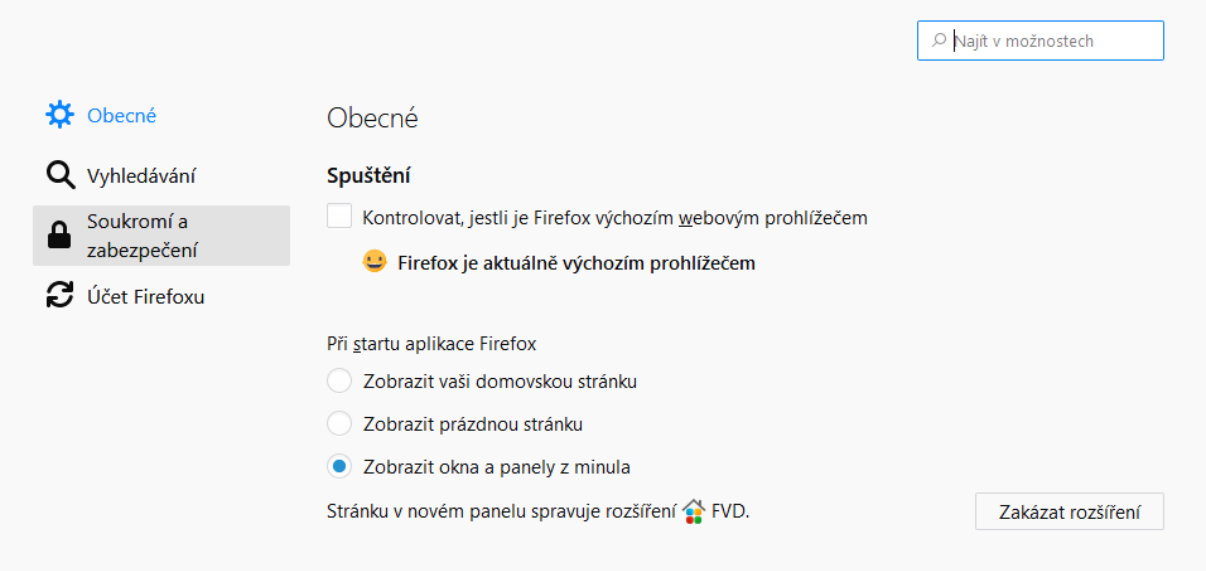
7.3 Integrace PKCS#11 do Mozilla Firefox

Pro ilustraci je v tomto dokumentu uvedena integrace ovladače občanského průkazu do aplikace Mozilla Firefox. Firefox je asi nejznámější a nejčastěji používanou aplikací, která využívá kryptografické rozhraní PKCS#11.

Do aplikace Firefox lze ovladač občanského průkazu přidat pomocí menu *Bezpečnostní zařízení* v nabídce *Možnosti → Soukromí a zabezpečení → Bezpečnostní zařízení.*

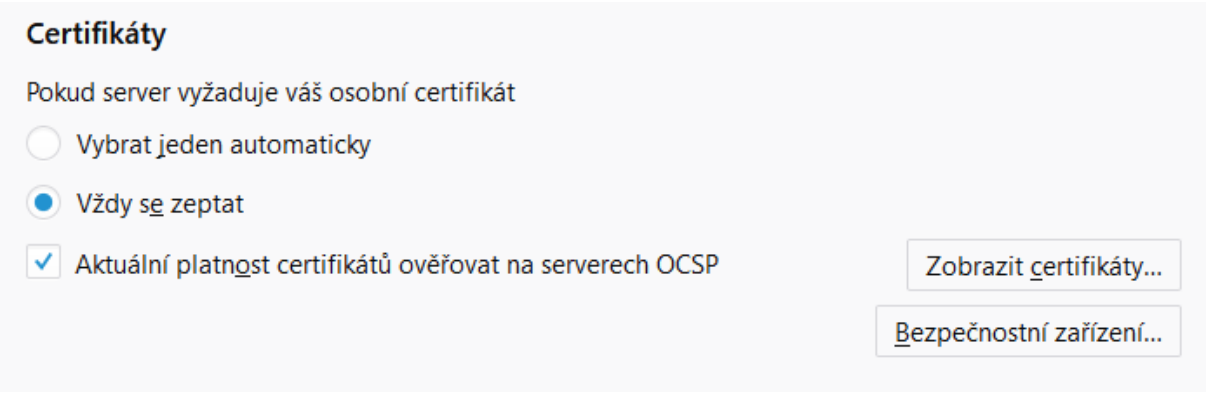


Obrázek 17: Menu aplikace Mozilla Firefox



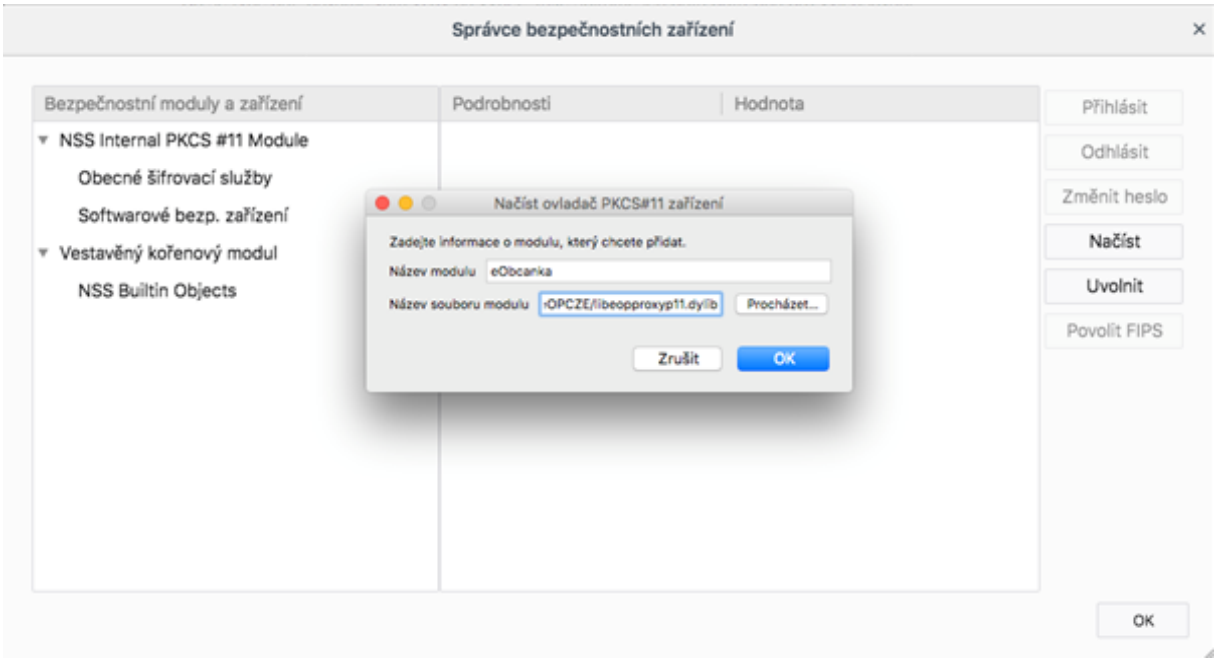
Obrázek 18: Okno pro nastavení Mozilla Firefox

V sekci *Certifikáty* je třeba stisknout tlačítko *Bezpečnostní zařízení*.



Obrázek 19: Nastavení zabezpečení v Mozilla Firefox

Zobrazí se okno *Správce bezpečnostních zařízení*. V tomto okně je třeba přidat nové bezpečnostní zařízení: občanský průkaz. Přidání se provede stiskem tlačítka *Načíst*, zobrazí se okno pro nalezení ovladače občanského průkazu:



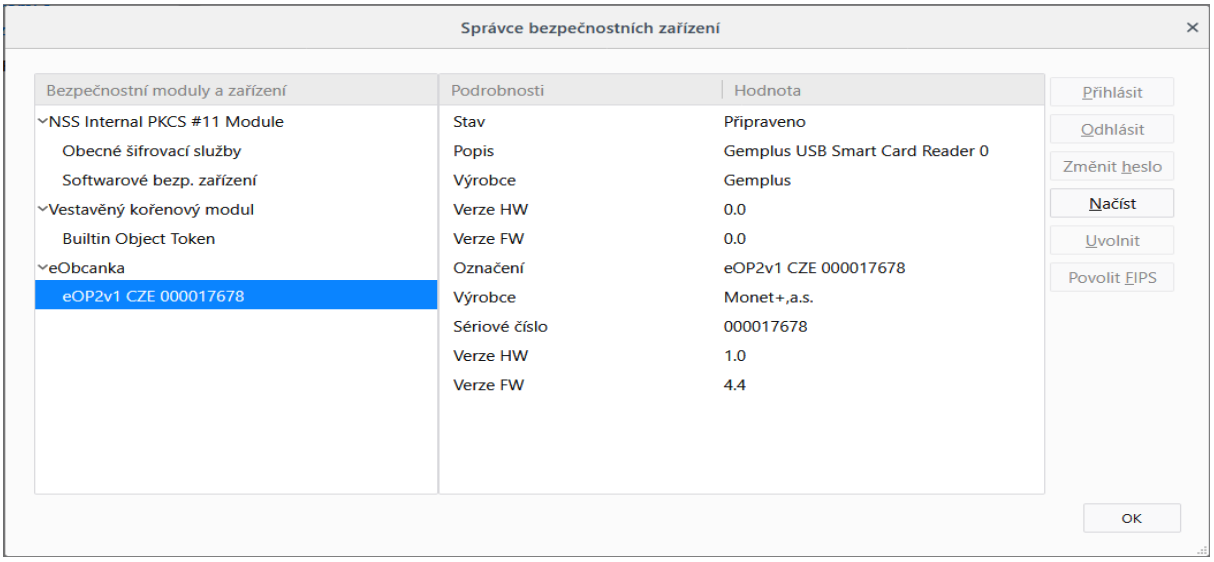
Obrázek 20: Přidání ovladače občanského průkazu do Mozilla Firefox

V okně *Nový ovladač PKCS#11 zařízení* je třeba:

1. Nastavit název modulu - libovolný, např. *eObcanka* nebo *Občanský průkaz.*
2. Uvést cestu k modulu *libeopproxyp11.dylib*

   Typicky */usr/local/lib/eOPCZE/libeopproxyp11.dylib*
3. Uložit nastavení tlačítkem *OK.*

Po stisku tlačítka *OK* se Firefox pokusí načíst zadaný modul ovladače. Po úspěšném načtení modulu zobrazí aplikace Firefox informace o připojené čtečce čipových karet případně informace o vloženém občanském průkazu:



Obrázek 21: Okno Mozilla Firefox se seznamem bezpečnostních modulů

Neúspěšné načtení knihovny je indikováno chybovým hlášením: *Nepodařilo se přidat modul.* Pokud se modul nepodaří přidat, měl by se uživatel ujistit, že při přidání uvedl správnou cestu a že se na uvedené cestě opravdu nachází soubor *libeopproxyp11.dylib*

7.4 Integrace PKCS#11 do dalších aplikací

Pokud uživatel používá jiné aplikace s kryptografickým rozhraním PKCS#11, je třeba do nich použití občanského průkazu konfigurovat způsobem, uvedeným v dokumentaci dané aplikace. Konfigurace se obvykle provádí tak, že se do příslušné konfigurační položky uvede cesta ke knihovně *libeopproxyp11.dylib* občanského průkazu.

7.5 Integrace identifikační funkce do webových prohlížečů

K provedení elektronické identifikace občanským průkazem slouží aplikace *eObčanka - Identifikace*. V průběhu identifikace tuto aplikaci spouští operační systém, na žádost webového prohlížeče, který uživatel používá pro přihlášení k webovým stránkám.

Aby bylo možné aplikaci *eObčanka - Identifikace* spustit z webové stránky, musí být aplikace registrována do operačního systému. Registraci automaticky zajistí instalační průvodce software *eObčanka* - uživatel nemusí pro registraci nic dělat.

Registrace zajistí spouštění aplikace *eObčanka - Identifikace* ze všech běžně používaných webových prohlížečů: např. Safari, Google Chrome, nebo Mozilla Firefox.

Při prvním provedení identifikace občanským průkazem se webový prohlížeč obvykle dotazuje uživatele, zda souhlasí se spuštěním aplikace *eObčanka - Identifikace*. Kromě udělení souhlasu může uživatel uvést, že se prohlížeč příště nemá dotazovat a má spouštět aplikaci *eObčanka - Identifikace* automaticky.

Více informací o ovládání a použití aplikace *eObčanka - Identifikace* jsou uvedeny v uživatelské příručce aplikace.

8 INSTALACE NOVĚJŠÍ VERZE

Pokud je k dispozici novější verze software *eObčanka*, měl by být na uživatelském počítači proveden upgrade. Nová verze může opravovat chyby a nabízet vylepšené funkce či ovládání.

Dostupnost nové uživateli nejčastěji oznámí aplikace *eObčanka - Identifikace* v průběhu přihlašování občanským průkazem. Uživatel také může dostupnost nové verze zkontrolovat na webových stránkách pro podporu občanského průkazu.

Aktualizace software *eObčanka* probíhá obdobným způsobem jako prvotní instalace:

- instalační balíček je nutné stáhnout z internetových stránek,
- spustit jej,
- řídit se pokyny instalačního průvodce.

Postup instalace je popsán v kapitole 4.

Upozornění: Stejně jako prvotní instalace, i aktualizace aplikace eObčanka musí být spuštěna pod uživatelským účtem s **oprávněním správce** operačního systému. Pokud je instalace spuštěna pod uživatelským účtem, který nemá správcovská oprávnění, zobrazí instalační průvodce v průběhu instalace okno operačního systému pro zvýšení (elevaci) uživatelských oprávnění. Neprivilegovaný uživatel může v tomto okně zadat jméno a heslo účtu správce a autorizovat tím následný proces instalace.

Aktualizace software *eObčanka* probíhá stejně jako prvotní instalace – viz kapitola 4.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

9 ODINSTALACE

Na operačních systémech macOS není automatická odinstalace aplikací běžně nabízena. Uživatel má možnost odstranit aplikace eObčanka přesunutím aplikačních adresářů ze složky *Aplikace* (*/Applications*) do koše. Jde o tyto aplikace, resp. aplikační adresáře:

Aplikace	Aplikační adresář
eObčanka – Identifikace	/Applications/Identifikace_eOP.app
eObčanka – Správce karty	/Applications/eObčanka – Správce karty.app
CryptoTokenKit	/Applications/CryptoTokenKit_eOP/Eop2v1CzeTokenApp.app /Applications/CryptoTokenKit_eOP/EopCzeTokenApp.app

Aplikace eObčanka ke svému běhu využívá řadu dalších souborů, které jsou instalovány do systémových adresářů a nejsou tak běžným uživatelům standardně dostupné. Jedná se o soubory uživatelských konfigurací, souborů s provozními záznamy a systémových komponent.

Na rozdíl od aplikačních adresářů, které je možné smazat běžným způsobem, je nutné u těchto adresářů a souborů použít elevaci oprávnění pomocí příkazu *sudo.* Seznam všech instalovaných adresářů a souborů je uveden níže:

Adresáře:

- /usr/local/lib/eOPCZE/
- /opt/eObcanka/
- ~/.config/eObcanka/
- ~/.eObcanka_logs/

Soubory:

- /usr/local/etc/crplus/eop2v1cze.cfg
- /usr/local/etc/crplus/eop2v1cze.tokend.cfg
- /usr/local/etc/crplus/eopcze.cfg
- /usr/local/etc/crplus/eopcze.tokend.cfg
- /usr/local/etc/crplus/eopproxy.cfg
- /usr/local/etc/crplus/sa2v1czep11.cfg
- /Library/Security/tokend/eOP2v1Cze.tokend
- /Library/Security/tokend/eOPCze.tokend

Pokud uživatel vymaže uvedený seznam souborů a adresářů, dosáhne tím odstranění software eObčanka. Software *eObčanka* lze do počítače kdykoli znovu instalovat.

Ovladače čteček nejsou součástí instalačního balíčku *eObčanka*. Odinstalaci čtečky je třeba provést samostatně, dle pokynů výrobce.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

10 OVĚŘENÍ INTEGRITY A PŮVODU INSTALAČNÍHO BALÍČKU

Uživatel by si před instalací software měl vždy ověřit, že daný software pochází z důvěryhodného zdroje a že s obsahem balíčku nikdo nemanipuloval. Instalací nedůvěryhodného či modifikovaného software hrozí riziko, že se do počítače dostane např. počítačový virus či jiný škodlivý software.

V případě software eObčanka lze ověřit integritu i původ dvěma způsoby:

- **Ověřením elektronického podpisu instalačního balíčku**.
  Ověření elektronického podpisu provádí operační systém macOS před instalací **automaticky**. Pokud by instalační balíček nebyl podepsán důvěryhodným certifikátem (resp. příslušným klíčem), operační systém zobrazí varování a neumožní, popř. nedoporučí instalaci provést.
- Stažením instalačního balíčku výhradně z webových stránek pro podporu software eObčanka a porovnáním otisku instalačního balíčku.

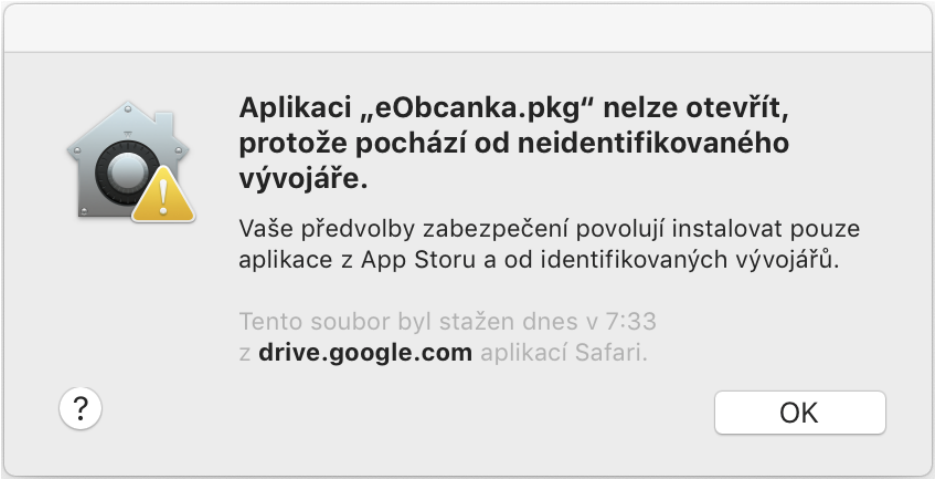
Po ověření elektronického podpisu, resp. otisku instalačního balíčku může uživatel důvěřovat tomu, že používá originální balíček eObčanka, který neobsahuje škodlivý software.

10.1 Ověření elektronického podpisu instalačního balíčku

Instalační balíček eObčanka pro macOS je vždy podepsán pomocí certifikátu, určeného pro elektronické podepisování instalačních balíčků macOS (*Developer ID Installer certificate*). Certifikát je vydán z certifikační autority společnost Apple, které operační systém macOS důvěřuje - je schopen ověřit důvěryhodnost certifikátu. Držitelem podpisového certifikátu je Ministerstvo vnitra ČR, které software eObčanka předává k distribuci.

Kromě elektronického podpisu prochází instalační balíček eObčanky také bezpečnostní kontrolou - procesem tzv. *notarizace*. Notarizaci provádí společnost Apple. Notarizované moduly jsou operačním systémem rozpoznávány jako od “známého vývojáře”. Pokud by instalované moduly nebyly notarizovány pak by je Gatekeeper operačního systému odmítnul instalovat.

Před započetím instalace operační systém automaticky ověří, zda aplikace pochází od známého vývojáře a zda je podpis balíčku vytvořen pomocí důvěryhodného certifikátu.
Pokud by původ či podpis nebyl důvěryhodný, zobrazí operační systém varování:
Aplikaci “eObcanka.pkg” nelze otevřít, protože pochází od neidentifikovaného vývojáře.
Uživatel by v takovém případě neměl pokračovat v instalaci. Měl by si stáhnout aktuální verzi instalačního balíčku a zahájit instalaci znovu.



Obrázek 22: Varování operačního systému, že instalovaný balíček je nedůvěryhodný

Uživatel si může - před instalací software eObčanka - důvěryhodnost podpisu prověřit pomocí příkazu *pkgutil --check-signature*.

```
pkgutil --check-signature /Volumes/eObcanka/eObcanka.pkg
Package "eObcanka.pkg":
   Status: signed by a certificate trusted by Mac OS X
   Certificate Chain:
    1. Developer ID Installer: MINISTERSTVO VNITRA (6UDP4A9V2U)
       SHA1 fingerprint: AA 8B 0F 91 5C 47 D5 5C A4 D1 BD A4 CC 13 F6 35 4C 2E 49 9E
       ------------------------------------------------------------------------
    2. Developer ID Certification Authority
       SHA1 fingerprint: 3B 16 6C 3B 7D C4 B7 51 C9 FE 2A FA B9 13 56 41 E3 88 E1 86
       ------------------------------------------------------------------------
    3. Apple Root CA
       SHA1 fingerprint: 61 1E 5B 66 2C 59 3A 08 FF 58 D1 4A E2 24 52 D1 98 DF 6C 60
```

Obrázek 23: Výpis programu pkgutil při ověřování podpisu instalačního balíčku

Pokud je elektronický podpis instalačního balíčku takto ověřen, pak instalační balíček pochází z důvěryhodného zdroje a lze jej bez obav použít pro instalaci software eObčanka.

10.2 Porovnání otisku instalačního balíčku

Na operačním systému macOS lze vypočítat hodnotu otisku souboru pomocí programu *openssl*. Pro výpočet SHA-1 otisku lze v příkazové řádce zadat: *openssl dgst -sha1 <cesta_k_inst_souboru>*
kde *<cesta_k_inst_souboru>* je cesta k souboru s instalačním balíčkem *eObcanka.dmg*.

Příklad výpočtu otisku SHA-256:
V adresáři se souborem instalačního balíčku lze v příkazovém řádku zadat:
openssl dgst -sha256 eObcanka.dmg
Hodnota otisku se vypíše jako:

SHA256(eObcanka.dmg)=
7f4be5f316b805261e0feb3791abc40fd1aea87596f661b442a70cc651dff499