SPRÁVA ZÁKLADNÍCH REGISTRŮ

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

eObčanka – Správce karty pro Linux

příručka uživatele

verze 0.90 ze dne 25. 10. 2018

SPRÁVA ZÁKLADNÍCH REGISTRŮ

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

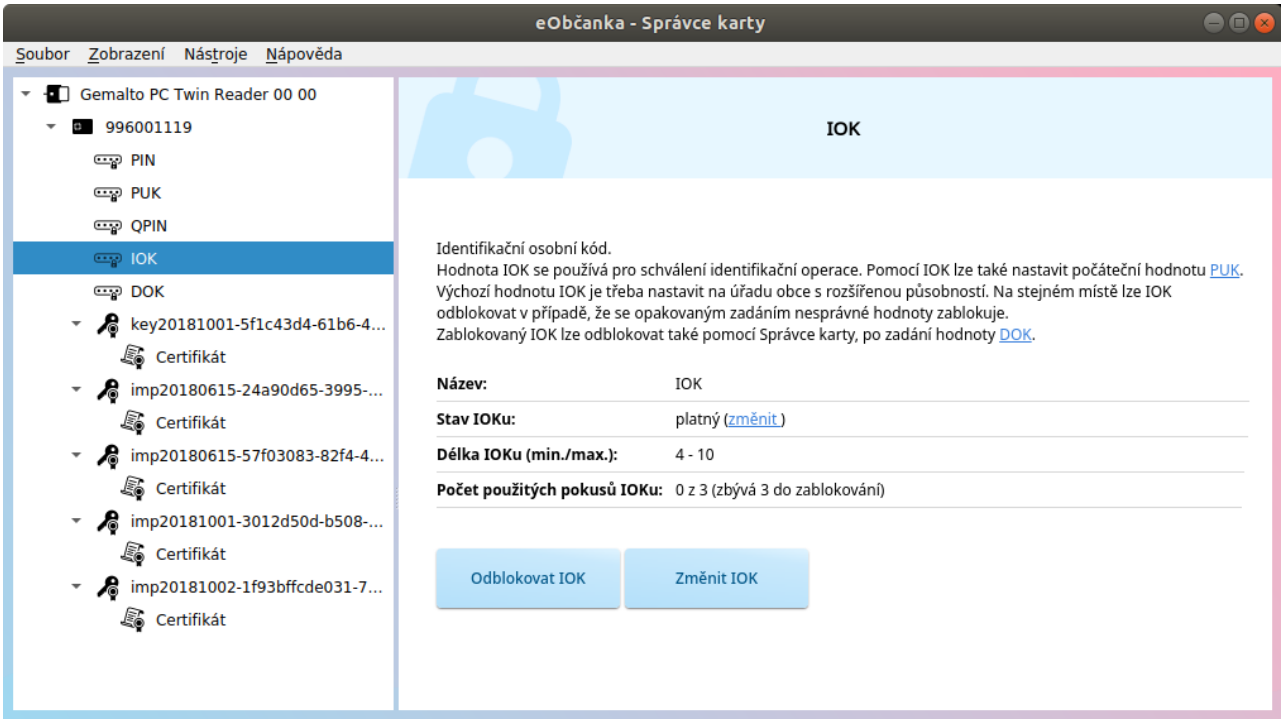
1 OBSAH

2 ÚVOD

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

Pomocí aplikace *Správce karty* uživatel může například:

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



Obrázek 1: Okno aplikace eObčanka - Správce karty

2.1 Správa certifikátů a klíčů

Do čipu občanského průkazu může držitel zapisovat certifikáty pro elektronické podepisování a pro autentizaci (spolu s certifikáty se do čipu zapisují příslušné kryptografické klíče).
Správce karty umožňuje **tyto certifikáty a klíče spravovat**.
Pomocí *Správce karty* může uživatel:

- **Zjistit**, jaké **klíče a certifikáty** má v čipu uloženy.
- **Smazat** nepotřebné klíče a certifikáty.
- **Importovat** klíče a certifikáty ze souboru do čipu.
- **Exportovat** certifikáty do souborů.

Podrobněji se správě certifikátů a klíčů v čipu občanského průkazu se věnuje kapitola 7.

2.2 Správa přístupových kódů

Používání klíčů a certifikátů je podmíněno zadáním příslušného přístupového kódu. Např. pro vytvoření elektronického popisu musí držitel zadat příslušný kód (buď PIN nebo QPIN). Podobně jsou pomocí přístupových kódů chráněny i další operace s čipem občanského průkazu. *Správce karty* umožňuje **spravovat přístupové kódy**.
Pomocí Správce karty může uživatel:

- **Zjistit** stav jednotlivých **přístupových kódů.**
- **Nastavit** výchozí hodnoty přístupových kódů.
- **Změnit** hodnotu zvoleného přístupového kódu.
- **Odblokovat** zablokovaný přístupový kód.

Správě přístupových kódů občanského průkazu se detailněji věnuje kapitola 8.

2.3 Detekce a řešení problémů

Kromě správy dat v čipu občanského průkazu umí *Správce karty* také **detekovat problémy** dat, uložených v čipu:

- **Upozorňuje** uživatele na nalezené **problémy.**
- **Navrhuje postup pro vyřešení** problémů.
- Umožňuje provést **diagnostiku** čipu občanského průkazu.
- Generuje **provozní záznamy**, pro případnou analýzu problému.
- Poskytuje formulář pro odeslání problému pracovníkům **technické podpory.**

Více o detekci a řešení problémů naleznete v kapitole 9.

2.4 Zprovoznění podpory certifikátů v občanském průkazu

Aby mohl uživatel používat občanský průkaz jako úložiště certifikátů, musí provést několik přípravných kroků:

- **Připravit počítač** pro podporu elektronických funkcí občanského průkazu.
  - **Instalovat software eObčanka**
  - **Připojit čtečku karet**
- **Nastavit přístupové kódy** občanského průkazu.
- **Požádat o vydání certifikátu** u zvolené certifikační autority.

Přípravné kroky jsou podrobněji popsány v kapitole 10.

3 PŘED SPUŠTĚNÍM SPRÁVCE KARTY

Před prvním spuštěním aplikace *eObčanka – Správce karty* je třeba na počítač instalovat software *eObčanka*. Aplikace *eObčanka – Správce karty* je součástí instalačního balíčku. Součástí balíčku jsou i další aplikace a ovladače potřebné pro správné fungování a používání elektronického čipu občanského průkazu.

Instalaci software *eObčanka* je třeba provést pod účtem správce operačního systému. Instalované aplikace (včetně *Správce karty*) jsou po instalaci dostupném všem uživatelům daného počítače.

Podrobný popis instalace software *eObčanka* je popsán v samostatné příručce.

Pro práci s aplikací *eObčanka - Správce karty* musí mít držitel občanského průkazu k počítači připojenu čtečku čipových karet. Čtečka může být buď přímo v počítači integrovaná, nebo se může k počítači připojovat jako externí zařízení, například pomocí kabelu a rozhraní USB. Pro zprovoznění některých čteček je třeba instalovat také příslušné ovladače. Při zprovoznění čtečky karet by se měl uživatel řídit pokyny výrobce nebo dodavatele čtečky.

Aplikace *eObčanka – Správce karty* spolupracuje s různými druhy čteček čipových karet.

- Čtečky integrované v některých noteboocích.
- Čtečky integrované v klávesnicích, připojených ke stolnímu počítači.
- Čtečky připojené k počítači pomocí kabelu.
- Čtečky s integrovanou klávesnicí a případně i displejem.

Po úspěšné instalaci software *eObčanka*, připojení čtečky a vložení občanského průkazu, může uživatel aplikaci *eObčanka – Správce karty* spustit a využívat.

eObčanka – Správce karty spolupracuje s občanskými průkazy České republiky s kontaktním elektronickým čipem, vydanými před 1. 7. 2018 (starší verze) i po 1. 7. 2018 (novější verze). Pro starší verzi občanských průkazů *Správce karty* nabízí jen omezenou sadu funkcí.

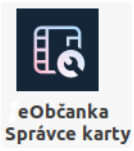
4 SPUŠTĚNÍ SPRÁVCE KARTY

Před spuštěním *Správce karty* se doporučuje připojit k počítači čtečku a vložit do ní občanský průkaz. (Tyto kroky nejsou povinné, čtečku lze připojit a občanský průkaz vložit i po spuštění *Správce karty*.)

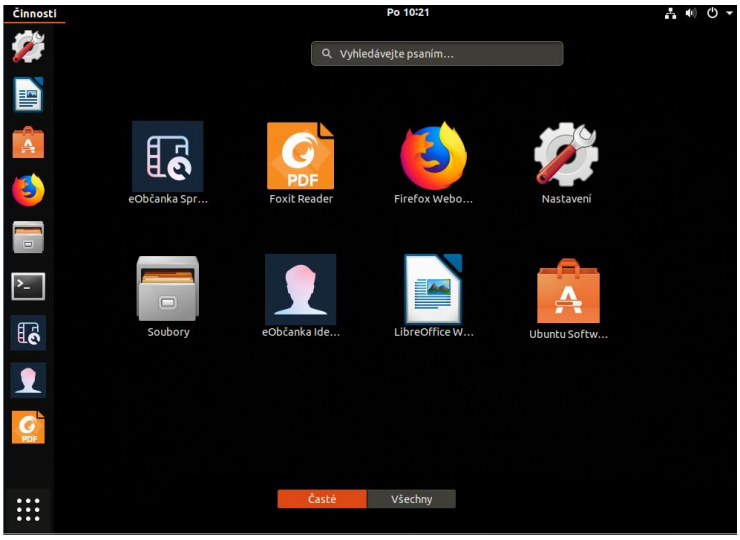
4.1 Spuštění aplikace

Aplikaci *eObčanka – Správce karty* lze spustit několika způsoby:

- Obvykle se aplikace spouští prostřednictvím zástupce *eObčanka – Správce karty* z menu *Aplikace*.



Obrázek 2: Zástupce aplikace eObčanka - Správce karty

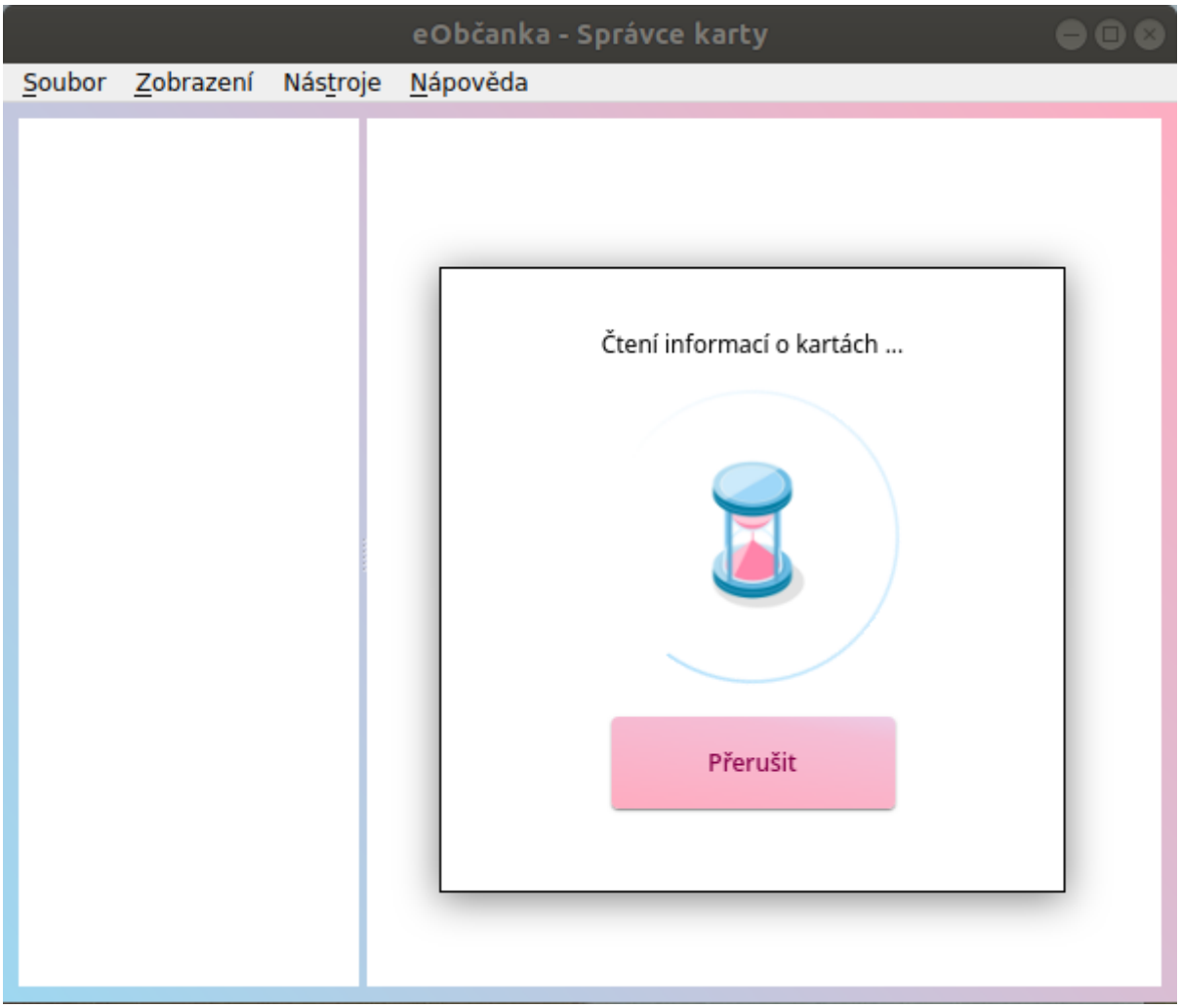


Obrázek 3: Okno s instalovanými aplikacemi, včetně zástupce Správce karty

- Správce karty lze spustit také pomocí spouštěcího skriptu v cestě */opt/eObcanka/SpravceKarty/eopcardman.sh*

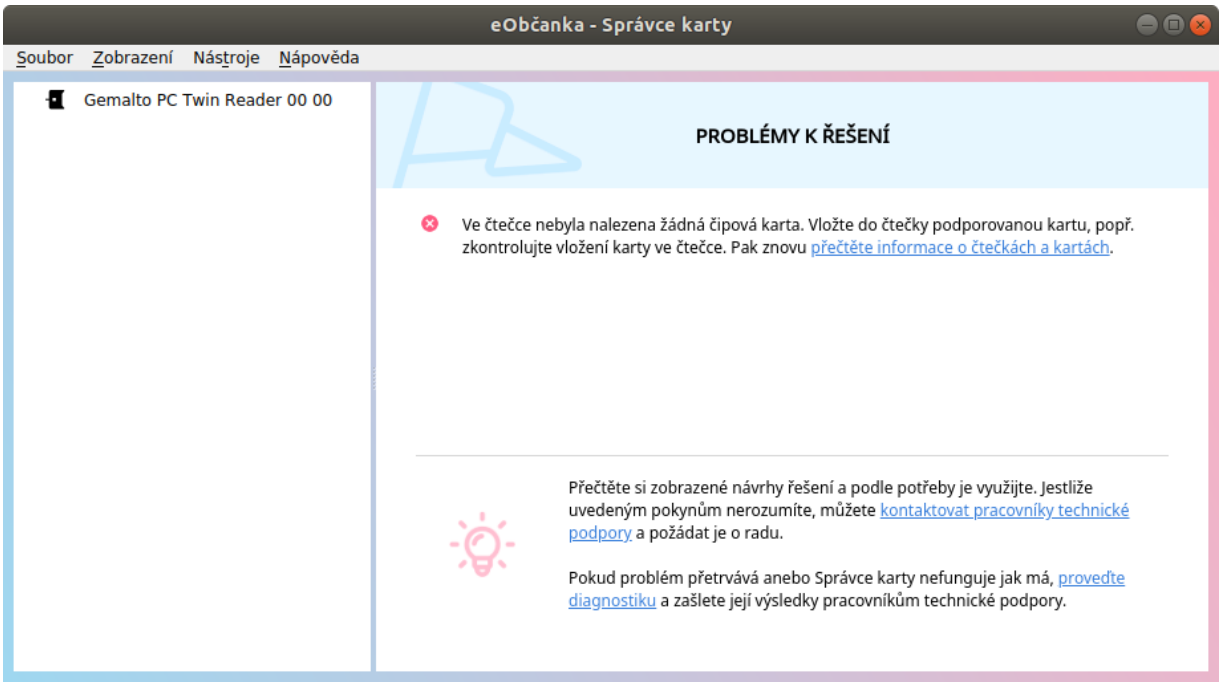
4.2 Vyčtení obsahu čipu občanského průkazu

Po spuštění se *Správce karty* pokouší automaticky detekovat připojené čtečky a přečíst obsah občanských průkazů, nalezených ve čtečkách:



Obrázek 4: Průběh čtení informací z čipu občanského průkazu

Po vyčtení se nalezené údaje zobrazí do okna aplikace (v levé části okna je výčet nalezených čteček a občanských průkazů, v pravé části okna pak detailní informace, případně problémy k řešení). Pokud aplikace nenalezne žádnou čtečku anebo není-li ve čtečce nalezen občanský průkaz, je uživatel vyzván k připojení čtečky či vložení občanského průkazu:



Obrázek 5: Okno s výzvou k vložení občanského průkazu a vyčtení obsahu čipu

Pro správné fungování je třeba přečíst obsah čipu občanského průkazu. *Správce karty* se snaží obsah čipu vyčíst automaticky po spuštění. Uživatel může vyčtení obsahu čipu kdykoli vynutit

- pomocí menu *Zobrazení* → *Obnovit,*
- anebo stiskem klávesy F5.

Uživatel může načítání obsahu přerušit pomocí tlačítka *Zrušit*. Aplikace zobrazí upozornění, že čtení dat bylo přerušeno. Pro korektní práci se *Správcem karty* je třeba vyčíst kompletní data z čipu.

eObčanka – Správce karty dokáže pracovat najednou i s více připojenými čtečkami čipových karet. v každé z připojených čteček může být vložen občanský průkaz. *Správce karty* načítá postupně obsah všech připojených občanských průkazů a následně s nimi umožní provádět podporované operace.

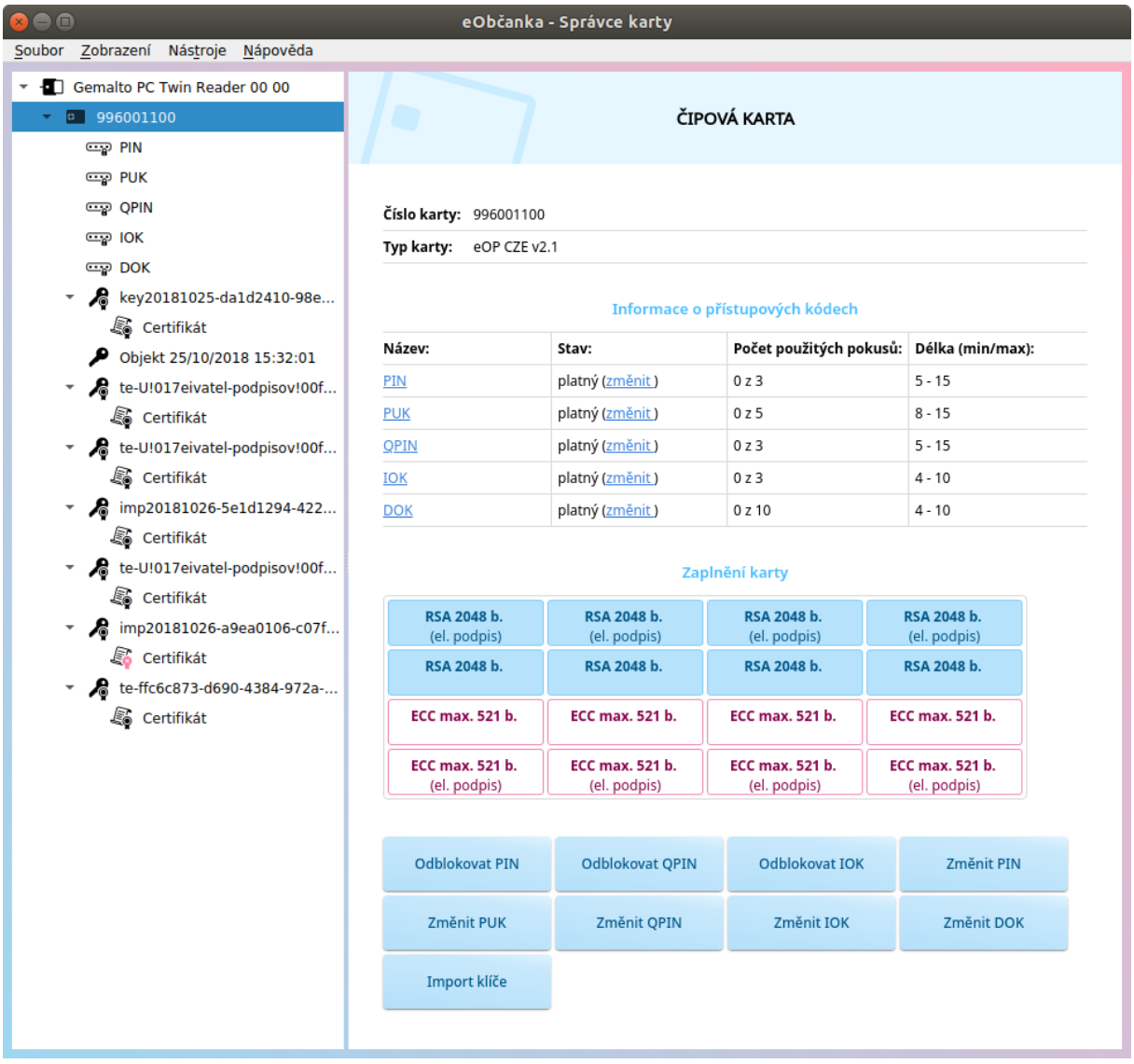
5 OVLÁDÁNÍ PROGRAMU

Správce karty je grafická aplikace s oknem rozděleným na levý a pravý panel. Pro ovládání aplikace jsou používány obvyklé prvky:

- Menu
- Tlačítka
- Odkazy

Uživatel kliká na nabízené možnosti a aplikace na ně příslušným způsobem reaguje.

Pro správnou funkci *Správce karty* je třeba přečíst obsah čipu občanského průkazu – viz kapitola 4.2. Většina aplikačních funkcí se zpřístupní až po úspěšném načtení dat z občanského průkazu.



Obrázek 6: Ilustrační obrázek grafického rozhraní aplikace eObčanka – Správce karty

5.1 Aplikační menu

Aplikační menu je zobrazeno v horní části okna aplikace, pod horní lištou aplikačního okna. Přes aplikační menu jsou dostupné základní položky pro práci s aplikací.

Aplikační menu má dvě úrovně a obsahuje tyto položky:

- *Soubor*
  - *Konec* - ukončí běh aplikace.
- *Zobrazení*
  - *Standardní* - přepne fungování *Správce karty* do režimu *standardního* zobrazení – viz kapitola 5.5.
  - *Rozšířené* - přepne fungování *Správce karty* do režimu *rozšířeného* zobrazení – viz kapitola 5.5.
  - *Obnovit F5* - přečte informace o připojených kartách a čtečkách, zobrazí aktualizované informace.
- *Nástroje*
  - *Zobrazit diagnostiku* - zobrazí do pravého panelu diagnostické informace – viz kapitola 9.3.
  - *Uložit diagnostiku* - umožní uživateli uložit diagnostické údaje do textového souboru – viz kapitola 9.3.
  - *Problémy k řešení* - zobrazí do pravého panelu seznam nalezených problémů a návrhy jejich řešení – viz kapitola 9.1.
  - *Nastavení* – umožní uživateli ovlivnit některé parametry chování aplikace – viz kapitola 9.6.
- *Nápověda*
  - *O aplikaci* - zobrazí informace o aplikaci (číslo verze software *eObčanka*, licenční ujednání, apod…).
  - *Uživatelská příručka* – zobrazí PDF dokument s uživatelskou příručkou *Správce karty*.
    Pro zobrazení se použije výchozí prohlížeč PDF dokumentů, instalovaný v počítači.

5.2 Levý panel se stromem informací

Po načtení obsahu čipu se v levém panelu zobrazí stromová struktura se zjištěnými informacemi:

- Není-li k PC připojena žádná čtečka, je obsah stromu prázdný. Uživatel by měl k PC připojit čtečku a vložit do ní občanský průkaz. Pak znovu načíst informace z čipu (pomocí stisku klávesy F5, nebo prostřednictvím aplikačního menu *Zobrazení* - *Obnovit*).
- Není-li ve čtečce vložen občanský průkaz, zobrazí se ve stromu pouze čtečka. Uživatel by měl do čtečky vložit občanský průkaz a pak znovu načíst informace (viz předchozí bod).
- Je-li ve čtečce vložen občanský průkaz, vyčte aplikace *eObčanka - Správce karty* informace z čipu a přehledně je zobrazí v levém panelu aplikace.

- K počítači může být připojeno více čteček a v nich vloženo více občanských průkazů. v takovém případě *Správce karty* vyčte a zobrazí informace ze všech nalezených občanských průkazů.

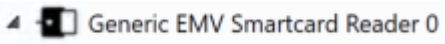
Obrázek 7: Okno levého panelu Správce karty se stromem informací

Jednotlivé údaje jsou ve stromu zobrazovány vždy jako dvojice: grafický symbol + textový popis.

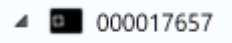
- **Symboly** zjednodušeně reprezentují typ a někdy i stav daného objektu. Díky symbolům ve stromu má uživatel stručný přehled o celkovém stavu karty. Růžovou barvou se zobrazují symboly objektů, které nejsou v pořádku; takovým objektům by uživatel měl věnovat pozornost.
- Textový **popis** uvádí základní informaci o daném objektu.

Ve stromu se zobrazuje hierarchie těchto objektů:

- **Čtečka** - v textovém popisu se zobrazuje název čtečky vyčtený z operačního systému.

- **Karta** (občanský průkaz) - v textovém popisu se uvádí číslo dokladu.

- **Přístupový kód** (typu PIN, IOK, atd…) - v textovém popisu se uvádí název přístupového kódu.

- Kryptografický **klíč** - v textovém popisu se uvádí identifikátor klíče.

- **Certifikát** - v textovém popisu se uvádí jméno držitele certifikátu.

Uživatel může myší označovat jednotlivé objekty ve stromu informací zobrazeném v levém panelu aplikace. Po kliknutí na objekt se v pravém panelu zobrazí podrobná informace o

označeném objektu. Pro označenou položku je také dostupné kontextové menu, které se zobrazí pomocí pravého tlačítka myši.

Označováním položek ve stromu informací uživatel může:

- Zjišťovat podrobné informace o jednotlivých objektech.
- Provádět operace s vybraným objektem.

5.3 Pravý panel s podrobnostmi o zvoleném objektu

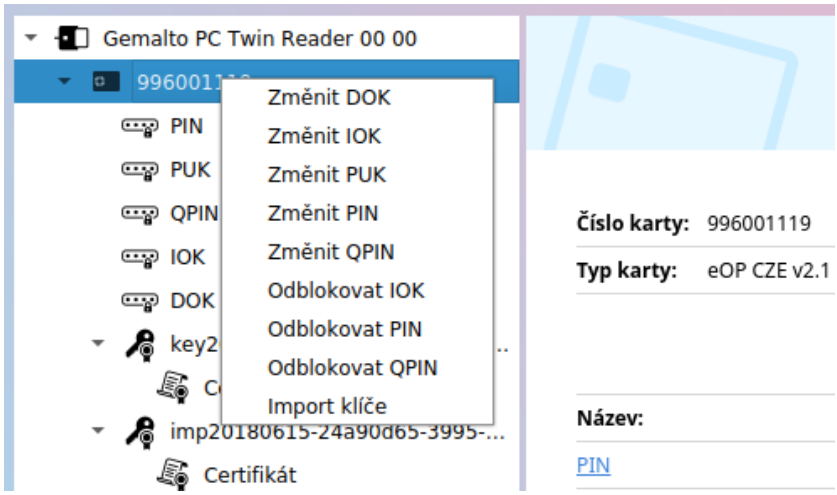
Po označení položky ve stromu informací se aktualizují informace v pravém panelu: zobrazí se informace o zvoleném objektu, a také seznam operací, které lze s označeným objektem provést. Uživatel může v pravém panelu:

- prohlížet zobrazené informace,
- spouštět akce nad zvoleným objektem (pomocí tlačítek či odkazů).

Podrobnosti o informacích, zobrazovaných v pravém panelu, jsou uvedeny v kapitole 6.

5.4 Kontextové menu

Silným nástrojem pro ovládání aplikace *eObčanka – Správce karty* je kontextové menu. Pokud uživatel označí objekt ve stromu informací a klikne na objekt pravým tlačítkem myši, zobrazí se kontextové menu. v kontextovém menu je nabídnuta sada operací, které lze nad označeným objektem aktuálně provést. (Nenabízí se operace, které pro daný objekt nemají smysl, nebo označený objekt není ve *stavu*, kdy by bylo možné určitou operaci provést.) Uživatel si může z kontextového menu zvolit, jakou z nabízených operací chce nad označeným objektem provést.



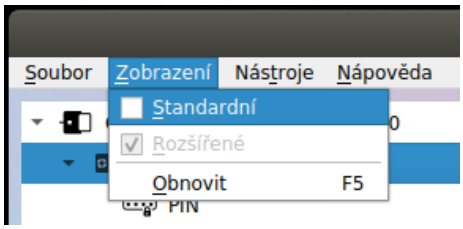
Obrázek 8: Kontextové menu objektu občanský průkaz (karta)

5.5 Standardní a rozšířené zobrazení

Aplikace *eObčanka – Správce karty* může fungovat v jednom ze dvou režimů zobrazení:

- Ve **standardním** zobrazení je uživateli dostupná *základní* sada běžně používaných informací a operací.
  Ve standardním zobrazení nejsou nabízeny operace mazání dat z čipu (aby nedošlo k nechtěnému smazání důležitých údajů).
- V **rozšířeném** zobrazení jsou uživateli dostupné *všechny* operace základního zobrazení, a navíc také:
  - operace **mazání dat** z čipu,
  - podrobnější informace o objektech karty, které běžný uživatel často nevyužije,
  - specifické operace expertního charakteru, které běžný uživatel většinou nepotřebuje, např. export veřejné části klíče.

Mezi standardním a rozšířeným zobrazením se uživatel může přepínat pomocí aplikačního menu *Zobrazení:*



Obrázek 9: Přepínání mezi standardním a rozšířeným zobrazením

5.6 Schvalování operací pomocí PIN či QPIN

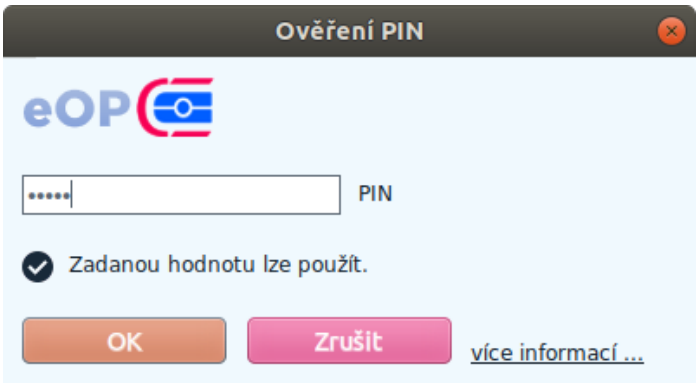
Řadu operací (import, mazání, atp…), které lze pomocí *Správce karty* provést, je třeba schválit pomocí přístupového kódu PIN, popř. QPIN.

Podle typu použité čtečky zadává uživatel hodnoty přístupových kódů:

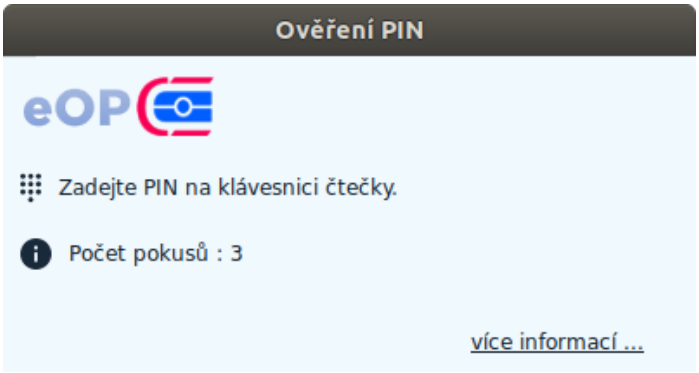
- Na klávesnici počítače (běžná čtečka bez klávesnice).
- Na klávesnici čtečky (čtečka s klávesnicí, popř. i displejem).

Při použití čtečky s integrovanou klávesnicí je třeba zadat přístupový kód v průběhu *každé* aktivní operace. Při použití běžné čtečky:

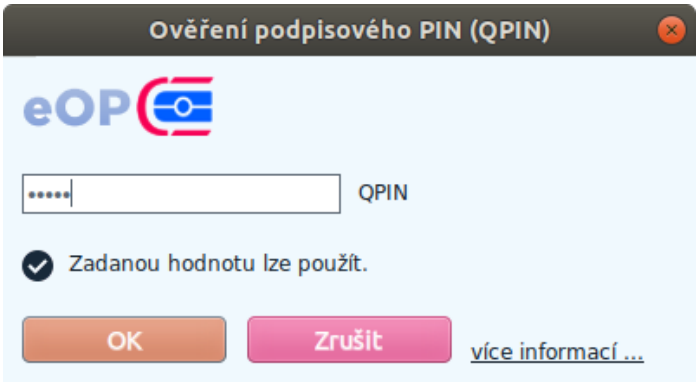
- Je třeba hodnotu QPIN zadávat *opakovaně*, pro každou operaci, která vyžaduje schválení pomocí QPIN.
- Hodnota PIN se zadává jen *jedenkrát*; pro další operace jsou operace s čipem automaticky schváleny a hodnotu PIN není třeba znovu zadávat.



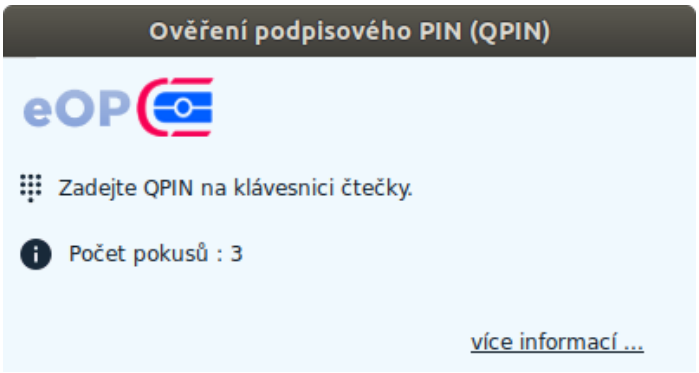
Obrázek 10: Okno pro zadání PIN na klávesnici počítače (použití běžné čtečky)



Obrázek 11: Okno s výzvou k zadání PIN na klávesnici čtečky



Obrázek 12: Okno pro zadání QPIN na klávesnici počítače (použití běžné čtečky)



Obrázek 13: Okno s výzvou k zadání QPIN na klávesnici čtečky (čtečka bez displeje)

Ovladače občanského průkazu vyzvou k zadání příslušného přístupového kódu vždy, když je to potřeba - zobrazí okno pro zadání přístupového kódu a informují uživatele, jaký kód má zadat. Pokud uživatel udělá při zadání přístupového kódu chybu, může zadat hodnotu kódu znovu.

Upozornění: Uživatel musí rozlišovat, jaký kód po něm ovladače požadují. Častou **chybou** je **záměna hodnot PIN a QPIN**. Opakovaným chybným zadáním se přístupový kód **zablokuje**.

Pokud uživatel opakovaným chybným zadáním zablokuje přístupový kód, může jej odblokovat pomocí *Správce karty* – viz kapitola 8.

6 ZOBRAZENÍ OBSAHU ČIPU

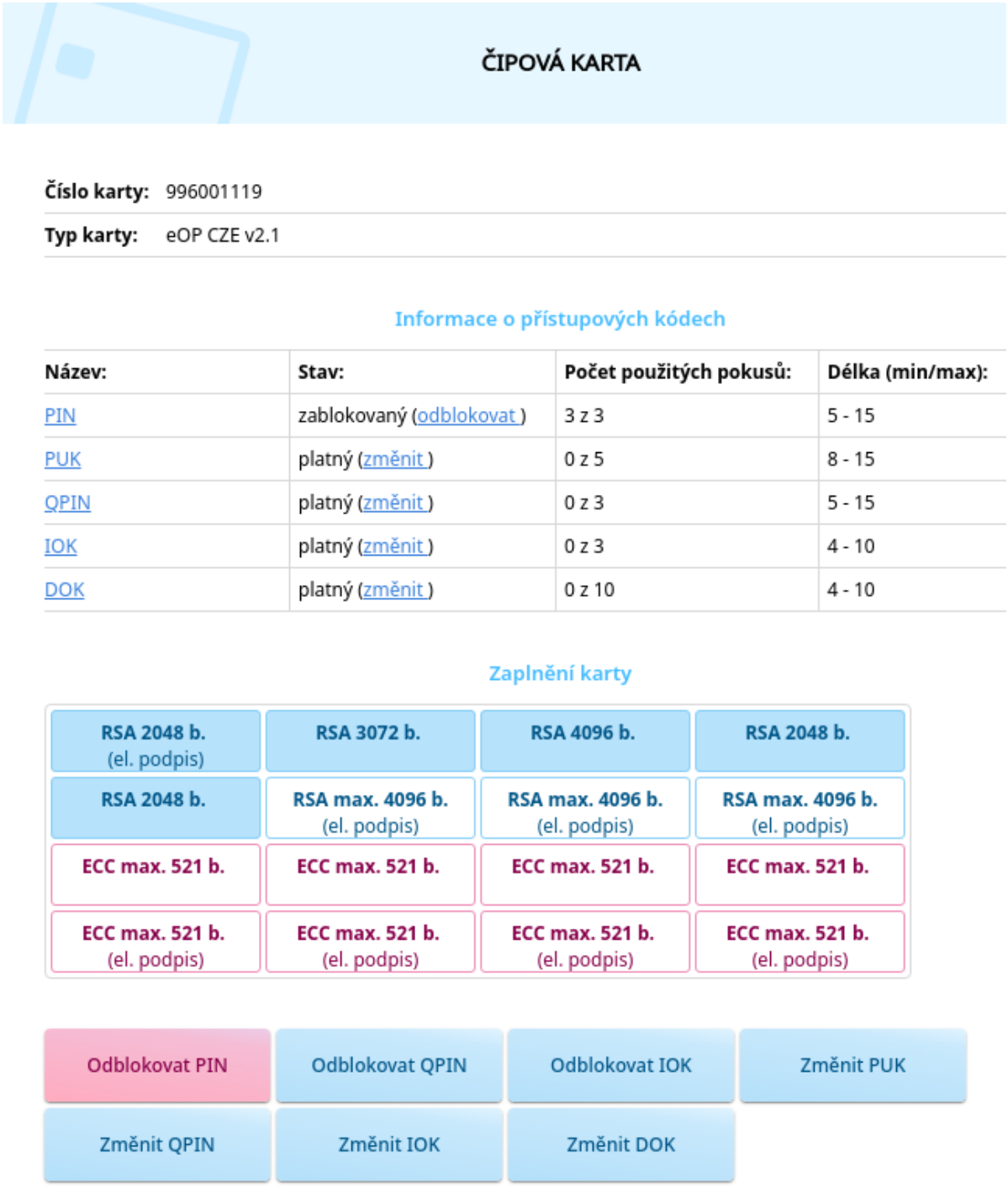
Po načtení dat z občanského průkazu může uživatel zobrazit obsah čipu. Do levého panelu se zobrazí strom zjištěných informací. Označováním jednotlivých položek ve stromu lze zobrazovat podrobnosti o označených položkách.

V následujících podkapitolách jsou podrobněji popsány informace, které se zobrazují o jednotlivých objektech stromu informací. Jsou také uvedeny akce, které lze s daným objektem provádět.

6.1 Informace o čipové kartě (čipu občanského průkazu)

V pravém panelu jsou dostupné podrobné informace o vloženém občanském průkazu.

- *Číslo karty* – číslo dokladu.
- *Typ karty* – technický identifikátor, pod kterým je občanský průkaz rozpoznán v operačním systému.
  - občanské průkazy, vydané před 1. 7. 2018 mají v této položce hodnotu *eOP CZE v1.0.*
  - občanské průkazy, vydané po 1. 7. 2018 mají v této položce hodnotu *eOP CZE v2.1.*



Obrázek 14: Panel s informacemi o čipové kartě (občanském průkazu)

6.1.1 Informace o přístupových kódech

Pod základní informací o čipu jsou zobrazeny informace o stavu **přístupových kódů** občanského průkazu. Počet přístupových kódů záleží na druhu občanského průkazu:

- Občanské průkazy vydávané po 1. 7. 2018 mají 5 přístupových kódů.

- Starší občanské průkazy mají pouze 2 přístupové kódy (PIN a PUK).

Tabulka uvádí jednotlivé přístupové kódy:

- PIN - slouží ke schvalování operací s certifikáty a kryptografickými klíči.
- QPIN – slouží ke schválení vytvoření kvalifikovaného podpisu.
- PUK – slouží k nastavení či odblokování přístupových kódů PIN a QPIN.
- IOK – slouží ke schvalování identifikace pomocí občanského průkazu, a také k nastavení kódu PUK.
- DOK - slouží k odblokování zablokovaného přístupového kódu IOK.

Informace o přístupových kódech

Název:	Stav:	Počet použitých pokusů:	Délka (min/max):
PIN	zablobkovaný (nelze odblokovat)	3 z 3	5 - 15
PUK	neinicializovaný (nastavit)	5 z 5	8 - 15
QPIN	zablobkovaný (nelze odblokovat)	3 z 3	5 - 15
IOK	platný (změnit)	0 z 3	4 - 10
DOK	platný (změnit)	0 z 10	4 - 10

Obrázek 15: Tabulka s informacemi o přístupových kódech

Každý z přístupových kódů je zobrazen jako jeden řádek tabulky. Ke každému z kódů jsou zobrazeny detailní informace a případně i další dostupné operace, které může uživatel s daným kódem provést:

- ***Název*** - název přístupového kódu, např. *PIN, PUK, IOK*….
  Pole *Název* slouží zároveň jako odkaz pro zobrazení podrobných informací o daném kódu – viz také kapitola 6.2.
- ***Stav*** - aktuální stav přístupového kódu, v závorce je zobrazen také odkaz na akci, která je pro přístupový kód aktuálně dostupná, např. *Zablokovaný (Odblokovat), Platný (Změnit)...* Viz také kapitola 8.
- ***Počet použitých pokusů*** - je zobrazen maximální počet pokusů pro zadání přístupového kódu do zablokování kódu a počet již použitých zadání nesprávné hodnoty. Např. *3 z 3, 0 z 10*...
- ***Délka (min. / max.)*** - Je zobrazena minimální požadovaná a maximální povolená délka přístupového kódu. Počet číslic pro daný přístupový kód. Např. 5 – 15 (číslic), 4 - 10...

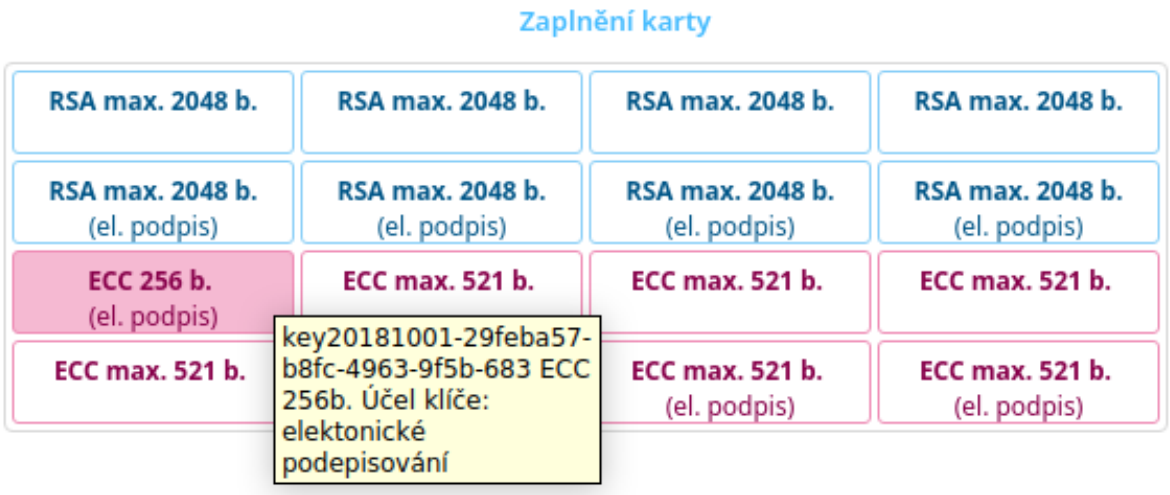
Pozn.: Přehled přístupových kódů občanského průkazu je uveden v kapitole 8.1.

6.1.2 Informace o zaplnění karty

Do čipu občanského průkazu lze uložit několik certifikátů s kryptografickým klíčem. Jednotlivé verze občanských průkazů se liší

- počtem certifikátů, které lze do čipu uložit,
- počtem a typem kryptografických klíčů, příslušných k jednotlivým certifikátům.

Pod informacemi o přístupových kódech je zobrazena grafická reprezentace občanského průkazu s přehledem kontejnerů, které jsou na občanském průkazu dostupné. Kontejner je logické místo v čipu občanského průkazu, do nějž lze uložit kryptografický klíč (klíčový pár) a certifikát.



Obrázek 16: Grafická reprezentace obsazení kontejnerů klíči a certifikáty

Díky tabulce s kontejnery získá uživatel jednoduchý přehled nad zaplněním čipu občanského průkazu (zjednodušeně: kolik je v občanském průkazu uloženo certifikátů a kolik jich do čipu ještě lze uložit).

O každém kontejneru se zobrazují informace:

- Zda je kontejner prázdný či zaplněný (kryptografickým klíčem). Prázdný kontejner je vyplněn bílou barvou.
- *Algoritmus klíče* – starší verze občanských průkazů podporují jen klíče s algoritmem RSA. Občanské průkazy, vydávané po 1. 7. 2018 podporují kontejnery pro klíče s algoritmy RSA nebo ECC.
- *Délka klíče* – je uvedena buď pevná délka klíče, nebo maximální délka klíče, který lze do daného kontejneru uložit, např. *384 b.,* nebo *max. 4096 b.*
- *Účel klíče* – kontejnery klíčů pro elektronické podepisování mají uvedeno *el. podpis*, ostatní kontejnery tuto informaci nemají uvedenu. (Klíče pro elektronické podepisování se generují v čipu občanského průkazu. Lze s nimi provádět pouze operace elektronického podepisování.)

Pokud uživatel nastaví kurzor myši na vybraný kontejner, zobrazí aplikace tooltipu s dalšími informacemi o kontejneru:

- *Klíč* - uvádí identifikátor klíče; pro kontejnery bez klíče je uvedeno: *(volný prostor pro klíč).*
- Algoritmus a délka klíče. Pro prázdné kontejnery bez klíče může být uvedena maximální délka klíče, který lze do kontejneru zapsat.
- *Účel klíče* – uvádí informaci, jaké operace lze s daným klíčem provádět:
  - Klíče, určené výhradně pro operace podepisování mají uvedeno: *elektronické podepisování.*
  - Klíče, které nemají omezení na provádění operací, mají uvedeno: *obecné použití.*

Po kliknutí na *obsazený* kontejner se do pravého panelu *Správce karty* zobrazí informace o zvoleném klíči. Viz také kapitola 6.3.

6.1.3 Tlačítka akcí

Pod informacemi o zaplnění karty jsou zobrazena tlačítka dostupných akcí přístupových kódů a možnost importu certifikátu s klíčem do čipu občanského průkazu.

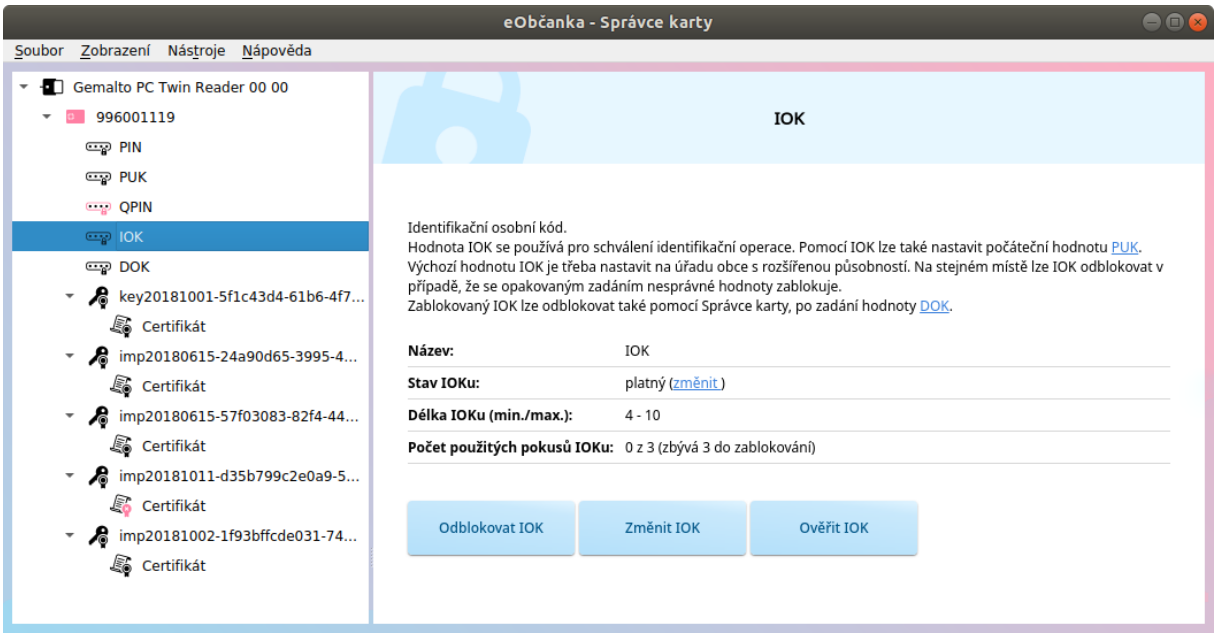
Obrázek 17: Seznam tlačítek akcí pro čip občanského průkazu

Seznam tlačítek se mění podle aktuálního stavu občanského průkazu. Stisknutím tlačítka může uživatel spustit příslušnou operaci (operace jsou popsány níž v tomto dokumentu).

6.2 Informace o přístupovém kódu

Pozn.: seznam přístupových kódů občanského průkazu je uveden v kapitole 6.1.1.

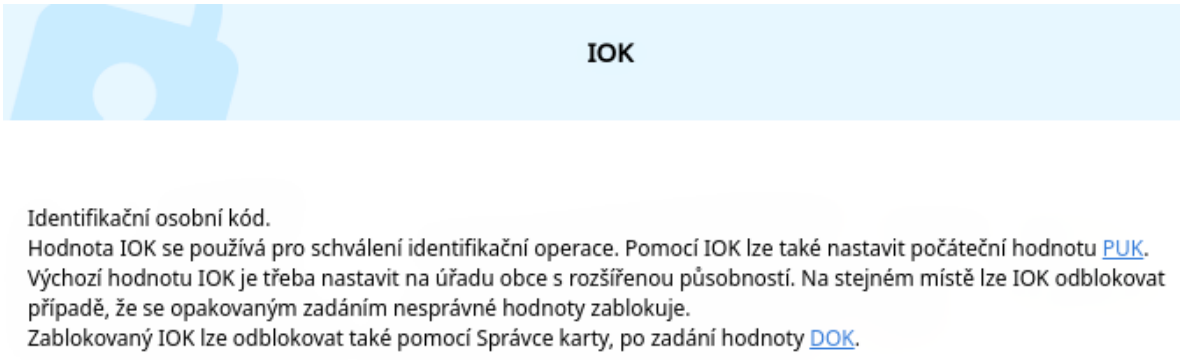
O každém z přístupových kódů občanského průkazu lze zobrazit podrobné informace:



Obrázek 18: Okno s informacemi o přístupovém kódu (IOK)

Informace se pro jednotlivé přístupové kódy liší a odrážejí aktuální stav daného kódu.

V horní části okna je uveden název kódu a zobrazena informace o účelu použití daného přístupového kódu. Informace slouží jako nápověda pro práci s tímto kódem a uvádí příklad jeho použití:



Obrázek 19: Informace o účelu použití přístupového kódu

Pod informací o přístupovém kódu se zobrazuje tabulka s podrobnými informacemi o daném kódu:

- ***Název*** - název přístupového kódu, např. *PIN, PUK, IOK*….
- ***Stav*** - aktuální stav přístupového kódu, v závorce je zobrazen také odkaz na akci, která je pro přístupový kód aktuálně dostupná, např. *Zablokovaný (Odblokovat), Platný (Změnit)...* Viz také kapitola 8.
- ***Délka (min. / max.)*** - Je zobrazena minimální požadovaná a maximální povolená délka přístupového kódu. Počet číslic pro daný přístupový kód. Např. 5 – 15 (číslic), 4 - 10...

- ***Počet použitých pokusů*** - je zobrazen počet již použitých zadání nesprávné hodnoty a maximální počet pokusů pro zadání přístupového kódu. Je také uvedeno, kolik nesprávných pokusů zbývá do zablokování kódu.

Název:	IOK
Stav IOKu:	platný (změnit)
Délka IOKu (min./max.):	4 - 10
Počet použitých pokusů IOKu:	0 z 3 (zbývá 3 do zablokování)

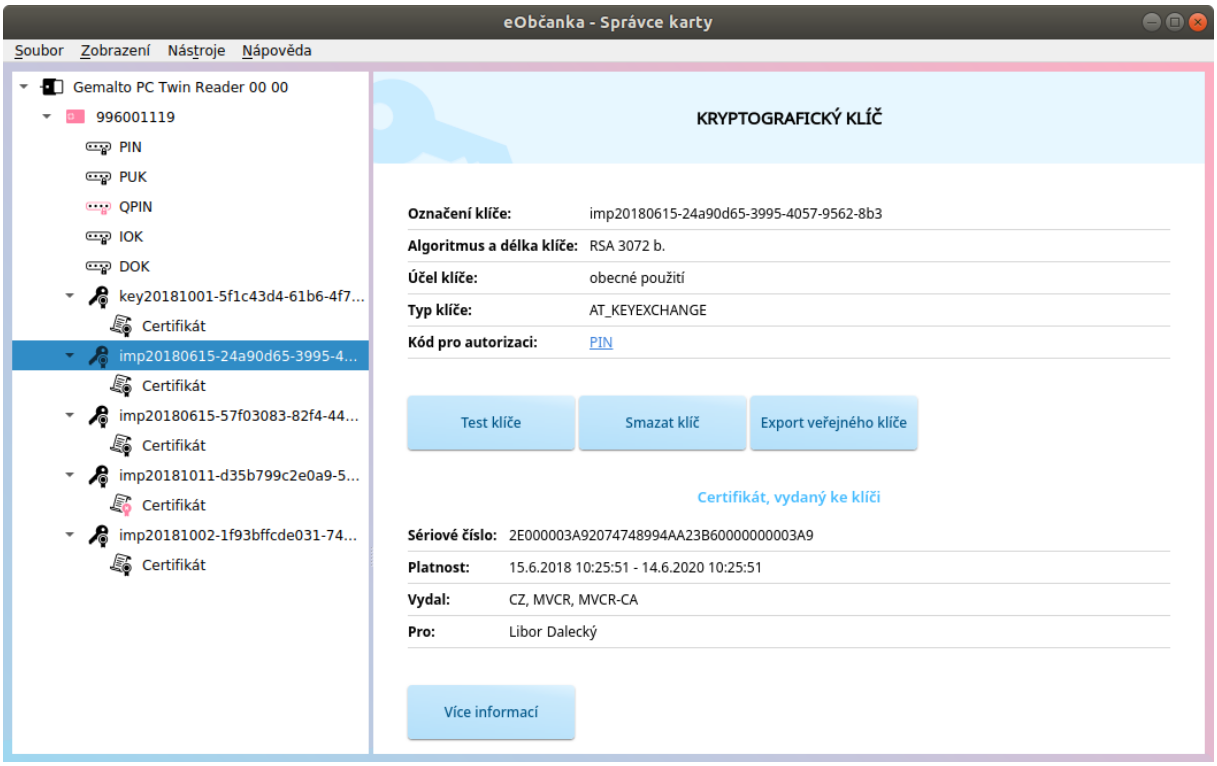
Obrázek 20: Tabulka informací o přístupovém kódu (IOK)

Pod tabulkou s informacemi o přístupovém kódu jsou zobrazena tlačítka akcí, které lze s daným přístupovým kódem provést. Tlačítka se zobrazují podle aktuálního stavu přístupového kódu. Obvykle se zobrazuje pouze jedno tlačítko:

- Pro *Platný* přístupový kód se nabízí tlačítko *Změnit* – viz kapitola 8.5.
- Pro *Neinicializovaný* přístupový kód se nabízí tlačítko *Nastavit* – viz také kapitola 8.4.
  - Některé přístupové kódy nelze nastavit pomocí Správce karty, např. DOK a IOK.
- Pro *Zablokovaný* přístupový kód se nabízí tlačítko *Odblokovat* – viz také kapitola 8.6.
  - Musí existovat platný přístupový kód, pomocí lze odblokování provést, např. odblokování PIN pomocí PUK.

6.3 Informace o kryptografickém klíči

Okno s informacemi o kryptografickém klíči a certifikátu, příslušném k danému klíči:



Obrázek 21: Okno s informacemi o kryptografickém klíči

Informací o klíči se zobrazuje poměrně málo. Pro uživatele jsou podstatnější informace, uložené v certifikátu daného klíče. Proto se v okně s informacemi o klíči zobrazují také základní informace o certifikátu (je-li certifikát dostupný).

6.3.1 Informace o klíči

Informace o klíči jsou sestaveny do tabulky s informacemi:

- **Označení klíče** - uvádí technický identifikátor klíče v čipu občanského průkazu.
- **Algoritmus a délka klíče** - uvádí algoritmus a délku klíče, např.: RSA 2048 b., ECC 384 b.
- **Účel klíče** - uvádí informaci o základním účelu klíče: *elektronické podepisování* nebo *obecné použití*. Rozlišuje se na základě příznaku, zda je klíč určen pouze pro podpis anebo zda s ním lze provádět i další operace.
- **Typ klíče** - technická informace o typu klíče. Pro klíče RSA se uvádí AT_SIGNATURE (podpisový) anebo AT_KEYEXCHANGE (obecné použití). Pro klíče ECC se uvádí AT_ECDSA_Pnnn (podpisový) anebo AT_ECDHE_Pnnn (autentizační, šifrovací).
  Tato informace se zobrazuje jen v rozšířeném zobrazení *Správce karty*, viz kapitola 5.5.
- **Kód pro autorizaci** - uvádí název přístupového kódu, který slouží pro schválení operací s daným klíčem. Po kliknutí na název autorizačního kódu se zobrazí informace o daném kódu. Viz také kapitola 6.2.

6.3.2 Tlačítka pro spouštění operací nad klíčem

Pod tabulkou s informacemi o klíči se zobrazují tlačítka pro spouštění operací, které lze nad daným klíčem provádět. Nabízejí se operace:

- **Test klíče** - spouští operaci pro otestování klíče. Uživatel může pomocí této operace prověřit, zda je klíč v pořádku a lze s ním provádět kryptografické operace. Viz také kapitola 7.4.
- **Import certifikátu** - spouští operaci importu certifikátu ze souboru.
  Zobrazuje se jen v případě, že ke klíči není nalezen certifikát - ani v čipu karty, ani v operačním systému. Viz také kapitola 7.1.2.
  Pozn.: tato funkce slouží pouze pro import certifikátu, jehož klíč je již v čipu uložen. Pro import klíče s certifikátem slouží operace *Import klíče*, dostupná z kontextového menu karty.
- **Smazat klíč** - spouští operaci smazání klíče z karty.
  Tlačítko pro smazání klíče se zobrazuje jen v režimu rozšířeného zobrazení *Správce karty*, viz kapitola 5.5.
- **Export veřejného klíče** - exportuje veřejnou část klíče do souboru. Viz také kapitola 7.2.2.
  Tlačítko pro export veřejného klíče se zobrazuje jen v režimu rozšířeného zobrazení *Správce karty*, viz kapitola 5.5.

6.3.3 Informace o certifikátu

Pokud je ke klíči dostupný certifikát (uložený v čipu anebo jen v operačním systému), je pod tlačítky, v sekci *Certifikát, vydaný ke klíči*, uvedena tabulka se základními informacemi o certifikátu:

- **Sériové číslo** - sériové číslo certifikátu.
- **Platnost** - platnost certifikátu od-do.
- **Vydal** - uvádí informaci o vydavateli certifikátu.
- **Pro** - uvádí informaci o držiteli certifikátu.

Obrázek 22: Informace o certifikátu, příslušnému k danému klíči

6.3.4 Odkazy na akce s certifikátem

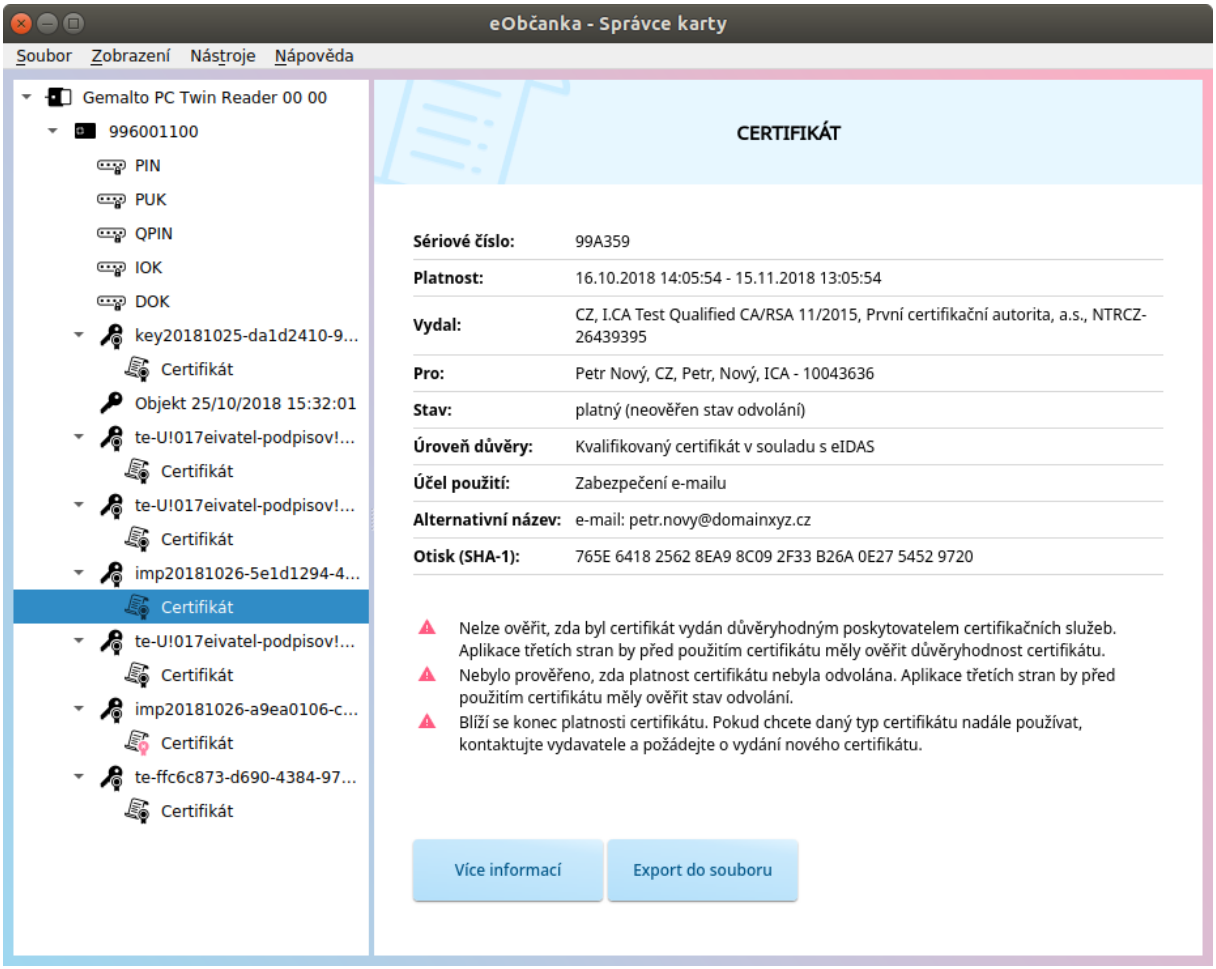
Pod tabulkou s informacemi o certifikátu se formou tlačítka zobrazují akce, které lze s certifikátem provést:

- **Více informací** - zobrazí okno s podrobnými informací o certifikátu – viz kapitola 6.4.

6.4 Informace o certifikátu

Ke každému kryptografickému klíči může být v čipu občanského průkazu uložen také certifikát. O certifikátu *Správce karty* zobrazuje:

- Tabulku se základními informacemi z certifikátu.
- Doplňující informace o certifikátu.
- Akce, které lze s certifikátem provést.



Obrázek 23: Okno s informacemi o certifikátu

6.4.1 Tabulka s informacemi o certifikátu

Tabulka s informacemi o certifikátu má proměnný počet řádků (některé informace nemusí být v certifikátu uvedeny - v takovém případě se v tabulce nezobrazují):

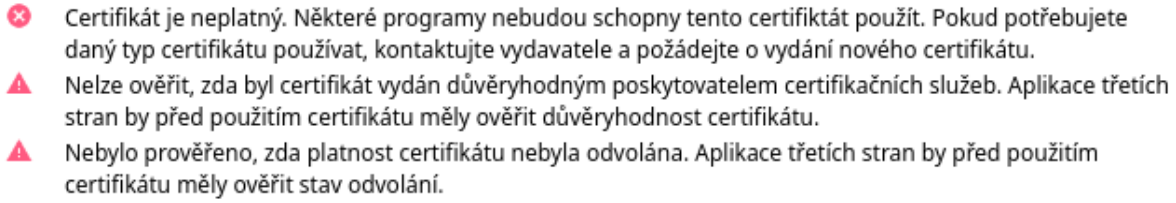
- **Sériové číslo** - sériové certifikátu.
- **Platnost** - platnost certifikátu od-do.
- **Vydal** - informace o vydavateli certifikátu.
- **Pro** - informace o držiteli certifikátu.
- **Stav** - informace o stavu certifikátu
  Mezi informacemi o stavu mohou být tyto hodnoty:
  - *platný* - Pokud časová platnost certifikátu dosud nevypršela, pak je certifikát označen jako platný.
    Správce karty při ověřování platnosti certifikátu nekontroluje, zda byla platnost certifikátu předčasně ukončena (nekontroluje se stav odvolání certifikátu). Pokud stav odvolání není prověřen, Správce karty na tuto skutečnost upozorní doplňujícím textem: *platný (neověřen stav odvolání).*
  - *expirovaný* - Certifikát je před započetím platnosti, anebo po vypršení platnosti. Kontrola se provádí proti lokálnímu času operačního systému.
- **Úroveň důvěry** - pro kvalifikované certifikáty se uvádí informace, že jde o kvalifikovaný certifikát podle parametrů daných nařízením eIDAS, popř. že je certifikát hostován na bezpečném prostředku pro vytváření podpisů.
  Položka se zobrazí, pokud je v certifikátu nalezen alespoň jeden z příznaků *QCStatements* dle normy ETSI EN 319 412-5.

  - Kvalifikovaný certifikát v souladu s eIDAS.
  - Klíč certifikátu je uložen v QSCD zařízení.

- **Účel použití** - uvádí seznam položek účelu použití (Extended Key Usage). Položky jsou zobrazeny jako textový popis, nebo OID identifikátor (pro méně známé účely použití).
- **Alternativní název** - uvádí seznam alternativních názvů držitele certifikátu, pokud jsou v certifikátu uvedeny. Např. UPN, e-mail, IP adresa, DNS.
- **Šablona** - identifikace šablony, podle níž byl certifikát vydán.
  Tato položka se typicky zobrazuje pro certifikáty vydané z certifikační autority v doméně MS Windows. Je uveden OID identifikátor šablony.
- **Otisk (SHA-1)** - hodnota SHA-1 hashe certifikátu.

6.4.2 Doplňující informace o certifikátu

Pod tabulkou se zobrazují doplňující informace o certifikátu, resp. upozornění na to, že je s certifikátem něco v nepořádku:



Obrázek 24: Doplňující informace o certifikátu

Aplikace *eObčanka – Správce karty* v některých případech nabízí uživateli možnost řešení nalezeného problému s certifikátem. v jiných případech pouze konstatuje zjištěnou skutečnost (např. *certifikát je neplatný*).

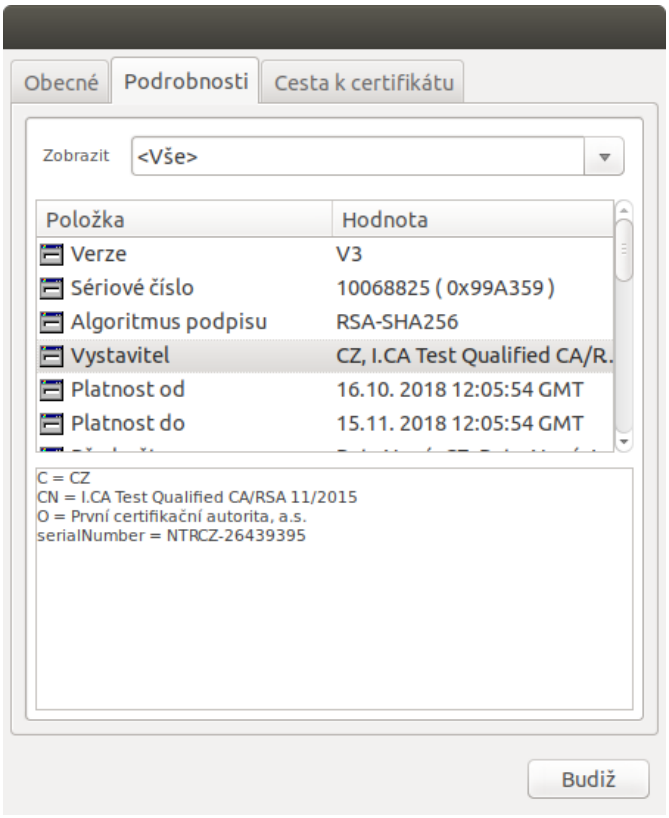
Jednotlivé typy informací se zobrazují pouze v případě, že jsou pro daný certifikát relevantní:

- Platnost certifikátu lze předčasně ukončit – certifikát lze odvolat a umístit na seznam odvolaných certifikátů.
  Správce karty nekontroluje, zda je daný certifikát umístěn na seznamu odvolaných certifikátů. Upozorní na to uživatele informací: *Nebylo prověřeno, zda platnost certifikátu nebyla odvolána. Aplikace třetích stran by před použitím certifikátu měly ověřit stav odvolání.*
  Informace se zobrazuje jen u certifikátů, které v sobě mají uvedenu adresu pro získání seznamu odvolaných certifikátů.
- Hostitelský operační systém neposkytuje informace o důvěryhodných poskytovatelích certifikačních služeb (důvěryhodných certifikačních autoritách). Správce karty proto není schopen ověřit, zda byl daný certifikát vydán důvěryhodným poskytovatelem. (Správce karty není schopen zkonstruovat tzv. certifikační cestu). Správce karty na tuto skutečnost upozorňuje informací: *Nelze ověřit, zda byl certifikát vydán důvěryhodným poskytovatelem certifikačních služeb. Aplikace třetích stran by před použitím certifikátu měly ověřit důvěryhodnost certifikátu.*
- Pokud je certifikát expirovaný, zobrazí se informace: *Certifikát je neplatný. Některé programy nebudou schopny tento certifikát použít. Pokud potřebujete daný typ certifikátu používat, kontaktujte vydavatele certifikátu a požádejte o vydání nového certifikátu.*
- Pokud se blíží expirace (platného) certifikátu, zobrazí se informace: *Blíží se konec platnosti certifikátu. Pokud chcete daný typ certifikátu nadále používat, kontaktujte vydavatele a požádejte o vydání nového certifikátu.*
  Informace o blížící se expiraci se zobrazuje 3 týdny před expirací. (Po expiraci se už toto upozornění nezobrazuje.)

6.4.3 Tlačítka pro operace s certifikátem

Pod seznamem s doplňujícími informacemi se formou tlačítek zobrazují akce, které lze s daným certifikátem provádět:

- **Více informací** - zobrazí okno s podrobnými informacemi o certifikátu.
- **Export do souboru** – spouští operaci exportu certifikátu do souboru – viz kapitola 7.2.1.
- **Smazat certifikát** - spouští operaci smazání certifikátu z čipu – viz kapitola 7.3.2
  Tlačítko pro smazání certifikátu se zobrazuje jen v režimu rozšířeného zobrazení *Správce karty*, viz kapitola 5.5.



Obrázek 25: Okno s informacemi o certifikátu - po stisku Více informací

7 SPRÁVA KLÍČŮ A CERTIFIKÁTŮ

V elektronickém čipu občanského průkazu mohou být uloženy kryptografické klíče a certifikáty. *eObčanka – Správce karty* umožňuje správu dat klíčů a certifikátů v čipu:

- **Importovat** klíče a certifikáty do čipu.
- **Exportovat** certifikáty a veřejné části klíčů do souboru.
- **Mazat** klíče a certifikáty z čipu.
- **Testovat** integritu a použitelnost klíčů.

7.1 Import dat do čipu občanského průkazu

Do čipu občanského průkazu lze importovat klíče a certifikáty:

- buď lze importovat klíč i s certifikátem,
- anebo lze ke klíči importovat do čipu příslušný certifikát.

Klíče se importují do logických oblastí, tzv. kontejnerů. Počet kontejnerů se pro jednotlivé verze občanských průkazů liší – zaplnění karty lze zjistit v okně s informacemi o kartě – viz kapitola 6.1.2.
Ke každému klíči lze do čipu uložit příslušný certifikát. Musí se shodovat veřejná část klíče v čipu s veřejným klíčem v certifikátu. Do čipu lze importovat pouze certifikáty, které mají v čipu uložen příslušný klíč (do čipu nelze importovat certifikát, jehož soukromý klíč není uložen v čipu).

7.1.1 Import klíče ze souboru

Do čipu občanského průkazu lze ze souboru importovat klíčový pár s certifikátem. Soubor, z nějž se data importují, musí být ve standardním formátu PKCS#12 (PFX). Data v souboru jsou zašifrována heslem.

Uživatel může do čipu importovat klíč s certifikátem, který mu byl vydán do souboru. Uložením klíče do čipu se zajistí vyšší ochrana a také mobilita klíče a certifikátu (uživatel si klíč s certifikátem bere s sebou na občanském průkazu).

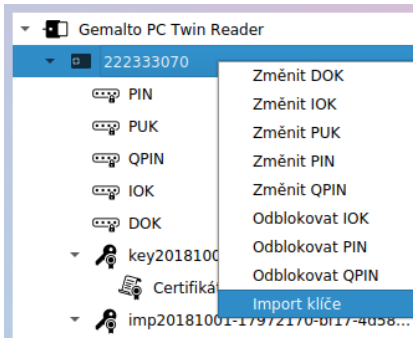
Import klíče se provede do prázdného kontejneru v čipu občanského průkazu. Ovladače zajistí výběr vhodného kontejneru – podle algoritmu importovaného klíče. Klíče se vždy importují do kontejnerů pro obecné použití, nikdy ne do kontejnerů pro podpisové klíče. Pokud v čipu není žádný volný (vhodný) kontejner, nelze import klíče dokončit – *Správce karty* při importu ohlásí chybu.

Po dokončení importu klíče do čipu nelze klíč (soukromou část klíče) exportovat ani přečíst. Kryptografické operace s importovaným klíčem probíhají v čipu občanského průkazu.

7.1.1.1 Spuštění importu klíče

Před importem klíče s certifikátem je třeba označit občanský průkaz, do nějž mají být data importována. (K počítači může být připojeno více čteček a ve čtečkách vloženo více občanských průkazů. Aplikace *eObčanka – Správce karty* musí vědět, do kterého čipu mají být data importována.)

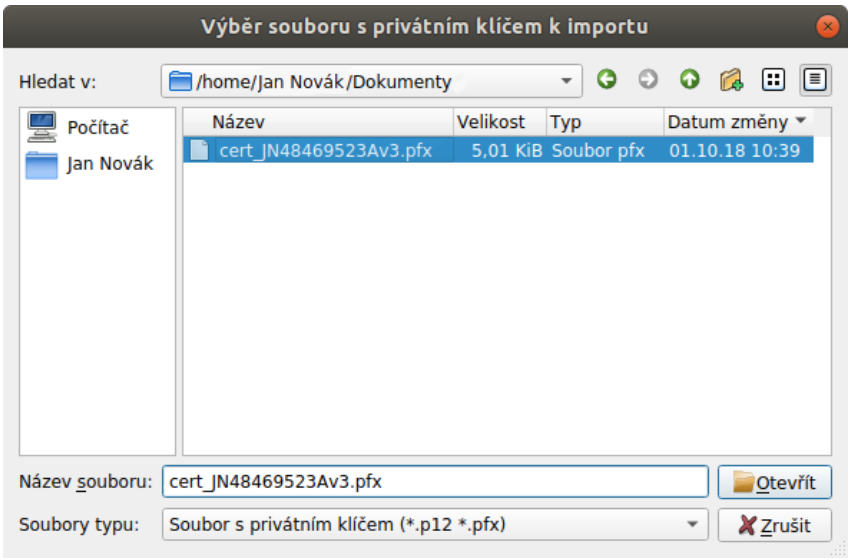
Pro import klíče s certifikátem slouží funkce *Import klíče*. Tato funkce je dostupná pomocí kontextového menu na občanském průkazu ve stromu informací anebo pomocí tlačítka *Import klíče v* okně s informacemi o kartě (viz také kapitola 6.1.3).



Obrázek 26: Spuštění importu klíče z kontextového menu karty

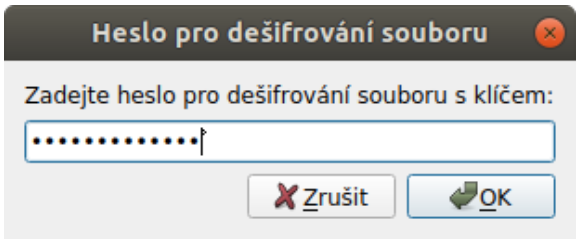
7.1.1.2 Průběh importu klíče

Po spuštění funkce *Import klíče* se zobrazí okno pro výběr souboru s klíčem. Klíče a certifikáty jsou typicky uloženy v souborech s příponou .pfx nebo .p12.



Obrázek 27: Okno pro výběr souboru s importovaným klíčem a certifikátem

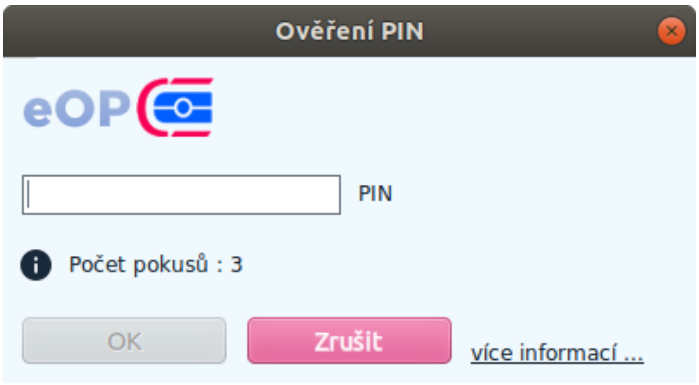
Uživatel zvolí soubor s klíčem, který chce importovat do čipu, a potvrdí tlačítkem *Otevřít*. Aplikace ze souboru vyčte obsah a vyzve uživatele k zadání šifrovacího hesla k vybranému souboru:



Obrázek 28: Zadání hesla pro dešifrování souboru s importovaným klíčem

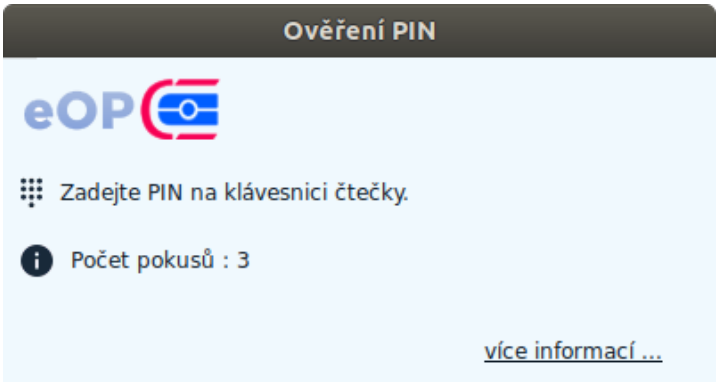
Uživatel zadá heslo a potvrdí tlačítkem *OK*. (Může také import klíče zrušit tlačítkem *Zrušit*.)

Po zadání hesla *Správce karty* dešifruje obsah souboru a zahájí import dat do čipu. Uživatel musí import dat schválit pomocí PIN. Zobrazí se proto okno pro zadání PIN:



Obrázek 29: Okno pro zadání PIN na klávesnici počítače

Pokud uživatel používá čtečku s integrovanou klávesnicí, vypadá okno pro zadání PIN jinak:



Obrázek 30: Okno pro zadání PIN na klávesnici čtečky

Po zadání PIN se provede import klíče (a případně i certifikátu) do vhodného prázdného kontejneru v čipu občanského průkazu. Při importu se generuje nový identifikátor klíče.

Pokud importní soubor obsahuje pouze klíč, aplikace do čipu občanského průkazu importuje pouze tento klíč. Pokud soubor obsahuje klíč s certifikátem, provede aplikace import klíče i certifikátu. Certifikát je při importu svázán s klíčem.

Aplikace *eObčanka – Správce karty* si po importu aktualizuje informace o daném občanském průkazu – aby získala informace o nově importovaném klíči a certifikátu. Mezi vyčtenými informacemi o objektech v čipu se nově objevují i importovaná data.

Úspěšný import je inzerován hlášením: *Import klíče byl úspěšně dokončen.*

7.1.1.3 Chyby při importu klíče

Pokud v průběhu importu nastane chyba, aplikace uživateli zobrazí chybu a v některých případech stručný návrh dalšího postupu.

Typické chyby, které nastávají při importu klíče, jsou:

- Importovaný soubor se nepodaří přečíst, např. z důvodu nedostatečných uživatelských oprávnění.
- Zadané šifrovací heslo k souboru není správné.
- Nesprávný formát souboru pro import – formát neodpovídá standardu PKCS#12.
- V čipu občanského průkazu není volný kontejner pro import daného typu klíče.

7.1.2 Import certifikátu ze souboru

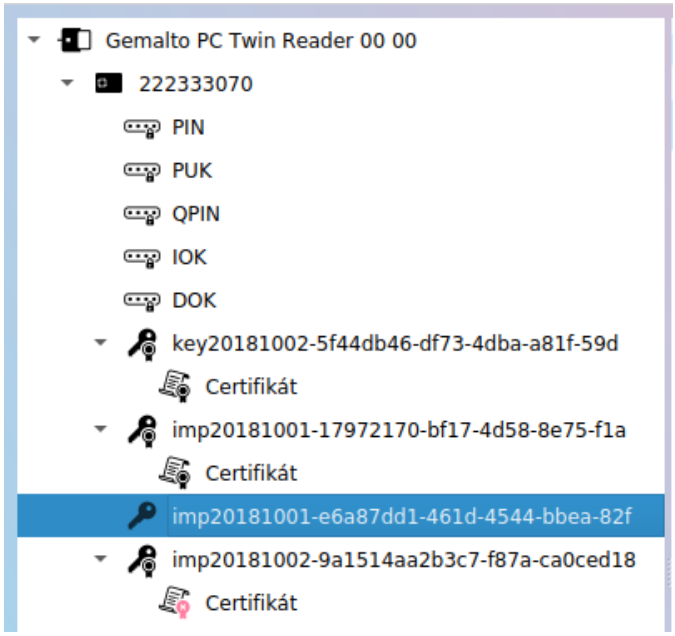
Pokud uživatel má v čipu občanského průkazu uložen pouze klíč bez certifikátu, může pomocí *Správce karty* certifikát importovat do čipu ze souboru. v souboru musí být uložen certifikát X.509, příslušný ke klíči v čipu občanského průkazu.

Importovat lze soubor s certifikátem ve formátu:

- binárně kódovaný soubor ASN.1 struktury X.509,
- ASN.1 struktura X.509, zakódovaná do BASE64.

7.1.2.1 Před spuštěním importu

Před importem musí uživatel označit klíč, k němuž chce certifikát importovat. k danému klíči nesmí být v čipu uložen certifikát (import certifikátu se v takovém případě nenabídne).



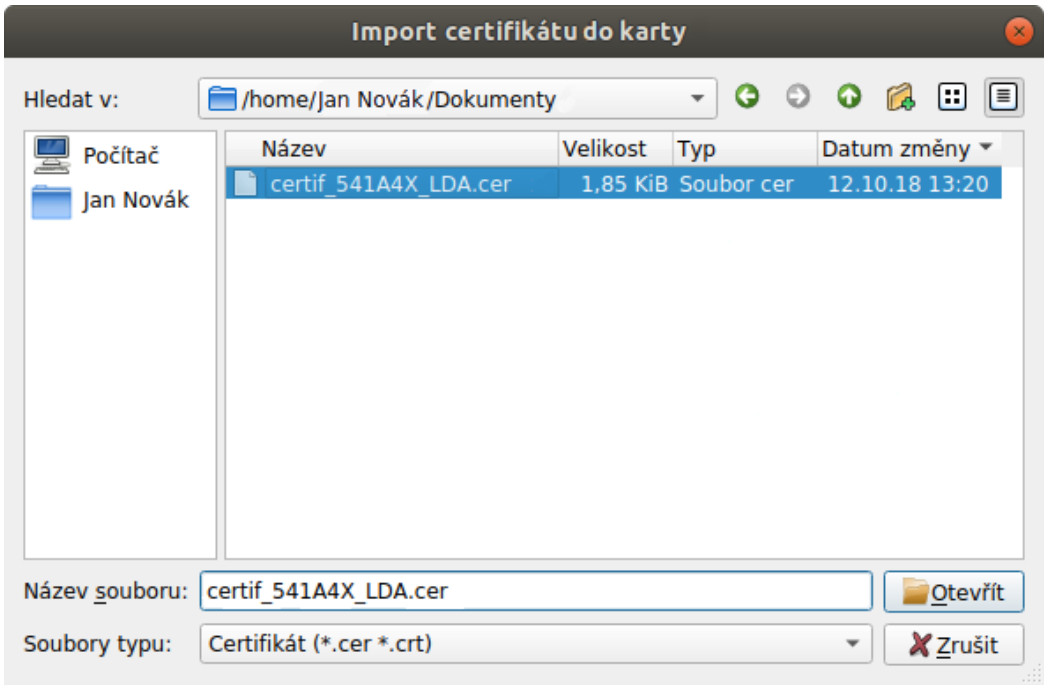
Obrázek 31: Označení klíče, k němuž má být importován certifikát

Import certifikátu lze spustit pomocí

- kontextového menu klíče (položka *Importovat certifikát ze souboru*),
- nebo pomocí tlačítka *Import certifikátu* z okna s informacemi o klíči (viz kapitola 6.3.2).

7.1.2.2 Průběh importu

Po spuštění importu certifikátu zobrazí aplikace okno pro výběr souboru s certifikátem. Certifikáty jsou typicky uloženy v souborech *.cer* a *.crt*, popř. *.pem*



Obrázek 32: Okno pro otevření souboru s importovaným certifikátem

Uživatel zvolí soubor s certifikátem a potvrdí pomocí tlačítka *Otevřít*. *Správce karty* zvolený soubor přečte a sestaví certifikát X.509. Pokud se certifikát nepodaří zkonstruovat, zobrazí se chybové hlášení o nesprávném formátu dat.

Po zkonstruování certifikátu *Správce karty* prověří, zda veřejný klíč certifikátu odpovídá klíči, k němuž je certifikát importován. Pokud se veřejné klíče liší, zobrazí se chyba: *Obsah importovaného certifikátu neodpovídá zvolenému klíči.*

Uživatel musí import certifikátu do čipu schválit zadáním platné hodnoty PIN – podobně jako při importu klíče, viz kapitola 7.1.1.2.

Po zadání PIN provede *Správce karty* import certifikátu do čipu občanského průkazu. v průběhu importu se neprovádí validace platnosti certifikátu, aplikace *eObčanka – Správce karty* umožní import i neplatných certifikátů.

Aplikace *eObčanka – Správce karty* si po importu aktualizuje informace o daném občanském průkazu – aby získala informace o nově importovaném certifikátu.

Úspěšné dokončení importu aplikace uživateli oznámí informací: *Import certifikátu byl úspěšně dokončen* a poté zobrazí okno s informacemi o importovaném certifikátu.

7.1.2.3 Chyby při importu certifikátu

Pokud při importu nastane chyba, zobrazí se chybové hlášení. Uživatel se může pokusit odstranit vzniklý problém a poté provést import certifikátu znovu.

Typické chyby, které nastávají při importu klíče, jsou:

- Soubor s certifikátem se nepodaří přečíst, např. z důvodu nedostatečných uživatelských oprávnění.
- Nesprávný formát souboru pro import; soubor neobsahuje certifikát X.509.
- Obsah importovaného certifikátu neodpovídá zvolenému klíči.

7.2 Export dat z čipu občanského průkazu

Veřejná data uložená v čipu občanského průkazu lze exportovat do souboru. Pomocí *Správce karty* lze provést export:

- certifikátu,
- veřejné části klíče.

Export uvedených dat není citlivou operací. Aplikace proto v průběhu exportu nevyžaduje schválení operace zadáním přístupového kódu.

Citlivé informace, jako např. soukromé klíče či hodnoty přístupových kódů, nelze z čipu přečíst ani exportovat.

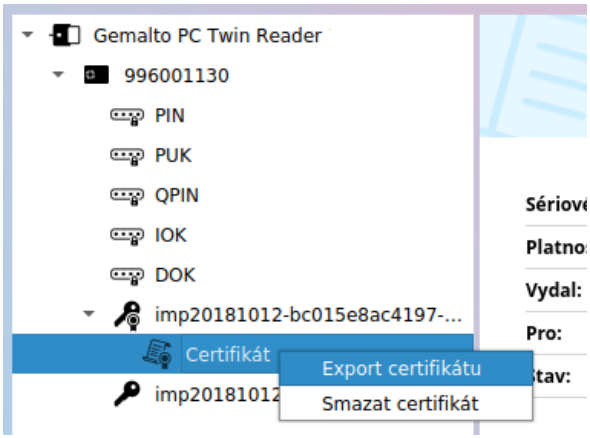
Funkce pro export dat umožňují uložení souboru do libovolného adresáře, který si uživatel zvolí: na disk počítače, přenosný USB flash disk, síťový disk, apod...

7.2.1 Export certifikátu do souboru

Certifikát lze z čipu exportovat do souboru. Uživatel ve stromu informací označí certifikát, který chce uložit a spustí operaci exportu. Aplikace *eObčanka – Správce karty* zobrazí standardní okno pro uložení souboru. Uživatel zvolí adresář a název souboru. Do zvoleného souboru pak aplikace *eObčanka – Správce karty* uloží data certifikátu, jako binárně kódovanou ASN.1 strukturu X.509.

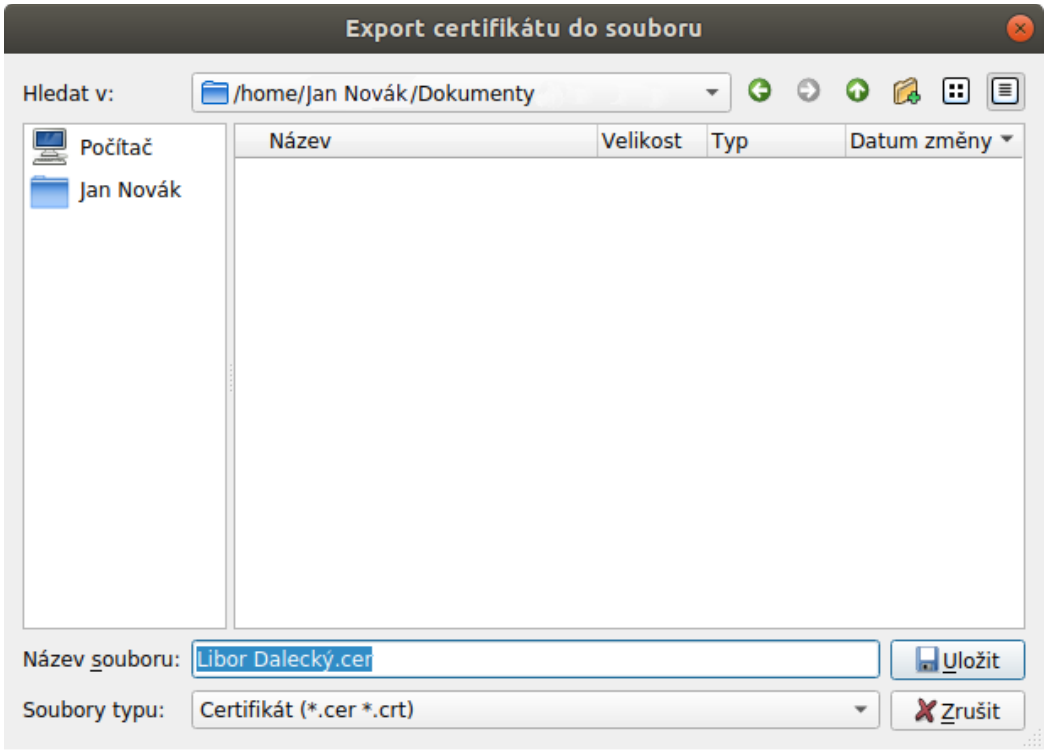
Export certifikátu se provádí pomocí funkce *Export certifikátu do souboru* dostupné:

- pomocí kontextového menu ve stromu informací certifikátu,
- nebo pomocí tlačítka *Export do souboru* v okně s informacemi o certifikátu.



Obrázek 33: Kontextové menu pro export certifikátu do souboru

Jakmile uživatel spustí export certifikátu, zobrazí aplikace okno pro uložení souboru:



Obrázek 34: Okno pro uložení certifikátu do souboru

Jako název souboru je přednastaven název držitele certifikátu. Výchozí přípona souboru je *.cer*

Uživatel zvolí adresář pro uložení souboru, může také změnit název i příponu souboru. Data do zvoleného souboru uloží stiskem tlačítka *Uložit.*

Aplikace *eObčanka – Správce* karty do zvoleného souboru zapíše certifikát X.509 jako binárně kódovanou *ASN.1* strukturu

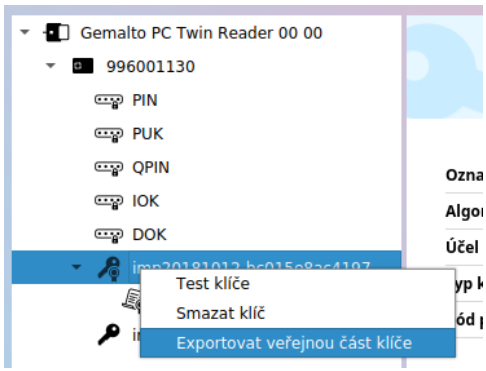
Po úspěšném dokončení operace aplikace zobrazí uživateli informaci: *Certifikát byl uložen do souboru…*

Pokud při exportu certifikátu nastane chyba, zobrazí aplikace chybové hlášení. Uživatel se může pokusit odstranit problém a spustit export dat znovu.

7.2.2 Export veřejné části klíče do souboru

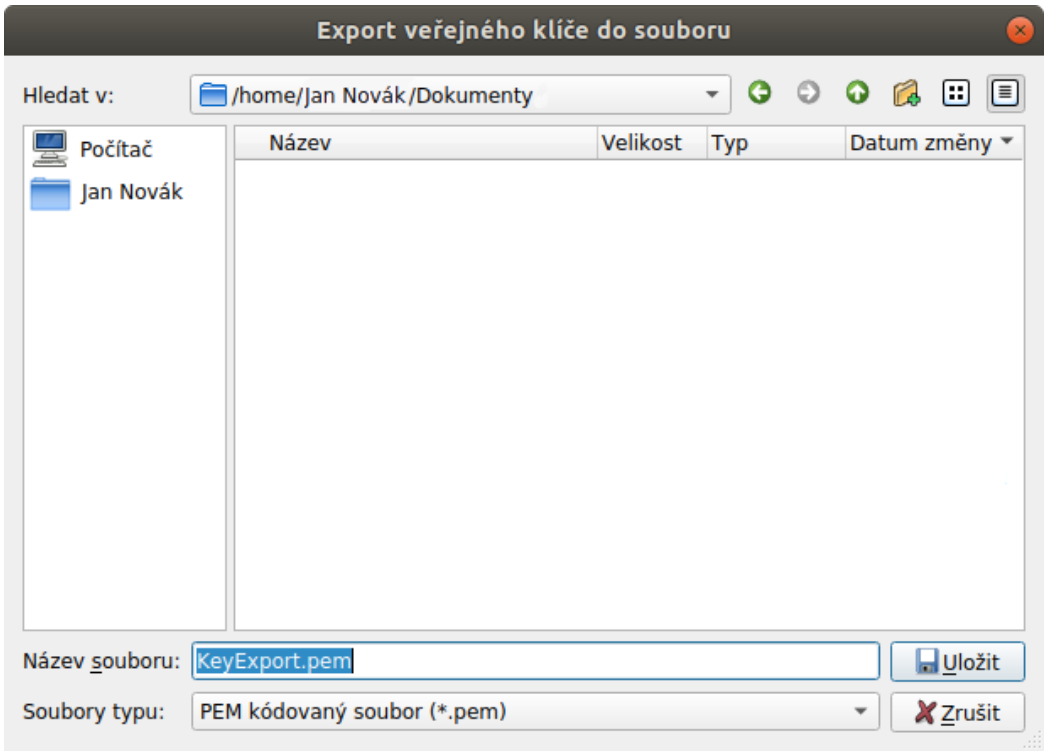
Aplikace *eObčanka – Správce karty* umožňuje exportovat z čipu veřejnou část kryptografického klíče. (Soukromý klíč exportovat nikdy nelze!)
Uživatel ve stromu informací označí klíč, který chce exportovat a spustí operaci exportu.
Export veřejné části klíče do souboru lze spustit pomocí

- funkce *Export veřejného klíče do souboru* z kontextového menu klíče,
- nebo pomocí tlačítka *Export veřejného klíče* v okně s informacemi o klíči.



Obrázek 35: Kontextové menu pro export veřejného klíče do souboru

Po spuštění exportu se zobrazí okno pro uložení souboru:



Obrázek 36: Okno pro uložení veřejného klíče do souboru

Výchozí název souboru je *KeyExport.pem*. Uživatel zvolí adresář, do nějž se mají data uložit; může také změnit název souboru. Tlačítkem *Uložit* se data veřejného klíče uloží do zvoleného souboru. Data souboru jsou kódována jako BASE64, ve formátu PEM.

Po úspěšném dokončení operace aplikace zobrazí uživateli informaci: *Veřejný klíč byl uložen do souboru…*

Pokud při exportu certifikátu nastane chyba, zobrazí aplikace chybové hlášení. Uživatel se může pokusit odstranit problém a spustit export dat znovu.

Export veřejného klíče se příliš často nepoužívá (častěji se provádí export certifikátu). Proto je akce exportu veřejného klíče dostupná pouze v případě, že je v aplikaci *eObčanka - Správce karty* zapnuto *rozšířené* zobrazení – viz kapitola 5.5.

7.3 Mazání dat z občanského průkazu

Data certifikátů i kryptografických klíčů lze z čipu vymazat. Vymazání dat je nevratná operace. Pokud má uživatel zálohu dat v souboru, může data do čipu opět importovat.

Kryptografické klíče, určené k elektronickému podepisování, jsou obvykle generovány v čipu občanského průkazu. v takovém případě neexistuje záloha klíče. (Export veřejného klíče není plnohodnotnou zálohou, soukromý klíč z čipu exportovat nelze.)

Pokud dojde ke smazání klíče, který byl generován v čipu, zanikne tím jediná kopie (originál) klíče.

Na rozdíl od kryptografických klíčů - v případě certifikátů většinou existuje zdroj, odkud data smazaného certifikátu znovu získat: buď má uživatel zálohu certifikátu v souboru anebo se může obrátit na certifikační autoritu, která certifikát vydala. Certifikát lze do čipu znovu importovat – viz kapitola 7.1.2.

Kvůli riziku nechtěné ztráty dat jsou operace mazání v aplikaci *eObčanka – Správce karty* dostupné jen v případě *rozšířeného* zobrazení – viz kapitola 5.5.

Uživatel musí operaci mazání dat z čipu schválit zadáním PIN.

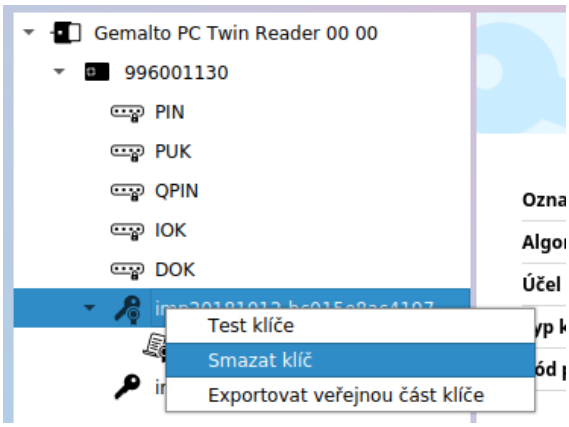
7.3.1 Smazání klíče

Funkce Smazání klíče umožní uživateli nevratně odstranit z občanského průkazu kryptografický klíč (klíčový pár). Spolu s klíčem je z čipu vymazán i příslušný certifikát.

Upozornění: Smazání klíče je nevratná operace! Mnohdy je soukromý klíč uložen pouze v čipu občanského průkazu. Smazáním klíče pak uživatel přijde o jedinou kopii soukromého klíče.

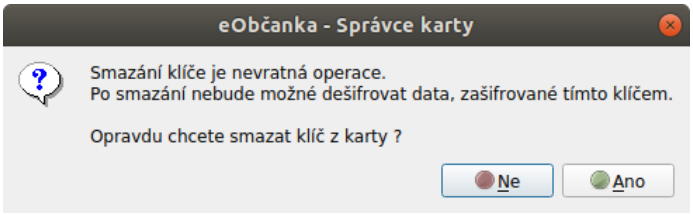
Funkce smazání klíče je v aplikaci *eObčanka - Správce karty* dostupná

- pomocí tlačítka *Smazat klíč* z okna s informacemi o klíči,
- a pomocí kontextového menu klíče.



Obrázek 37: Kontextové menu pro smazání klíče z čipu občanského průkazu

Po spuštění mazání aplikace varuje před nevratností operace:



Obrázek 38: Varování před smazáním kryptografického klíče z čipu

Uživatel může mazání přerušit tlačítkem *Ne*. Pokud operaci odsouhlasí (*Ano*), započne proces mazání klíče.

Uživatel je požádán o zadání hodnoty PIN, podobně jako v případě importu klíče – viz kapitola 7.1.1.2. Zadáním PIN uživatel schválí operací mazání dat.

Aplikace potom:

- smaže se z čipu certifikát (pokud je v čipu uložen),
- smaže z čipu klíč.

Po dokončení mazání aplikace nezobrazuje žádnou informaci, pouze aktualizuje strom informací a zobrazí informace o kartě.

Pokud při mazání klíče nastane chyba, zobrazí aplikace chybové hlášení. Uživatel se může pokusit odstranit problém a spustit operaci znovu.

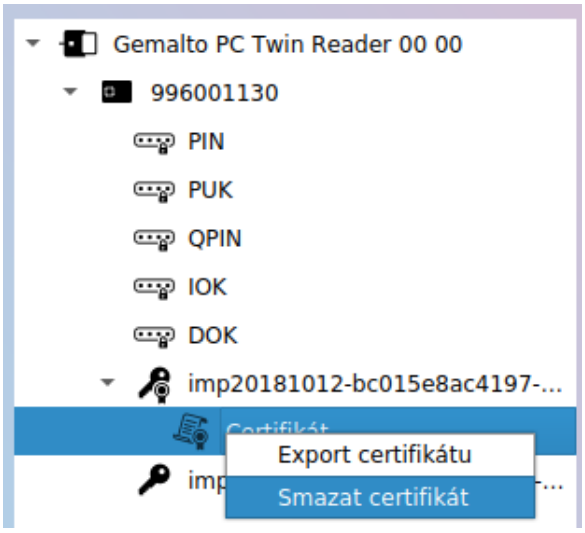
7.3.2 Smazání certifikátu

Pokud uživatel označí certifikát, uložený v čipu, umožní mu aplikace *eObčanka – Správce karty* zvolený certifikát smazat. (Klíč, příslušný k danému certifikátu, není touto operací nijak zasažen.)

Před výmazem dat zobrazí aplikace *eObčanka - Správce karty* varování, že bez certifikátu pravděpodobně nebude možné v aplikacích použít příslušný klíč. Pokud uživatel odsouhlasí výmaz dat, zobrazí se dialog pro zadání PIN. Po zadání platné hodnoty PIN je zvolený certifikát z čipu vymazán. Při smazání je certifikát také odregistrován z operačního systému.

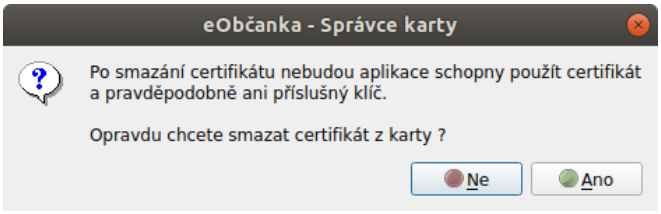
Funkce smazání certifikátu je v aplikaci *eObčanka - Správce karty* dostupná

- pomocí tlačítka Smazat certifikát z okna s informacemi o certifikátu,
- a pomocí kontextového menu zvoleného certifikátu.



Obrázek 39: Kontextové menu pro smazání certifikátu

Po spuštění mazání aplikace uživatele informuje o závažnosti operace:



Obrázek 40: Varování před smazáním certifikátu

Uživatel může mazání přerušit tlačítkem *Ne*. Pokud operaci odsouhlasí (*Ano*), započne proces mazání certifikátu.

Uživatel je požádán o zadání hodnoty PIN, podobně jako v případě importu klíče – viz kapitola 7.1.1.2. Zadáním PIN uživatel schválí operací mazání dat.

Aplikace potom smaže certifikát z čipu občanského průkazu.

Po dokončení mazání aplikace nezobrazuje žádnou informaci, pouze aktualizuje strom informací a zobrazí informace o kartě.

Pokud při mazání certifikátu nastane chyba, zobrazí aplikace chybové hlášení. Uživatel se může pokusit odstranit problém a spustit operaci znovu.

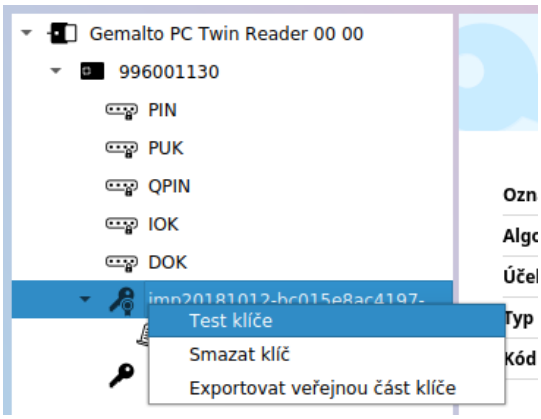
7.4 Test klíče

Funkce *Test klíče* ověří integritu a použitelnost zvoleného klíčového páru. Aplikace provede s klíčem aktivní operaci:

- s klíčem, určeným pro podepisování se provede elektronický podpis náhodných dat a ověření podpisu,
- pro ostatní klíče se provede zašifrování a dešifrování.

Test klíče se spouští

- pomocí tlačítka *Test klíče* z okna s informacemi o klíči,
- nebo z kontextového menu zvoleného klíče.

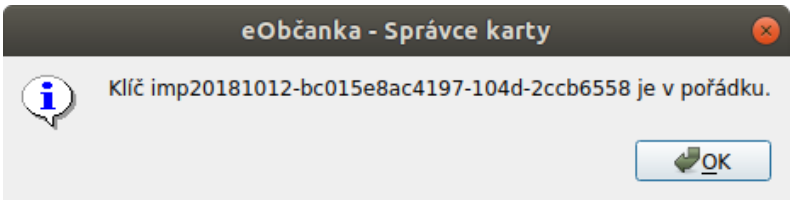


Obrázek 41: Kontextové menu pro test klíče

Po spuštění testu klíče uživatel musí vyčkat, dokud operace neskončí.

V průběhu testu může být uživatel vyzván k zadání přístupového kódu PIN či QPIN. Hodnotu přístupového kódu zadává buď na klávesnici počítače, nebo na klávesnici čtečky – podle použitého typu čtečky. Aplikace vždy vyzve k zadání příslušného přístupového kódu zobrazením okna s instrukcemi.

Pokud test klíče skončí úspěšně, aplikace zobrazí uživateli informaci:



Obrázek 42: Okno s informací o úspěšném dokončení testu klíče

Pokud by test nebyl úspěšný, zobrazí aplikace chybové hlášení.

Poznámka: Test klíče pracuje pouze s veřejným a soukromým klíčem, nepracuje s certifikátem. Neověřuje platnost certifikátu, ani certifikát při testu nevyužívá. Test klíče lze provést i v případě, že k danému klíčovému páru není dostupný certifikát ani v čipu občanského průkazu, ani v operačním systému.

8 SPRÁVA PŘÍSTUPOVÝCH KÓDŮ

S občanským průkazem je spojeno několik číselných kódů - každý z nich slouží k jinému účelu, každý chrání jinou funkci občanského průkazu. Pomocí *Správce karty* lze přístupové kódy občanského průkazu spravovat:

- Zjistit *stav* jednotlivých přístupových kódů.
- Nastavovat a měnit hodnoty přístupových kódů.

Upozornění: Uživatel **není povinen nastavit si všechny přístupové kódy** občanského průkazu. Stačí, když si nastaví ty přístupové kódy, které jsou nezbytné pro práci s elektronickými funkcemi občanského průkazu, které chce využívat:

- Pokud uživatel **nechce využívat** žádné elektronické funkce občanského průkazu, **nemusí si aktivovat žádný** přístupový kód.
- Pokud chce uživatel využívat **pouze identifikační funkci** občanského průkazu, stačí, když si **aktivuje DOK a IOK** (nemusí mít nastaveny PUK, PIN a QPIN).
- Pokud chce uživatel **pracovat s certifikáty**, musí (postupně) nastavit **všechny přístupové kódy** občanského průkazu.

Hodnoty všech přístupových kódů musí být ve výhradním držení držitele občanského průkazu. Držitel občanského průkazu by neměl přístupové kódy občanského průkazu nikomu sdělovat a ani si je nikam poznamenávat. Přístupové kódy by neměly být uchovávány společně s občanským průkazem. Uživatel by si také přístupové kódy neměl poznamenávat na občanský průkaz.

Každý z přístupových kódů umožňuje pouze několik chybných po sobě jdoucích zadání. Pokud uživatel zadá několikrát po sobě špatnou hodnotu přístupového kódu, dojde k jeho zablokování. Každý z přístupových kódů má různý počet chybných pokusů do zablokování – viz níže.

Pokud po několika chybných pokusech zadá uživatel správnou hodnotu přístupového kódu, počet neúspěšných pokusů se vynuluje – uživatel má opět plný počet pokusů pro zadání nesprávné hodnoty.

K zablokování přístupového kódu občanského průkazu může dojít kdykoli při jeho použití, pokud uživatel vyčerpá počet neúspěšných pokusů pro zadání. k zablokování může dojít při použití aplikace, která provádí operace s certifikáty v občanském průkazu, např. elektronické podepisování. Zablokovaný přístupový kód nelze použít. Pro opětovné povolení použití přístupového kódu je nutno tento přístupový kód odblokovat.

Každý přístupový kód má definovánu minimální a maximální počet číslic, které si uživatel může nastavit. Uživatel může tedy volit jakoukoli kombinaci číslic v rozmezí minimálního a maximálního povoleného počtu znaků.

8.1 Přehled přístupových kódů občanského průkazu

Pro jednotlivé verze občanských průkazů se liší počet přístupových kódů.

8.1.1 Občanský průkaz s čipem, vydávaný od 1. 7. 2018

S občanským průkazem, vydávaným od 1. 7. 2018, je spojeno 5 přístupových kódů:

- **DOK**
  - Deblokační osobní kód.
  - Používá se zřídka, slouží pro odblokování a nastavení kódu IOK.
  - Nastavuje a odblokovává se na úřadu obce s rozšířenou působností.
  - Délka kódu je 4 až 10 číslic.
  - Po 10 špatných po sobě jdoucích chybných zadáních kódu dojde k jeho zablokování.
- **IOK**
  - Identifikační osobní kód.
  - Schvaluje identifikační operace občanského průkazu; zadává se při každé identifikační operaci občanským průkazem.
  - Nastavuje se na úřadu obce s rozšířenou působností.
  - Po zablokování lze odblokovat pomocí kódu DOK.
  - Délka kódu je 4 až 10 číslic.
  - Po 3 špatných po sobě jdoucích chybných zadáních kódu dojde k jeho zablokování.
- **PUK**
  - PIN Unblocking Key.
  - Používá se zřídka, slouží pro nastavení a odblokování kódů PIN a QPIN.
  - Nastavuje se pomocí kódu IOK; nastavit lze jen jedenkrát.
  - Po zablokování se nedá odblokovat.
  - Délka kódu je 8 až 15 číslic.
  - Po 5 špatných po sobě jdoucích chybných zadáních kódu dojde k jeho trvalému zablokování.
  - **Pokud se PUK zablokuje, nelze jej znovu odblokovat!**
- **PIN**
  - Personal Identification Number.
  - Používá se pro schvalování většiny operací s certifikáty a klíči (generování či import klíčů, zápis certifikátů do čipu, mazání dat z čipu, přihlašování pomocí certifikátu, …).
  - Nastavuje se pomocí kódu PUK, po zablokování lze odblokovat pomocí PUK
  - Délka kódu je 5 až 15 číslic.
  - Po 3 špatných po sobě jdoucích chybných zadáních kódu dojde k jeho zablokování.
- **QPIN**
  - PIN pro kvalifikované elektronické podpisy.
  - Používá se pro schválení každé podpisové operace s certifikáty, určenými po podepisování
  - Nastavuje se pomocí kódu PUK, po zablokování lze odblokovat pomocí PUK.

- Délka kódu je 5 až 15 číslic.
- Po 3 špatných po sobě jdoucích chybných zadáních kódu dojde k jeho zablokování.

8.1.2 Občanský průkaz s čipem, vydávaný do 1. 7. 2018

S občanským průkazem, vydávaným do 1. 7. 2018, jsou spojeny 2 přístupové kódy:

- **PUK**
  - PIN Unblocking Key.
  - Používá se zřídka, slouží pro odblokování kódu PIN.
  - Nastavuje se na úřadu obce s rozšířenou působností.
  - Délka kódu je 5 až 15 číslic.
  - Po 3 špatných po sobě jdoucích chybných zadáních kódu dojde k jeho trvalému zablokování.
  - Hodnotu PUK nelze odblokovat.
- **PIN**
  - Personal Identification Number.
  - Používá se pro schvalování operací s certifikáty a klíči.
  - Nastavuje se na úřadu obce s rozšířenou působností, po zablokování lze odblokovat pomocí PUK.
  - Délka kódu je 5 až 15 číslic.
  - Po 3 špatných po sobě jdoucích chybných zadáních kódu dojde k jeho zablokování.

8.2 Operace s přístupovými kódy

S přístupovými kódy lze provádět tři základní operace:

- **Nastavení**
  - Pokud přístupový kód dosud nebyl v občanském průkazu nastaven.
  - Před prvním použitím je třeba kód nastavit. Nastavení se schvaluje jiným přístupovým kódem.
  - Nastavit lze: PUK pomocí IOK, PIN pomocí PUK, QPIN pomocí PUK.
- **Změna**
  - Pokud uživatel zná platnou hodnotu přístupového kódu, může změnit hodnotu daného kódu.
  - Změnu kódu je třeba schválit zadáním platné hodnoty daného kódu.
  - Změnit lze kterýkoli kód občanského průkazu.
- **Odblokování**
  - Pokud byl kód zablokován opakovaným chybným zadáním, lze nastavit novou hodnotu zablokovaného kódu.
  - Odblokování se schvaluje jiným přístupovým kódem.
  - Odblokovat lze: IOK pomocí DOK, PIN pomocí PUK, QPIN pomocí PUK.
  - Zablokovanou hodnotu PUK nelze odblokovat

S většinou přístupových kódů lze uvedené operace provádět v aplikaci *eObčanka – Správce karty*. **Výjimku tvoří kódy:**

- DOK a IOK, které je třeba nastavit a příp. odblokovat na úřadu obce s rozšířenou působností.
- PUK a PIN **starší verze** občanského průkazu (vydáván do 1. 7. 2018), které je třeba nastavit na úřadu obce s rozšířenou působností.
  PUK a PIN novější verze občanského průkazu se nastavuje pomocí aplikace *eObčanka - Správce karty*.

8.3 Upozornění na potíže s přístupovými kódy

Aplikace *eObčanka - Správce karty* upozorňuje uživatele na problém s přístupovým kódem:

- Barvou přístupového kódu ve stromu informací (viz kapitola 5.2).
- Upozorněním v okně s problémy k řešení (viz kapitola 9.1).

Za problematický stav přístupového kódu se pokládá každá situace, kdy kód není *platný*:

- Kód není (dosud) nastaven.
- Kód je zablokovaný.

Uživatel může rozpoznat problémové přístupové kódy ve stromu informací: růžově označené přístupové kódy vyžadují pozornost uživatele (nastavit nebo odblokovat).

- 

kód není platný, vyžaduje pozornost.
- 

přístupový kód je platný, nejsou nalezeny problémy.

Označením „problémového“ přístupového kódu se v pravém panelu zobrazí podrobnější informace a nabídnou se také možnosti řešení. Akce, které jsou dostupné, lze zobrazit také pomocí kontextového menu zvoleného přístupového kódu.

8.4 Nastavení přístupového kódu

Nastavení přístupového kódu občanského průkazu se provádí před jeho prvním použitím.

Pomocí aplikace *eObčanka – Správce karty* lze nastavit tyto kódy:

- PUK (nastavení pomocí IOK).
- PIN (odblokování pomocí PUK – viz kapitola 8.6).
- QPIN (odblokování pomocí PUK – viz kapitola 8.6).

Pozn.: Uvedené kódy lze nastavit v občanském průkazu, vydaném po 1. 7. 2018. Pro starší verzi občanského průkazu se PIN a PUK nastavují při převzetí občanského průkazu na úřadu s rozšířenou působností.

Aby bylo možno nastavit PUK, musí si držitel občanského průkazu nejprve nastavit IOK. Hodnotu IOK je třeba nastavit (spolu s DOK) na úřadu obce s rozšířenou působností. IOK pak lze ve *Správci karty* použít pro nastavení PUK. Pomocí PUK pak lze odblokovat PIN a QPIN – viz kapitola 8.6.

Po nastavení (odblokování) PIN a QPIN lze začít využívat občanský průkaz jako bezpečné úložiště certifikátů s klíči.

Jakmile je PUK jednou nastaven, nelze jej nastavit znovu. PUK lze při znalosti aktuální hodnoty kdykoli změnit. **Zablokovaný PUK nelze odblokovat.**

Pokud operace nastavení PUK není úspěšně dokončena, lze ji opakovat, dokud se nezablokuje hodnota IOK.

8.4.1 Spuštění operace nastavení PUK

Nastavení PUK lze v aplikaci *eObčanka – Správce karty* spustit pomocí:

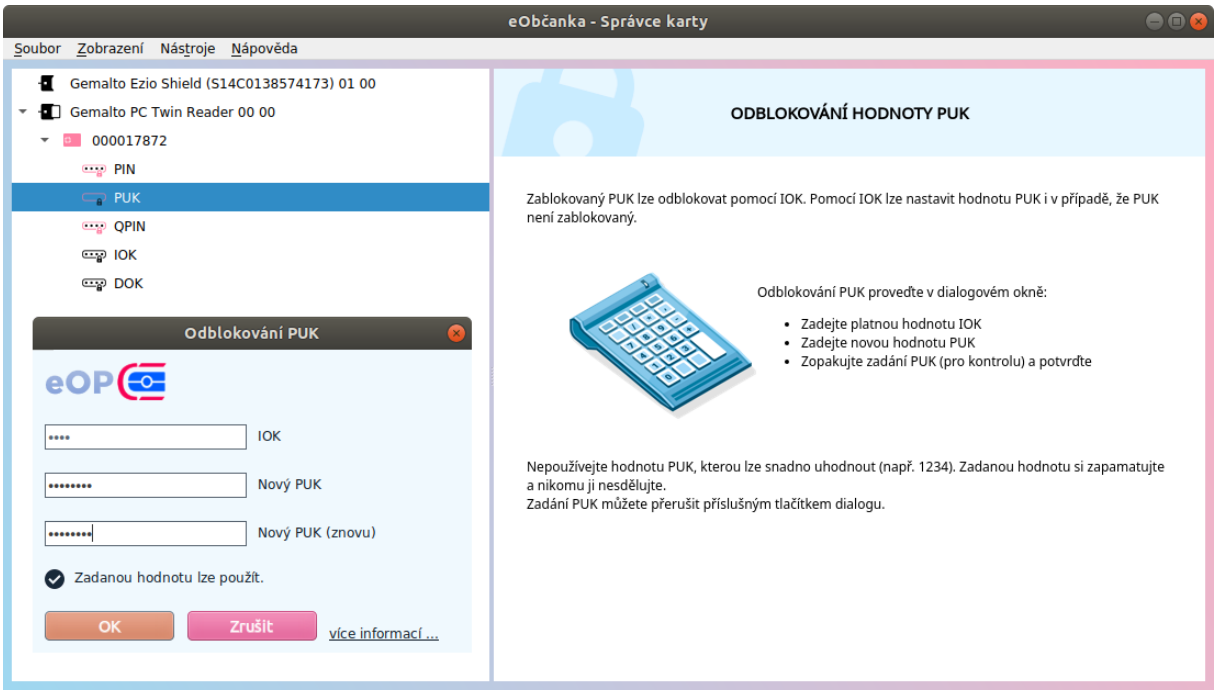
- tlačítka z informačního okna o kartě (občanském průkazu),
- informačního okna o kódu PUK,
- kontextového menu karty,
- kontextového menu PUK,
- odkazu mezi problémy k řešení – viz kapitola 9.1.

Postup nastavení PUK se mírně liší podle toho, zda uživatel používá běžnou čtečku (bez klávesnice) anebo čtečku s klávesnicí. v obou případech je pro nastavení PUK potřeba (v uvedeném pořadí):

- Zadat platnou hodnotu IOK
- Zadat novou hodnotu PUK
- Opakovat novou hodnotu PUK (pro kontrolu)

8.4.2 Nastavení PUK na běžné čtečce

Při použití běžné čtečky se PUK nastavuje v pravém panelu aplikace *Správce karty*. Zobrazí se informace pro uživatele, která popisuje postup změny:

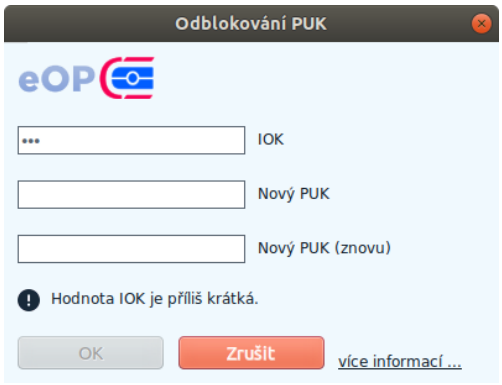


Obrázek 43: Okno Správce karty pro nastavení PUK na běžné čtečce

Uživatel zadá číselné hodnoty kódů:

- Do pole *IOK* aktuální hodnotu přístupového kódu IOK, pro schválení operace.
- Do pole *PUK* novou hodnotu PUK.
- Do pole *PUK (pro kontrolu)* zopakuje novou hodnotu PUK, kvůli eliminaci překlepů a kontrole.

Pod editačními poli aplikace zobrazuje stručnou nápovědu, dle stavu zadané hodnoty:



Obrázek 44: Nápověda editačních polí pro nastavení PUK

Pokud je u přístupového kódu IOK vypotřebován alespoň jeden neúspěšný pokus zadání, aplikace zobrazuje také počet zbývajících pokusů.

Po zadání hodnot přístupových kódů provede uživatel nastavení nové hodnoty PUK stiskem tlačítka *OK*. (Aplikace umožní tlačítko použít až potom, co uživatel správně vyplní všechna požadovaná pole.)

Po stisku tlačítka aplikace *eObčanka – Správce karty* ověří hodnotu IOK a nastaví novou hodnotu PUK v čipu občanského průkazu. Po dokončení operace se zobrazí informace o úspěšné změně přístupového kódu.

Pokud se změna přístupového kódu nezdaří, aplikace vyprázdní editační pole a zobrazí upozornění, že se přístupový kód nepodařilo změnit. Uživatel může pokračovat dalším pokusem – dokud se nezablokuje kód IOK.

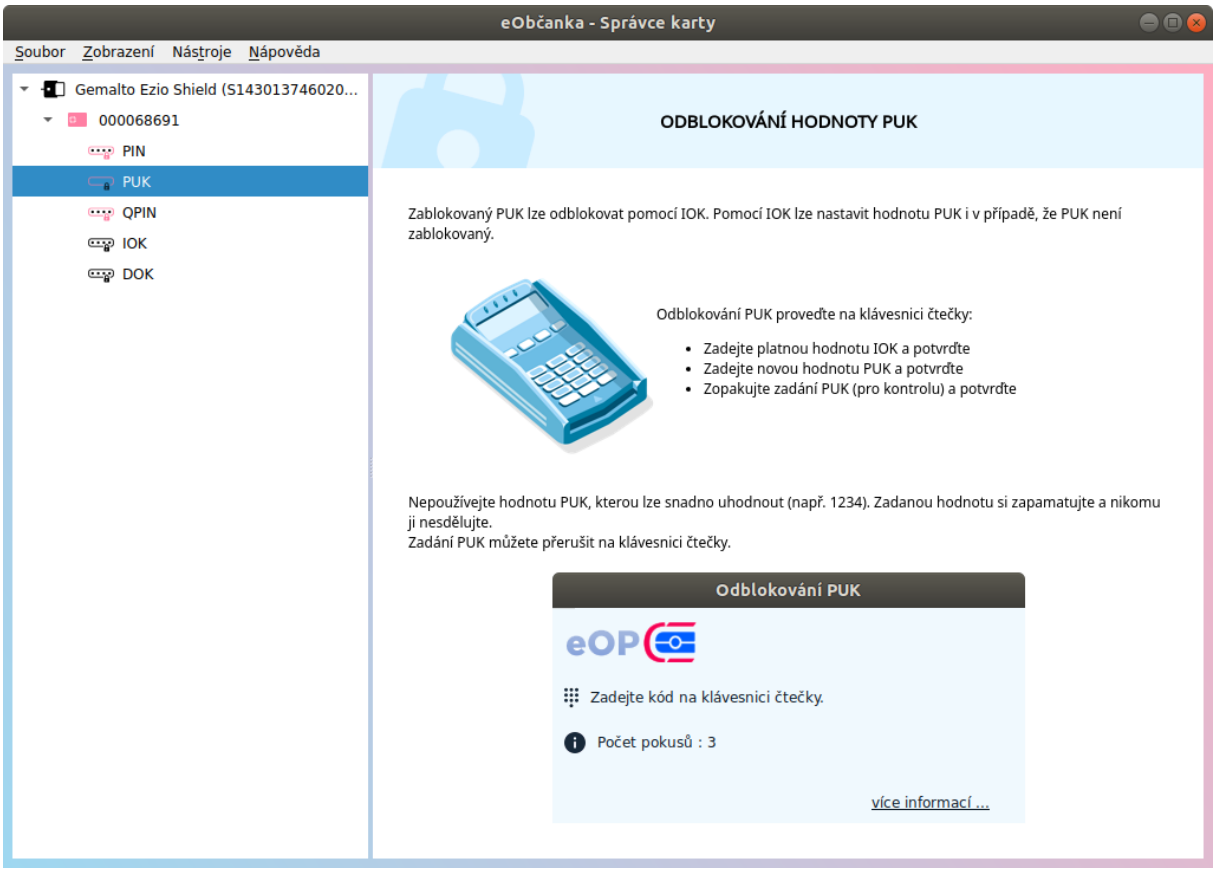
Při změně přístupového kódu může dojít k typickým chybám:

- Byla zadána nesprávná hodnota IOK.
- Vypršel časový limit pro zadání přístupového kódu (délka časového limitu je dána použitou čtečkou).

8.4.3 Nastavení PUK na čtečce s klávesnicí

Při použití čtečky s integrovanou klávesnicí uživatel zadává hodnoty přístupových kódů na klávesnici čtečky. Operaci zadání přístupového kódu řídí čtečka čipových karet.

Pokud uživatel používá čtečku s klávesnicí i displejem, instrukce na zadání přístupových kódů jsou zobrazeny na displeji čtečky.



Obrázek 45: Okno pro nastavení PUK na čtečce s klávesnicí a displejem

Upozornění: Instrukce na displeji čtečky mohou být nesprávné! Čtečka může nesprávně pojmenovat názvy zadávaných přístupových kódů. Uživatel se nesmí nechat instrukcemi na displeji zmást a musí zadávat kódy v pořadí: IOK → PUK → PUK. Při manipulaci se čtečkou mohou uživateli pomoci instrukce v okně *Správce karty*.

Ať už uživatel používá čtečku s displejem či bez, musí na klávesnici čtečky zadat kódy v tomto pořadí:

- IOK (+potvrdit na klávesnici čtečky).
- PUK (+potvrdit na klávesnici čtečky).
- PUK (+potvrdit na klávesnici čtečky).

Po potvrzení druhé z hodnot PUK se provede nastavení nové hodnoty PUK do čipu občanského průkazu. *Správce karty* informuje o výsledku operace.

Pokud operace skončí neúspěchem, zobrazí se chybové hlášení. Uživatel může nastavení PUK opakovat (dokud nezablokuje IOK).

Jakmile je PUK jednou nastaven, nelze jeho hodnotu odblokovat. Lze změnit hodnotu PUK, pokud uživatel zná aktuální hodnotu PUK – viz kapitola 8.5.

Po nastavení PUK nabídne *Správce karty* možnost nastavení (odblokování) hodnoty PIN – viz kapitola 8.6.

8.5 Změna přístupového kódu

Pomocí aplikace *eObčanka – Správce karty* lze provést změnu kteréhokoli přístupového kódu občanského průkazu. Pro provedení změny přístupového kódu:

- Musí být daný kód **platný** (musí být nastaven a nesmí být zablokován).
- Uživatel musí **znát aktuální hodnotu** daného kódu.

Pozn.: Změna všech přístupových kódů občanského průkazu se provádí podobně. v této příručce je proto popsán obecný postup změny přístupového kódu a jsou použity ilustrační obrázky změny kódu PIN. Změny ostatních přístupových kódů se provádějí analogicky.

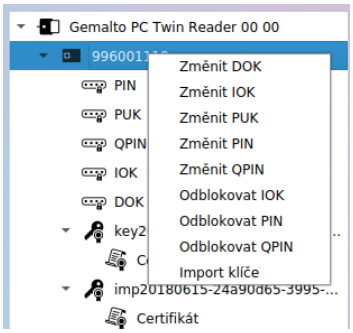
Přístupové kódy lze měnit opakovaně (neexistuje žádný limit na počet změn).

Pro změnu kódu je nutno zadat správnou aktuální hodnotu daného kódu. Pokud uživatel zadá nesprávnou hodnotu, zobrazí se chybové hlášení a sníží se počet pokusů pro zadání daného kódu. v případě, že uživatel vyčerpá povolený počet pokusů, hodnota daného kódu se zablokuje. Některé přístupové kódy lze po zablokování odblokovat – viz kapitola 8.6.

8.5.1 Spuštění operace změny přístupového kódu

Změnu kódu lze v aplikaci *eObčanka – Správce karty* spustit pomocí:

- tlačítka z informačního okna o kartě (občanském průkazu),
- informačního okna o přístupovém kódu,
- kontextového menu karty,
- kontextového menu platného přístupového kódu.



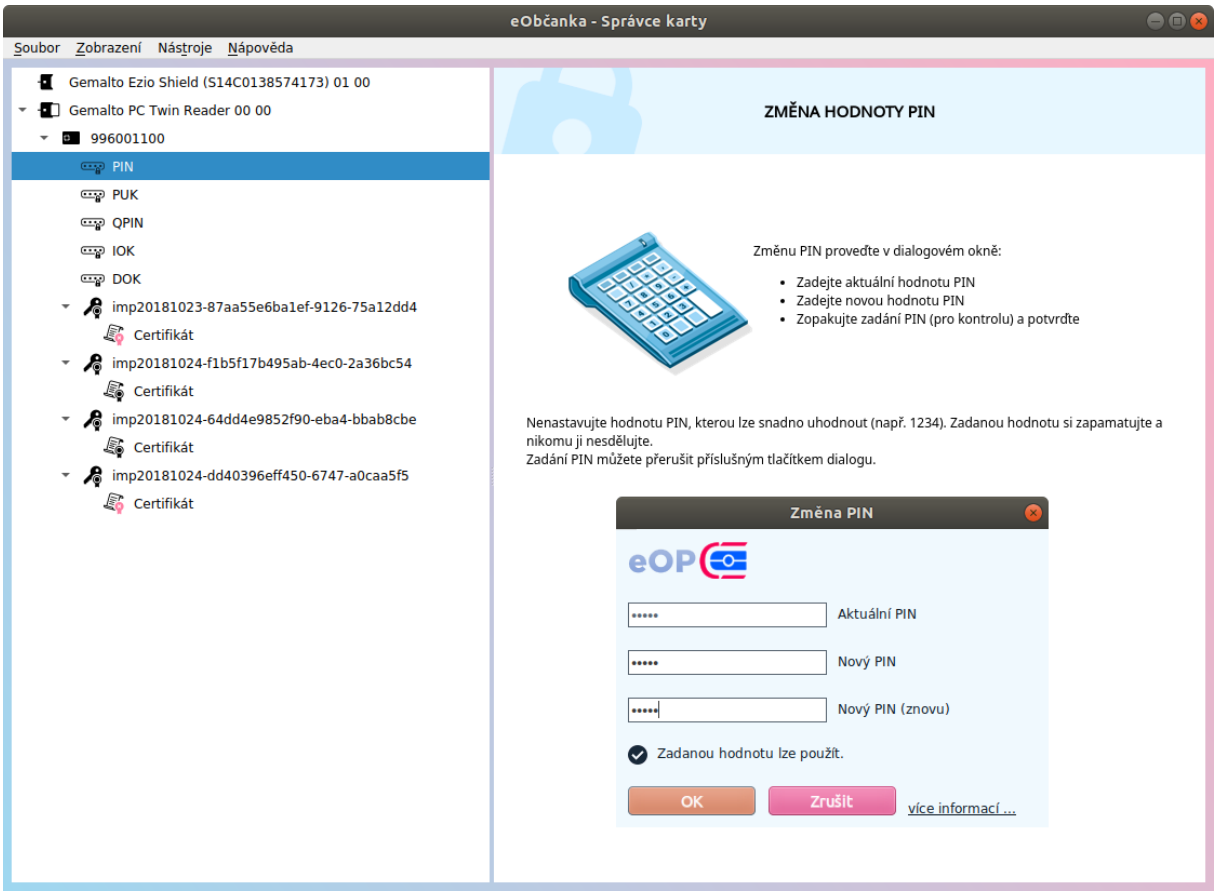
Obrázek 46: Kontextové menu karty s nabídkou změny přístupových kódů

Postup změny přístupového kódu se mírně liší podle toho, zda uživatel používá běžnou čtečku (bez klávesnice) anebo čtečku s klávesnicí. v obou případech je pro změnu kódu potřeba (v uvedeném pořadí):

- Zadat platnou / aktuální hodnotu daného přístupového kódu.
- Zadat novou hodnotu přístupového kódu.
- Opakovat novou hodnotu přístupového kódu (pro kontrolu).

8.5.2 Změna přístupového kódu na běžné čtečce

Při použití běžné čtečky se změna přístupového kódu provádí v pravém panelu aplikace *Správce karty.* Zobrazí se informace pro uživatele, která popisuje postup změny:



Obrázek 47: Okno pro změnu PIN na běžné čtečce (bez klávesnice)

Uživatel zadá číselné hodnoty kódů:

- Do prvního pole aktuální hodnotu přístupového kódu, pro schválení operace.
- Do druhého pole novou hodnotu přístupového kódu.
- Do třetího pole zopakuje novou hodnotu kódu, kvůli eliminaci překlepů a kontrole.

Pod editačními poli aplikace zobrazuje stručnou nápovědu, dle stavu zadané hodnoty:

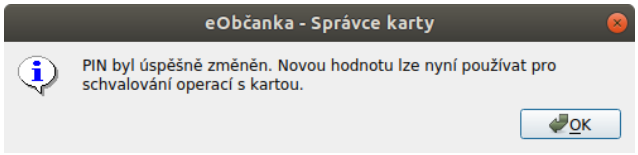
Obrázek 48: Stručná nápověda při změně přístupového kódu

Při změně přístupového kódu uživatel postupuje podle instrukcí zobrazených na obrazovce. Pole pro zadání přístupových kódů nezobrazují skutečné (zadané) číslice, ale pouze zástupné znaky.

Pokud je u přístupového kódu vypotřebován alespoň jeden neúspěšný pokus zadání, aplikace zobrazuje také počet zbývajících pokusů.

Po zadání hodnot přístupových kódů provede uživatel změnu hodnoty kódu stiskem tlačítka *OK*. (Aplikace umožní tlačítko použít až potom, co uživatel správně vyplní všechna požadovaná pole.)

Po stisku tlačítka aplikace *eObčanka – Správce karty* ověří stávající hodnotu kódu a nastaví novou hodnotu kódu do čipu občanského průkazu. Po dokončení operace se zobrazí informace o úspěšné změně přístupového kódu:



Obrázek 49: Informace o úspěšné změně přístupového kódu

Pokud se změna přístupového kódu nezdaří, aplikace vyprázdní editační pole a zobrazí upozornění, že se přístupový kód nepodařilo změnit. Uživatel může pokračovat dalším pokusem – dokud se daný kód nezablokuje.

Obrázek 50: Příklad chybového hlášení po neúspěšné změně kódu

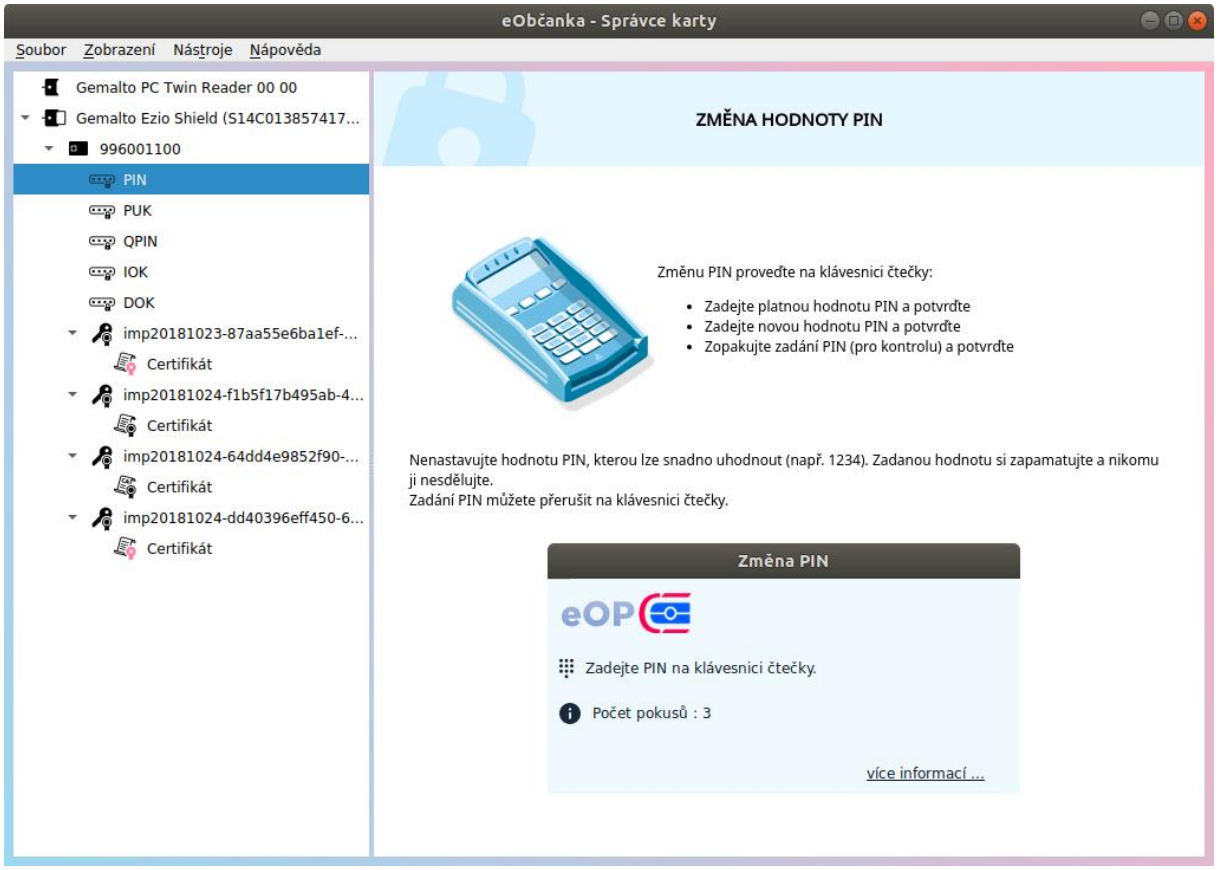
Při změně přístupového kódu může dojít k typickým chybám:

- Byla zadána nesprávná hodnota kódu.
- Vypršel časový limit pro zadání přístupového kódu (délka časového limitu je dána použitou čtečkou).

8.5.3 Změna přístupového kódu na čtečce s klávesnicí

Při použití čtečky s integrovanou klávesnicí uživatel zadává hodnoty přístupových kódů na klávesnici čtečky. Operaci změny přístupového kódu řídí čtečka čipových karet.

Pokud uživatel používá čtečku s klávesnicí i displejem, instrukce na zadání přístupových kódů jsou zobrazeny na displeji čtečky. Instrukce jsou také zobrazeny v pravém panelu Správce karty.



Obrázek 51: Okno pro změnu přístupového kódu na čtečce s displejem

Upozornění: Instrukce na displeji čtečky mohou být nesprávné! Čtečka může nesprávně pojmenovat názvy zadávaných přístupových kódů. Uživatel se nesmí nechat instrukcemi na displeji zmást a musí zadávat hodnotu kódu, který se rozhodnul změnit. Při manipulaci se čtečkou mohou uživateli pomoci instrukce v okně *Správce karty*.

Ať už uživatel používá čtečku s displejem či bez, musí na klávesnici čtečky zadat kódy v tomto pořadí:

- Aktuální hodnota kódu (+potvrdit na klávesnici čtečky).
- Nová hodnota kódu (+potvrdit na klávesnici čtečky).
- Nová hodnota kódu (+potvrdit na klávesnici čtečky).

Po potvrzení třetí hodnoty se provede nastavení nové hodnoty přístupového kódu do čipu občanského průkazu. *Správce karty* informuje o výsledku operace. Pokud operace skončí neúspěchem, zobrazí se chybové hlášení. Uživatel může nastavení kódu opakovat (dokud daný kód nezablokuje).

8.6 Odblokování přístupového kódu

Pomocí aplikace *eObčanka – Správce karty* lze odblokovat přístupové kódy, které jsou zablokované a umožňují odblokování:

- Zablokovaný IOK lze odblokovat pomocí DOK.
- Zablokovaný PIN lze odblokovat pomocí PUK.
- Zablokovaný QPIN lze odblokovat pomocí PUK.

Ostatní přístupové kódy pomocí *Správce karty* odblokovat nelze:

- Zablokovaný PUK nelze (nijak) odblokovat.
- Odblokování DOK je třeba provést na úřadu obce s rozšířenou působností.

Pozn.: *Odblokovat* lze i přístupové kódy, které nejsou aktuálně zablokované. Je to vhodné pro případy, kdy uživatel např. zapomene hodnotu PIN, ale zná hodnotu PUK. Pomocí PUK si v takovém případě může odblokovat (=nastavit) hodnotu PIN.

Pro odblokování přístupového kódu:

- Musí být pro zablokovaný kód definován kód pro odblokování (viz výše, pro některé kódy neexistuje odblokovací kód).
- Musí být odblokovací kód platný (musí být nastaven a nesmí být zablokován).
- Uživatel musí znát aktuální hodnotu odblokovacího kódu.

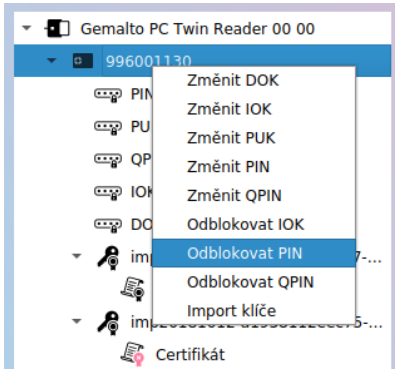
Pozn.: Odblokování všech přístupových kódů občanského průkazu se provádí podobně. v této příručce je proto popsán obecný postup odblokování přístupového kódu a jsou použity ilustrační obrázky odblokování PIN pomocí PUK. Odblokování ostatních přístupových kódů se provádí analogicky.

Odblokování kódů lze provádět opakovaně; počet opakovaných odblokování není omezen.

8.6.1 Spuštění operace odblokování přístupového kódu

Odblokování přístupového kódu lze v aplikaci *eObčanka – Správce karty* spustit pomocí:

- tlačítka z informačního okna o kartě (občanském průkazu),
- informačního okna o přístupovém kódu,
- kontextového menu karty,
- kontextového menu zablokovaného přístupového kódu.



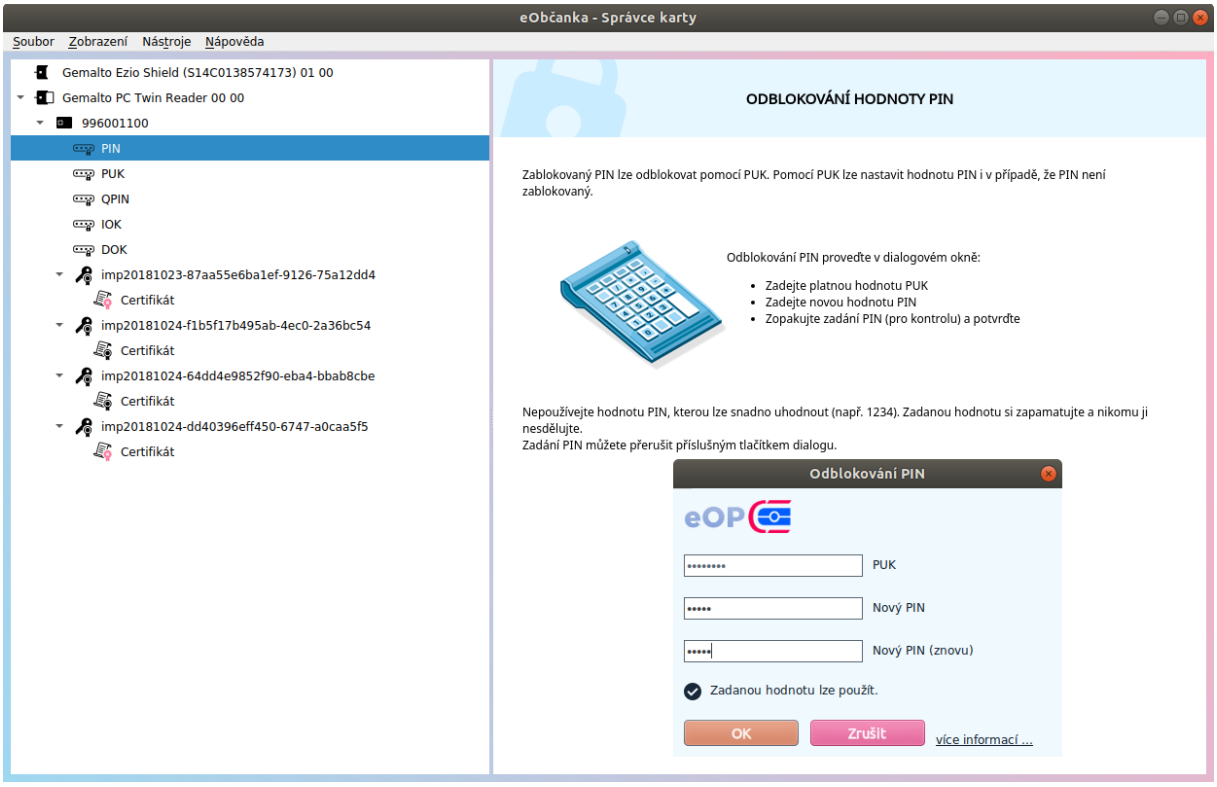
Obrázek 52: Kontextové menu karty (občanského průkazu)

Postup odblokování přístupového kódu se mírně liší podle toho, zda uživatel používá běžnou čtečku (bez klávesnice) anebo čtečku s klávesnicí. v obou případech je pro odblokování kódu potřeba (v uvedeném pořadí):

- Zadat platnou hodnotu odblokovacího kódu.
- Zadat novou hodnotu zablokovaného přístupového kódu.
- Opakovat novou hodnotu přístupového kódu (pro kontrolu).

8.6.2 Odblokování přístupového kódu na běžné čtečce

Při použití běžné čtečky se odblokování přístupového kódu provádí v pravém panelu aplikace *Správce karty*. Zobrazí se informace pro uživatele, která popisuje postup změny:

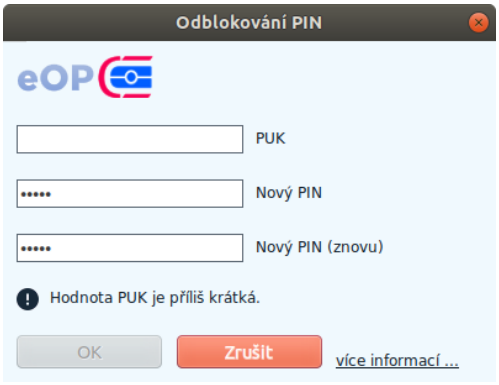


Obrázek 53: Okno pro odblokování PIN pomocí PUK na běžné čtečce

Uživatel zadá číselné hodnoty kódů:

- Do prvního pole aktuální hodnotu odblokovacího kódu, pro schválení operace. Aplikace uživatele instruuje, jaký kód má pro odblokování použít.
- Do druhého pole novou hodnotu zablokovaného přístupového kódu
- Do třetího pole zopakuje novou hodnotu kódu, kvůli eliminaci překlepů a kontrole.

Vedle editačních polí aplikace zobrazuje stručnou nápovědu, dle stavu zadané hodnoty:



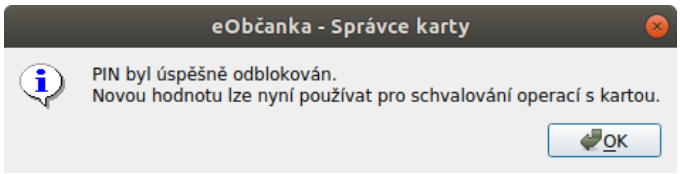
Obrázek 54: Stručná nápověda při odblokování přístupového kódu

Při odblokování přístupového kódu uživatel postupuje podle instrukcí zobrazených na obrazovce. Pole pro zadání přístupových kódů nezobrazují skutečné (zadané) číslice, ale pouze zástupné znaky.

Pokud je u odblokovacího kódu vypotřebován alespoň jeden neúspěšný pokus zadání, aplikace zobrazuje také počet zbývajících pokusů.

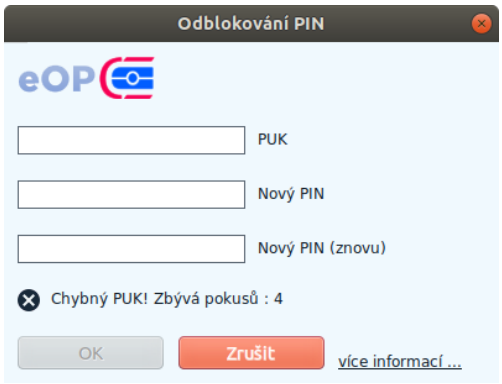
Po zadání hodnot přístupových kódů provede uživatel změnu hodnoty kódu stiskem tlačítka *OK*. (Aplikace umožní tlačítko použít až potom, co uživatel správně vyplní všechna požadovaná pole.)

Po stisku tlačítka aplikace *eObčanka – Správce karty* ověří hodnotu odblokovacího kódu a nastaví novou hodnotu kódu do čipu občanského průkazu. Po dokončení operace se zobrazí informace o úspěšném odblokování přístupového kódu:



Obrázek 55: Informace o úspěšném odblokování přístupového kódu

Pokud se odblokování přístupového kódu nezdaří, aplikace vyprázdní editační pole a zobrazí upozornění, že se přístupový kód nepodařilo odblokovat. Uživatel může pokračovat dalším pokusem – dokud se nezablokuje odblokovací kód.



Obrázek 56: Příklad chybového hlášení po neúspěšném odblokování kódu

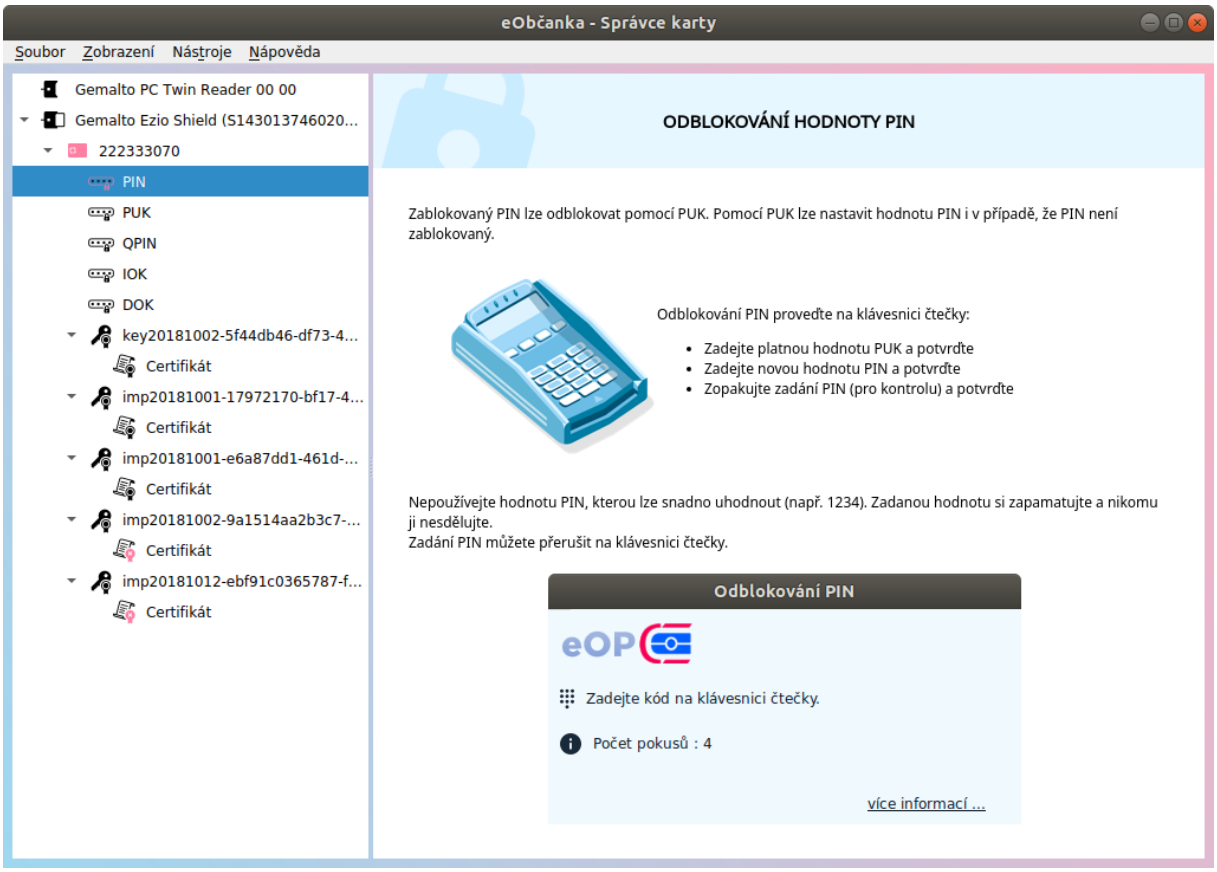
Při změně přístupového kódu může dojít k typickým chybám:

- Byla zadána nesprávná hodnota odblokovacího kódu.
- Vypršel časový limit pro zadání přístupového kódu (délka časového limitu je dána použitou čtečkou).

8.6.3 Odblokování přístupového kódu na čtečce s klávesnicí

Při použití čtečky s integrovanou klávesnicí uživatel zadává hodnoty přístupových kódů na klávesnici čtečky. Operaci odblokování přístupového kódu řídí čtečka čipových karet.

Pokud uživatel používá čtečku s klávesnicí i displejem, instrukce na zadání přístupových kódů jsou zobrazeny na displeji čtečky. Podrobnější instrukce se zobrazují také v pravém panelu aplikace Správce karty:



Obrázek 57: Okno pro odblokování přístupového kódu na čtečce s klávesnicí

Upozornění: Instrukce na displeji čtečky mohou být nesprávné! Čtečka může nesprávně pojmenovat názvy zadávaných přístupových kódů. Uživatel se nesmí nechat instrukcemi na displeji zmást a musí zadávat nejprve hodnotu odblokovacího kódu a poté dvakrát hodnotu kódu, který má být odblokován. Při manipulaci se čtečkou mohou uživateli pomoci instrukce v okně *Správce karty*.

Ať už uživatel používá čtečku s displejem či bez, musí na klávesnici čtečky zadat kódy v tomto pořadí:

- Aktuální hodnota odblokovacího kódu (+potvrdit na klávesnici čtečky).
- Nová hodnota kódu, který má být odblokován (+potvrdit na klávesnici čtečky).
- Nová hodnota kódu, který má být odblokován (+potvrdit na klávesnici čtečky).

Po potvrzení třetí hodnoty se provede nastavení nové hodnoty přístupového kódu do čipu občanského průkazu. *Správce karty* informuje o výsledku operace. Pokud operace skončí neúspěchem, zobrazí se chybové hlášení. Uživatel může nastavení kódu opakovat (dokud odblokovací kód nezablokuje).

9 ŘEŠENÍ PROBLÉMŮ

Pokud má uživatel s použitím certifikátů v občanském průkazu potíže, měl by nejprve prověřit, zda provedl potřebné kroky pro zprovoznění podpory certifikátů v občanském průkazu – viz kapitola 3.

Pokud byly všechny přípravné kroky provedeny, lze spustit aplikaci *eObčanka – Správce karty* a zkusit načíst obsah čipu občanského průkazu.

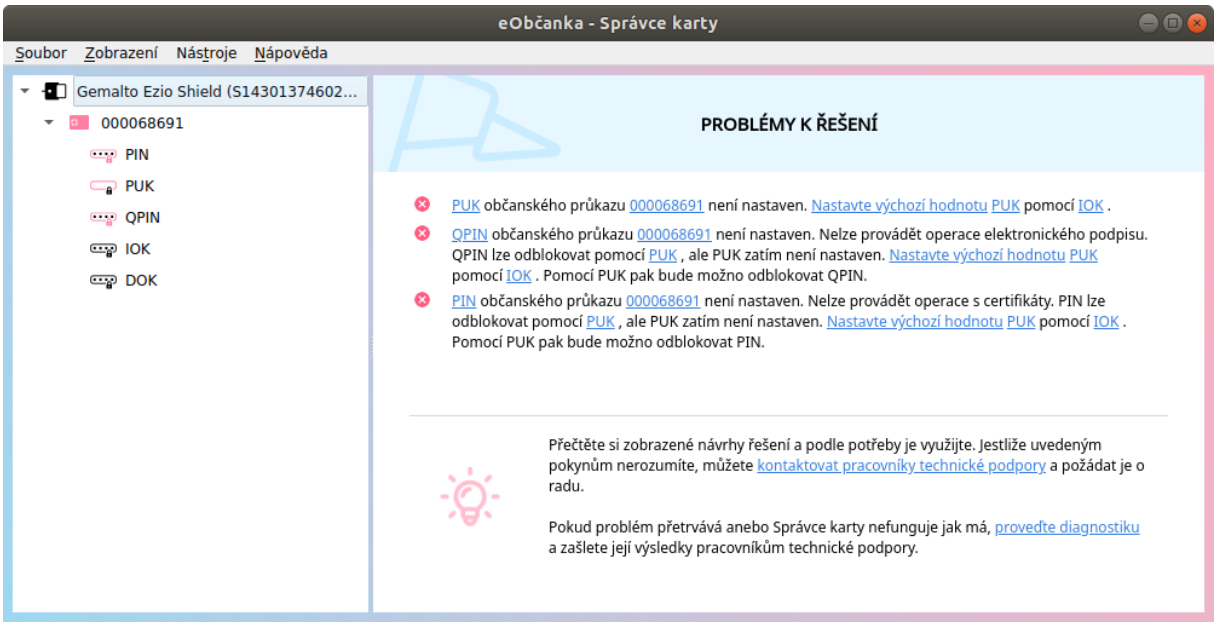
- Jestliže obsah čipu načíst lze, je podpora certifikátů v občanském průkazu v zásadě funkční.
- V případě, že se obsah čipu nepodaří přečíst (a k počítači je připojena čtečka a do čtečky je vložen občanský průkaz), je třeba zjistit příčinu problému. Pomocí *Správce karty* lze provést diagnostiku a výsledky poslat k analýze pracovníkům technické podpory.

9.1 Problémy k řešení

Problematika certifikátů na čipových kartách je pro běžného uživatele poměrně odtažitá. Velký počet přístupových kódů, spojených s občanským průkazem, práci s certifikáty ještě více komplikuje. Běžný uživatel se v problematice obtížně orientuje; není schopen rozpoznat, co je v čipu nastaveno správně a co je třeba ještě nastavit, aby bylo možno používat certifikáty.

Aplikace *eObčanka – Správce karty* se snaží uživateli pomoci. Snaží se identifikovat potíže, které uživateli mohly zkomplikovat či znemožnit práci s certifikáty. Vyhodnocuje data, zapsaná do čipu občanského průkazu, vyhledává potenciální problémy a navrhuje jejich řešení.

Vyhodnocení potenciálních potíží se provádí automaticky po přečtení informací z čipu občanského průkazu. Pokud aplikace identifikuje nějaké problémy, zobrazí je uživateli v okně *Problémy k řešení*. (Seznam *problémů k řešení* lze zobrazit také na vyžádání pomocí menu *Nástroje – Problémy k řešení*).

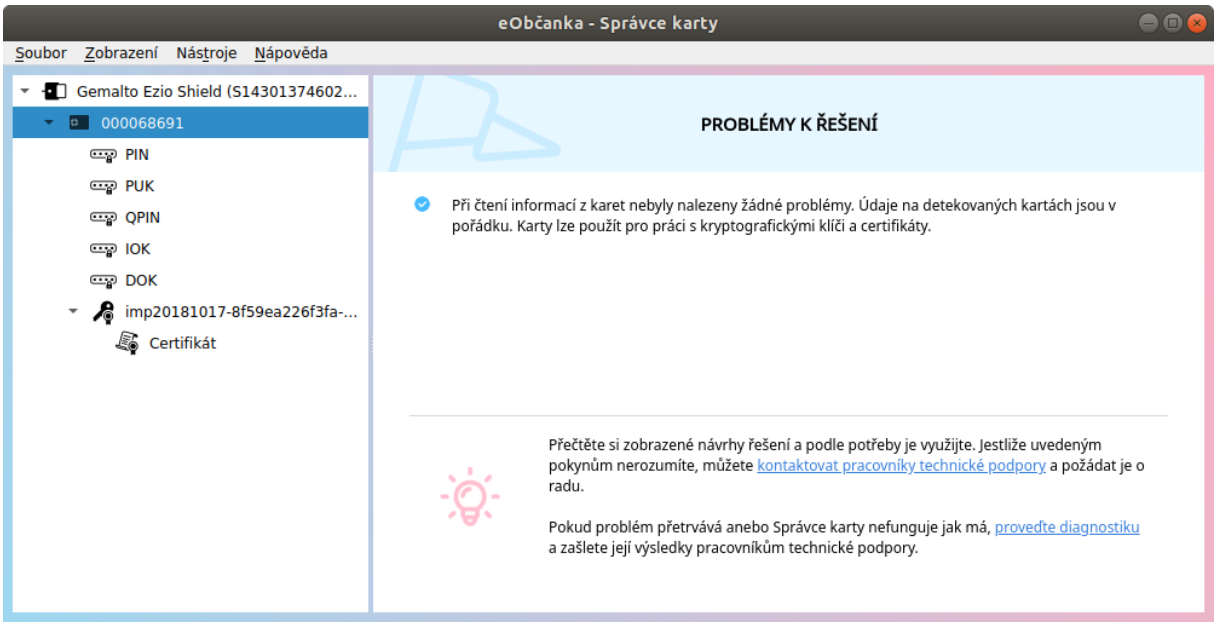


Obrázek 58: Okno Správce karty s problémy k řešení

Je běžné, že se při vyhodnocení nalezne více potíží. Jednotlivé problémové informace se zobrazují jako položky v seznamu.

Uživatel může mezi zobrazenými informacemi najít potíže, které mu komplikují práci s certifikáty nebo obecně s elektronickými funkcemi občanského průkazu. v takovém případě by měl využít návrhů řešení, které aplikace nabízí. Některé z návrhů dokonce obsahují odkazy na spuštění akce, která může nalezený problém vyřešit. Jiné položky alespoň na nalezený problém upozorňují.

Pokud není žádný problém nalezen (vše je v pořádku), zobrazí se v okně *Problémy k řešení* informace: *Při čtení informací z karet nebyly zjištěny žádné problémy*:



Obrázek 59: Žádné problémy s občanským průkazem nebyly zjištěny

V dolní části okna, pod seznamem problémů k řešení, jsou uvedeny instrukce pro případ, že by uvedené návrhy nevedly k vyřešení problému:

- Primárně se nabízí možnost kontaktovat pracovníky technické podpory, pomocí integrovaného formuláře – viz kapitola 9.2.
- Lze také vygenerovat diagnostiku *Správce karty*, kterou pak lze poslat k analýze pracovníkům technické podpory.

9.1.1 Příklady detekovaných problémů

Následující seznam uvádí některé typy problémů, které *Správce karty* detekuje a zobrazuje mezi *Problémy k řešení*:

- Nefunkční podpora čipových karet v operačním systému, nelze detekovat připojené čtečky. Možné příčiny:
  - V operačním systému není aktivována podpora čteček a čipových karet – PC/SC.
  - Podpora čteček je poškozena a nefunkční.
  - Ovladač čtečky znemožňuje správné fungování podpory čteček v operačním systému.
- K počítači není připojena žádná funkční čtečka čipových karet.
- Ve čtečce karet nebyla nalezena žádná podporovaná karta. Ve čtečce může být vložena neznámá či nepodporovaná karta.
  Aplikace *eObčanka - Správce karty* spolupracuje pouze s občanskými průkazy ČR.
- Uživatel předčasně přerušil načítání informací o obsahu karet. Načtené informace nemusejí být kompletní a mohou být zavádějící.
- Při čtení dat z karty nastala chyba; karta může být poškozená.

- Některý z přístupových kódů je zablokován nebo nenastaven. Pokud je to možné, aplikace nabízí nastavení či odblokování přístupového kódu.
- Blížící se expirace certifikátu.
  - Zbývající platnost certifikátu je 3 týdny nebo méně.
  - Doporučuje se včas požádat o obnovu certifikátu.

Upozornění: Seznam problémů k řešení je ovlivněn tím, zda je *Správce karty* přepnut do *standardního* či *rozšířeného* zobrazení (viz kapitola 5.5):

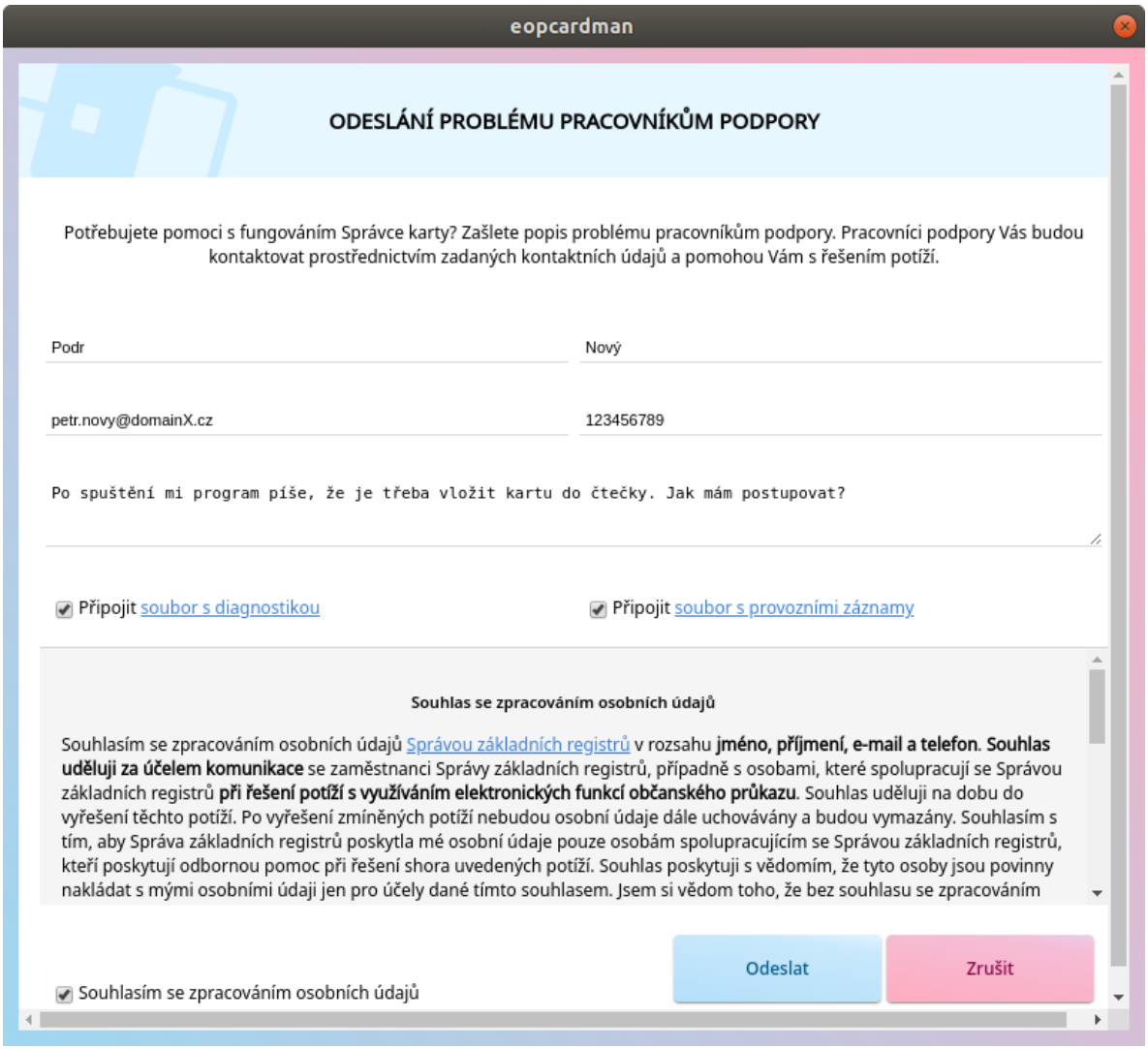
- Ve *standardním* zobrazení se v seznamu zobrazují pouze závažnější potíže. Seznam je obvykle kratší.
- V *rozšířeném* zobrazení se zobrazuje kompletní seznam nalezených potíží, tedy i méně významné problémy.

9.2 Odeslání problému pracovníkům technické podpory

Pokud uživatel není schopen sám vyřešit potíže s čipem občanského průkazu nebo s fungováním aplikace *eObčanka – Správce karty*, může zaslat dotaz pracovníkům technické podpory. Formulář pro odeslání dotazu lze zobrazit pomocí:

- odkazu ze stránky s výsledky diagnostického testu – viz kapitola 9.3.
- odkazu ze stránky *Problémy k řešení* – viz kapitola 9.1.

Aplikace zobrazí formulář, v němž lze popsat problém odeslat jej pracovníkům technické podpory:



Obrázek 60: Okno pro odeslání problému pracovníkům technické podpory

Před odesláním je třeba uvést informace:

- **Kontaktní údaje**: jméno, příjmení, e-mailovou adresu, telefonní číslo.
  Tyto údaje jsou povinné - bez nich nelze problém pracovníkům podpory odeslat.
- **Popis problému**: uvést, jak se chyba projevuje, co je při chybě vidět na obrazovce, atp…
- **Souhlas se zpracováním osobních údajů.**
  Přečíst text informace o ochraně osobních údajů a vyjádřit souhlas zaškrtnutím pole *Souhlasím se zpracováním osobních údajů*.

Bez vyplnění uvedených údajů nelze problém pracovníkům podpory odeslat (tlačítko *Odeslat* je neaktivní).

Spolu se zadanými údaji se doporučuje ponechat zaškrtnutá pole *Připojit soubor s diagnostikou* a *Připojit soubor s provozními záznamy*. Tyto volby připojí k odesílaným informacím soubory s technickými informacemi, které jsou pro pracovníky podpory důležitým

zdrojem informací. Pracovníci podpory informace ze souborů analyzují a získají tím údaje, které by uživatel byl schopen jen velmi obtížně poskytnout. Přiložené soubory neobsahují citlivé ani osobní údaje, o čemž se lze přesvědčit zobrazením obsahu souborů (kliknutím na příslušný odkaz v popisu zaškrtávacího pole).

Popsaný problém lze pracovníkům podpory zaslat stiskem tlačítka *Odeslat*. Aplikace shromáždí zadané údaje a zapíše je do systému technické podpory. Po úspěšném odeslání se uživateli zobrazí informace s potvrzením odeslání.

Pracovníci podpory analyzují přijatý problém a poté uživatele kontaktují a pomohou s řešením problému.

9.3 Diagnostika

Aplikace *eObčanka – Správce karty* umí vygenerovat diagnostiku prostředí uživatelského počítače.

Informace v diagnostice jsou poměrně technické a běžný uživatel jim nemusí rozumět. Informace však lze zaslat pracovníkům podpory, kterým diagnostické údaje pomohou v analýze problému.

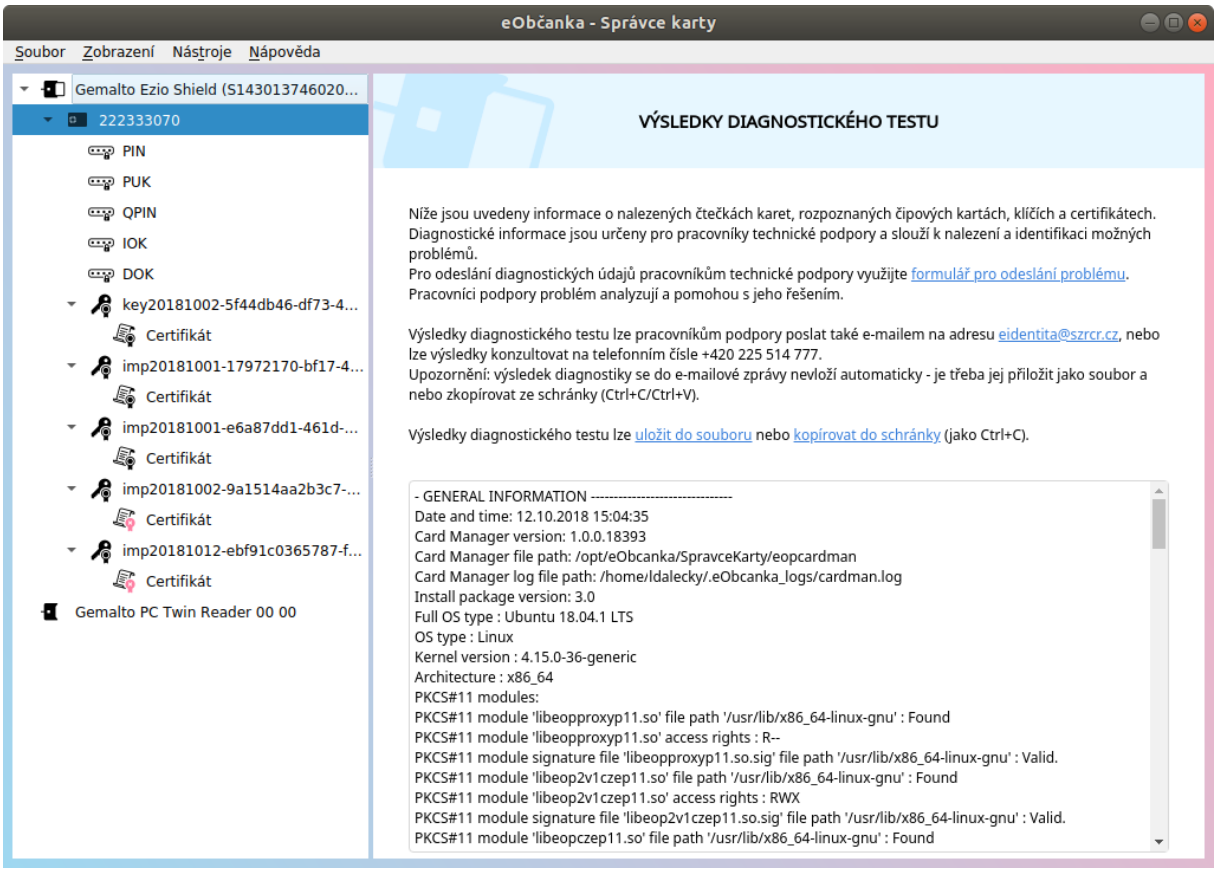
Diagnostika prostředí obsahuje mj. tyto informace:

- stav operačního systému,
- informace o ovladačích občanského průkazu,
- dostupné čtečky,
- nalezené občanské průkazy s čipem,
- stavy přístupových kódů občanského průkazu,
- charakteristiky certifikátů, nalezených v čipu občanského průkazu.

Diagnostické údaje neobsahují osobní údaje (ani osobní údaje z certifikátů). Ve výsledku diagnostiky jsou obsaženy pouze obecné technické informace, potřebné k analýze potíží s fungováním elektronických funkcí občanského průkazu.

Funkce diagnostika prověřuje nejen fungování aplikace *eObčanka – Správce karty*. Součástí je také prověření funkčnosti ovladačů občanského průkazu. Při podezření na nefunkčnost ovladačů občanského průkazu se doporučuje provést diagnostiku v aplikaci eObčanka - *Správce karty*.

Diagnostiku lze spustit pomocí menu *Nástroje – Zobrazit diagnostiku*. Aplikace vyčte a zobrazí diagnostické informace:



Obrázek 61: Okno s výsledkem diagnostického testu

Výsledek diagnostiky lze pracovníkům technické podpory nejsnáze zaslat pomocí integrovaného formuláře (viz kapitola 9.2).

Diagnostické údaje lze také

- uložit do souboru (viz kapitola 9.3.1),
- nebo kopírovat do schránky a přiložit je k e-mailové zprávě, zaslané technické podpoře na adresu eidentita@szrcz.cz (viz kapitola 9.3.2).

9.3.1 Uložení diagnostických informací do souboru

Pomocí *Správce karty* lze uložit výsledky diagnostiky do souboru; soubor pak lze např. přiložit k e-mailové zprávě a zaslat pracovníkům technické podpory (viz také kapitola 9.3.2).

Uložení diagnostických údajů do souboru lze spustit:

- pomocí menu *Nástroje – Uložit diagnostiku,*
- anebo pomocí odkazu z okna s výsledky diagnostiky.

Aplikace zobrazí systémové okno pro uložení souboru. Jako výchozí název je zvolen *CardManager.txt*. Uživatel může změnit název souboru a může také zvolit adresář, do nějž má být soubor uložen. Tlačítkem *Uložit* se diagnostické údaje uloží do zvoleného textového souboru. Obsah souboru lze prohlédnout běžným textovým editorem.

9.3.2 Odeslání diagnostických informací pracovníkům technické podpory

Upozornění: **Jednodušší** cestou, jak kontaktovat pracovníky technické podpory, je využití **integrovaného formuláře** – viz kapitola 9.2. Při použití integrovaného formuláře se diagnostické údaje přiloží k odesílaným datům automaticky. Pokud je to možné, doporučuje se využít integrovaný formulář – zaslání informací e-mailem by mělo být použito v případě, že se data z integrovaného formuláře nepodaří odeslat.

Výsledky diagnostiky lze zaslat pracovníkům technické podpory, jako přílohu e-mailové zprávy. Diagnostická data je třeba nejprve uložit do souboru a poté přidat jako přílohu e-mailové zprávy, zaslané na adresu eidentita@szrcz.cz.

Před odesláním e-mailové zprávy pracovníkům technické podpory je třeba do e-mailové zprávy uvést:

- Kontaktní údaje: jméno a příjmení, popř. telefonní číslo
- Popis problému – chování aplikace, neobvyklý vzhled aplikačního okna, chybové hlášení, apod…

9.4 Kontakt na pracovníky technické podpory

Pracovníky technické podpory je nejvhodnější kontaktovat pomocí integrovaného formuláře – viz kapitola 9.2.

Pokud ke kontaktování technické podpory nelze integrovaný formulář použít (např. proto, že aplikaci *Správce karty* vůbec nelze spustit), lze pracovníky podpory kontaktovat:

- Prostřednictvím e-mailové zprávy, na adresu eidentita@szrcz.cz.
  - Je třeba doplnit kontaktní údaje a popis problému, viz také kapitola 9.3.2.
- Telefonicky, na čísle 225 514 777.
  - Telefonický kontakt je poměrně neefektivní cesta k vyřešení problému. Telefon nelze použít pro zaslání diagnostických údajů či jiných technických podrobností. Pracovníci podpory v takovém případě nemají dostatek informací pro analýzu problému.

9.5 Provozní záznamy

Správce karty zapisuje o své činnosti provozní záznamy, na lokální disk hostitelského počítače. Do souboru s provozními záznamy se průběžně zapisují informace o:

- operacích, které *Správce karty* provádí,
- a chybách, které při práci se *Správcem karty* mohou vznikat.

Soubory s provozními záznamy vznikají pro případ potíží se *Správcem karty*: uživatel může zaslat soubory s provozními záznamy pracovníkům technické podpory (viz kapitola 9.2). Pracovníci podpory analyzují provozní záznamy a získají podklady pro vyřešení vzniklých potíží.

Do souborů s provozními záznamy se nezapisují žádné osobní informace anebo bezpečnostní kódy. Soubory obsahují pouze provozní informace o prováděných funkcích, a základní informace o zpracovávaných datech.

Soubory s provozními záznamy se na disku počítače průběžně přepisují. Nehrozí tak zaplnění disku provozními záznamy.

Ve výchozím stavu (např. po instalaci software *eObčanka*) se zapisuje *základní* úroveň provozních záznamů. Ten pro detekci složitějších problémů nemusí dostačovat. v případě řešení potíží může být uživatel požádán pracovníky podpory, aby aktivoval *rozšířený* zápis provozních údajů. Rozšířené provozní údaje obsahují více podrobností, které mohou být pro analýzu problému nezbytné. Úroveň podrobností provozních záznamů uživatel může ovlivnit pomocí okna pro uživatelské nastavení – viz kapitola 9.6. Pomocí nastavení může uživatel zápis provozních údajů také zcela vypnout.

9.6 Uživatelské nastavení

Pomocí menu *Nástroje* – *Nastavení* může uživatel zobrazit okno pro nastavení parametrů, které ovlivňují chování aplikace *Správce karty*:

Obrázek 62: Okno pro nastavení uživatelských parametrů

V okně lze nastavit úroveň podrobností zápisu provozních údajů (viz také kapitola 9.5).
k dispozici jsou tyto položky nastavení:

- *Zapisovat provozní záznamy*
  Je-li zaškrtnuto, zapisuje *Správce karty* provozní záznamy (základní úroveň). Není-li zaškrtnuto, aplikace provozní záznamy vůbec nezapisuje.
  Výchozí nastavení je: *zapisovat provozní záznamy*.
- *Zapisovat rozšířené provozní záznamy*
  Je-li zaškrtnuto, zapisuje *Správce karty* rozšířený formát provozních záznamů (podrobnější záznamy). Není-li zaškrtnuto, aplikace zapisuje žurnál podle nastavení *Zapisovat provozní záznamy*.
  Výchozí nastavení je *nezapisovat rozšířené provozní záznamy*.

Položka *Zapisovat rozšířené provozní záznamy* je dostupná jen pokud je zaškrtnutá položka *Zapisovat provozní záznamy*. Pokud položka *Zapisovat provozní záznamy* zaškrtnuta není, je položka *Zapisovat rozšířené provozní záznamy* nedostupná.

V dolní části okna, pod seznamem parametrů, jsou tlačítka *OK* a *Zrušit*. Po stisku kteréhokoli z tlačítek se okno s nastavením uzavře:

- Po stisku *OK* se nejprve uloží aktuálně nastavené hodnoty parametrů.
- Po stisku *Zrušit* se okno uzavře bez uložení parametrů.

Po uložení (tlačítkem *OK*) jsou nově nastavené hodnoty parametrů okamžitě používány. Pro použití nově nastavených parametrů není třeba restartovat aplikaci *Správce karty*.

10 ZPROVOZNĚNÍ PODPORY CERTIFIKÁTŮ

Tato kapitola se zabývá typickou situací: uživateli je vydán nový občanský průkaz s čipem. Držitel chce nový občanský průkaz využít pro uložení certifikátů. v této kapitole je stručně popsáno, jaké kroky je třeba podniknout, aby uživatel mohl certifikáty v občanském průkazu používat.

Před vydáním certifikátu do čipu občanského průkazu je třeba vytvořit podmínky:

- **Připravit počítač** pro podporu elektronických funkcí občanského průkazu.
  - **Instalovat software eObčanka.**
  - **Připojit čtečku karet.**
    (podrobněji je postup popsán v kapitole 3).
- **Nastavit přístupové kódy** občanského průkazu: PUK, PIN, resp. QPIN.
  Informace o přístupových kódech občanského průkazu jsou uvedeny v kapitole 8.1.
  Postup nastavení přístupových kódů se liší pro jednotlivé verze občanských průkazů; postup je popsán v níže uvedených podkapitolách 10.1, resp. 10.2.

Jakmile je počítač i občanský průkaz připraven, lze oslovit certifikační autoritu a **požádat o vydání certifikátu**. Postup a podmínky vydání certifikátu se pro jednotlivé certifikační autority liší. Uživatel by měl zvolit certifikační autoritu, u níž chce požádat o certifikát. Certifikační autorita by měla uživatele informovat - obvykle prostřednictvím svých webových stránek - o postupu vydání certifikátu do občanského průkazu.

10.1 Nastavení přístupových kódů v občanském průkazu, vydaném před 1. 7. 2018

Přístupové kódy **PIN a PUK** občanských průkazů, vydaných před 1. 7. 2018, **je třeba nastavit na úřadu obce s rozšířenou působností**.

Nastavené hodnoty PIN a PUK lze následně spravovat pomocí aplikace *Správce karty*:

- Změnit hodnotu PIN či PUK – viz kapitola 8.5.
- Odblokovat zablokovaný PIN pomocí PUK – viz kapitola 8.6.

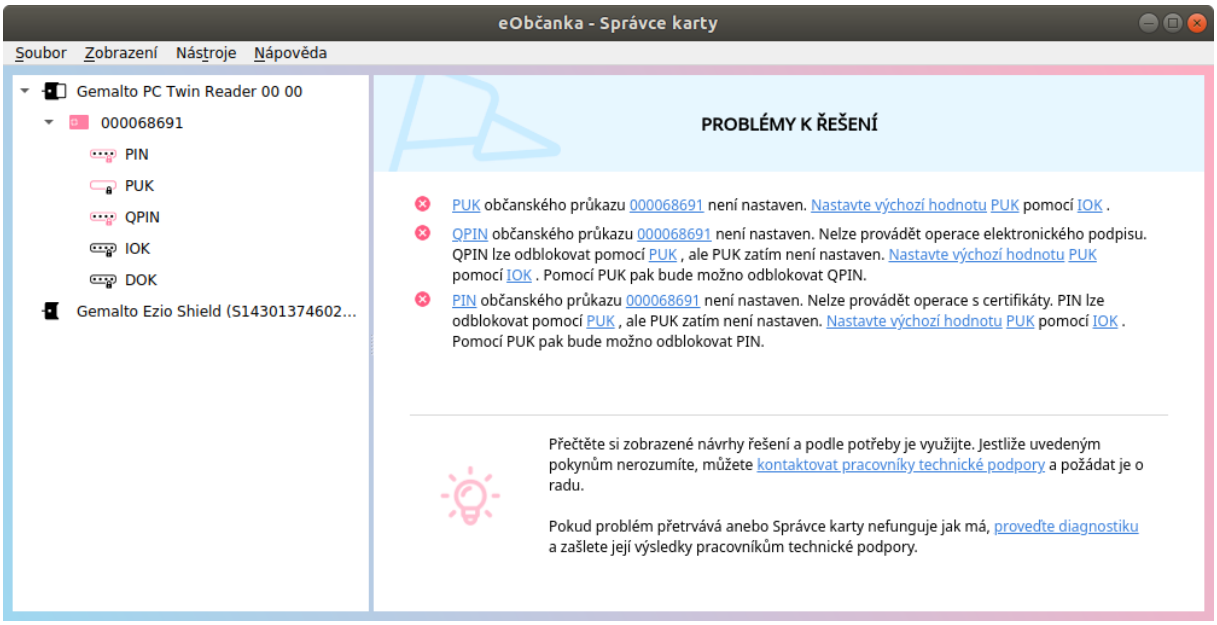
10.2 Nastavení přístupových kódů v občanském průkazu, vydaném po 1. 7. 2018

Pro nastavení přístupových kódů občanských průkazů, vydaných po 1. 7. 2018, je třeba provést několik kroků:

- **Nejprve** je třeba **na úřadu obce s rozšířenou působností nastavit hodnoty DOK a IOK**.
  Uživatel si může tyto kódy nastavit při převzetí občanského průkazu anebo kdykoli později.
- **Po nastavení DOK a IOK** je třeba použít aplikaci ***Správce karty* pro postupné nastavení zbývajících přístupových kódů**:
  - Nastavení **PUK** pomocí IOK – viz kapitola 8.4.

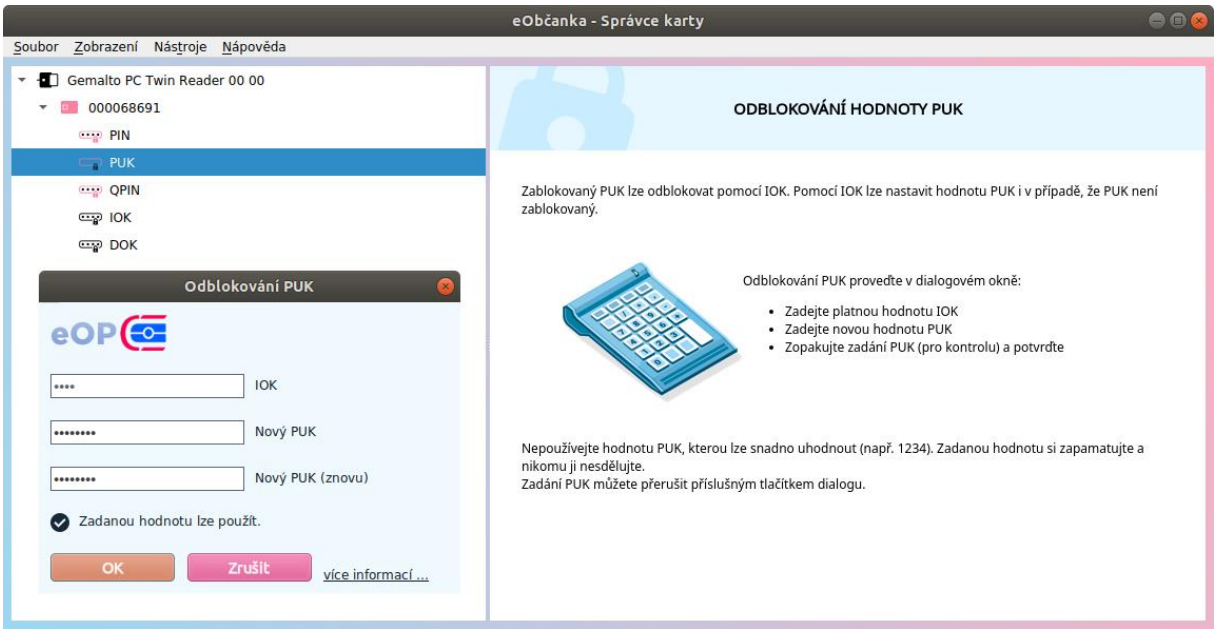
- Odblokování **PIN** pomocí PUK – viz kapitola 8.6.
- Odblokování **QPIN** pomocí PUK – viz kapitola 8.6.

Správce karty se snaží uživateli s nastavením přístupových kódů (PUK, PIN, QPIN) pomoci. Po přečtení obsahu čipu (viz kapitola 4.2) *Správce karty* automaticky rozpozná, že má uživatel nastaveny hodnoty DOK a IOK, ale nemá nastaveny hodnoty PUK, PIN, resp. QPIN. v takovém případě *Správce karty* nabídne uživateli nastavení jednotlivých kódů.



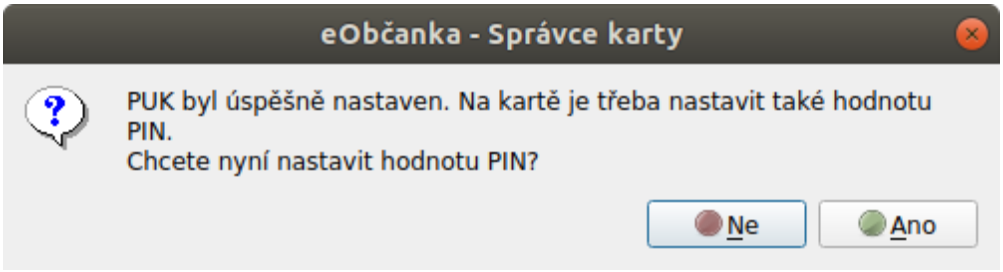
Obrázek 63: Občanský průkaz má nastaven DOK a IOK, hodnoty PUK, PIN a QPIN nejsou nastaveny

Pokud není nastaven PUK, nabídne se uživateli možnost nastavit PUK. (Postup nastavení PUK je uveden v kapitole 8.4.)



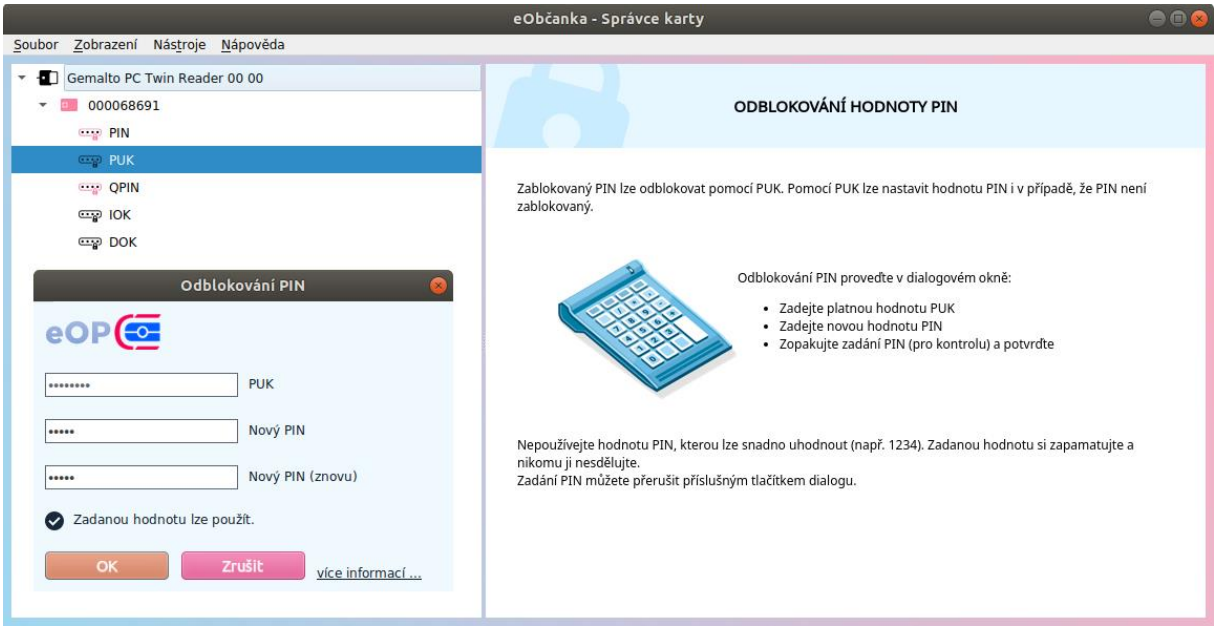
Obrázek 64: Okno pro nastavení PUK pomocí IOK

Po nastavení hodnoty PUK nabídne *Správce karty* možnost nastavení PIN:



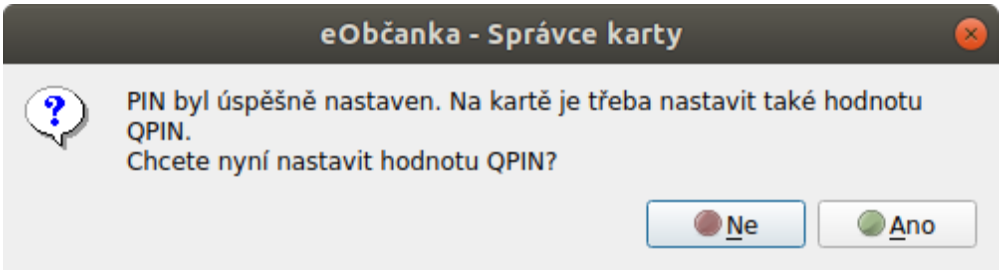
Obrázek 65: Okno s informací o nastavení PUK a s nabídkou nastavení PIN

Postup odblokování PIN pomocí PUK je popsán v kapitole 8.6.



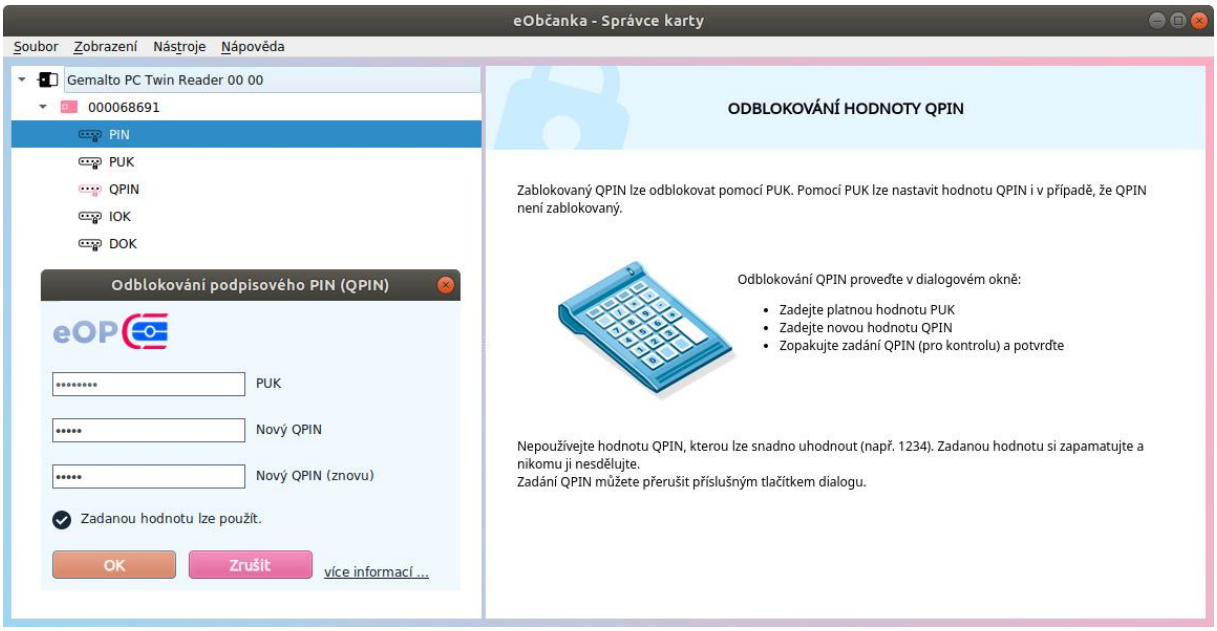
Obrázek 66: Okno pro nastavení hodnoty PIN pomocí PUK

Po nastavení hodnoty PIN nabídne *Správce karty* možnost nastavení QPIN.



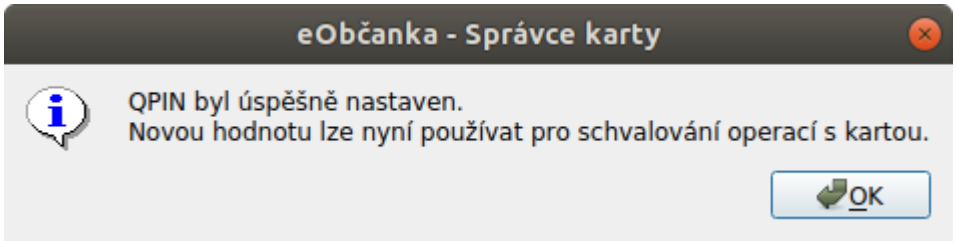
Obrázek 67: Okno s informací o nastavení PIN a s nabídkou nastavení QPIN

Postup odblokování QPIN pomocí PUK je popsán v kapitole 8.6.



Obrázek 68: Okno pro nastavení QPIN pomocí PUK

Po dokončení uvedeného procesu má uživatel nastaveny PUK, PIN i QPIN, tedy všechny kódy, potřebné pro práci s certifikáty.



Obrázek 69: Okno s informací o úspěšném nastavení QPIN

Pozn.: Uživatel nemusí realizovat nastavení všech kódů v jednom sledu. Může řetězec nastavování kódů přerušit a nastavit kódy později (opět pomocí aplikace *Správce karty*).