

ProID

Inštalácia softvéru ProID+ pre Ubuntu Linux

Inštalačná príručka

Predkladá	MONET+, a. s.
	Za Dvorem 505, Zlín – Štípa
Spracovanie:	21. 4. 2023
Číslo verzie:	1.1

1 VYHLÁSENIE O AUTORSTVE

Informácie obsiahnuté v tomto dokumente (t. j. vrátane nákresov, plánikov, obrázkov atď.) sú predmetom obchodného tajomstva (podľa § 504 zákona č. 89/2012 Zb. v platnom znení) spoločnosti MONET+, a. s., (IČO 26217783), a disponovanie nimi podlieha právnemu poriadku Českej republiky.

Spoločnosť MONET+, a. s., (IČO 26217783), je podľa zákona č. 121/2000 Zb. o autorskom práve, o právach súvisiacich s autorským právom a o zmene niektorých zákonov, v znení neskorších predpisov, vykonávateľom majetkových práv k príslušným častiam tohto dokumentu.

2 OBSAH

1	Vyhlásenie o autorstve	2
2	Obsah	3
3	Úvod	4
4	Inštalovaný softvér	5
4.1	Správca karty ProID	5
4.2	Ovládače čipu	5
5	Pred spustením inštalácie.....	7
5.1	Stav počítača pred spustením inštalácie	7
5.2	Stiahnutie inštalačného balíčka	7
5.3	Overenie pôvodu inštalačného balíčka.....	8
5.4	Porovnanie odtlačku inštalačného balíčka	8
6	Spustenie a vykonanie inštalácie.....	9
6.1	Inštalácia pomocou grafického nástroja Ubuntu Software	9
6.1.1	Inštalácia ovládača čipu pomocou grafického nástroja Ubuntu Software	9
6.1.2	Inštalácia Správcu karty ProID pomocou grafického nástroja Ubuntu Software	12
6.2	Inštalácia pomocou konzolového nástroja Apt.....	15
6.2.1	Inštalácia ovládača čipu pomocou konzolového nástroja apt	15
6.2.2	Inštalácia Správcu karty ProID pomocou konzolového nástroja apt	16
7	Čítačky.....	18
7.1	Výber čítačky	18
7.2	Ovládač čítačky.....	18
7.2.1	Overenie funkčnosti ovládača čítačky.....	18
7.3	Pripojenie čítačky.....	19
8	Integrácia inštalovaného softvéru.....	20
8.1	Integrácia PKCS#11 do aplikácie Mozilla Firefox.....	20
8.2	Integrácia PKCS#11 do ďalších aplikácií	23
9	Inštalácia novej verzie	24
10	Odiinštalovanie	25
10.1	Odiinštalovanie ovládača čipu pomocou konzolového nástroja apt.....	25
10.2	Odiinštalovanie správcu karty proid pomocou konzolového nástroja apt	26

3 ÚVOD

Na používanie elektronických funkcií v prostredí Ubuntu Linux je potrebné nainštalovať do počítača softvér ProID+.

Aktuálnou verziou balíčka sa inštaluje podpora pre karty ProID+, ProID+Q a ProID+NG.

V tomto dokumente sa opisuje spôsob inštalácie softvéru *ProID+* do počítača s operačným systémom Ubuntu Linux.

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

4 INŠTALOVANÝ SOFTVÉR

Softvérový balíček ProID+ v sebe obsahuje kompletnú podporu elektronických funkcií pre Ubuntu Linux. Po úspešnej inštalácii budú mať používatelia počítača dostupné všetky softvérové aplikácie, ktoré sa pre karty ProID v Ubuntu Linux ponúkajú.

Softvér ProID+ je rozdelený do dvoch samostatných inštalačných balíčkov. Ide o:

- » ovládače čipu (PKCS#11) kariet ProID+, ProID+NG, ProID+Q a ProID+QSeal na prácu s certifikátmi a vytváranie elektronických podpisov. Balíček má názov *libproidplus-gui*.
- » aplikáciu Card Manager (ďalej len Správca karty ProID) na správu certifikátov a prístupových kódov čipových kariet ProID. Balíček má názov *proidcm*.

V nasledujúcich podkapitolách je stručne opísaná charakteristika jednotlivých nainštalovaných aplikácií.

4.1 SPRÁVCA KARTY PROID

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

Pomocou Správcu karty ProID môže používateľ 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 umožnia 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. na webové stránky).

Ovládače však slúžia aj na **spravovanie 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 hodnôt kódu oproti čipu,
- » zmena hodnoty kódu,

- » zablokovanie kódu po opakovanom chybnom zadaní
- » atď.

Ovládače spĺňajú uznávané technické normy týkajúce sa integrácie čipových kariet do operačných systémov Ubuntu Linux:

- » **PKCS#11** – ovládač pre aplikácie, ktoré sa nespoliehajú na kryptografické funkcie systému Ubuntu Linux, ale implementujú vlastnú kryptografiu (napr. Firefox, Thunderbird atď.).

5 PRED SPUSTENÍM INŠTALÁCIE

Pri inštalácii softvéru *ProID+* je potrebné postupovať podľa týchto krokov:

- » Stiahnuť inštalačný balíček:
 - » pozri kapitolu 5.2.
- » Spustiť inštalačný balíček:
 - » pod účtom správcu operačného systému,
 - » pozri kapitolu 6.
- » Vykonať všetky kroky inštalácie:
 - » grafický sprievodca inštaláciou poskytuje priebežné pokyny pre používateľa,
 - » pozri kapitolu 6.

5.1 STAV POČÍTAČA PRED SPUSTENÍM INŠTALÁCIE

Operačný systém nie je potrebné pred inštaláciou špeciálne upravovať. Všetko potrebné zaistí inštalačný softvér v rámci OS a nainštaluje softvérové *ProID+*.

V priebehu inštalácie sa môžu do operačného systému nainštalovať balíčky z internetových repozitárov, preto sa odporúča vykonávať inštaláciu na počítači pripojenom k internetu. Ak operačný systém už obsahuje všetky závislé moduly potrebné na spustenie aplikácie *ProID+*, potom na samotnú inštaláciu nie je pripojenie k internetu potrebné.

Pri inštalácii softvéru *ProID+* nie je potrebné mať k počítaču pripojenú čítačku a nainštalované ovládače čítačiek. Inštaláciu čítačky je možné vykonať až po inštalácii softvéru *ProID+*. Napriek tomu sa odporúča, aby sa **čítačka nainštalovala pred inštaláciou softvéru *ProID+***.

Inštaláciu softvéru *ProID+* je potrebné spúšťať pod používateľským účtom, ktorý má **oprávnenia správcu** (Administrator) operačného systému Ubuntu, t. j. má právo elevácie oprávnení pomocou príkazu *sudo*. Ak používateľ nemá k dispozícii uvedené oprávnenia, mal by sa obrátiť na správcu operačného systému a požiadať o vykonanie inštalácie.

Pred spustením inštalácie sa odporúča uložiť rozrobenú prácu a ukončiť spustené aplikácie.

5.2 STIAHNUTIE INŠTALAČNÉHO BALÍČKA

Aplikácie *ProID* sa inštalujú pomocou inštalačného balíčka. **Súbor s inštalačnými balíčkami je uložený vo formáte súborov DEB a musí sa stiahnuť z internetu z [webových stránok na podporu kariet ProID](#).**

Pri sťahovaní inštalačného balíčka by si mal používateľ všimnúť, do ktorého priečinka sa stiahnutý súbor uloží – aby potom mohol z tohto priečinka inštalačný program spustiť.

5.3 OVERENIE PÔVODU INŠTALAČNÉHO BALÍČKA

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

V prípade softvéru ProID+ sa dá integrita overiť týmto spôsobom:

- » Stiahnutím inštalačného balíčka výhradne z [webových stránok na podporu softvéru ProID](#) a porovnaním odtlačku inštalačného balíčka.

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

5.4 POROVNANIE ODTLAČKU INŠTALAČNÉHO BALÍČKA

Inštalačný balíček ProID+ pre systém Linux je nutné overiť, čo sa vykonáva pomocou kontrolného súčtu.

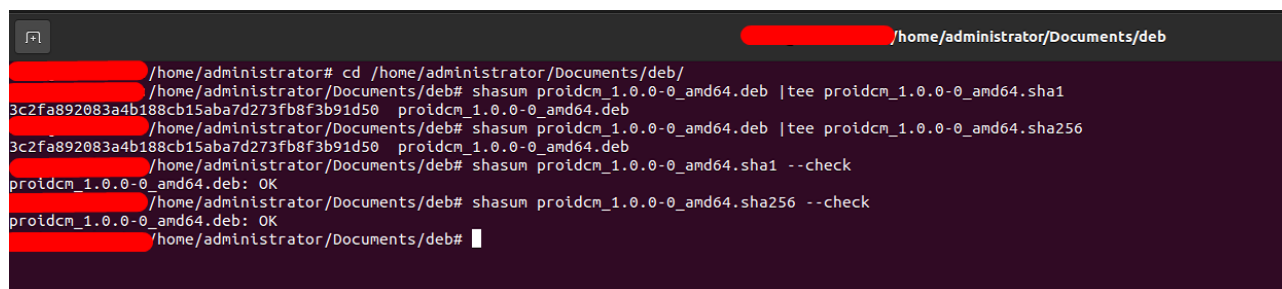
Ak sa súbor korektne stiahol alebo ak si chcete overiť pravosť a skontrolovať hash kontrolného súčtu, môžete použiť príkaz na vygenerovanie kontrolného súčtu. Ten sa líši v závislosti od hashovacieho algoritmu. V tomto prípade sú to SHA256 a SHA1.

Používateľ si môže pred inštaláciou softvéru ProID+ overiť dôveryhodnosť kontrolného súčtu pomocou príkazu:

```
shasum proid.sha --check
```

Alebo porovnať kontrolný súčet s inštalačným súborom:

```
Shasum proid.deb |tee proid.sha
```



```

/home/administrator# cd /home/administrator/Documents/deb/
/home/administrator/Documents/deb# shasum proidcm_1.0.0-0_amd64.deb |tee proidcm_1.0.0-0_amd64.sha1
3c2fa892083a4b188cb15aba7d273fb8f3b91d50  proidcm_1.0.0-0_amd64.deb
/home/administrator/Documents/deb# shasum proidcm_1.0.0-0_amd64.deb |tee proidcm_1.0.0-0_amd64.sha256
3c2fa892083a4b188cb15aba7d273fb8f3b91d50  proidcm_1.0.0-0_amd64.deb
/home/administrator/Documents/deb# shasum proidcm_1.0.0-0_amd64.sha1 --check
proidcm_1.0.0-0_amd64.deb: OK
/home/administrator/Documents/deb# shasum proidcm_1.0.0-0_amd64.sha256 --check
proidcm_1.0.0-0_amd64.deb: OK
/home/administrator/Documents/deb#
  
```

Obrázok 1: Výpis programu shasum pri overovaní podpisu inštalačného balíčka správcu karty

Kontrolný súčet sa objaví na ďalšom riadku terminálu. Porovnajte ho s kontrolným súčtom vygenerovaným dodávateľom softvéru a uistite sa, že zodpovedá.

Ak sa oba kontrolné súčty zhodujú, nebol súbor poškodený ani zmenený oproti pôvodnej verzii a je možné ho spustiť.

6 SPUSTENIE A VYKONANIE INŠTALÁCIE

Ovládací softvér ProID sa inštaluje pomocou dodaného inštalačného balíčka s využitím systémových nástrojov (grafických alebo nástrojov príkazového riadka). Inštalačný balíček je koncipovaný tak, aby čo najviac uľahčil prácu bežnému používateľovi:

- » definuje závislé balíčky, ktoré sú nevyhnutné na beh aplikácie ProID,
- » umiestňuje súbory do očakávaných priečinkov,
- » vytvára zástupcu na jednoduché spustenie aplikácie ProID – Správca karty.

V nasledujúcich podkapitolách sú opísané postupy inštalácie pomocou grafického nástroja a textovej konzoly. Výsledok inštalácie je v oboch prípadoch zhodný.

6.1 INŠTALÁCIA POMOCOU GRAFICKÉHO NÁSTROJA UBUNTU SOFTWARE

Správca aplikácií Ubuntu Software je predvolený grafický nástroj na správu inštalovaných programov v distribúcii Ubuntu.

Ďalší postup predpokladá, že už došlo k stiahnutiu inštalačných balíčkov (pozri kapitolu 5.2).

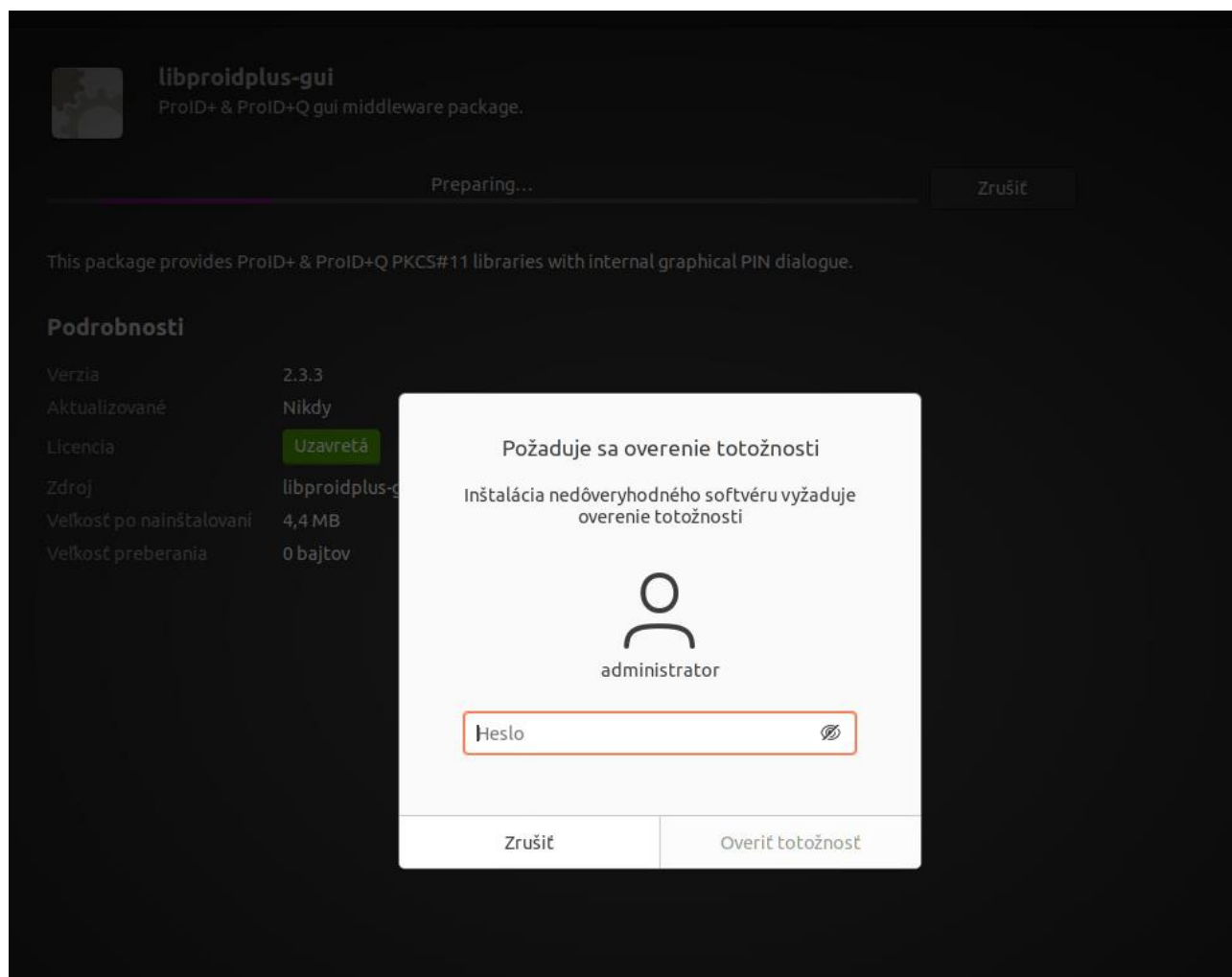
Ide o balíček s ovládačom čipu (knihnica PKCS#11) *libproidplus-gui* a o grafickú aplikáciu Správca kariet *proidcm*.

6.1.1 Inštalácia ovládača čipu pomocou grafického nástroja Ubuntu Software

Pomocou správcu súborov (ako je program Súbory) je potrebné vyhľadať stiahnutý súbor *libproidplus-gui.deb*. Dvojitým kliknutím na súbor balíčka sa spustí aplikácia priradená na správu balíčkov DEB (v predvolenom nastavení ide o aplikáciu Ubuntu Software).

V okne Ubuntu Software sú zobrazené základné informácie vyčítané z inštalačného balíčka. Samotná inštalácia sa spustí stlačením tlačidla Inštalovať.

Pred spustením inštalácie potrebuje inštalačný program získať oprávnenia správcu, aby mohol zapísať súbory do systémových priečinkov. Elevácia oprávnení sa vykoná zadáním používateľského hesla do poľa Heslo v systémovom dialógu. Pokračujte stlačením tlačidla Overiť totožnosť.



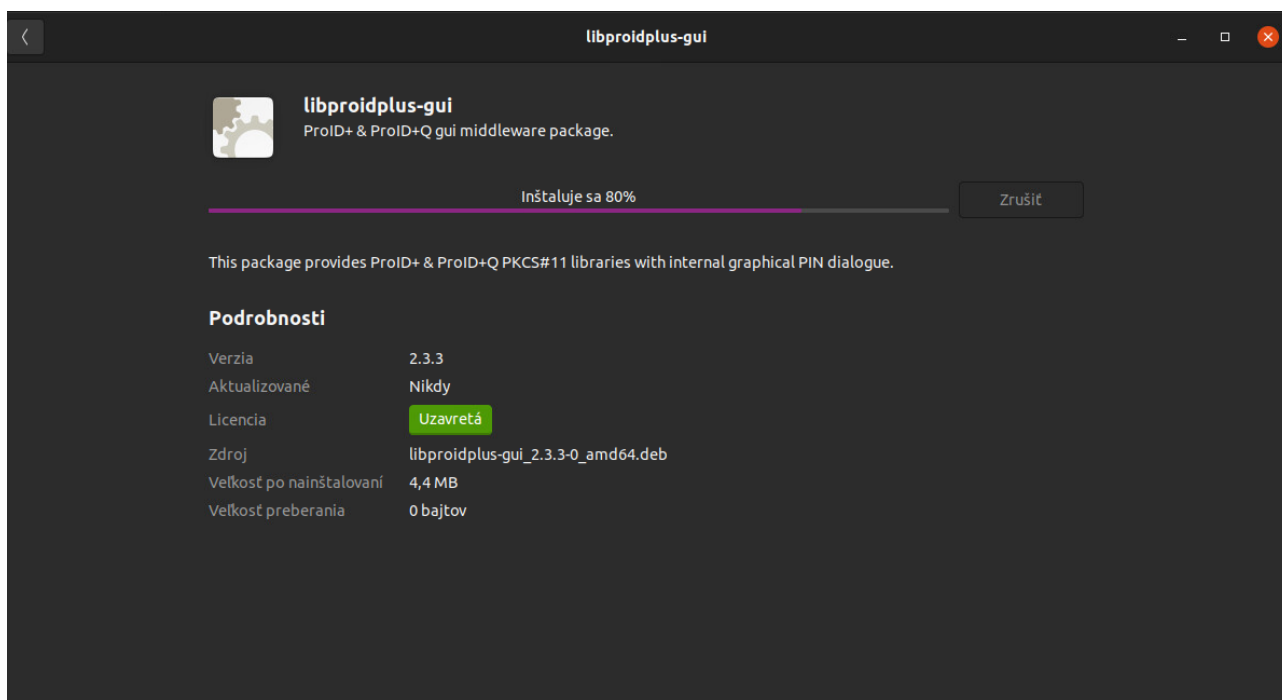
Obrázok 2: Elevácia oprávnení na inštaláciu ovládača čipu



Obrázok 3: Ubuntu Software s načítaným balíčkom libproidplus-gui.deb

Po úspešnom overení sa spustí samotná inštalácia súborov do systému. Inštalačný balíček automaticky vykonáva všetky potrebné kroky:

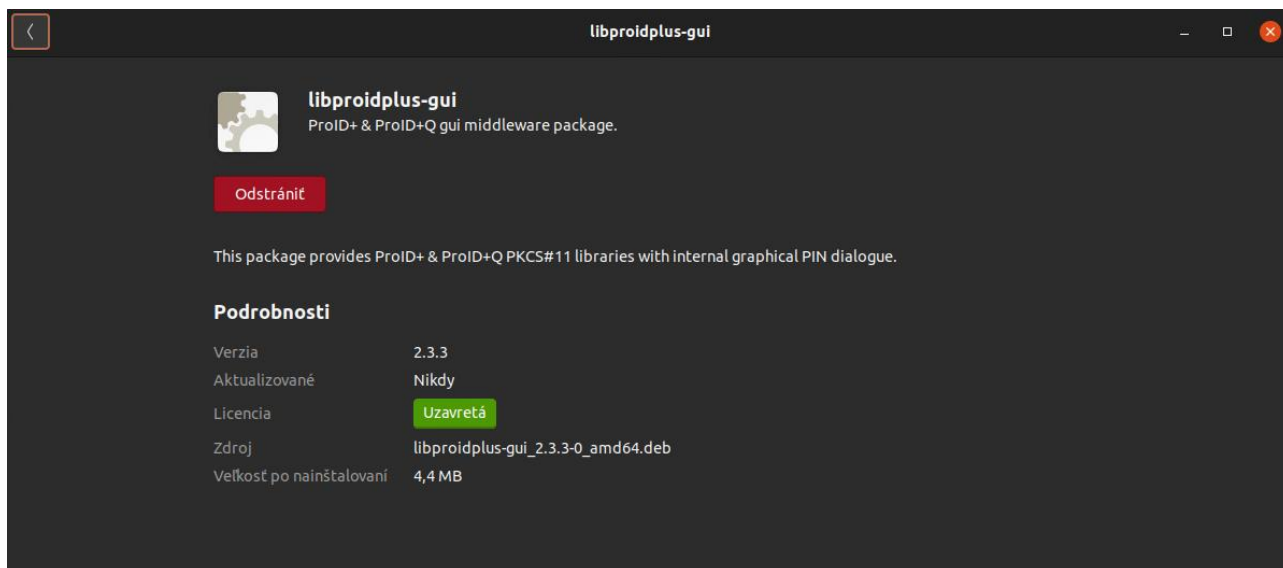
- » inštaluje aplikačné a konfiguračné súbory do priečinka programu /opt/ProID/lib,
- » inštaluje závislé balíčky/modules z repozitárov Ubuntu,
- » vykonáva registráciu aplikácie do systémových nastavení.



Obrázok 4: Priebeh inštalácie ovládača čipu

Používateľ nemá v priebehu inštalácie možnosť zmeniť inštalačný priečinok. Inštalačný balíček používa vopred definovaný priečinok `/usr/lib/x86_64-linux-gnu`.

Po úspešnej inštalácii sa tlačidlo Install (slovensky Inštalovať) zmení na Remove (slovensky Odstrániť).



Obrázok 5: Ukončená inštalácia aplikácie ovládača čipu

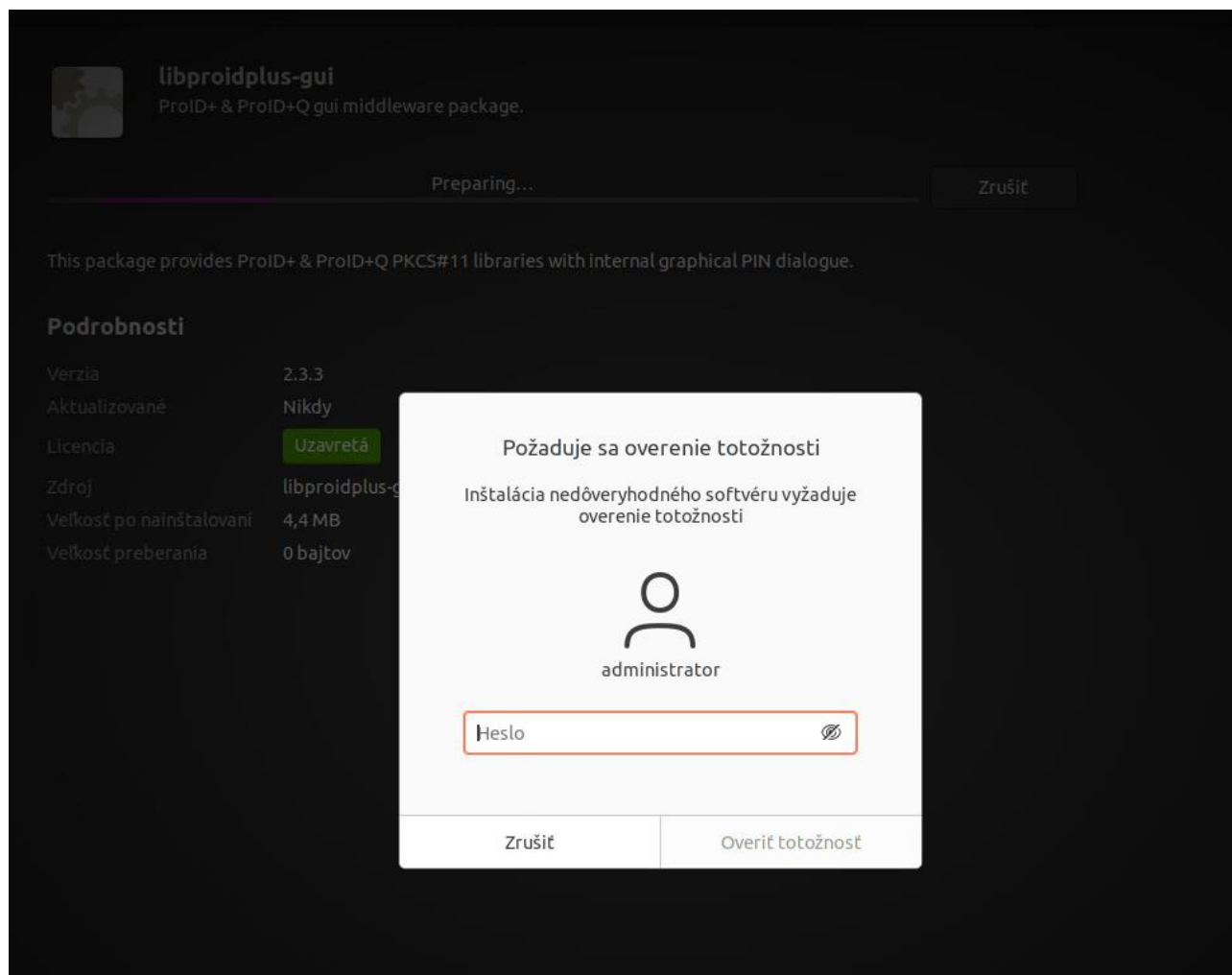
Ak sa pri inštalácii pomocou Ubuntu Software vyskytnú problémy, odporúča sa prístupit' k inštalácii pomocou konzolového nástroja *apt* (pozri kapitolu 6.2.1).

6.1.2 Inštalácia Správcu karty ProID pomocou grafického nástroja Ubuntu Software

Pomocou správcu súborov (ako je program Súbory) je potrebné vyhľadať stiahnutý súbor *proidcm.deb*. Dvojité kliknutím na súbor balíčka sa spustí aplikácia priradená na správu balíčkov DEB (v predvolenom nastavení ide o aplikáciu Ubuntu Software).

V okne Ubuntu Software sú zobrazené základné informácie vyčítané z inštalačného balíčka. Samotná inštalácia sa spustí stlačením tlačidla Inštalovať.

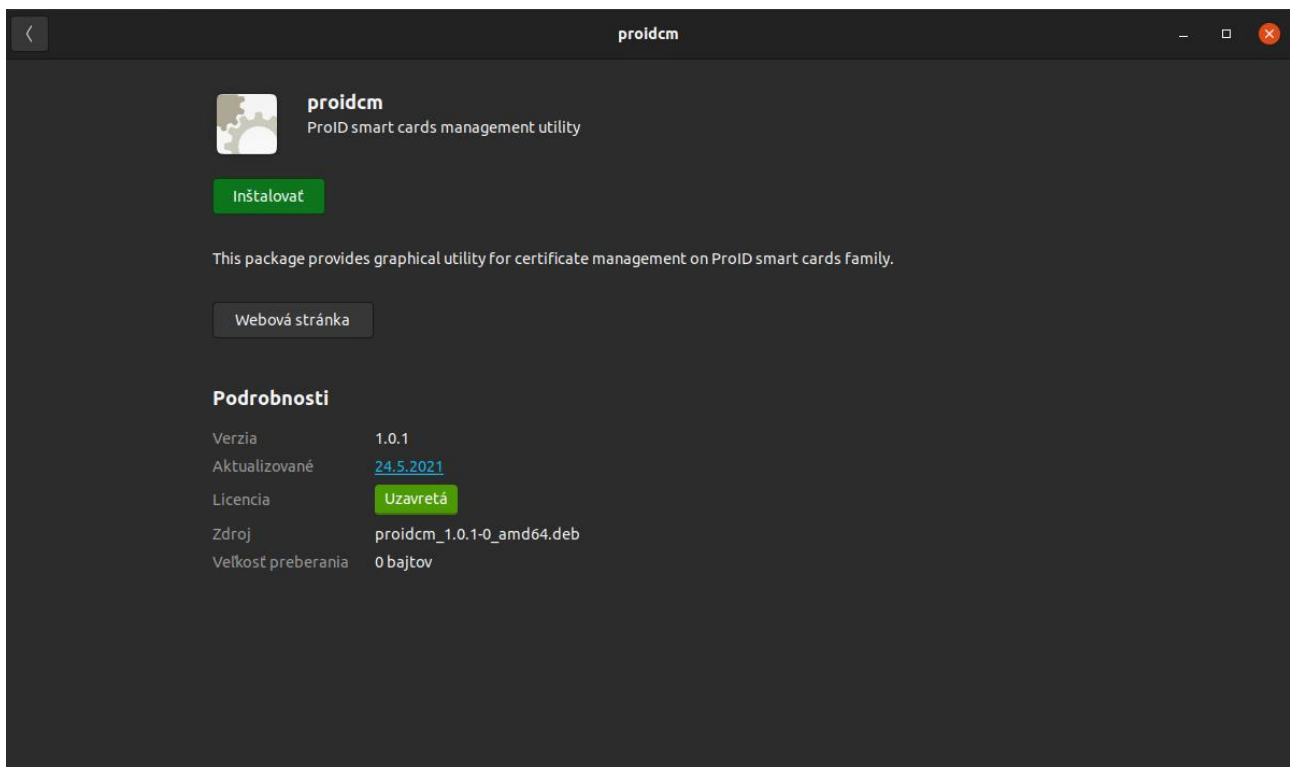
Pred spustením inštalácie potrebuje inštalačný program získať oprávnenia správcu, aby mohol zapísať súbory do systémových priečinkov. Elevácia oprávnení sa vykoná zadáním používateľského hesla do poľa Heslo v systémovom dialógu. Pokračujte stlačením tlačidla Overiť totožnosť.



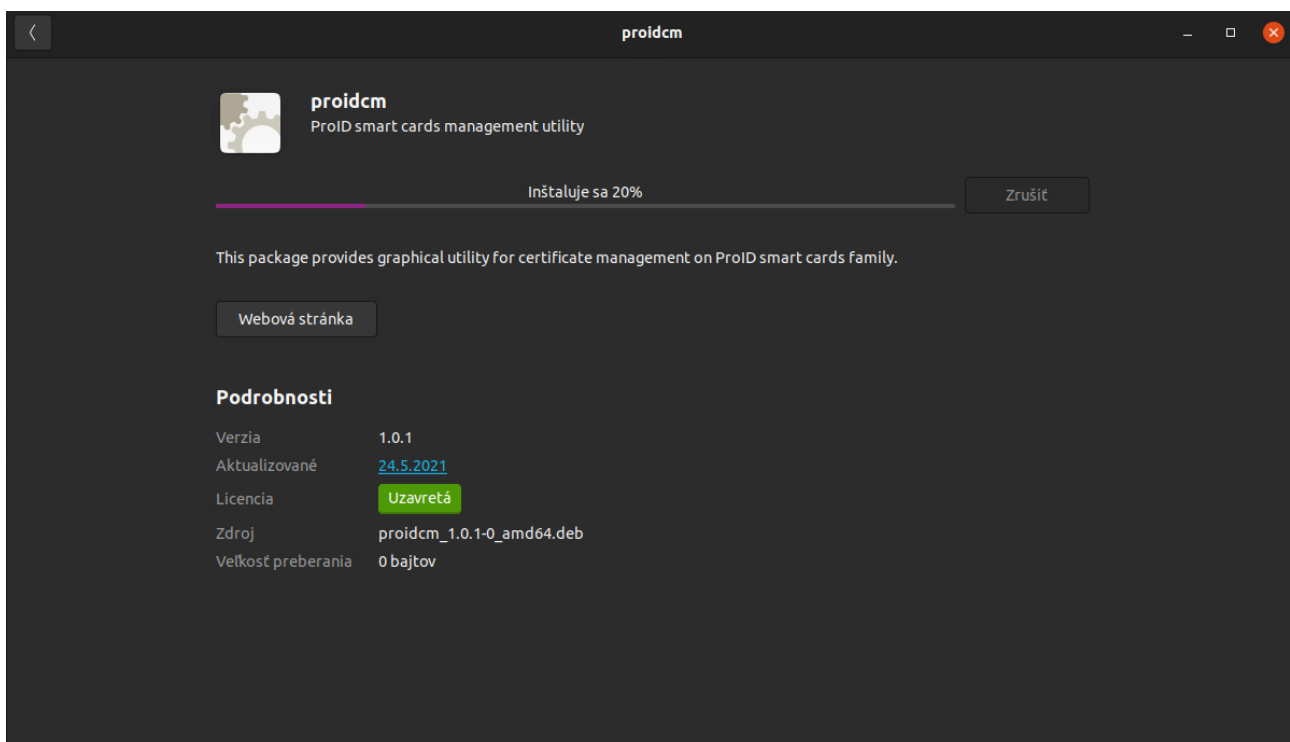
Obrázok 6: Elevácia oprávnení na inštaláciu Správcu karty ProID

Po úspešnom overení sa spustí samotná inštalácia súborov do systému. Inštalačný balíček automaticky vykonáva všetky potrebné kroky:

- » inštaluje aplikačné a konfiguračné súbory do priečinka programu /opt/ProID/,
- » inštaluje závislé balíčky/moduly z repozitárov Ubuntu,
- » vykonáva registráciu aplikácie do systémových nastavení,
- » inštaluje zástupcu aplikácií.



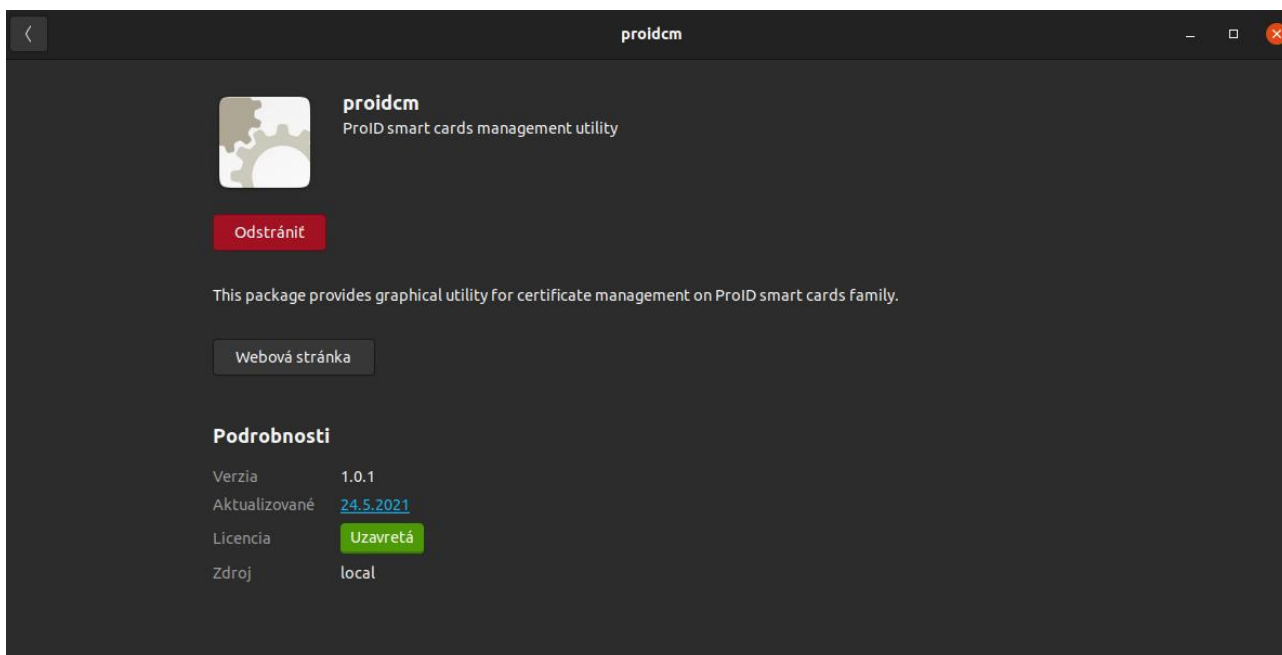
Obrázok 7: Ubuntu Software s načítaným balíčkom proidcm.deb



Obrázok 8: Priebeh inštalácie aplikácie Správca kariet ProID

Používateľ nemá v priebehu inštalácie možnosť zmeniť inštalačný priečinok. Inštalačný balíček používa vopred definovaný priečinok /opt/ProID/SpravceKarty.

Po úspešnej inštalácii sa tlačidlo Install (slovensky Inštalovať) zmení na Remove (slovensky Odstrániť).



Obrázok 9: Ukončená inštalácia aplikácie Správca karty ProID

Ak sa pri inštalácii pomocou Ubuntu Software vyskytnú problémy, odporúča sa prístup k inštalácii pomocou konzolového nástroja *apt* (pozri kapitolu 6.2.2).

6.2 INŠTALÁCIA POMOCOU KONZOLOVÉHO NÁSTROJA APT

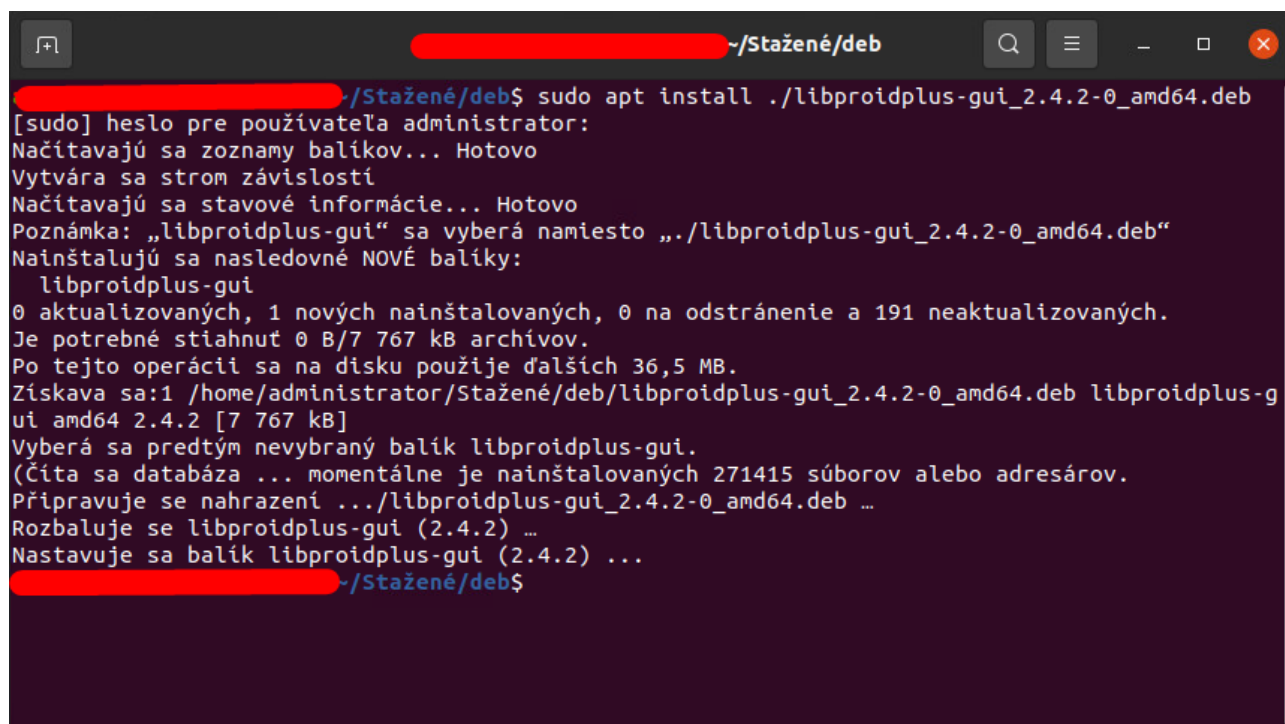
Pre väčšinu používateľov je najprijemnejším spôsobom inštalácie balíčkov použitie grafického správcu balíčkov (napr. Ubuntu Software) – pozri kapitolu 6.1. V určitých prípadoch (napr. keď sa inštalácia pomocou Ubuntu Software nepodarí) je však výhodnejšie prístup k inštalácii pomocou nástrojov príkazového riadka, najmä pre podrobnejší výpis vykonávaných akcií a ich výsledkov.

6.2.1 Inštalácia ovládača čipu pomocou konzolového nástroja apt

Balíček sa nainštaluje príkazom v terminále systému Linux (napr. gnome-terminal):

```
sudo apt install ./libproidplus-gui.deb
```

v priečinku s uloženým balíčkom. Program apt automaticky stiahne všetky potrebné závislé balíčky.



```

~/Stážené/deb$ sudo apt install ./libproidplus-gui_2.4.2-0_amd64.deb
[sudo] heslo pre používateľa administrator:
Načítavajú sa zoznamy balíkov... Hotovo
Vytvára sa strom závislostí
Načítavajú sa stavové informácie... Hotovo
Poznámka: „libproidplus-gui“ sa vyberá namiesto „./libproidplus-gui_2.4.2-0_amd64.deb“
Nainštalujú sa nasledovné NOVÉ balíky:
  libproidplus-gui
0 aktualizovaných, 1 nových nainštalovaných, 0 na odstránenie a 191 neaktualizovaných.
Je potrebné stiahnuť 0 B/7 767 kB archívov.
Po tejto operácii sa na disku použije ďalších 36,5 MB.
Získava sa:1 /home/administrator/Stážené/deb/libproidplus-gui_2.4.2-0_amd64.deb libproidplus-g
ui amd64 2.4.2 [7 767 kB]
Vyberá sa predtým nevybraný balík libproidplus-gui.
(Číta sa databáza ... momentálne je nainštalovaných 271415 súborov alebo adresárov.
Pripravuje sa nahrazení .../libproidplus-gui_2.4.2-0_amd64.deb ...
Rozbaluje se libproidplus-gui (2.4.2) ...
Nastavuje sa balík libproidplus-gui (2.4.2) ...
~/Stážené/deb$

```

Obrázok 10: Inštalácia ovládača karty pomocou nástroja apt

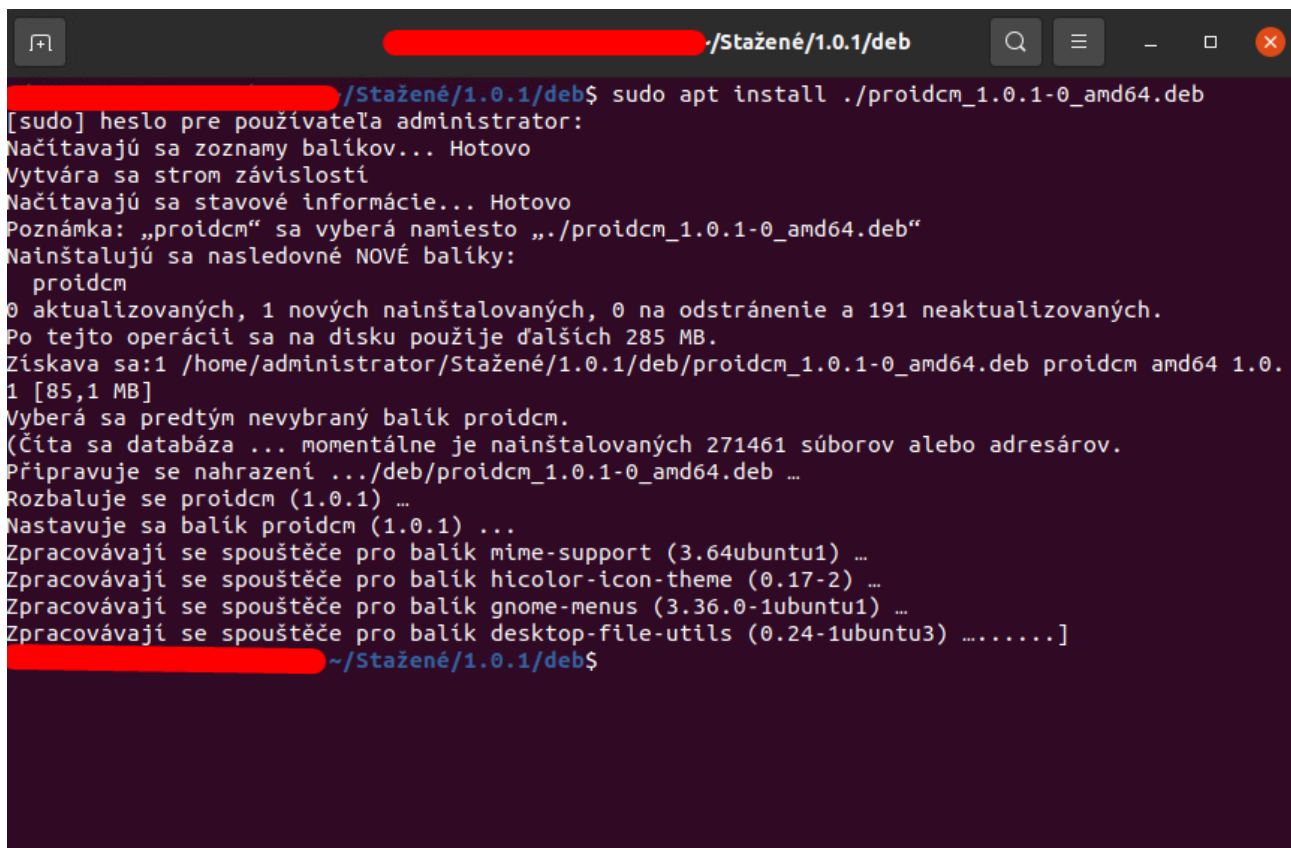
Priebeh inštalácie by mal zodpovedať výpisu uvedenému na Obrázok 10. Pri úspešnej inštalácii nie sú do výpisu programu *apt* zahrnuté žiadne chybové hlásenia. Program *apt* automaticky stiahne všetky potrebné závislé balíčky.

6.2.2 Inštalácia Správcu karty ProID pomocou konzolového nástroja apt

Balíček sa nainštaluje príkazom v termináli systému Linux (napr. *gnome-terminal*):

```
sudo apt install ./proidcm.deb
```

v priečinku s uloženým balíčkom. Program *apt* automaticky stiahne všetky potrebné závislé balíčky.

A terminal window with a dark background and light text. The window title is "/Stážené/1.0.1/deb". The user is at the prompt "~/Stážené/1.0.1/deb\$". They enter the command "sudo apt install ./proidcm_1.0.1-0_amd64.deb". The terminal shows the progress of the installation, including package selection, disk space requirements, and the installation of dependencies like mime-support, hicolor-icon-theme, gnome-menus, and desktop-file-utils. The installation completes successfully without any error messages.

```
~/Stážené/1.0.1/deb$ sudo apt install ./proidcm_1.0.1-0_amd64.deb
[sudo] heslo pre používateľa administrator:
Načítavajú sa zoznamy balíkov... Hotovo
Vytvára sa strom závislostí
Načítavajú sa stavové informácie... Hotovo
Poznámka: „proidcm“ sa vyberá namiesto „./proidcm_1.0.1-0_amd64.deb“
Nainštalujú sa nasledovné NOVÉ balíky:
  proidcm
0 aktualizovaných, 1 nových nainštalovaných, 0 na odstránenie a 191 neaktualizovaných.
Po tejto operácii sa na disku použije ďalších 285 MB.
Získava sa:1 /home/administrator/Stážené/1.0.1/deb/proidcm_1.0.1-0_amd64.deb proidcm amd64 1.0.
1 [85,1 MB]
Vyberá sa predtým nevybraný balík proidcm.
(Číta sa databáza ... momentálne je nainštalovaných 271461 súborov alebo adresárov.
Pripravuje sa nahrazení .../deb/proidcm_1.0.1-0_amd64.deb ...
Rozbaluje se proidcm (1.0.1) ...
Nastavuje sa balík proidcm (1.0.1) ...
Zpracovávajú se spouštěče pro balík mime-support (3.64ubuntu1) ...
Zpracovávajú se spouštěče pro balík hicolor-icon-theme (0.17-2) ...
Zpracovávajú se spouštěče pro balík gnome-menus (3.36.0-1ubuntu1) ...
Zpracovávajú se spouštěče pro balík desktop-file-utils (0.24-1ubuntu3) .....]
~/Stážené/1.0.1/deb$
```

Obrázok 11: Inštalácia Správcu karty ProID pomocou nástroja apt

Pri úspešnej inštalácii nie sú do výpisu programu *apt* zahrnuté žiadne chybové hlásenia.

Program *apt* automaticky stiahne všetky potrebné závislé balíčky.

7 ČÍTAČKY

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

- » získať vhodnú čítačku kariet,
- » pripojiť čítačku k počítaču,
- » prípadne nainštalovať ovládače čítačky.

7.1 VÝBER ČÍTAČKY

K počítaču s operačným systémom Ubuntu Linux je potrebné si zaobstarat' a pripojiť čítačku, ktorá je v súlade s normou CCID a spolupracuje so subsystémom PC/SC operačného systému.

Softvér *ProID+* dokáže 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 iné zariadenie pripojené k PC, musí mať v operačnom systéme nainštalovaný príslušný ovládač. Ak správny ovládač nie je nainštalovaný, operačný systém nevie s čítačkou komunikovať a čítačka potom nefunguje.

Upozornenie: **Ovládače čítačky nie sú súčasťou inštalačného balíčka *ProID+*.** Čítačku (vrátane prípadnej inštalácie ovládačov) je potrebné sprevádzkovať samostatne – mimo inštaláciu softvéru *ProID+*.

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

Predajca alebo dodávateľ čítačky by mal používateľa informovať, či je potrebné (do daného operačného systému) ovládače inštalovať. Ak je inštalácia nutná, predajca alebo dodávateľ dát by mal priložiť inštalačný balíček s ovládačmi čítačky. Používateľ potom musí zaistiť inštaláciu ovládačov.

7.2.1 Overenie funkčnosti ovládača čítačky

V operačnom systéme Ubuntu Linux je funkčnosť čítačiek závislá od služby *PC/SC Lite*. Táto služba nie je štandardnou súčasťou operačného systému a musí sa doinštalovať.

Inštalácia pomocou príkazového riadka:

```
sudo apt install libpcsclite1 pcscd pcsc-tools
```

Funkčnosť čítačky sa dá overiť napríklad príkazom *pcsc_scan* spusteným z terminálu príkazového riadka. Program vypíše všetky pripojené čítačky (karta musí byť vložená v čítačke). Po ukončení kontroly aplikácie sa zobrazí stav. Používateľ by mal počas testu vidieť ATR karty (*ATR*) a názov čítačky (*Reader*).

```

~$ pcsc_scan
Using reader plug'n play mechanism
Scanning present readers...
0: Alcor Micro AU9560 00 00

Fri Apr 30 09:48:49 2021
Reader 0: Alcor Micro AU9560 00 00
Event number: 0
Card state: Card inserted,
ATR: 3B 7F 94 00 00 80 25 A0 00 00 00 28 57 80 10 30 01 00 01 00

ATR: 3B 7F 94 00 00 80 25 A0 00 00 00 28 57 80 10 30 01 00 01 00
+ TS = 3B --> Direct Convention
+ T0 = 7F, Y(1): 0111, K: 15 (historical bytes)
  TA(1) = 94 --> Fi=512, Di=8, 64 cycles/ETU
    62500 bits/s at 4 MHz, fMax for Fi = 5 MHz => 78125 bits/s
  TB(1) = 00 --> VPP is not electrically connected
  TC(1) = 00 --> Extra guard time: 0
+ Historical bytes: 80 25 A0 00 00 00 28 57 80 10 30 01 00 01 00
  Category indicator byte: 80 (compact TLV data object)
    Tag: 2, len: 5 (issuer identification number, ISO 7812-1)
      Issuer identification number: A0 00 00 00 28
    Tag: 5, len: 7 (card issuer's data)
      Card issuer data: 80 10 30 01 00 01 00

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
3B 7F 94 00 00 80 25 A0 00 00 00 28 57 80 10 30 01 00 01 00
  ProID+ (PKI)
  http://proid.cz

```

Obrázok 12: Overenie funkčnosti čítačky pomocou príkazu pcsc_scan

Viac informácií o testovaní sa dozviete tu:

<https://help.ubuntu.com/community/CommonAccessCard>

7.3 PRIPOJENIE ČÍTAČKY

Čítačku je nutné pripojiť k počítaču prostredníctvom konektora daného typu čítačky. Najbežnejšie čítačky sa dodávajú s USB káblom. Tieto čítačky treba pripojiť do voľného USB portu počítača. USB čítačky sú napájané priamo pomocou USB portu počítača a dajú sa teda používať hneď po inštalácii ovládačov.

USB kábel čítačky nie je vhodné z dôvodu poklesu napájacieho napätia predlžovať pomocou predlžovacích USB kábllov.

8 INTEGRÁCIA INŠTALOVANÉHO SOFTVÉRU

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

Súčasťou inštalácie ProID sú aj ovládače čipu na prácu s certifikátmi na čipových kartách rodiny ProID.

Aplikácie, ktoré **nevyužívajú kryptografické rozhranie operačného systému, komunikujú priamo s knižnicou PKCS#11**. Aby tieto aplikácie dokázali pracovať s certifikátmi na kartách ProID, musí do nich používateľ nakonfigurovať správnu knižnicu PKCS#11 (niekedy sa nazýva aj *Cryptoki*). Spôsob konfigurácie knižnice sa pre jednotlivé aplikácie líši. Používateľ by mal nájsť správny spôsob v technickej dokumentácii danej aplikácie.

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

- » Karta ProID+
 - » Umiestnenie knižnice PKCS#11: `/usr/lib/x86_64-linux-gnu/libproidcm11.so`
- » Karta ProID+Q
 - » Umiestnenie knižnice PKCS#11: `/usr/lib/x86_64-linux-gnu/libproidqcm11.so`
- » Karta ProID+NG
 - » Umiestnenie knižnice PKCS#11: `/usr/lib/x86_64-linux-gnu/libproidngcm11.so`

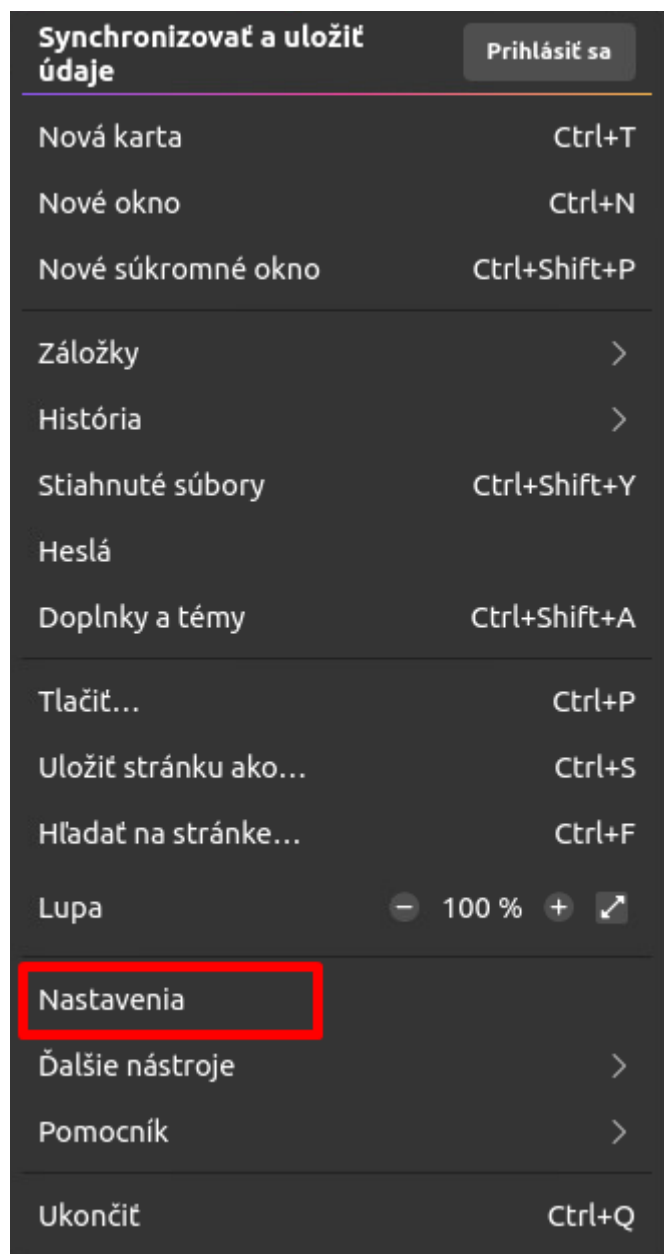
V záujme maximálneho zjednodušenia konfigurácie aplikácií, ktoré využívajú rozhranie PKCS#11, je súčasťou inštalácie aj knižnica *libproidproxyp11.so*, ktorá zaisťuje komunikáciu so všetkými typmi kariet ProID. Tento súbor sa nachádza v priečinku `/usr/lib/x86_64-linux-gnu`.

Postup konfigurácie ovládača PKCS#11 do prehliadača Firefox a ďalších aplikácií je opísaný v kapitolách 8.1 a 8.2.

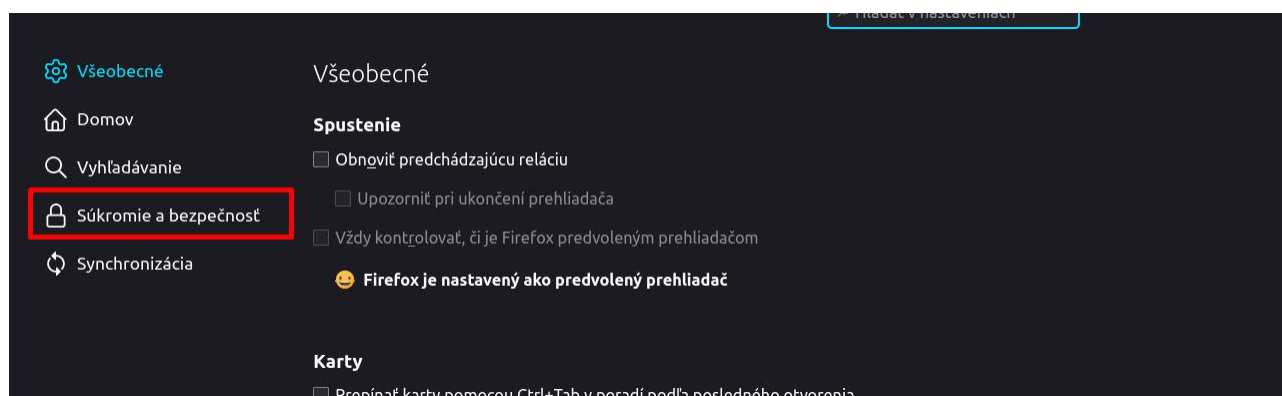
8.1 INTEGRÁCIA PKCS#11 DO APLIKÁCIE MOZILLA FIREFOX

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

Do aplikácie Firefox je možné ovládač kariet ProID pridať pomocou ponuky *Bezpečnostné zariadenia* v ponuke *Nastavenia* → *Súkromie a bezpečnosť* → *Bezpečnostné zariadenia*.

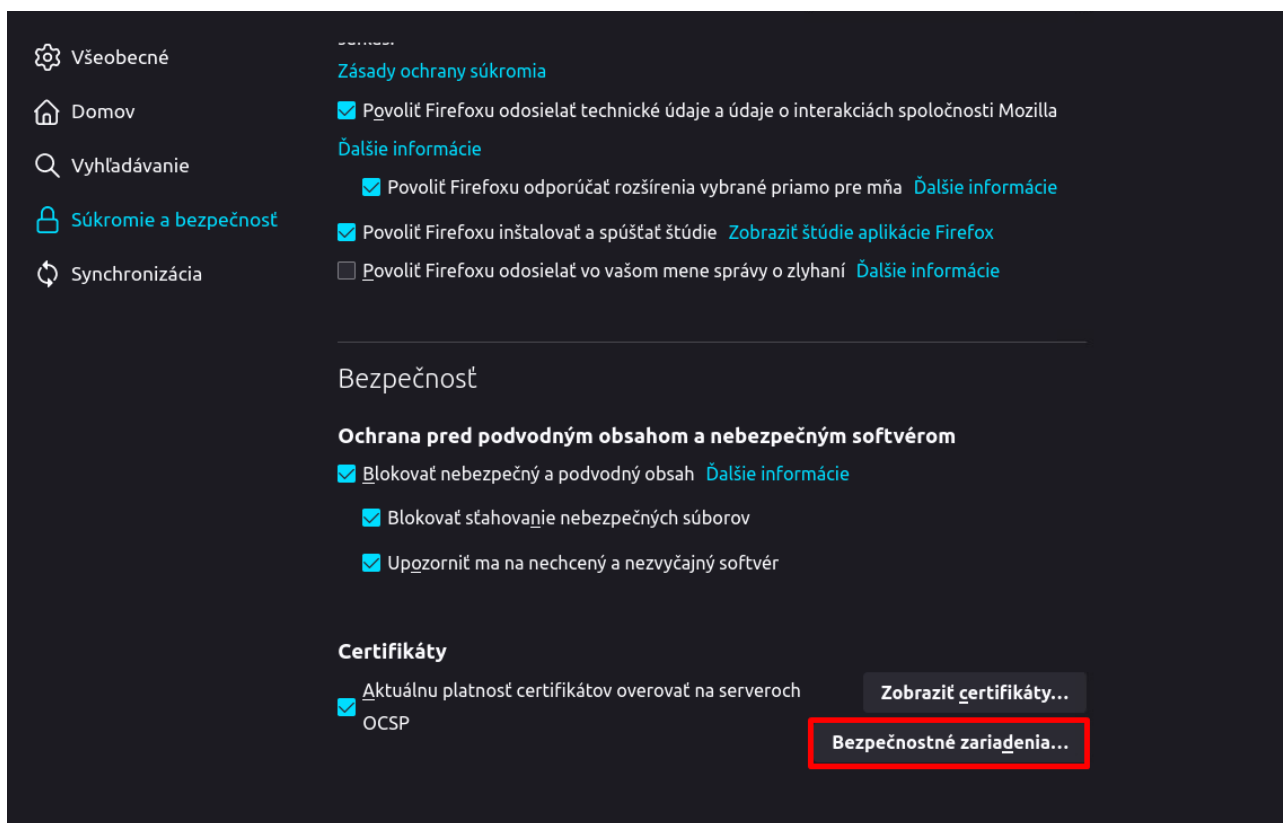


Obrázok 13: Ponuka aplikácie Mozilla Firefox



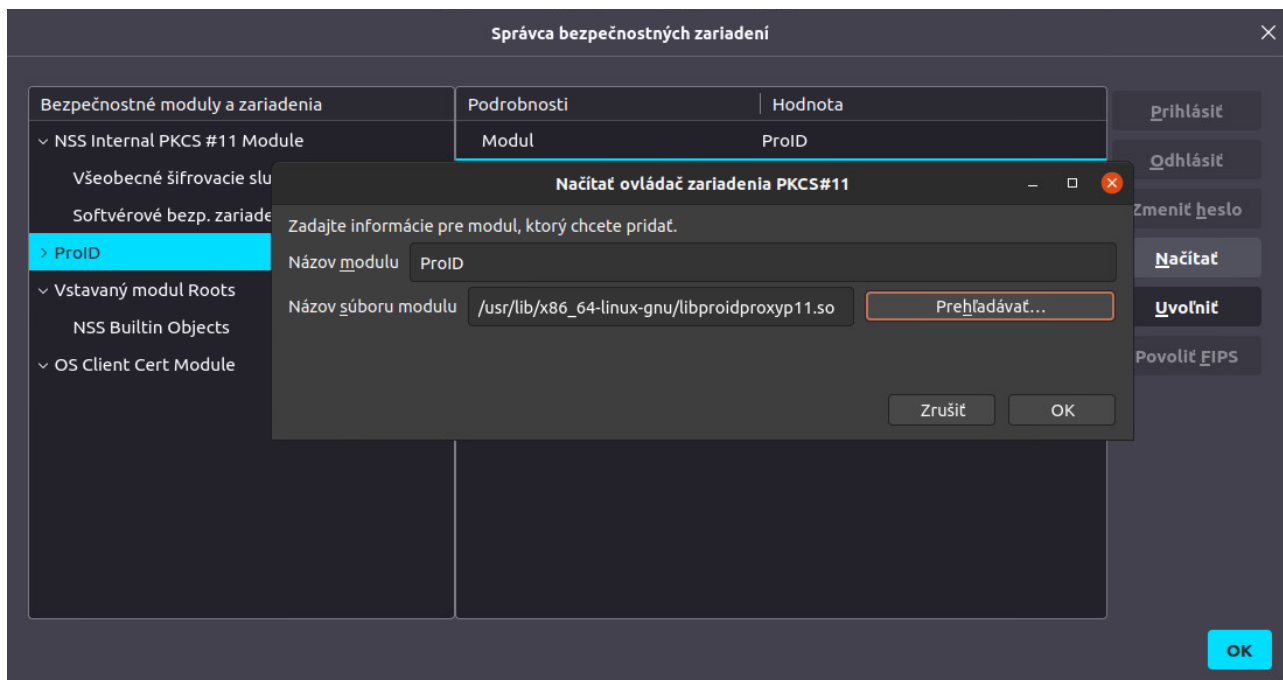
Obrázok 14: Okno na nastavenie aplikácie Mozilla Firefox

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



Obrázok 15: Nastavenie zabezpečenia aplikácie Mozilla Firefox

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

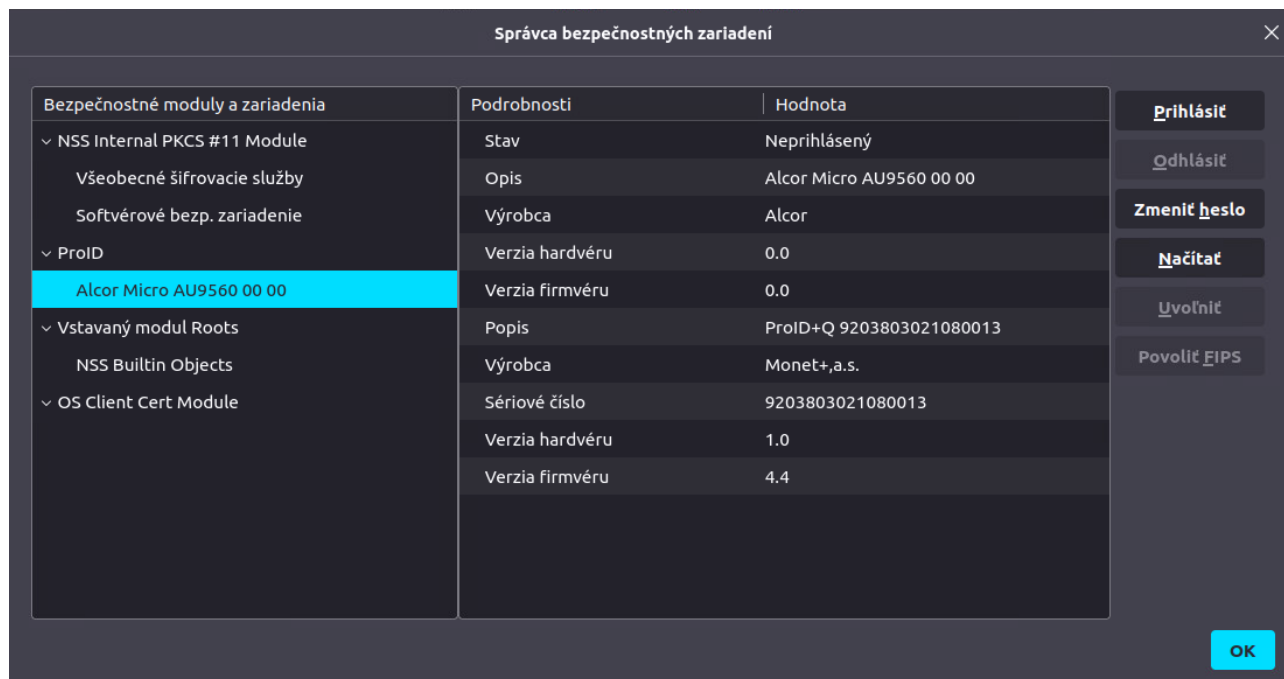


Obrázok 16: Pridanie ovládača čipovej karty do aplikácie Mozilla Firefox

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

- » nastaviť názov modulu – ľubovoľný, napr. ProID,
- » zadať cestu k modulu libproidproxyp11.so, zvyčajne /usr/lib/x86_64-linux-gnu/libproidproxyp11.so,
- » uložiť nastavenie stlačením tlačidla 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 informácie o vlozenej čipovej karte:



Obrázok 17: Okno aplikácie Mozilla Firefox so zoznamom bezpečnostných modulov

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

8.2 INTEGRÁCIA PKCS#11 DO ĎALŠÍCH APLIKÁCIÍ

Ak používateľ používa iné aplikácie s kryptografickým rozhraním PKCS#11, je potrebné v nich použitie čipovej karty nakonfigurovať spôsobom, ktorý je uvedený v dokumentácii danej aplikácie. Konfigurácia sa zvyčajne vykonáva tak, že sa do príslušnej konfiguračnej položky uvedie cesta ku knižnici *libproidproxyp11.so* čipovej karty.

9 INŠTALÁCIA NOVŠEJ VERZIE

Ak je k dispozícii novšia verzia softvéru *ProID+*, na počítači používateľa by sa mala vykonať inovácia. Nová verzia môže opravovať chyby a ponúkať vylepšené funkcie alebo ovládanie.

Dostupnosť nového balíčka ProID+ môže používateľ skontrolovať na [webových stránkach ProID](#).

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

- » z internetových stránok treba stiahnuť inštalačný balíček,
- » spustiť ho,
- » postupovať podľa pokynov sprievodcu inštaláciou.

Postup inštalácie je opísaný v kapitole 6.

Upozornenie: Rovnako ako prvotná inštalácia, aj aktualizácia aplikácie ProID+ musí byť spustená pod používateľským účtom s **oprávnením správcu** operačného systému. Ak je inštalácia spustená pod používateľským účtom, ktorý nemá oprávnenia správcu, sprievodca inštaláciou zobrazí v priebehu inštalácie okno operačného systému na zvýšenie (eleváciu) používateľských oprávnení. Neprivilegovaný používateľ môže v tomto okne zadať meno a heslo účtu správcu a autorizovať tak proces inštalácie, ktorý bude nasledovať.

Aktualizácia softvéru *ProID+* prebieha rovnako ako prvotná inštalácia – pozri kapitolu [Spustenie a vykonanie inštalácie](#).

10 ODINŠTALOVANIE

Softvér ovládača čipu a Správca karty ProID je možné odinštalovať pomocou nástroja príkazového riadka na správu balíčkov (napr. apt alebo dpkg).

Upozornenie: Podobne ako pri inštalácii, aj odinštalovanie musí prebiehať pod účtom správcu operačného systému – pozri tiež kapitolu 6.

Po dokončení odinštalovania sú z operačného systému odobrané komponenty softvéru ProID:

- » odstránené súbory a priečinky softvéru proidcm a libproidplus-gui,
- » odobraní zástupcovia programov z ponuky Zobrazit' aplikácie.

Po odinštalovaní nedochádza k odstráneniu používateľských konfigurácií a súborov z nasledujúcich priečinkov, ktoré obsahujú záznamy o prevádzke:

Priečinky:

- » ~/.config/ProID/
- » ~/.ProIDCM_logs/

Uvedené priečinky je možné po odinštalovaní odstrániť.

Po odinštalovaní nie je možné ďalej používať žiadny zo softvérových modulov ProID. Softvér proidcm a libproidplus-gui je možné do počítača znova nainštalovať kedykoľvek neskôr.

V nasledujúcich podkapitolách je opísaný postup odinštalovania pomocou riadkového príkazu.

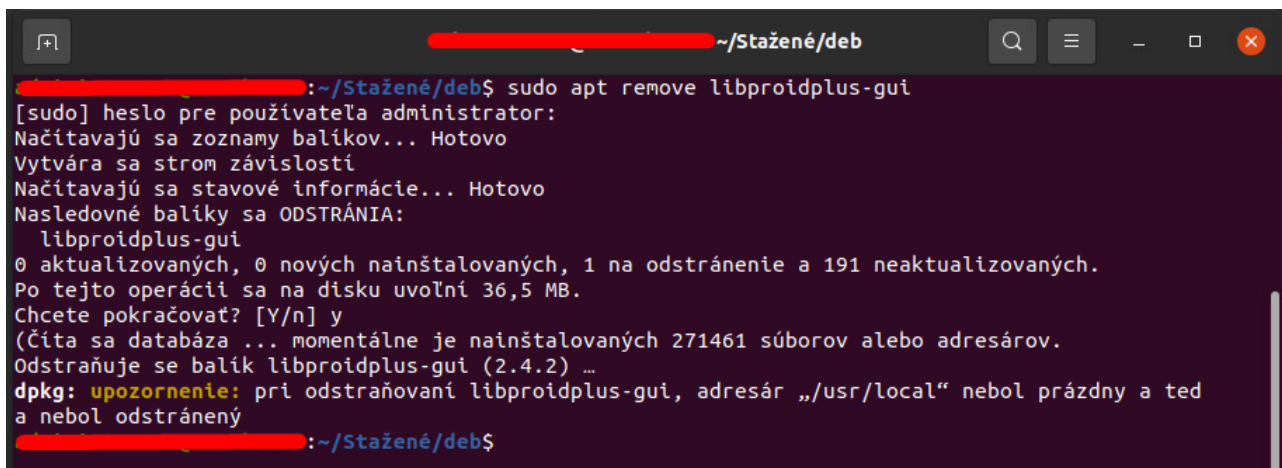
10.1 ODINŠTALOVANIE OVLÁDAČA ČIPU POMOCOU KONZOLOVÉHO NÁSTROJA APT

Program apt je nástrojom príkazového riadka. Jeho spustenie treba inicializovať z okna terminálu (napr. gnome-terminal), ktoré je možné spustiť napr. z ponuky Zobrazit' aplikácie.

Odstránenie aplikácie ovládača čipu sa vykoná príkazom v okne terminálu:

```
sudo apt remove libproidplus-gui
```

Po spustení príkazu sa odstráni softvér ovládača čipu z operačného systému:



```

~/.Stażené/deb$ sudo apt remove libproidplus-gui
[sudo] heslo pre používateľa administrator:
Načítavajú sa zoznamy balíkov... Hotovo
Vytvára sa strom závislostí
Načítavajú sa stavové informácie... Hotovo
Nasledovné balíky sa ODSTRÁNIA:
  libproidplus-gui
0 aktualizovaných, 0 nových nainštalovaných, 1 na odstránenie a 191 neaktualizovaných.
Po tejto operácii sa na disku uvoľní 36,5 MB.
Chcete pokračovať? [Y/n] y
(Číta sa databáza ... momentálne je nainštalovaných 271461 súborov alebo adresárov.
Odstraňuje sa balík libproidplus-gui (2.4.2) ...
dpkg: upozornenie: pri odstraňovaní libproidplus-gui, adresár „/usr/local“ nebol prázdny a teda nebol odstránený
~/.Stażené/deb$
  
```

Obrázok 18: Odinštalovanie ovládača čipu pomocou nástroja apt

Po úspešnom overení dôjde k odstráneniu softvéru ovládača čipu z operačného systému. Položka ovládača čipu sa odstráni zo zoznamu inštalovaných aplikácií.

Úspešné odinštalovanie je možné overiť napríklad neexistenciou priečinka `/usr/local/etc/crplus`.

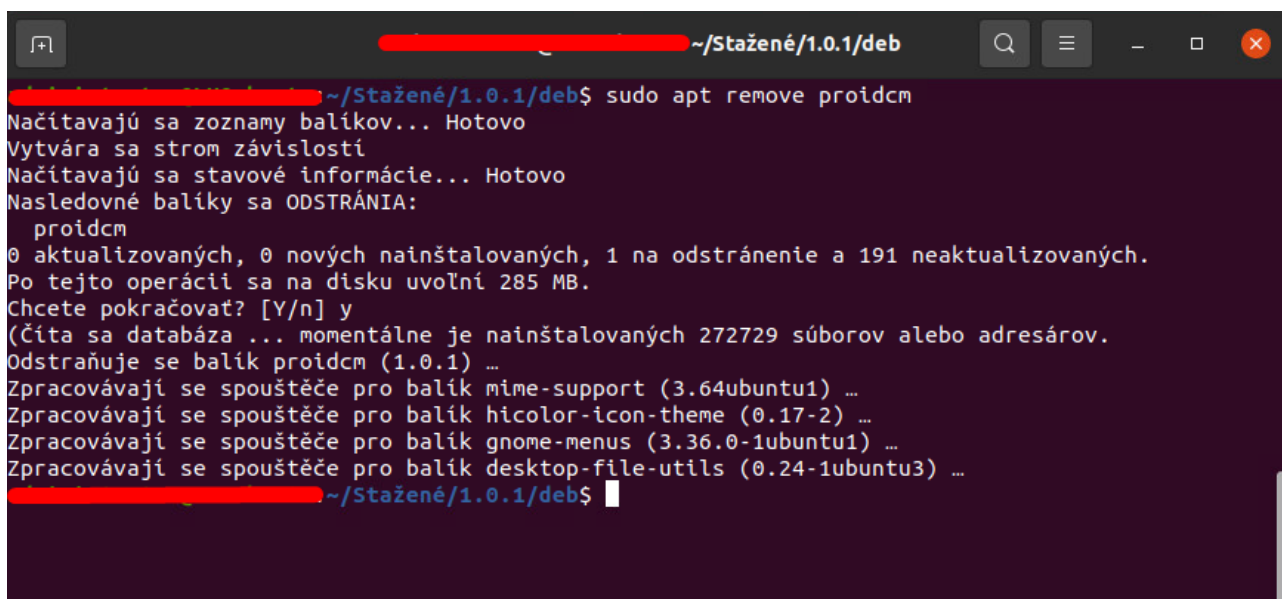
10.2 ODINŠTALOVANIE SPRÁVCU KARTY PROID POMOCOU KONZOLOVÉHO NÁSTROJA APT

Program `apt` je nástrojom príkazového riadka. Jeho spustenie treba inicializovať z okna terminálu (napr. `gnome-terminal`), ktoré je možné spustiť napr. z ponuky Zobraziť aplikácie.

Odstránenie aplikácie ovládača čipu sa vykoná príkazom v okne terminálu:

```
sudo apt remove proidcm
```

Po spustení príkazu sa odstráni softvér ovládača čipu z operačného systému:



```
~/Stažené/1.0.1/deb$ sudo apt remove proidcm
Načítavajú sa zoznamy balíkov... Hotovo
Vytvára sa strom závislostí
Načítavajú sa stavové informácie... Hotovo
Nasledovné balíky sa ODSTRÁNIA:
  proidcm
0 aktualizovaných, 0 nových nainštalovaných, 1 na odstránenie a 191 neaktualizovaných.
Po tejto operácii sa na disku uvoľní 285 MB.
Chcete pokračovať? [Y/n] y
(Číta sa databáza ... momentálne je nainštalovaných 272729 súborov alebo adresárov.
Odstraňuje se balík proidcm (1.0.1) ...
Zpracovávajú se spouštěče pro balík mime-support (3.64ubuntu1) ...
Zpracovávajú se spouštěče pro balík hicolor-icon-theme (0.17-2) ...
Zpracovávajú se spouštěče pro balík gnome-menus (3.36.0-1ubuntu1) ...
Zpracovávajú se spouštěče pro balík desktop-file-utils (0.24-1ubuntu3) ...
~/Stažené/1.0.1/deb$
```

Obrázok 19: Odinštalovanie Správca karty ProID pomocou nástroja apt

Po úspešnom overení dôjde k odstráneniu softvéru Správca karty ProID z operačného systému. Položka ovládača čipu sa odstráni zo zoznamu inštalovaných aplikácií.

Úspešné odinštalovanie je možné overiť napríklad neexistenciou priečinka `/opt/ProID/SpravceKarty`.