ProID

Inštalácia softvéru ProID+ pre macOS

Inštalačná príručka

Predkladá MONET+,a.s.
Za Dvorem 505, Zlín - Štípa
Spracovanie: 23. 9. 2021
Verzia číslo: 1.1

1 VYHLÁSENIE O AUTORSTVE

Informácie v tomto dokumente obsiahnuté (t. j. vrátane nákresov, mapiek, obrázkov atď.) sú predmetom obchodného tajomstva (podľa §504 Zákona č. 89/2012 Sb. v platnom znení) spoločnosti MONET+,a.s., IČO 26217783 a dispozícia s nimi podlieha právnemu poriadku Českej republiky.
Spoločnosť MONET+,a.s., IČO 26217783 je podľa „zákona č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů“, v znení neskorších predpisov, vykonávateľom majetkových práv k príslušným častiam tohto dokumentu.

2 OBSAH

3 ÚVOD

Na používanie elektronických funkcií v prostredí macOS je potrebné na počítač nainštalovať software ProID+.

Aktuálna verzia balíčka inštaluje podporu pre karty ProID+, ProID+Q, ProID+NG a ProID+QSeal.

Tento dokument popisuje spôsob inštalácie softvéru *ProID+* do počítača s operačným systémom macOS.

Softvér sa inštaluje pomocou inštalačného balíčka typu PKG, ktorý slúži ako grafický sprievodca inštaláciou.

4 INŠTALOVANÝ SOFTVÉR

Softvérový balíček ProID+ obsahuje kompletnú podporu elektronických funkcií pre macOS. Po úspešnej inštalácii budú mať užívatelia počítača dostupné všetky softvérové aplikácie, ktoré sú pre karty ProID na macOS ponúkané.

Súčasťou inštalovaného balíčka ProID+ je niekoľko samostatných softvérových aplikácií, ktoré pracujú s čipom kariet ProID. Ide o:

» Ovládače čipu (PKCS#11, CryptoTokenKit, tokenD) kariet ProID+, ProID+NG, ProID+Q a ProID+QSeal na prácu s certifikátmi a vytváranie elektronických podpisov.

» Aplikáciu CardManProID.app (ďalej len Správca karty ProID) na správu certifikátov a prístupových kódov kariet.

V nasledujúcich podkapitolách je stručne popísaná charakteristika jednotlivých inštalovaných aplikácií.

4.1 SPRÁVCA KARTY PROID

Správca karty ProID je aplikácia na spravovanie užívateľských certifikátov a prístupových kódov kariet ProID.

Pomocou Správcu karty ProID užívateľ môže napr.:

» Zobraziť zoznam kryptografických kľúčov v čipe.

» Zobraziť informácie o certifikátoch v čipe.

» Importovať alebo zmazať certifikát.

» Nastaviť, odblokovať alebo zmeniť niektorý z prístupových kódov (PUK, PIN,...).

» Diagnostikovať problémy s čítačkou, čipom, certifikátmi, ...

4.2 OVLÁDAČE ČIPU

Na prácu s elektronickými certifikátmi je nutné do operačného systému nainštalovať kryptografické ovládače.

Ovládače kariet ProID umožňujú aplikáciám pracovať s certifikátmi, uloženými v čipe kariet. Prostredníctvom ovládačov sa dajú certifikáty (a kľúče) používať na:

» elektronické podpisovanie (dokumentov, e-mailov, a pod.);

» prihlasovanie (napr. do webových stránok).

Ovládače ale slúžia tiež na **správu certifikátov** v čipe:

» Čítanie informácií o uložených certifikátoch.

» Vytváranie alebo zápis nových certifikátov a kryptografických kľúčov.

» Mazanie nepotrebných certifikátov a kľúčov.

Ďalšou dôležitou funkciou ovládačov je práca s **prístupovými kódmi**:

» zobrazovanie okna na zadanie kódu;

» kontrola hodnoty kódu s čipom;

» zmena hodnoty kódu;

- zablokovanie kódu po opakovanom chybnom zadaní;
- atď.

Ovládače dodržiavajú uznávané technické štandardy pre integráciu čipových kariet do operačných systémov macOS:

- **CryptoTokenKit -** ovládač je určený na prácu s certifikátmi v natívnych aplikáciách macOS (napr.: Mail, Safari a pod.).
- **tokenD** – staršia verzia ovládača, používaná natívnymi aplikáciami macOS (napr.: Kľúčenka, Mail, Safari a pod.). Tento ovládač je možné inštalovať na staršie verzie macOS (do verzie 10.15).
- **PKCS#11** - ovládač k aplikáciám, ktoré sa nespoliehajú na kryptografické funkcie macOS, ale implementujú vlastnú kryptografiu (napr. Firefox, Thunderbird, a pod.).

5 PRED ZAHÁJENÍM INŠTALÁCIE

Inštaláciu softvéru *ProID+* je potrebné vykonať v týchto krokoch:

- Stiahnuť inštalačný balíček
  - pozri kapitolu 5.2.
- Spustiť inštalačný balíček
  - pod účtom správcu operačného systému,
  - pozri kapitolu 6.1.
- Vykonať všetky kroky inštalácie
  - grafický inštalačný sprievodca užívateľa priebežne inštruuje,
  - pozri kapitolu 6.

5.1 STAV POČÍTAČA PRED ZAHÁJENÍM INŠTALÁCIE

Operačný systém nemusí byť na vykonanie inštalácie špeciálne upravovaný. Všetko potrebné zaistí inštalačný sprievodca softvéru *ProID+*.

Na samotnú inštaláciu softvéru *ProID+* nie je nutné byť pripojený na internet. Pripojenie na internet je potrebné len na stiahnutie inštalačného balíčka.

Na inštaláciu softvéru *ProID+* nie je nutné mať k počítaču pripojenú čítačku a nainštalované ovládače čítačiek. Inštaláciu čítačky kariet je možné vykonať až po inštalácii softvéru *ProID+*. Napriek tomu možno odporučiť, aby bola **čítačka nainštalovaná pred inštaláciou softvéru *ProID+***.

Inštaláciu softvéru *ProID+* je potrebné spúšťať pod užívateľským účtom, ktorý má **oprávnenie správcu** operačného systému. Ak užívateľ nemá k dispozícii uvedené oprávnenie, mal by sa obrátiť na správcu operačného systému a požiadať ho o vykonanie inštalácie.

Pred spustením inštalácie sa odporúča uložiť rozpracovanú činnosť a ukončiť bežiace aplikácie. Inštalačný sprievodca vyžaduje po dokončení inštalácie reštartovanie operačného systému.

5.2 STIAHNUTIE INŠTALAČNÉHO BALÍČKA

Inštalácia aplikácie *ProID* sa vykonáva pomocou inštalačného balíčka. **Súbor s inštalačným programom je uložený vo forme diskového obrazu (DMG) a je potrebné ho stiahnuť z internetu**, z webových stránok na podporu kariet ProID.

V samotnom obraze disku (DMG) je uložený grafický inštalačný balíček vo formáte PKG, ktorý prevedie užívateľa procesom inštalácie.

Pri sťahovaní inštalačného balíčka by si užívateľ mal všímať, do ktorého adresára sa stiahnutý súbor uloží - aby potom z tohto adresára mohol inštalačný program spustiť.

Pomocou inštalačného balíčka je možné vykonať ako *prvotnú* inštaláciu, tak *upgrade* softvéru *ProID+*. Užívateľ, ktorý má nainštalovanú staršiu verziu, si môže stiahnuť aktuálnu verziu a spustiť inštaláciu - nastane upgrade na novšiu verziu.

5.3 OVERENIE PÔVODU INŠTALAČNÉHO BALÍČKA

Užívateľ by si pred inštaláciou softvéru mal vždy overiť, že daný softvér pochádza z dôveryhodného zdroja a že s obsahom balíčka nikto nemanipuloval. Pri inštalácii nedôveryhodného či modifikovaného softvéru hrozí riziko, že sa do počítača dostane napr. počítačový vírus alebo iný škodlivý softvér.

Inštalačný balíček ProID+ je elektronicky podpísaný pomocou certifikátu Monet+,a.s. Operačný systém macOS pred inštaláciou automaticky overuje elektronický podpis inštalačného balíčka. Ak by inštalačný balíček nebol podpísaný dôveryhodným certifikátom (resp. príslušným kľúčom), operačný systém neumožní inštaláciu vykonať.

Po overení elektronického podpisu inštalačného balíčka môže užívateľ dôverovať tomu, že používa originálny balíček ProID+, ktorý neobsahuje škodlivý softvér.

Viac o overení integrity a pôvodu inštalačného balíčka v kapitole 11.

6 SPUSTENIE A VYKONANIE INŠTALÁCIE

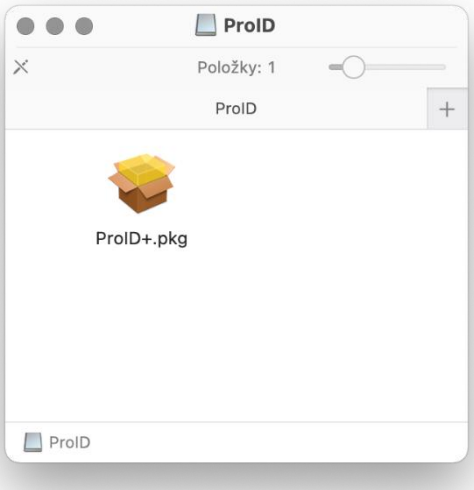
Inštalácia ovládacieho softvéru *ProID+* sa vykonáva pomocou **grafického inštalačného sprievodcu**, uloženého v stiahnutom diskovom obraze.
Grafický inštalačný sprievodca riadi priebeh inštalácie a je koncipovaný tak, aby čo najviac uľahčil prácu bežného užívateľa.

6.1 SPUSTENIE INŠTALÁCIE

Inštalácia sa odštartuje spustením inštalačného programu, stiahnutého z internetových stránok podpory ProID. Užívateľ stiahne obraz disku vo formáte DMG a z neho spustí inštalačný program uložený v súbore *ProID+.pkg*

6.2 PRIPOJENIE OBRAZU DISKU

Po spustení DMG obrazu disku sa automaticky prejde na pripojenie obrazu. Operačný systém následne automaticky zobrazí jeho obsah.



Obrázok 1: Pripojenie obrazu disku

Užívateľ musí v obraze disku vybrať inštalačný súbor *ProID+.pkg* a spustiť ho.

6.3 UVÍTACIE OKNO

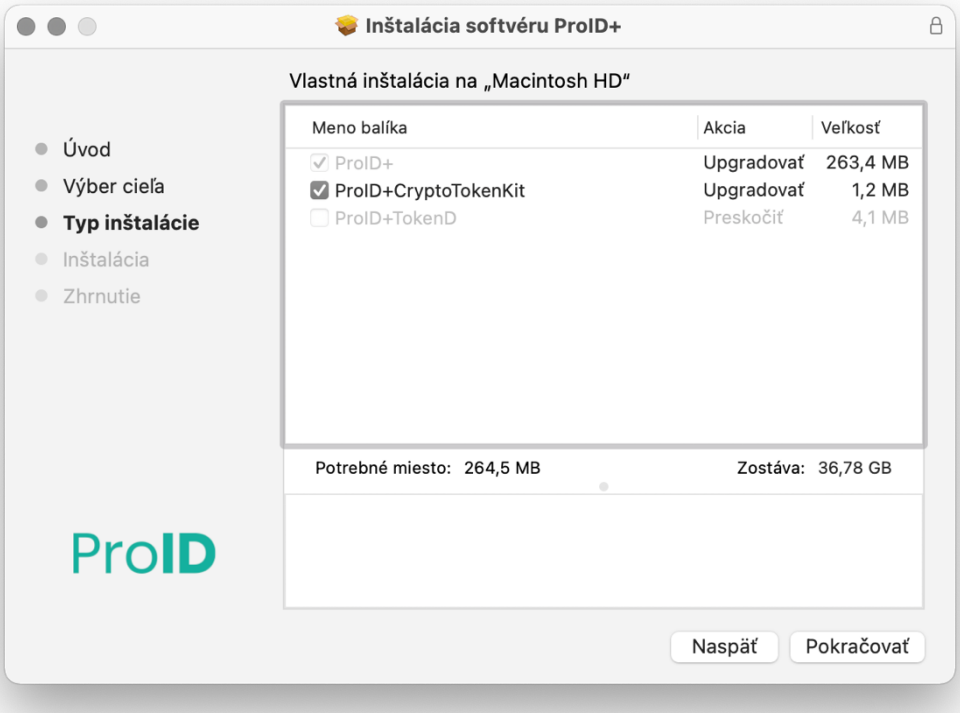
Ako ďalší krok sa zobrazí okno inštalačného sprievodcu softvéru *ProID+*:

Obrázok 2: Uvítacie okno inštalačného sprievodcu ProID+

Na pokračovanie v procese inštalácie je potrebné stlačiť tlačidlo *Pokračovať*.

6.4 TYP INŠTALÁCIE

V ďalšom okne sa zobrazia možnosti vlastnej inštalácie:



Obrázok 3: Okno s možnosťami inštalácie

V tomto okne je možné zmeniť bežne inštalovaný ovládač CryptoTokenKit na ovládač tokenD.

» Ovládač CryptoTokenKit je možné nainštalovať na operačné systémy macOS 10.13.5 a vyššie.

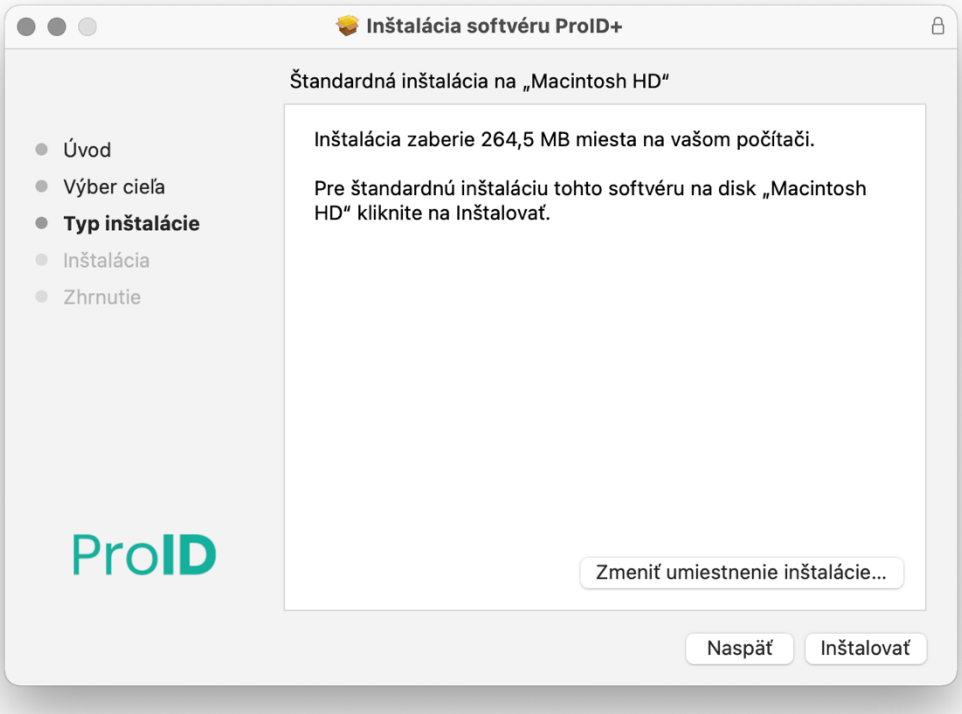
» Ovládač tokenD je možné nainštalovať na operačné systémy macOS 10.15 alebo staršie.

Vždy je možné inštalovať iba jeden typ ovládača. Viac o ovládačoch kariet ProID je uvedené v kapitole 8.1.

Na pokračovanie v procese inštalácie je potrebné stlačiť tlačidlo *Pokračovať*.

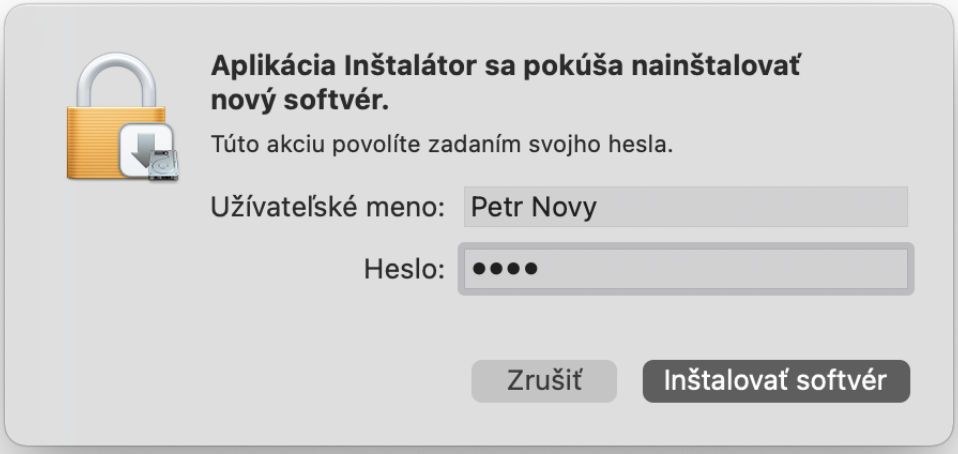
6.5 PRIEBEH INŠTALÁCIE

V ďalšom kroku spustí užívateľ inštaláciu tlačidlom *Inštalovať*:



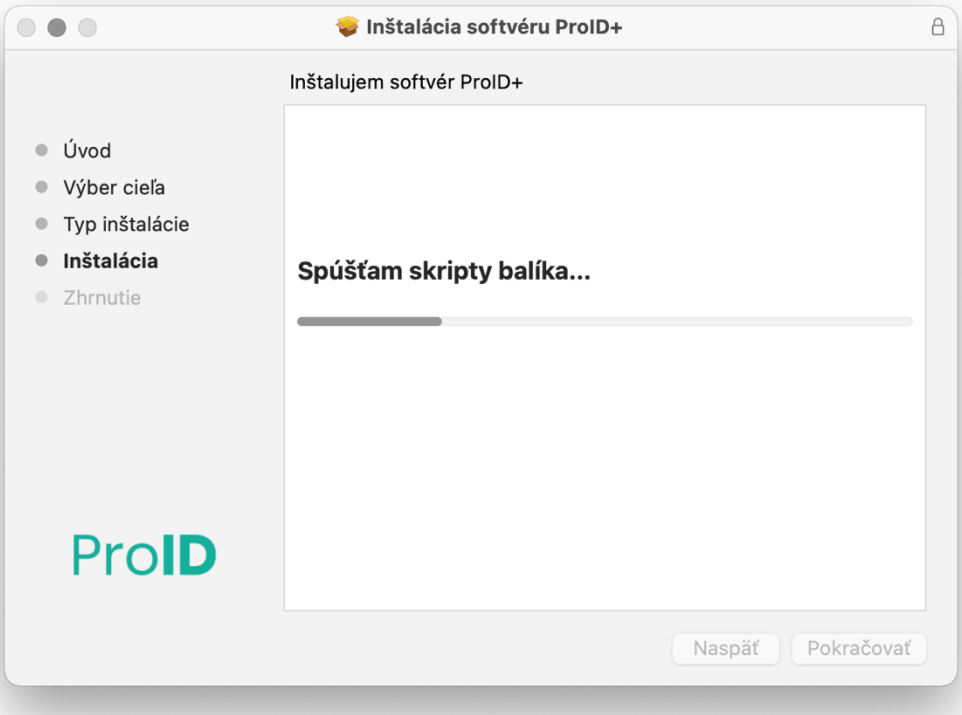
Obrázok 4: Okno na spustenie procesu inštalácie

Upozornenie: Inštalačný program musí byť spustený pod užívateľským účtom s **oprávnením správcu** operačného systému. Ak je inštalácia spustená pod užívateľským účtom, ktorý nemá správcovské oprávnenie, zobrazí inštalačný sprievodca okno operačného systému na zvýšenie (eleváciu) užívateľských oprávnení. Neprivilegovaný užívateľ môže v tomto okne zadať meno a heslo účtu správcu a autorizovať tým následný proces inštalácie. Po dokončení inštalácie bude softvér *ProID+* dostupný všetkým užívateľom počítača.



Obrázok 5: Okno elevácie práv, na schválenie inštalácie účtom správcu

Po spustení sa vykoná inštalácia súborov a konfigurácia operačného systému. Proces inštalácie prebieha automaticky; je potrebné počkať na dokončenie procesu:



Obrázok 6: Priebeh inštalácie softvéru ProID+

Inštalačný balíček automaticky vykonáva všetky potrebné kroky:

» Inštaluje aplikačné a konfiguračné súbory.

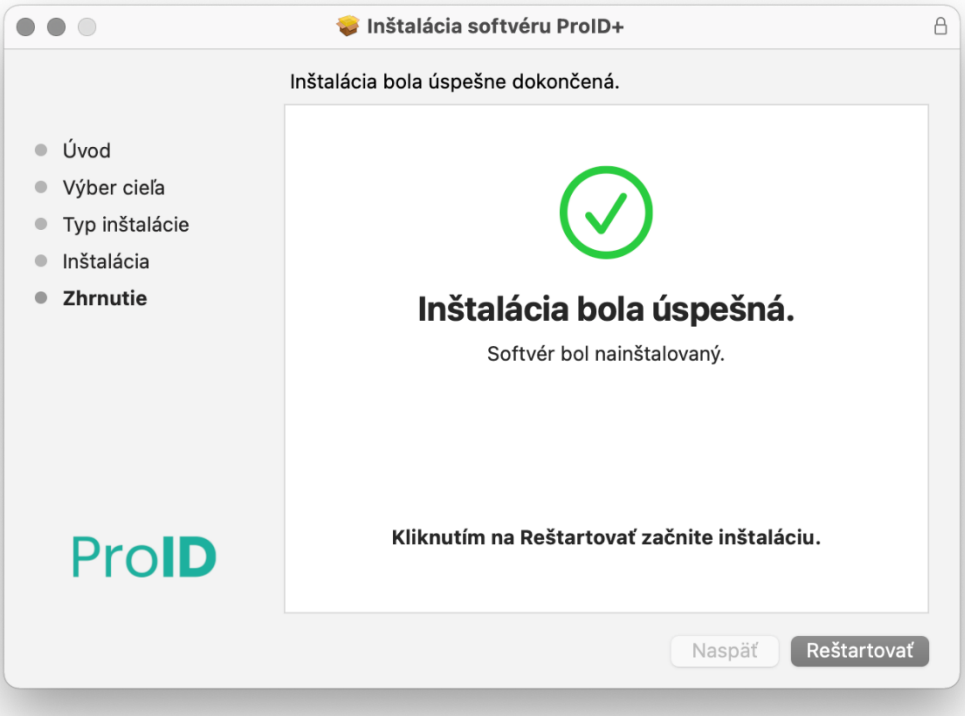
- Vykonáva registráciu aplikácie.
- Inštaluje aplikáciu do priečinka *Aplikácie* (*/Applications*).

Počas inštalácie môže inštalačný sprievodca vyžadovať povolenie na spravovanie počítača, v takomto prípade je potrebné povolenie udeliť. Inštalačný sprievodca v tomto kroku registruje ovládače kariet ProID (rozhranie CryptoTokenKit, prípadne tokenD).

Obrázok 7: Priebeh inštalácie softvéru ProID+ - povolenie na spravovanie

6.6 DOKONČENIE INŠTALÁCIE

Po dokončení inštalácie zobrazí inštalačný sprievodca informácie o výsledku:



Obrázok 8: Okno s informáciou o dokončení inštalácie softvéru ProID+

Na úspešné dokončenie inštalácie je teraz nutné operačný systém reštartovať.

Spustiteľná aplikácia Správca karty ProID je po inštalácii dostupná v obvyklom priečinku Aplikácie (/Applications):

» CardManProID.app.

Okno inštalačného sprievodcu je možné zavrieť a spustiť reštart počítača tlačidlom *Reštartovať*.

7 ČÍTAČKY

Softvér *ProID+* komunikuje s čipom kariet prostredníctvom čítačky čipových kariet. Bez čítačky čipových kariet nie je možné používať elektronické funkcie. Užívateľ teda musí:

» získať vhodnú čítačku kariet,

» pripojiť čítačku k počítaču,

» príp. nainštalovať ovládače čítačky.

7.1 VÝBER ČÍTAČKY

K počítaču s operačným systémom macOS je potrebné zaobstarať a pripojiť čítačku, ktorá je v súlade so štandardom CCID a spolupracuje s PC/SC subsystémom operačného systému.

Softvér *ProID+* vie spolupracovať:

» ako s bežnými čítačkami (bez integrovanej klávesnice);

» tak aj s čítačkami, ktoré majú vlastnú klávesnicu, príp. aj displej.

7.2 OVLÁDAČ ČÍTAČKY

Čítačka kariet, ako každé zariadenie pripojené k PC, musí mať v operačnom systéme nainštalovaný príslušný ovládač. Ak nie je nainštalovaný správny ovládač, operačný systém s čítačkou nedokáže komunikovať a čítačka potom nefunguje.

Upozornenie: **Ovládače čítačiek nie sú súčasťou inštalačného balíčka *ProID+*.** Spustenie čítačky (vrátane prípadnej inštalácie ovládačov) je potrebné vykonať samostatne - mimo inštalácie softvéru *ProID+*.

Niektoré čítačky (Plug&Play) *nevyžadujú* inštaláciu ovládačov, resp. si operačný systém nájde a nainštaluje potrebné ovládače sám. U iných čítačiek je potrebné ovládač inštalovať samostatne. Na inštaláciu ovládačov sa vyžaduje privilegované oprávnenie - ovládače môže inštalovať len užívateľ s oprávnením správcu operačného systému.

Predajca alebo dodávateľ čítačky by mal užívateľa informovať, či je potrebné (do daného operačného systému) ovládače inštalovať. Ak je inštalácia nutná, mal by predajca alebo dodávateľ dať k dispozícii inštalačný balíček s ovládačmi čítačky. Užívateľ potom musí zaistiť inštaláciu ovládačov.

7.2.1 Overenie funkčnosti ovládača čítačky

V operačnom systéme macOS je funkčnosť čítačiek závislá na službe *PC/SC Lite*. Táto služba je štandardnou súčasťou operačného systému.

Funkčnosť čítačky sa dá overiť napríklad príkazom *pcsctest*, spusteným z terminálu príkazového riadku. Program vypíše všetky pripojené čítačky a vyzve užívateľa vybrať čítačku, ktorá bude testovaná. Následne je užívateľ vyzvaný vložiť kartu do požadovanej čítačky. Prebehne prvá časť testu a užívateľ je znovu vyzvaný vybrať testovanú čítačku. Po skončení testu aplikácia zobrazí výsledný status. Užívateľ by mal počas testu vidieť ATR karty (*Current Reader ATR Value*) a názov čítačky (*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 !
```

Obrázok 9: Overenie funkčnosti čítačky pomocou pcsctest

Po úspešnom dokončení testu by sa mala vypísať informácia: *PC/SC Test Completed Sucessfully!*

7.3 PRIPOJENIE ČÍTAČKY

Čítačku je nutné pripojiť k počítaču prostredníctvom konektora daného typu čítačky. Najbežnejšie čítačky sa dodávajú s USB káblom. Tieto čítačky je potrebné pripojiť do voľného USB portu počítača. USB čítačky sú napájané priamo pomocou USB portu počítača, a tak je ich možné po inštalácii ovládačov ihneď používať.

USB kábel čítačky nie je vhodné predlžovať pomocou predlžovacích USB káblov, a to z dôvodu poklesu napájania.

8 INTEGRÁCIA INŠTALOVANÉHO SOFTVÉRU

Na prácu s **elektronickými certifikátmi** je do operačného systému, resp. do používaných aplikácií, **nutné integrovať ovládače** kariet ProID. Ovládače sú súčasťou inštalácie – je potrebné ich prepojiť s aplikáciami. Postup integrácie ovládačov do operačného systému a do aplikácií je popísaný v nasledujúcich podkapitolách.

8.1 TYPY OVLÁDAČOV KARIET PROID

Súčasťou inštalácie ProID+ sú aj ovládače čipu. Na prácu s certifikátmi sú inštalované ovládače:

- **CryptoTokenKit -** ovládač je určený na prácu s certifikátmi v natívnych aplikáciách macOS (napr.: Mail, Safari a pod.).
- **tokenD** – staršia verzia ovládača, používaná natívnymi aplikáciami macOS (napr.: Kľúčenka, Mail, Safari a pod.). Tento ovládač je možné nainštalovať na staršiu verziu macOS (do verzie 10.15).
- **PKCS#11** - ovládač na aplikácie, ktoré sa nespoliehajú na kryptografické funkcie macOS, ale implementujú vlastnú kryptografiu (napr. Firefox, Thunderbird a pod.).

8.1.1 CryptoTokenKit

Ovládač CryptoTokenKit je možné (v závislosti na type certifikátu) využiť na tri základné operácie:

- Prihlásenie / autentizácia (Safari, LoginWindow, PKINIT, SSH, Screensaver)
- Podpis (Mail)
- Šifrovanie (Mail, Keychain Access)

Prihlásenie (autentizácia)

Operačný systém podporuje overovanie pomocou čipových kariet, vrátane prihlásenia certifikátom na webové stránky pomocou Safari.
macOS tiež podporuje overovanie pomocou protokolu Kerberos.

Digitálny podpis a šifrovanie v aplikácii Mail

V aplikácii Mail (Pošta) môže užívateľ odosielať správy, ktoré sú digitálne podpísané a šifrované. E-mailová adresa odosielateľa sa musí zhodovať s e-mailom uvedeným v certifikáte.

Ochrana dát Kľúčenky

Heslá v Kľúčenke sa dajú chrániť pomocou kryptografických kľúčov, uložených s certifikátmi na kartách ProID. Karty ProID je možné využiť na zabezpečenie používania hesiel z Kľúčenky. Hesla z Kľúčenky sa dajú použiť po vložení karty ProID do čítačky a zadaní PIN.

8.1.2 PKCS#11

Aplikácie, ktoré **nevyužívajú kryptografické rozhranie operačného systému**, **komunikujú priamo s knižnicou PKCS#11**. Aby tieto aplikácie vedeli pracovať s certifikátmi na kartách ProID, musí do nich užívateľ nakonfigurovať správnu knižnicu PKCS#11 (niekedy nazývanú tiež *Cryptoki*). Spôsob konfigurácie knižnice sa u jednotlivých aplikácií líši, užívateľ by mal nájsť správny spôsob v technickej dokumentácii danej aplikácie.

Pre každý typ karty ProID je určená iná knižnica PKCS#11:

- Karta ProID+
  - Umiestnenie PKCS#11 knižnice /usr/local/lib/ProIDPlus/libproidcm11.dylib
- Karta ProID+Q

- Umiestnenie PKCS#11 knižnice /usr/local/lib/ProIDPlus/libproidqcm11.dylib

- Karta ProID+NG
  - Umiestnenie PKCS#11 knižnice /usr/local/lib/ProIDPlus/libproidngcm11.dylib

Postup konfigurácie ovládača PKCS#11 do Firefoxu a ďalších aplikácií je popísaný v kapitolách 8.3 a 8.4.

8.1.3 tokenD

Staršia verzia ovládača. V novších verziách macOS je *tokenD* nahradený ovládačom *CryptoTokenKit*.

Aplikácie, ktoré využívajú ovládače cez tokenD, nie je potrebné nijak konfigurovať. Operačný systém sám zaistí, aby tieto aplikácie vedeli s kartou ProID pracovať.

Certifikáty z kariet ProID sa dajú pomocou tokenD zobraziť v aplikácii Kľúčenka (*Keychain Access*).

8.2 INTEGRÁCIA OVLÁDAČA CRYPTOTOKENKIT

Operačný systém macOS od verzie 10.14 už nepodporuje rozhranie tokenD. Softvér ProID+ reaguje na zmenu podporovaných ovládačov kariet v macOS. V novších verziách preto ProID+ inštaluje ovládač CryptoTokenKit. Pomocou rozhrania CryptoTokenKit je možné používať certifikáty z kariet ProID v natívnych aplikáciách, ako sú Mail, Safari, a pod.

Z pohľadu užívateľa znamená prechod na CryptoTokenKit nové možnosti, ale tiež niektoré obmedzenia:

- Pomocou kryptografického kľúča z certifikátu je možné zašifrovať dáta Kľúčenky (*Keychain Access*). Po zašifrovaní je možné kartou ProID schváliť bezpečné použitie dát Kľúčenky – napr. na prihlásenie do operačného systému. Viac o ochrane Kľúčenky v kapitole 8.2.1.
  Na aktiváciu ochrany Kľúčenky je potrebné spárovať kartu ProID s operačným systémom – pozri kapitolu 8.2.2.

- Užívateľ nemôže zvoliť, ktorý certifikát má byť použitý v natívnych aplikáciách, napríklad na elektronický podpis e-mailu.
  (Pôvodný ovládač tokenD umožňoval voľbu certifikátu v Kľúčenke.)

- V Kľúčenke nie je možné zobraziť zoznam certifikátov uložených v čipovej karte. (Kľúčenka takúto možnosť ponúkala pre starší ovládač tokenD.)
  Obsah čipu kariet ProID je možné zobraziť pomocou aplikácie *Správca karty ProID*, pozri tiež kapitolu 4.1. Pre technické zobrazenie obsahu čipu sa dá použiť taktiež terminálový príkaz: *system_profiler SPSmartCardsDataType:*
  `$ system_profiler SPSmartCardsDataType`

8.2.1 Ochrana dát Kľúčenky pomocou kariet ProID

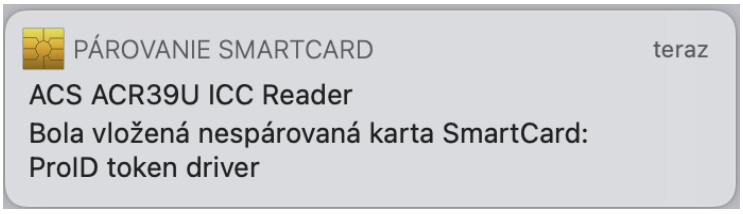
Užívateľ, ktorý má v karte ProID uložený *komerčný* certifikát, môže použiť kartu na zabezpečenie dát Kľúčenky. Kľúčom komerčného certifikátu môže zašifrovať heslá v Kľúčenke. Následne môže kartu ProID využiť na schválenie použitia hesiel z Kľúčenky. Kartu ProID potom užívateľ môže použiť napríklad na prihlásenie do operačného systému alebo na webové stránky v Safari. Použitie karty ProID na prihlásenie musí užívateľ potvrdiť zadaním PIN.

Technicky sa dáta v Kľúčenke zašifrujú verejným kľúčom zvoleného certifikátu. Pred použitím dát z Kľúčenky je potrebné použiť súkromný kľúč (chránený v čipe) na dešifrovanie dát. Operáciu so súkromným kľúčom musí užívateľ schváliť pomocou PIN.

Ak operačný systém zistí, že je v čipe karty ProID uložený vhodný certifikát s kľúčom, automaticky ponúkne možnosť použiť kľúč na ochranu dát Kľúčenky. Po vložení karty do čítačky sa spustí proces párovania karty. V priebehu párovania sa zvolí kľúč, ktorým majú byť chránené dáta Kľúčenky. Postup párovania je popísaný v kapitole Párovanie kariet ProID.

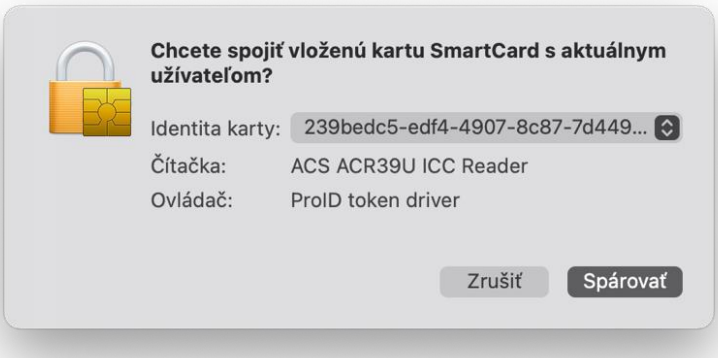
8.2.2 Párovanie kariet ProID

Po vložení nespárovanej karty do čítačky spustí operačný systém automaticky proces párovania:



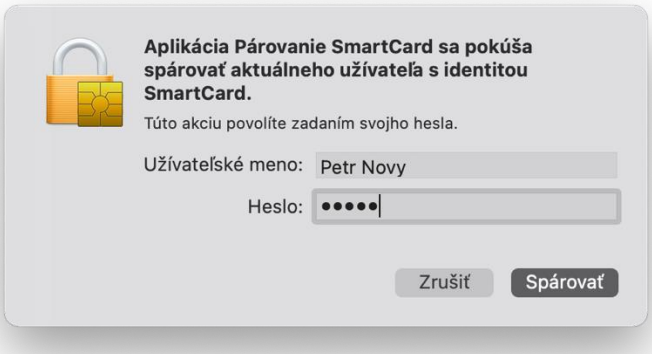
Obrázok 10: Okno s výzvou párovať kartu s účtom užívateľa

Užívateľ vyberie v zozname *ID karty* identifikátor kľúča certifikátu, ktorý si želá spárovať so svojím užívateľským účtom. Párovanie sa potvrdí tlačidlom *Spárovať*:



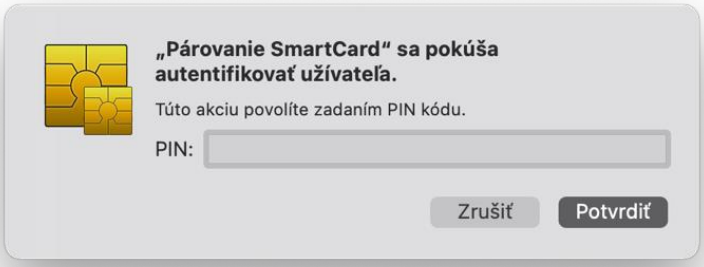
Obrázok 11: Potvrdenie párovania karty s účtom užívateľa

Kliknutím na *Spárovať* sa spáruje zvolený certifikát k účtu užívateľa. Užívateľ je vyzvaný zadať heslo k užívateľskému účtu:



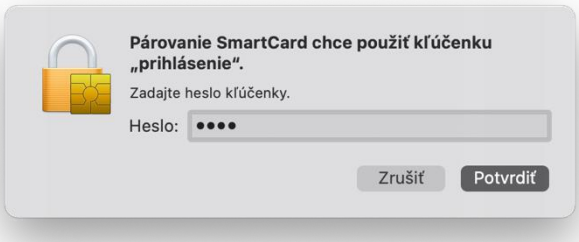
Obrázok 12: Zadanie hesla na schválenie párovania

Po zadaní hesla je užívateľ vyzvaný zadať hodnotu PIN karty ProID:



Obrázok 13: Potvrdenie párovania karty ProID s účtom užívateľa

Po zadaní platnej hodnoty PIN je užívateľ znovu vyzvaný zadať heslo k užívateľskému účtu:



Obrázok 14: Zadanie hesla na schválenie párovania

Párovanie certifikátu na karte ProID je týmto krokom dokončené. Párovanie neoveruje platnosť certifikátu a je tak platné až dovtedy, kým ho užívateľ nezruší.

Úspešné spárovanie certifikátu je možné overiť príkazom *sc_auth list,* ktorý sa spustí v okne terminálu. Príkazom sa zobrazí odtlačok (hash) identifikátoru kľúča spárovaného certifikátu. Ak je spárovaných viac certifikátov (z rôznych čipových kariet), sú zobrazené všetky.

Príklad výpisu spárovaných certifikátov:

```
$ sc_auth list

Hash: 0B2BEA714EE562AAD60C33D5C7F82572AB26C2C7
```

Ak chce užívateľ zrušiť spárovanie certifikátu, môže použiť príkaz *sc_auth unpair hash.* Zrušiť párovanie je vhodné napríklad v okamihu, keď nastane exspirácia spárovaného certifikátu a je potrebné spárovať nový certifikát.

```
$ sc_auth unpair 0B2BEA712EE563AAD60C33D5C7F82572AB26C2C7
```

8.2.3 Ďalšie informácie k párovaniu kariet ProID

Spárovaním karty ProID nevzniká *povinnosť* používať kartu pri každom prístupe k dátam Kľúčenky. Ak nie je spárovaná karta vložená do čítačky, použijú sa heslá z Kľúčenky rovnako, ako keby užívateľ vôbec žiadnu kartu nespároval. Aj do operačného systému sa dá vždy prihlásiť heslom.

Párovanie sa ponúka iba v prípade, že je v čipe uložený *komerčný* certifikát s kľúčom. Kľúče *komerčného* certifikátu je možné použiť na šifrovacie operácie. Ak je v čipe nájdený iba certifikát pre *elektronický podpis*,

potom sa párovanie ani ochrana dát Kľúčenky neponúkajú. Kľúč podpisového certifikátu sa nedá používať na šifrovanie.

Užívateľ môže párovanie čipovej karty odmietnuť. V takomto prípade operačný systém opakovane vyzýva na párovanie pri každom vložení nespárovanej karty.

Operačný systém nekontroluje platnosť certifikátu, ktorého kľúčom sú chránené dáta Kľúčenky. Ochrana dát Kľúčenky funguje aj po vypršaní platnosti certifikátu.

S užívateľským účtom je možné spárovať vždy len jeden certifikát, resp. kľúč z karty ProID. Ak je v čipe uložených viac použiteľných certifikátov, musí užívateľ pri párovaní zvoliť, ktorý má byť použitý na ochranu dát Kľúčenky. Po úspešnom spárovaní už operačný systém neupozorňuje na možnosť párovania.

Užívateľ má možnosť vypnúť výzvu na párovanie, pomocou príkazu *sc_auth pairing_ui -s disable*:

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

Tento príkaz trvale vypne výzvu na párovanie pre všetky čipové karty (nielen pre karty ProID).

Aktiváciu/deaktiváciu párovania je možné overiť príkazom *sc_auth pairing_ui -s status*:

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

Deaktivované párovanie sa dá znovu aktivovať príkazom *sc_auth pairing_ui -s enable:*

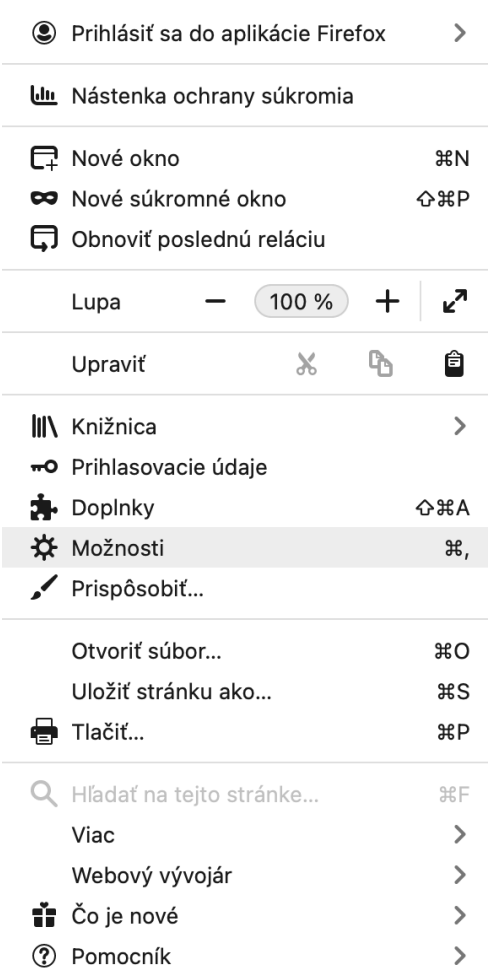
```
$ sc_auth pairing_ui -s enable
```

Dáta Kľúčenky je možné zašifrovať pomocou niekoľkých kľúčov - z rôznych čipových kariet. Pred použitím dát z Kľúčenky potom operačný systém deteguje vloženú kartu a použije dostupný kľúč na sprístupnenie dát Kľúčenky.

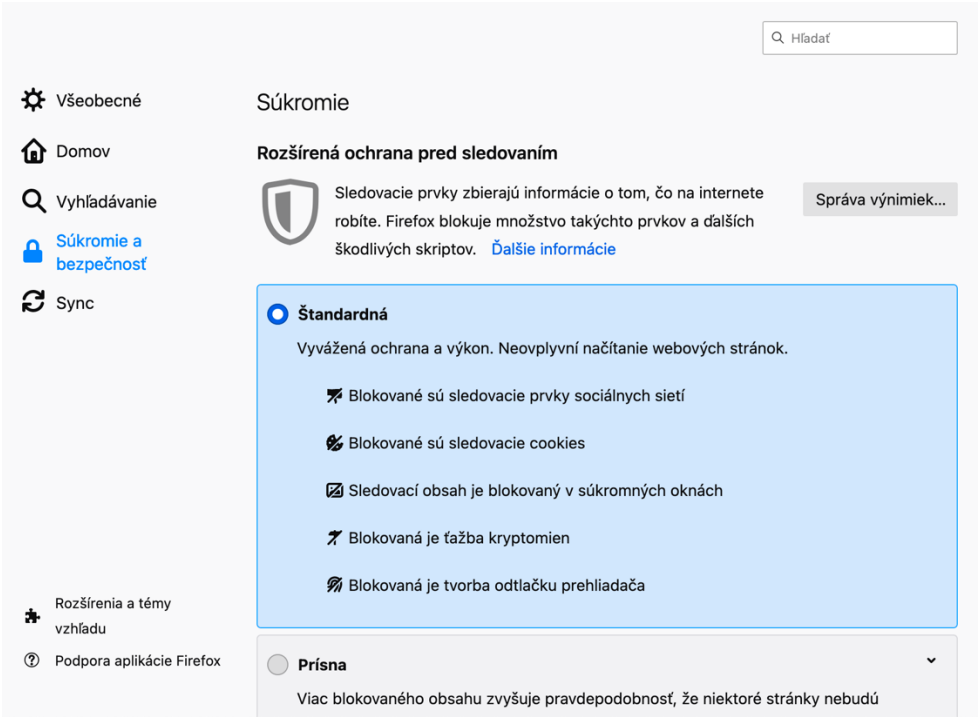
8.3 INTEGRÁCIA PKCS#11 DO MOZILLY FIREFOX

Na ilustráciu je v tomto dokumente uvedená integrácia ovládača karty ProID do aplikácie Mozilla Firefox. Firefox je asi najznámejšou a najčastejšie používanou aplikáciou, ktorá využíva kryptografické rozhranie PKCS#11.

Do aplikácie Firefox sa dá ovládač kariet ProID pridať pomocou menu *Bezpečnostné zariadenia* v ponuke *Možnosti → Súkromie a zabezpečenie → Bezpečnostné zariadenia.*

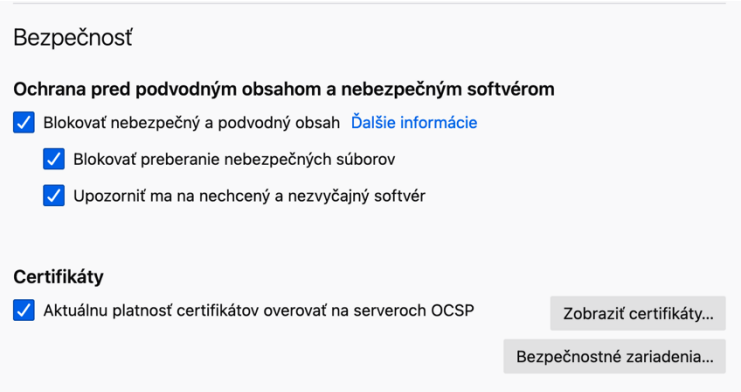


Obrázok 15: Menu aplikácie Mozilla Firefox



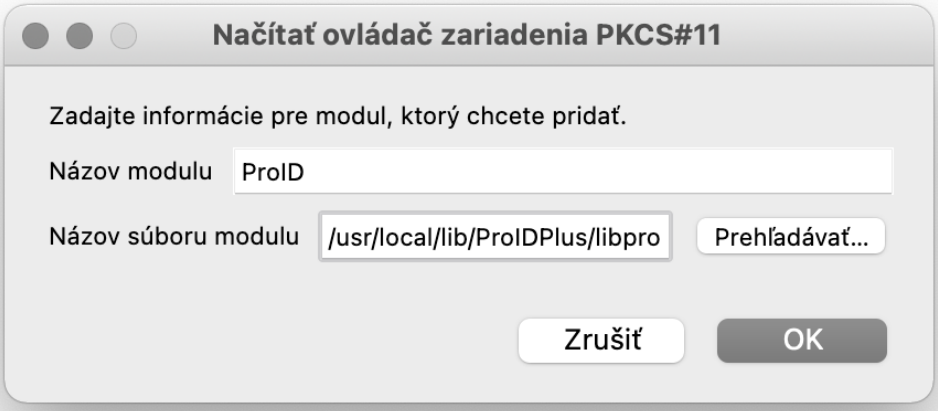
Obrázok 16: Okno na nastavenie Mozilly Firefox

V sekcii *Certifikáty* je potrebné stlačiť tlačidlo *Bezpečnostné zariadenia*.



Obrázok 17: Nastavenia zabezpečenia v Mozille Firefox

Zobrazí sa okno *Správca bezpečnostných zariadení*. V tomto okne je potrebné pridať nové bezpečnostné zariadenie: čipovú kartu. Pridanie sa vykoná stlačením tlačidla *Načítať*, zobrazí sa okno na nájdenie ovládača čipovej karty:

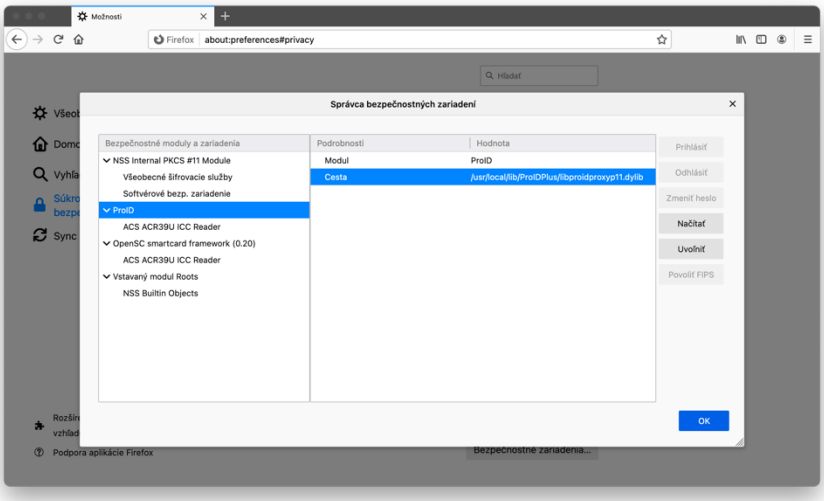


Obrázok 18: Pridanie ovládača čipovej karty do Mozilly Firefox

V okne *Nový ovládač PKCS#11 zariadení* je potrebné:

- Nastaviť názov modulu - ľubovoľný, napr. ProID alebo ProID+Q.
- Uviesť cestu k modulu libproidproxyp11.dylib
- Typicky /usr/local/lib/ProIDPlus/libproidproxyp11.dylib
- Uložiť nastavenia tlačidlom OK.

Po stlačení tlačidla *OK* sa Firefox pokúsi načítať zadaný modul ovládača. Po úspešnom načítaní modulu zobrazí aplikácia Firefox informácie o pripojenej čítačke čipových kariet, prípadne aj informácie o vloženej čipovej karte:



Obrázok 19: Okno Mozilly Firefox so zoznamom bezpečnostných modulov

Neúspešné načítanie knižnice je indikované chybovým hlásením: *Nepodarilo sa pridať modul.* Ak sa modul nepodarí pridať, mal by sa užívateľ uistiť, že pri pridaní uviedol správnu cestu a že sa na uvedenej ceste skutočne nachádza súbor *libproidproxyp11.dylib*

8.4 INTEGRÁCIA PKCS#11 DO ĎALŠÍCH APLIKÁCIÍ

Ak užívateľ používa iné aplikácie s kryptografickým rozhraním PKCS#11, je potrebné do nich použitie čipovej karty konfigurovať spôsobom uvedeným v dokumentácii danej aplikácie. Konfigurácia sa obvykle vykonáva tak, že sa do príslušnej konfiguračnej položky uvedie cesta ku knižnici *libproidproxyp11.dylib* čipovej karty.

9 INŠTALÁCIA NOVŠEJ VERZIE

Ak je k dispozícii novšia verzia softvéru *ProID+*, mal by byť na užívateľskom počítači vykonaný upgrade. Nová verzia môže opravovať chyby a ponúkať vylepšené funkcie či ovládanie.

Dostupnosť nového balíčka ProID+ môže užívateľ skontrolovať na webových stránkach ProID.

Aktualizácia softvéru *ProID+* prebieha obdobným spôsobom ako prvotná inštalácia:

- inštalačný balíček je nutné stiahnuť z internetových stránok,
- spustiť ho,
- riadiť sa pokynmi inštalačného sprievodcu.

Postup inštalácie je popísaný v kapitole 6.

Upozornenie: Rovnako ako prvotná inštalácia, aj aktualizácia aplikácie ProID+ musí byť spustená pod užívateľským účtom s **oprávnením správcu** operačného systému. Ak je inštalácia spustená pod užívateľským účtom, ktorý nemá správcovské oprávnenie, zobrazí inštalačný sprievodca v priebehu inštalácie okno operačného systému na zvýšenie (elevéciu) užívateľských oprávnení. Neprivilegovaný užívateľ môže v tomto okne zadať meno a heslo účtu správcu a autorizovať tým následný proces inštalácie.

Aktualizácia softvéru *ProID+* prebieha rovnako ako prvotná inštalácia – pozri kapitolu Spustenie a vykonanie inštalácie.

Na operačných systémoch macOS nie je automatické odinštalovanie aplikácií bežne ponúkané. Užívateľ má možnosť odstrániť aplikácie ProID+ presunutím aplikačných adresárov z priečinka *Aplikácie* (*/Applications*) do koša. Ide o tieto aplikácie, resp. aplikačné adresáre:

10 ODINŠTALOVANIE

Na operačných systémoch macOS nie je automatické odinštalovanie aplikácií bežne ponúkané. Užívateľ má možnosť odstrániť aplikácie ProID+ presunutím aplikačných adresárov z priečinka *Aplikácie* (*/Applications*) do koša. Týka sa to týchto aplikácií, resp. aplikačného adresára:

Aplikácia	Aplikačný adresár
Správca karty ProID	/Applications/CardManProID.app
CryptoTokenKit	/Applications/CryptoTokenKit_ProID/ProIDNGTokenApp.app /Applications/CryptoTokenKit_ProID/ProIDTokenApp.app /Applications/CryptoTokenKit_ProID/ProIDQSealTokenApp.app /Applications/CryptoTokenKit_ProID/ProIDQTokenApp.app

Aplikácia ProID+ na svoju činnosť využíva množstvo ďalších súborov, ktoré sú nainštalované do systémových adresárov a nie sú tak pre bežných užívateľov štandardne prístupné. Ide o súbory užívateľských konfigurácií, súborov s prevádzkovými záznamami a systémové komponenty.

Na rozdiel od aplikačných adresárov, ktoré je možné zmazať bežným spôsobom, je nutné u týchto adresárov a súborov použiť eleváciu oprávnenia pomocou príkazu *sudo*. Zoznam všetkých nainštalovaných adresárov a súborov je uvedený nižšie:

Adresáre:

- /usr/local/lib/ProIDPlus/
- /opt/ProIDCM/
- ~/.config/ProID/
- ~/.ProIDCM_logs/

Súbory:

- /usr/local/etc/crplus/proidcm.cfg
- /usr/local/etc/crplus/proidcm.tokend.cfg
- /usr/local/etc/crplus/proidngcm.cfg
- /usr/local/etc/crplus/proidngcm.tokend.cfg
- /usr/local/etc/crplus/proidqcm.cfg
- /usr/local/etc/crplus/proidqcm.tokend.cfg
- /usr/local/etc/crplus/proidqscm.cfg
- /usr/local/etc/crplus/proidqscm.tokend.cfg
- /usr/local/etc/crplus/proidproxy.cfg
- /Library/Security/tokend/proidcm.tokend
- /Library/Security/tokend/proidqcm.tokend
- /Library/Security/tokend/proidqscm.tokend

Ak užívateľ vymaže uvedený zoznam súborov a adresárov, dosiahne tým odstránenie softvéru ProID+. Softvér *ProID+* je možné do počítača kedykoľvek znova nainštalovať.

Ovládače čítačiek nie sú súčasťou inštalačného balíčka *ProID+*. Odinštalovanie čítačky je potrebné vykonať samostatne, podľa pokynov výrobcu.

11 OVERENIE INTEGRITY A PÔVODU INŠTALAČNÉHO BALÍČKA

Užívateľ by si pred inštaláciou softvéru mal vždy overiť, že daný softvér pochádza z dôveryhodného zdroja a že s obsahom balíčka nikto nemanipuloval. S inštaláciou nedôveryhodného či modifikovaného softvéru hrozí riziko, že sa do počítača dostane napr. počítačový vírus či iný škodlivý softvér.
V prípade softvéru ProID+ je možné overiť integritu aj pôvod dvoma spôsobmi:

» **Overením elektronického podpisu inštalačného balíčka**.
Overenie elektronického podpisu vykonáva operačný systém macOS pred inštaláciou **automaticky**. Ak by inštalačný balíček nebol podpísaný dôveryhodným certifikátom (resp. príslušným kľúčom), operačný systém zobrazí varovanie a neumožní, príp. neodporučí, inštaláciu vykonať.

» Stiahnutím inštalačného balíčka výhradne z webových stránok na podporu softvér ProID a porovnaním odtlačku inštalačného balíčka.

Po overení elektronického podpisu, resp. odtlačku inštalačného balíčka, môže užívateľ dôverovať tomu, že používa originálny balíček ProID+, ktorý neobsahuje škodlivý softvér.

11.1 OVERENIE ELEKTRONICKÉHO PODPISU INŠTALAČNÉHO BALÍČKA

Inštalačný balíček ProID+ pro macOS je vždy podpísaný pomocou certifikátu, určeného na elektronické podpisovanie inštalačných balíčkov macOS (*Developer ID Installer certificate*). Certifikát je vydaný z certifikačnej autority spoločnosti Apple, ktorej operačný systém macOS dôveruje - je schopný overiť dôveryhodnosť certifikátu. Držiteľom podpisového certifikátu je Monet+,a.s.
Okrem elektronického podpisu prechádza inštalačný balíček ProID tiež bezpečnostnou kontrolou - procesom tzv. *notarizácie*. Notarizáciu vykonáva spoločnosť Apple. Notarizované moduly sú operačným systémom rozpoznávané ako od "známeho vývojára". Ak by inštalované moduly neboli notarizované, potom by ich Gatekeeper operačného systému odmietol inštalovať.

Pred zahájením inštalácie operačný systém automaticky overí, či aplikácia pochádza od známeho vývojára a či je podpis balíčka vytvorený pomocou dôveryhodného certifikátu. **Ak by pôvod alebo podpis nebol dôveryhodný, operačný systém by zobrazil varovanie:** *Aplikáciu "ProID+.pkg" nie je možné otvoriť, pretože pochádza od neidentifikovaného vývojára*. **Užívateľ by v takomto prípade nemal pokračovať v inštalácii.** Mal by si stiahnuť aktuálnu verziu inštalačného balíčka a zahájiť inštaláciu znova.

Užívateľ si môže - pred inštaláciou softvéru ProID+ overiť dôveryhodnosť podpisu pomocou príkazu *pkgutil --check-signature*.

```
pkgutil --check-signature /Volumes/ProID/ProID+.pkg
Package "ProID+.pkg":
   Status: signed by a developer certificate issued by Apple for distribution
   Signed with a trusted timestamp on: 2021-01-13 09:45:22 +0000
   Certificate Chain:
    1. Developer ID Installer: Monet, a.s. (A8X9UKGE74)
       Expires: 2025-09-25 14:25:11 +0000
       SHA256 Fingerprint:
           B0 AD 82 A4 89 CE BA C5 13 8D 2A 08 8E 27 7B 57 7F 10 25 DC 1F F8
           5A 0E B9 1C AF 93 91 8F F5 7A
       ------------------------------------------------------------------------
    2. Developer ID Certification Authority
       Expires: 2027-02-01 22:12:15 +0000
       SHA256 Fingerprint:
           7A FC 9D 01 A6 2F 03 A2 DE 96 37 93 6D 4A FE 68 09 0D 2D E1 8D 03
           F2 9C 88 CF B0 B1 BA 63 58 7F
       ------------------------------------------------------------------------
    3. Apple Root CA
       Expires: 2035-02-09 21:40:36 +0000
       SHA256 Fingerprint:
           B0 B1 73 0E CB C7 FF 45 05 14 2C 49 F1 29 5E 6E DA 6B CA ED 7E 2C
           68 C5 BE 91 B5 A1 10 01 F0 24
```

Obrázok 20: Výpis programu pkgutil pri overovaní podpisu inštalačného balíčka

Ak je elektronický podpis inštalačného balíčka takto overený, potom inštalačný balíček pochádza z dôveryhodného zdroja a dá sa bez obáv použiť na inštaláciu softvéru ProID+.

11.2 POROVNANIE ODTLAČKU INŠTALAČNÉHO BALÍČKA

Na operačnom systéme macOS je možné vypočítať hodnotu odtlačku súboru pomocou programu *openssl*.
Na výpočet SHA-256 odtlačku je možné v príkazovom riadku zadať: *openssl dgst –sha256 <cesta_k_inst_souboru>*,
kde <*cesta_k_inst_souboru*> je cesta k súboru s inštalačným balíčkom *ProID.dmg*.

Príklad výpočtu odtlačku SHA-256:
V adresári so súborom inštalačného balíčka je možné v príkazovom riadku zadať:
openssl dgst -sha256 ProID.dmg
Hodnota odtlačku sa vypíše ako:
SHA256(ProID.dmg)= 8f2be5f316b806352e0feb2691abc40fd1aea87596f652b442a70cc651df5499