Analýza podpůrných aplikací spojených s elektronickým občanským průkazem

David Drexler, DiS.

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David Drexler, DiS.**
Osobní číslo:	**A16010**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Analýza podpůrných aplikací spojených s elektronickým občanským průkazem**
Téma anglicky:	**Analysis of Support Applications Associated With an Electronic Identity Card**

Zásady pro vypracování:

1. **Proveďte literární rešerši na téma elektronické identifikační nástroje.**
2. **Popište technologii a služby použité u elektronického občanského průkazu (eOP).**
3. **Analyzujte integrované a rozšířené možnosti eOP.**
4. **Definujte reálné možnosti a omezení eOP spojené s kvalifikovanými poskytovateli.**
5. **Ověřte u zvolených poskytovatelů funkčnost a uživatelskou přívětivost na vybraných platformách.**
6. **Vyhodnoťte získané poznatky a proveďte diskusi nad vhodností eOP.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MATES, Pavel a Vladimír SMEJKAL. E-government v České republice: právní a technologické aspekty. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6.**
2. **ŠPAČEK, David. EGovernment: cíle, trendy a přístupy k jeho hodnocení. V Praze: C.H. Beck, 2012. Beckova edice ekonomie. ISBN 978-80-7400-261-8.**
3. **Úvodní strana – Ministerstvo vnitra České republiky [online]. Praha: Ministerstvo vnitra České republiky, c2018 [cit. 2018-11-18]. Dostupné z: https://www.mvcr.cz/ministerstvo-vnitra-ceske-republiky.aspx**
4. **Elektronická identita – informační web [online]. Praha: Správa základních registrů, c2018 [cit. 2018-11-18]. Dostupné z: https://info.eidentita.cz/**
5. **Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Zlín: AION CS, c2010-2018 [cit. 2018-11-18]. Dostupné z: https://www.zakonyprolidi.cz/**

Vedoucí bakalářské práce: **prof. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Ing. Martin Sysel, Ph.D.
garant oboru

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 21. května 2019

David Drexler, v. r.
podpis diplomanta

ABSTRAKT

Bakalářská práce se zabývá elektronickým občanským průkazem a jeho podpůrnými aplikacemi. V práci jsou popsány technologie využívané elektronickým občanským průkazem s novým čipem. V teoretické části jsou uvedeny elektronické nástroje k identifikaci a autentizaci. Je zde rozebrána problematika šifrování a elektronického podpisu. Praktická část práce je zaměřena na elektronický občanský průkaz. Jsou zde popsány jeho možnosti, funkce, legislativa, kvalifikovaní poskytovatelé služeb, bezpečnostní kódy, čtečky karet a podpůrné aplikace. V analýze aplikací je testována funkčnost, možnosti a přívětivost na vybraných platformách. Jsou vyhodnoceny získané poznatky a diskutována vhodnost elektronického občanského průkazu.

Klíčová slova: elektronický občanský průkaz, identifikace, autentizace, eGovernment, eIDAS, kvalifikovaní poskytovatelé, podpůrné aplikace

ABSTRACT

This bachelor thesis deals with electronic identity card and its supporting applications. The thesis describes technologies used by the electronic identity card with a new chip. Electronic tools for identification and authentication are introduced in the theoretical part. Encryption and electronic signature is described there. The practical part is focused on electronic identity card. It describes its capabilities, features, legislation, qualified service providers, security codes, card readers, and support applications. Application analysis tests functionality, capabilities, and friendliness on selected platforms. The acquired knowledge is evaluated and the suitability of the electronic identity card is discussed.

Keywords: electronic identity card, identification, authentication, eGovernment, eIDAS, qualified providers, support applications

Děkuji vedoucímu bakalářské práce prof. Mgr. Romanu Jaškovi, Ph.D. za náměty a připomínky k jejímu zpracování.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 AUTENTIZACE **11**
1.1 HESLO A PIN 11
1.1.1 Single sign-on (SSO) 13
1.2 TOKEN 13
1.3 BIOMETRIKA 13
2 ŠIFROVÁNÍ **15**
2.1 SYMETRICKÉ ŠIFROVÁNÍ 15
2.1.1 Blokové šifry 16
2.1.2 Proudové šifry 16
2.2 ASYMETRICKÉ ŠIFROVÁNÍ 16
2.3 HASH 17
2.4 PRETTY GOOD PRIVACY 17
3 ELEKTRONICKÝ PODPIS **18**
3.1 ELEKTRONICKÁ ZNAČKA A PEČEŤ 19
3.2 CERTIFIKÁTY 19
3.2.1 Třídy certifikátů 19
3.2.2 Kvalifikované a komerční certifikáty 20
3.3 CERTIFIKAČNÍ AUTORITY 20
3.4 ČASOVÉ RAZÍTKO 21
II PRAKTICKÁ ČÁST **22**
4 ELEKTRONICKÝ OBČANSKÝ PRŮKAZ **23**
4.1 VYDÁNÍ OBČANSKÉHO PRŮKAZU 23
4.2 LEGISLATIVA 24
4.3 KVALIFIKOVANÍ POSKYTOVATELÉ 26
5 KÓDY PRO OCHRANU OBČANSKÉHO PRŮKAZU **30**
5.1 OCHRANA KÓDŮ 31
5.2 HLEDISKA ČLENĚNÍ PŘÍSTUPOVÝCH KÓDŮ 32
6 ČTEČKY KARET **33**
6.1 ČTEČKY KARET PRO PŘIPOJENÍ K PC 33
6.2 ČTEČKY KARET PRO PŘIPOJENÍ K MOBILNÍMU ZAŘÍZENÍ 36
7 PODPŮRNÉ APLIKACE **39**
7.1 APLIKACE PRO PC 39
7.1.1 eObčanka – identifikace 40
7.1.2 eObčanka – Správce karty 41
7.1.3 Ovladače pro podporu práce s certifikáty 42
7.2 APLIKACE PRO MOBILNÍ ZAŘÍZENÍ 42
8 ANALÝZA PODPŮRNÝCH APLIKACÍ **44**

8.1 APLIKACE EOBČANKA NA MS WINDOWS 44
8.1.1 Identifikace pomocí eOP na PC 57
8.2 APLIKACE EOBČANKA PRO ANDROID 62
8.2.1 Identifikace pomocí eOP na mobilním zařízení 65
8.3 SROVNÁNÍ APLIKACÍ PRO PC A MOBILNÍ ZAŘÍZENÍ 66
9 VYHODNOCENÍ A DISKUSE 68
ZÁVĚR 70
SEZNAM POUŽITÉ LITERATURY 72
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 80
SEZNAM OBRÁZKŮ 82
SEZNAM TABULEK 84

ÚVOD

S rozvojem informačních a komunikačních technologií se moderní společnost stále více zajímá o využití možností těchto technologií v běžném životě. Veřejná správa zaznamenala tuto skutečnost a dokázala přijít s projekty, které se staly důležitou součástí elektronizace veřejné správy mezinárodně označovaný jako eGovernment. Mezi takové projekty se zcela jistě řadí i zaručený nástroj pro identifikaci a autentizaci občana pomocí elektronického občanského průkazu. V České republice již řadu let elektronický občanský průkaz existuje, avšak v nedávné době došlo k zásadní změně. Tato změna umožnila rozvinout potenciál fungování eGovernmentu u nás a zpřístupnit jeho možnosti značné části občanů. Protože však každá taková implementace sebou nese požadavky nejenom na legislativu či samotné řízení státní správy, ale i na dotčené subjekty jako jsou občané. Je proto důležité seznámit potencionálního uživatele této technologie o jejím fungování, možnostech a technologických aspektech elektronického občanského průkazu a jeho podpůrných aplikací.

Cílem této práce je analyzovat prostředí nové platformy pro občanské průkazy.

V teoretické části seznámit se základními pojmy v oblasti elektronických nástrojů pro identifikaci a autentizaci. K ucelenému pohledu na danou problematiku je nutné seznámit se s nástroji, které využívá nebo by mohl využívat elektronický občanský průkaz. Jsou zde popsány metody autentizace, téma šifrování a elektronického podpisu.

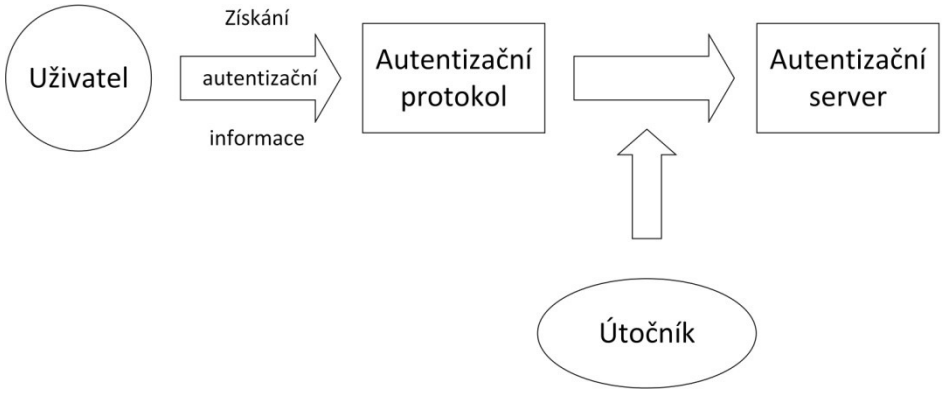
Praktická část je zaměřena na elektronický občanský průkaz a jeho podpůrné aplikace. Jsou zde popsány použité technologie a služby. Jeho možnosti a analýza podpůrných aplikací. V analýze aplikací je ověřena funkčnost, možnosti a přívětivost na vybraných platformách. Na závěr je provedena diskuse nad vhodností elektronického průkazu a vyhodnoceny získané poznatky.

I. TEORETICKÁ ČÁST

1 AUTENTIZACE

Je důležité rozlišovat dva pojmy a to **autentizace** a **identifikace**. Pod identifikací si lze přestavit odpověď na otázku *„kdo jsem?“*. Tím však není potvrzeno, že daný subjekt je tím, za koho se vydává. Autentizace je potom předem stanovený proces, u kterého za pomocí různých prostředků uživatel nebo entita v systému prokazuje svoji identitu. K ověření dané identity uživatele se stále častěji využívá důvěryhodná třetí strana, která může předat nutné informace za účelem autentizace. Autentizace může probíhat jak jednosměrně (autorizuje se pouze jedna strana), tak i oboustranně (sdílení tajné informace mezi oběma stranami). [1] [2]

Schéma činností autentizačního protokolu je znázorněn na Obr. 1.



Obr. 1 – Činnosti autentizačního protokolu [1]

Metody autentizace jsou založené na třech základních principech.

1. *Na něčem co daný uživatel zná (heslo, PIN)*
2. *Na něčem co daný uživatel má (fyzický objekt - token)*
3. *Na něčem, čím daný uživatel je (biometrika)*

Dvoufaktorová autentizace označuje kombinaci dvou různých metod. Tato forma bývá také nejvíce využívána. **Třífaktorová** autentizace je potom kombinací metod ze všech tří skupin. [3]

Autorizace probíhá až po úspěšné autentizaci *„specifikuje, jaké operace uživatelé mohou v systému provádět a jaká data jsou pro ně dostupná“*. [1]

1.1 Heslo a PIN

Metoda autentizace založená na abstraktní znalosti informace, kterou daný uživatel vlastní. Výhoda této metody je především v její jednoduchosti. Nevýhodou je poměrně nízká bez-

pečnost. Samotná bezpečnost této metody závisí na délce či složitosti hesla. Za bezpečné heslo se považuje takový řetězec, jehož prolomení je časově náročné běžnými technikami. Silné heslo je obvykle složeno z 8 až 12 znaků a obsahuje více skupin znaků např. malá a velká písmena, číslice a jiné speciální znaky. Heslo by však mělo být uživatelem snadno zapamatovatelné. Uživatel své heslo předkládá systému společně se svým uživatelským jménem (login). Systém poté kontroluje vložená data s daty uloženými u uživatele. [3] [4]

Zásady používání hesel:

- nesdílet heslo s více lidmi
- heslo nesmí být snadno uhodnutelné
- schopnost odolat slovníkovému útoku
- pravidelná změna hesla uživatelem
- neopakovatelnost stejného hesla
- uložení hesla na bezpečném místě
- minimální délka 8 znaků
- kombinace velkých a malých písmen
- heslo by mělo obsahovat alespoň jednu číslici
- bezpečnost hesla zvyšuje využití symbolů např. ? % / !
- nepoužívat řadu a opakující se znaky např. 1234568, qwerty
- vyvarovat se používání diakritiky
- nepoužívat jednoduchá hesla typu vlastní jméno, datum narození apod.
- nezadávat či dbát na zvýšené opatrnosti při zadávání hesla v cizích zařízeních např. internetové kavárny (využívání anonymního režimu prohlížeče)
- zrušení hesla při prozrazení či změně možnosti jeho používání [4] [5] [6]

Nutnost pamatovat si složitá hesla eliminuje tzv. PIN, který využívá omezený počet pokusů k uhádnutí jeho hodnoty. Jestliže uživatel zadá po sobě v daném počtu nesprávnou hodnotu PINu, dojde k jeho zablokování. Pro odblokování slouží další mechanizmy jako zadání jiného speciálního PINu nebo osobní návštěva a předložení potřebných dokladů u poskytovatele služby. Typický PIN se díky tomuto mechanizmu může skládat pouze z číslic o délce 4 až 8 znaků. Tímto došlo oproti využití hesla ke značnému zjednodušení. Při využívání PINů a blokačního mechanizmu je však nutné oproti heslům vlastnit fyzický předmět sloužící k autentizaci (token). Bez tohoto předmětu není možné PIN zadat. Pokud by totiž nebyl vázán na fyzický objekt, ale jen na uživatelské jméno hrozila by situace, že ně-

kdo záměrně využije blokační funkce a zadá několikrát správné přihlašovací jméno a nesprávné heslo. [3]

1.1.1 Single sign-on (SSO)

Proces jednotného přihlášení, při kterém se uživatel autentizuje u tzv. poskytovatele identity. Ten poskytuje autentizaci jiným aplikacím, ke kterým se chce uživatel přihlásit. Přes aplikaci vyžadující přihlášení je požadavek na přihlášení přesměrován na poskytovatele identit. Poskytovatel vykoná autentizaci uživatele a přesměruje jej zpět do aplikace. Pokud se chce uživatel přihlásit k další aplikaci, již se nemusí znovu autentizovat. U běžných uživatelů mezi nejznámější SSO řešení patří OpenID, MojeID, přihlášení pomocí Google či Facebook účtu. [7]

1.2 Token

Fyzický objekt označován jako tzv. token je něco co uživatel vlastní a používá k autentizaci. Tokeny mohou mít specifické fyzické vlastnosti. Mohou obsahovat tajné informace či provádět specifické výpočty. Tokeny mají nesporné výhody např. jejich obtížné kopírování, snadná zjistitelnost, přesnosnost a jednoduchost použití. Použití může být vázáno na znalost PINu. Tím se zvyšuje ochrana a minimalizuje riziko případného zneužití při ztrátě či krádeži tokenu. Avšak je tu i nutnost pořízení čtecího zařízení např. u čipových karet. Uživatele bez tokenu nelze autentizovat a po jeho ztrátě musí být nahrazen novým. Často poruchu tokenu lze zjistit až při pokusu o autentizaci. Nejběžnější formou tokenu jsou karty s magnetickým proužkem nebo čipové karty (např. platební či SIM karta). Další formou jsou tzv. autentizační kalkulátory, kde může být tajná informace uložena přímo v kalkulátoru a v autentizačním serveru, nebo na synchronizovaných hodinách. Dalším předmětem je tzv. USB token, který je založen na stejné technologii jako čipové karty. Lze jej připojit pomocí USB prakticky ke každému počítači. [3] [4]

1.3 Biometrika

Biometriky představují automatizované hodnotitelné biologické informace. Prakticky se jedná o část těla (fyziologické vlastnosti) či charakteristiku dané osoby (chování). Bezpečnost této metody závisí na přesnosti automatického měření. Technologicky je tato metoda náročnější jak z pohledu hardwaru tak i softwaru. Biometrické informace jsou totiž obtížně měřitelné a je velmi důležité, co je měřeno. Z tohoto důvodu systém pracuje s určitou pravděpodobností, hodnotící zda jde o daného jedince. Je důležité zmínit, že sa-

motné biometrické znaky mohou postupem času vykazovat změny. To je důležité z pohledu použitelnosti v praxi, proto není vždy možné naměřit stejné hodnoty biometrických charakteristik. Tudíž je nutné počítat s variabilitou těchto charakteristik a vyhodnocovat drobné odchylky. Fyziologická měření jsou obvykle považována za výhodnější, protože přinášení vyšší stabilitu během života jedince. V praxi nejsou vystaveny účinkům stresu, na rozdíl od identifikace chování. [3] [4] [8]

Mezi biometrické technologie identifikace patří:

- Analýza DNA
- Otisk prstu
- Geometrie ruky či jiné části těla
- Tvar ucha
- Snímání sítnice oka
- Rozpoznávání duhovky oka
- Rozpoznání obličeje
- Snímání žil a cév v ruce
- Analýza chůze
- Hlasový vzorek
- Dynamika podpisu
- Další způsoby měření chování – způsob použití objektů, gesta, dynamika stisknutí kláves atd. [8] [9] [10]

2 ŠIFROVÁNÍ

Šifrováním dosáhneme nečitelnosti obsahu dat při případném vniknutí do systému či počítače. Nejvhodnější způsobem ochrany před zneužitím dat a úspěšným útokem je kombinace více ochranných složek jako hesla, šifrování a hardwarové klíče. [4]

Podle toho jaká data je nutné chránit, šifrování rozlišíme na *on-line, off-line* a *on-demand*.

On-line šifrování dat probíhá v reálném čase při čtení či ukládání na disk. Identita uživatele se ověřuje při požadavku otevření či uložení daného souboru. Pokud vlastní uživatel příslušný šifrovací klíč je mu soubor dešifrován či naopak pokud podmínky nesplnil je mu přístup k soboru zamítnut. [4]

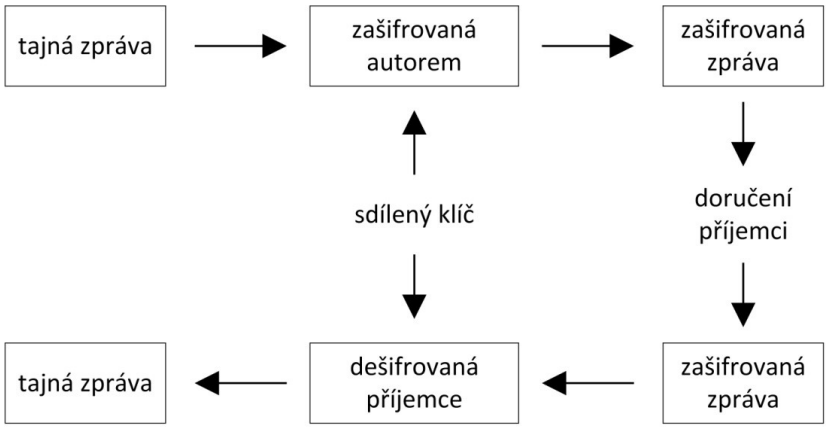
Off-line šifrování je vhodné k zašifrování menšího objemu dat. K šifrování či dešifrování dochází jednorázově po úspěšném přihlášení nebo odhlášení uživatele. [4]

On-demand je nejjednodušší způsob, kdy k šifrování dochází na požadavek uživatele. [4]

2.1 Symetrické šifrování

Pracuje s jedním šifrovacím klíčem, který pro porozumění obsahu předávaných zpráv musí mít jak odesílatel, tak i příjemce. Výhodou zde je, že takovéto šifry jsou velmi rychlé díky nízké náročnosti na výpočty a hodí se tedy na šifrování velkých dat např. celý oddíl disku. Bezpečnost závisí na zabezpečení předání šifrovacího klíče, a to není zrovna nejbezpečnější, pokud by se mělo jednat o velmi důležité obsahy zpráv např. přihlašovací údaje k elektronickému bankovnictví. [11] [12] [13]

Princip šifrování zprávy touto metodou je vidět na Obr. 2.



Obr. 2 – Princip symetrického šifrování [1]

2.1.1 Blokové šifry

Šifrují se jednotlivé části („bloky“) textu a poté stejné části se také dešifrují. Rozdělením do bloků, nejčastěji o velikosti 64 bitů, se zvýší bezpečnost. [13]

Nejznámější metody blokových šifer:

- **DES** (Data Encryption Standard) – vytvořena v 70. letech pro potřebu šifrování. Šifrovací klíč má délku 56 bitů, to však nestačí dnešním požadavků. Proto byla verze vylepšena na **Triple DES (3DES)**, která používá klíč o délce 112 nebo 168 bitů. [4]
- **IDEA** (International Data Encryption Algorithm) – délka klíče je 128 bitů. Velmi rychlá a s mnohem vyšším stupněm bezpečnosti proti DES. [4]
- **BlowFish** – proměnlivá délka klíče od 32 do 448 bitů. Obvykle však 128 bitů. Volně využitelný, bezpečný a rychlý. [4]
- **CAST –** charakteristikou podobný algoritmu BlowFish, obvykle s délkou 128 bitů a možností i jiných délek klíče. [4]
- **AES** (Advanced Encryption Standard) – délka klíče je zde 128, 196 nebo 256 bitů. Pracuje s bloky o délce 128 bitů. Bezpečná šifra zejména díky velké délce klíče. Je časově odolná proti útokům hrubou silou. [14]

2.1.2 Proudové šifry

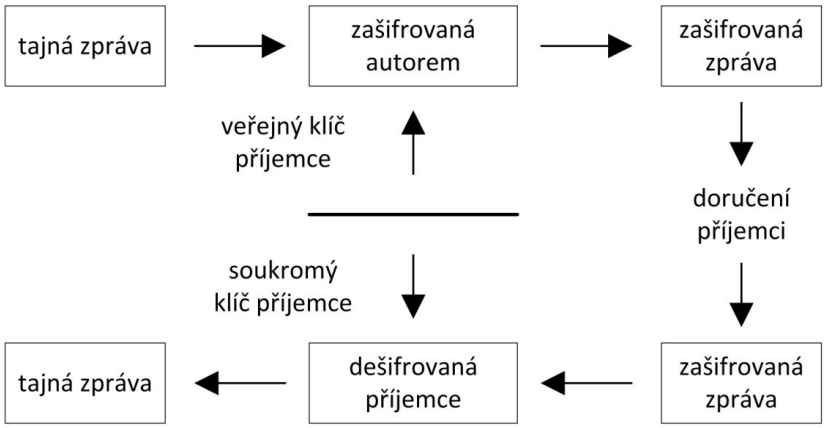
Tento typ šifer postupně šifruje jeden bit za druhým. Využívají se v oblastech, kde by mohlo docházet k větším ztrátám dat. Jelikož zde není datový tok po blocích ale po jednotlivých bitech, jedná se o rychlejší metodu, než u blokových šifer. Nejpoužívanější šifrou je zde **RC4**, která se a využívá pro šifrovaný přenos webových stránek či zabezpečení Wi-Fi. [13] [15]

2.2 Asymetrické šifrování

Způsob šifrování, kde soukromý klíč je doplněn o klíč veřejný. Soukromým klíčem se zašifruje klíč veřejný. Veřejný klíč se poté může bez problémů poslat, protože bez soukromého klíče se nikdo nedozví obsah. Jestliže někdo pošle s daným veřejným klíčem nějaký obsah, tak osoba se soukromým klíčem (u sebe) opět může dešifrovat obsah. Jsou zde tedy dva typy klíčů, jeden veřejný a několik soukromých, ovšem soukromý má každý svůj a veřejný je jeden společný. Uvedený princip je znázorněn na Obr. 3. [11] [16]

Nejčastější algoritmy asymetrického šifrování:

- **RSA** – název vychází ze spojení jmen zakladatelů Rivest, Shamir a Adelman. Tento algoritmus se dnes běžně využívá hlavně při elektronických podpisech. Jeho bezpečnost by měla být dostačující již při délce klíče 1024 bitů, ovšem doporučovaná velikost klíče je 2048 bitů. Jelikož je výpočet velmi náročný, tak je nemožné při takové délce vypočítat soukromý klíč. [16]
- **DSA** – jedná se o algoritmus asymetrického šifrování, který se zaměřuje na použití u digitálních podpisů, ale ne k šifrování dat. [17]



Obr. 3 – Princip asymetrického šifrování [1]

2.3 HASH

Hashovací funkcí můžeme získat tzv. otisk dokumentu. Tento otisk, je kód, který je jedinečný pro dokument, právě ve chvíli, kdy jej uděláme. Pokud bychom v dokumentu změnili jakoukoliv maličkost, například pouze vepsali jeden znak, hash kód by se tak změnil a bylo by poznat, že dokument byl nějak pozměněn. Důležitou vlastností je jednocestnou funkce. Takováto funkce nám tedy zaručuje integritu i při podepisování elektronickým podpisem. Máme různé hashovací funkce, nejpoužívanější v této době je **SHA**. [11] [18]

2.4 Pretty Good Privacy

Na základě asymetrického šifrování vznikla myšlenka PGP. Jde o elektronickou komunikaci založenou na decentralizovaném modelu potvrzování veřejných klíčů. Uživatel může potvrzovat klíče jiným uživatelům a naopak. Každý uživatel si může stáhnout OpenPGP software, který si nainstaluje na své zařízení, následně si vygeneruje svůj soukromý klíč a také veřejný klíč pro ostatní. [18] [19]

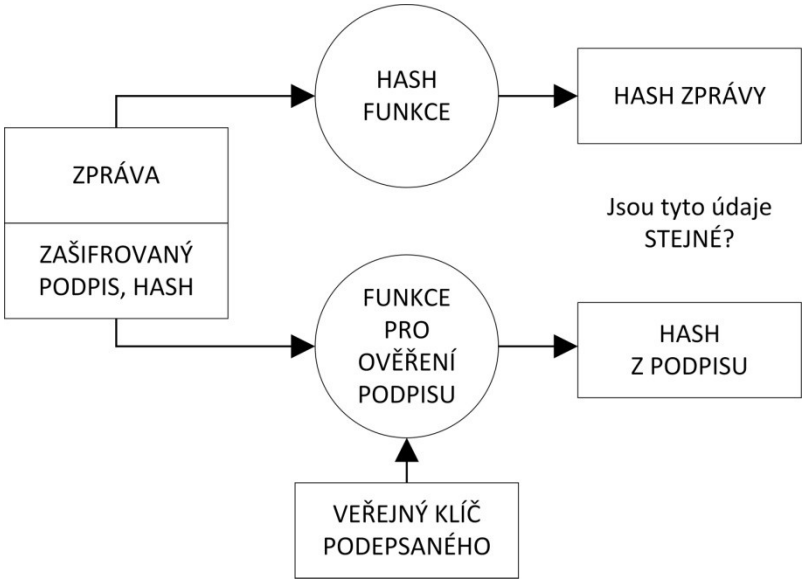
3 ELEKTRONICKÝ PODPIS

Jde o obdobu vlastnoručního podpisu v digitální podobě. Díky použití algoritmů je jeho zfalšování časově i výpočetně velmi náročné. Jeho ověření pravosti je jednodušší než u klasického podpisu. Ověřením tzv. integrity zprávy, tudíž zprávy, která byla digitálně podepsána lze zaručit její neporušenost. Obsah takové zprávy je shodný s obsahem v době jeho podpisu. Tímto má také elektronický podpis vlastnost nepopiratelnosti. Společně se šifrováním lze ověřit podpis až po dešifrování zprávy. Za právně uznatelný elektronický podpis je označován tzv. zaručený elektronický podpis. [4]

Požadavky zaručeného elektronického podpisu jsou:

- jednoznačné spojení s podepisující osobou,
- identifikace podepisující osoby k datové zprávě,
- vytvoření a připojení k datové zprávě prostředky, které má podepisující osoba pod svojí kontrolou,
- možnost zjistit jakoukoli změnu dat ve vztahu k datové zprávě. [4] [18]

Speciálním případem elektronického podpisu je tzv. **digitální podpis**. Samotný elektronický podpis je širší pojem, který zahrnuje i možnosti prokazování identity podepisujícího jako například biometrie člověka či čipové karty. S tímto pojmem pracuje legislativa a Digitální podpis slouží k ověřování dokumentu na bázi šifrování. [4] Schéma ověření pravosti digitálního podpisu lze vidět na Obr. 4.



Obr. 4 – Ověření pravosti digitálního podpisu [1]

3.1 Elektronická značka a pečeť

Elektronickou značkou může označit elektronický dokument jak fyzické, právnické osoby či organizační složky státu. Podnět ke vzniku elektronické značky může dát i program bez účasti člověka. Ten kdo nastavuje daný program, se nazývá označující osobou a nese případné právní důsledky. Označením vyjadřuje subjekt projev vlastní vůle, obdoba podepisování. [2] [20]

Elektronickou pečeť vytváří pouze právnická osoba či organizační složka státu. Opatřením elektronickou pečetí deklaruje právnická osoba původ toho čím je pečeť označeno. Pečetí může subjekt označit pouze něco vlastního, nikoli např. cizí dokument jak je tomu u elektronické značky. [20]

3.2 Certifikáty

Slouží k správě, distribuci a uchování klíčů. Obsahují zejména veřejný klíč a jméno osoby, pro kterou byl certifikát vydán. Dalšími údaji jsou např. datum počátku a ukončení platnosti, certifikační autoritu vydávající certifikát či sériové číslo. Certifikační autorita je důvěryhodný subjekt poskytující certifikační služby. Vystupuje jako třetí strana mezi komunikací dvou subjektů. Vydání certifikátu jednoznačně potvrzuje identifikaci daného subjektu s jeho dvojicí klíčů (elektronickou identitou). [21]

Certifikáty dělíme na osobní a systémové. **Osobní certifikáty** jsou vydávány pouze fyzickým osobám. **Systémové certifikáty** se vydávají jak fyzickým, tak i právnickým osobám či organizačním složkám státu. Systémové certifikáty lze využívat např. pro tvorbu elektronických značek, časových razítek, identifikace serverů. [2]

3.2.1 Třídy certifikátů

Mezinárodní rozdělení, které vyjadřují důvěryhodnost certifikátů, dle anglického označení „Class“.

Class 1 Trial – využití pro testovací účely. Mají omezenou platnost a jsou bez záruky vydavatele za používání. Jsou poskytovány bezplatně. [14]

Class 1 – zpracování informací nízké hodnoty v prostředí s nízkou úrovní rizika. Kontrola pouze existence e-mailové adresy. Nekomerční využití bez poskytnutí záruky. [14]

Class 2 – zpracování informací nízké hodnoty v prostředí se střední úrovní rizika. Porovnání a udělení patřičné úrovně dle poskytnutých identifikačních dokumentů žadatele o certifikát. [14]

Class 3 – zpracování informací střední a vysoké hodnoty v prostředí s nízkou nebo střední úrovní rizika. Osobní ověření identity po předložení potřebných identifikačních dokumentů. Jsou vydávány osobám (Class 3 osobní) i organizacím (Class 3 pro organizace). Použití např. v elektronickém obchodě. [14]

Class 4 – zpracování střední hodnoty v prostředí s vysokou úrovní rizika. Nejvyšší ověření identity. Osobní návštěva a ověření požadovaných dokumentů a jejich dalších vlastností. Nutnost předložení rodného listu. Použití hardwarového zařízení pro uchování příslušných klíčů. [14]

Class 5 – zpracování vysoké hodnoty v prostředí s vysokou úrovní rizika. Identifikační požadavky jsou shodné s třídou Class 4, avšak je nutné použití hardwarového zařízení pro provádění kryptografických operací. [14]

Mimo jiné je možné vytvořit tzv. **Self Signed** certifikát, který není podepsán žádnou certifikační autoritou. U takovéhoto certifikátu se shoduje vydavatel s osobou, pro kterou byl certifikát vydán. [2] [14]

3.2.2 Kvalifikované a komerční certifikáty

Kvalifikované certifikáty jsou přesně vymezené zákonem a slouží především k podepisování a ověření samotných podpisů, značek a razítek. Poskytují nejvyšší možnou důvěru, za kterou se zaručuje autorita vydávající daný certifikát na základě prověření identity pro koho je certifikát vydáván. Za komerční certifikáty mohou být označovány všechny ostatní certifikáty, které nejsou kvalifikovanými. Oproti kvalifikovaným certifikátům se ty komerční využívají např. pro přihlášení, prokazování identity, autentizace uživatele či šifrování. [2]

3.3 Certifikační autority

Za certifikační autoritu se označuje subjekt, který vydává certifikáty. Všechny certifikační autority mohou vydávat komerční certifikáty, avšak pouze kvalifikované certifikační autority mohou vydat kvalifikované certifikáty. Získáním akreditace od státu se kvalifikovaná certifikační autorita označuje i jako tzv. akreditovaná certifikační autorita. Získáním certi-

fikátu od této autority se splňují zákonem stanovené podmínky pro použití uznávaných elektronických podpisů, kterými lze komunikovat s orgány veřejné moci. [2]

Kvalifikované certifikační autority s akreditací v České republice:

- První certifikační autorita, a.s.
- Certifikační autorita PostSignum (Česká pošta s.p.)
- eIdentity

3.4 Časové razítko

Garantuje čas vzniku toho čím je opatřeno. Kvalifikovaná časová razítka vytváří kvalifikovaný poskytovatel certifikačních služeb. Takto vytvořená a poskytovaná razítka mají definovanou úroveň bezpečnosti podmíněnou kvalitami služeb a požadovanou akreditací. Časové razítko není vázáno na osobu nebo vlastníka, ale je spojeno s dokumentem. Definuje jeho vlastnosti a to čas existence. [2] [21]

II. PRAKTICKÁ ČÁST

4 ELEKTRONICKÝ OBČANSKÝ PRŮKAZ

Od 1. 7. 2018 jsou plošně vydávány občanům ČR občanské průkazy se strojově čitelnými údaji a kontaktním elektronickým čipem (dále jen eOP). Již před tímto datem byl občanům dobrovolně vydáván průkaz se starší verzí čipu, kde však identifikace a podpora elektronického podepisování nebyla na úrovni kvalifikovaného prostředku. Pokud chce držitel tohoto průkazu využívat nejnovějších elektronických funkcí, musí požádat o nový občanský průkaz. [22]

Nový čip v eOP umožňuje:

- *Identifikaci vůči online službám zejména veřejné správy*
- *Vytváření kvalifikovaných elektronických podpisů*
- *Autentizaci pomocí certifikátů vůči informačním systémům*

Funkce Identifikace

Občanský průkaz s aktivovanou identifikační funkcí je prostředkem pro elektronickou identifikaci s vysokou úrovní záruky. Je nejvyšší a nejbezpečnější identifikační prostředek, který definuje Nařízení Evropského parlamentu a Rady č. 910/2014 (eIDAS). [22]

Vytváření kvalifikovaných elektronických podpisů

V souladu s nařízení eIDAS je eOP kvalifikovaným prostředkem pro vytváření elektronických podpisů. Dle platné legislativy má kvalifikovaný elektronický podpis stejnou hodnotu jako podpis vlastnoruční. [22]

Autentizace pomocí certifikátů vůči informačním systémům

Do čipu eOP lze nahrávat kvalifikované certifikáty a generovat kryptografické klíče. Pomocí certifikátů a klíčů se lze přihlašovat k vybraným informačním systémům. O vydání certifikátu lze požádat u kvalifikovaného poskytovatele služeb vytvářející důvěru. [22]

4.1 Vydání občanského průkazu

Dle zákona č. 328/1999 Sb., o občanských průkazech je občanský průkaz *„veřejná listina, kterou občan prokazuje své jméno, popřípadě jména, příjmení, podobu a státní občanství České republiky, jakož i další údaje v ní zapsané podle tohoto zákona.“* [23]

„Občanský průkaz je povinen mít občan České republiky, který dosáhl věku 15 let a má trvalý pobyt na území České republiky.“ [23]

„Občan může požádat o vydání občanského průkazu u kteréhokoliv obecního úřadu obce s rozšířenou působností.“ [23]

„Jedná-li se o vydání občanského průkazu se strojově čitelnými údaji a s kontaktním elektronickým čipem, je nutná při podání žádosti osobní přítomnost občana, jemuž bude občanský průkaz vydán, z důvodu pořizování jeho fotografie a podpisu.“ [23]

„Každý, kdo žádá o vydání občanského průkazu, je povinen prokázat svou totožnost.“ [23]

„Občanský průkaz se strojově čitelnými údaji a s kontaktním elektronickým čipem se vyhotoví do 30 dnů ode dne podání žádosti, anebo za správní poplatek ve zkrácené lhůtě, a to v pracovních dnech do 24 hodin, nebo do 5 pracovních dnů.“ [23]

„Občanský průkaz převezme občan u obecního úřadu obce s rozšířenou působností, u kterého byla podána žádost o vydání občanského průkazu.“ [23]

„V případě vydávání občanského průkazu ve zkrácené lhůtě je vydávajícím orgánem Ministerstvo vnitra.“ [23]

„Při převzetí občanského průkazu si občan zadá bezpečnostní osobní kód, který slouží k autentizaci držitele při fyzickém prokázání jeho totožnosti.“ [23]

„Občan může při převzetí občanského průkazu nebo kdykoli poté u kteréhokoliv obecního úřadu obce s rozšířenou působností zadat identifikační osobní kód a deblokační osobní kód pro účely aktivace identifikačního certifikátu.“ [23]

4.2 Legislativa

Důležitými zákony vztahující se k eOP a elektronické identifikaci jsou:

- Zákon č. 328/1999 Sb., o občanských průkazech
- Zákon č. 250/2017 Sb., o elektronické identifikaci
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 111/2009 Sb., o základních registrech
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (zkráceně eIDAS)

Zákon č. 328/1999 Sb., o občanských průkazech

Platnost zákona od 27. 12. 1999, účinnost od 1. 7. 2000.

„Tento zákon upravuje vydávání občanských průkazů státním občanům České republiky, způsob prokazování totožnosti a vedení agendového informačního systému evidence občanských průkazů.“ [23]

Zákon č. 250/2017 Sb., o elektronické identifikaci

Platnost zákona od 18. 8. 2017, účinnost od 1. 7. 2018.

„Tento zákon upravuje v návaznosti na přímo použitelný předpis Evropské unie upravující elektronickou identifikaci využití elektronické identifikace, působnost Ministerstva vnitra a Správy základních registrů na úseku elektronické identifikace a přestupky na úseku elektronické identifikace.“ [24]

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

Platnost zákona od 19. 9. 2016, účinnost od 19. 9. 2016.

„Tento zákon upravuje v návaznosti na přímo použitelný předpis Evropské unie některé postupy poskytovatelů služeb vytvářejících důvěru, některé požadavky na služby vytvářející důvěru, působnost Ministerstva vnitra v oblasti služeb vytvářejících důvěru a sankce za porušení povinností v oblasti služeb vytvářejících důvěru.“ [25]

Zákon č. 111/2009 Sb., o základních registrech

Platnost zákona od 27. 4. 2016, účinnost od 1. 7. 2010.

„Tento zákon vymezuje obsah základních registrů, informačního systému základních registrů a informačního systému územní identifikace a stanoví práva a povinnosti, které souvisejí s jejich vytvářením, užíváním a provozem, zřizuje Správu základních registrů.“ [26]

Nařízení Evropského parlamentu a Rady č. 910/2014 (eIDAS)

Platnost nařízení od 23. 7. 2014, účinnost od 1. 7. 2016.

V souvislosti s účinností bylo v českém právním řádu toto nařízení reflektováno zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Hlavním cílem nařízení je důvěryhodnost a bezpečnost služeb poskytovaných na trhu EU. Vytváří standardy a nástroje pro bezpečné a důvěryhodné poskytování elektronických transakcí a elektronických dokumentů. Reguluje nástroje pro vzájemné uznávání prostředků pro on-

line identifikaci a autentizace. Dílčím cílem je interoperabilita[1], v praxi to představuje přeshraniční uznávání elektronických identit. Vytvořením společných standardů harmonizuje služby vytvářející důvěru (elektronické podpisy, pečetě, časové značky, doručování a autentizace webu). [27] [28]

4.3 Kvalifikovaní poskytovatelé

Kvalifikovaný poskytovatel může být jak úřad, tak i soukromoprávní subjekt, nabízející službu při které je povinností prokázat svou totožnost.

Seznam akreditovaných poskytovatelů v květnu 2019 dle portálu eIdentita.cz:

- *Správa základních registrů*
- *Státní ústav pro kontrolu léčiv*
- *Česká správa sociálního zabezpečení (ČSSZ)*
- *Ministerstvo vnitra České republiky*
- *Generální finanční ředitelství*
- *Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví (OZP)*
- *Město Pelhřimov*
- *Město Říčany* [29]

Zákon č. 250/2017 Sb. o elektronické identifikaci říká, že *„ten, kdo umožňuje prokázání totožnosti, které vyžaduje právní předpis nebo výkon působnosti, s využitím elektronické identifikace (dále jen „kvalifikovaný poskytovatel“), vyrozumí o této skutečnosti správce národního bodu, a to bez zbytečného odkladu poté, co nastala. Kvalifikovaný poskytovatel ve vyrozumění uvede on-line službu nebo jinou činnost, při nichž prokázání totožnosti s využitím elektronické identifikace umožňuje, a úroveň záruky prostředku pro elektronickou identifikaci, kterou při prokázání totožnosti s využitím elektronické identifikace požaduje.“* [24]

U tohoto poskytovatele je možné přihlásit se do on-line služeb pomocí eOP. Ověření totožnosti probíhá vždy přes národní bod pro identifikaci a autentizaci.

---

[1] **Interoperabilita** – schopnost systémů, strojů či zařízení vzájemné spolupráce, porozumění či funkčnosti. Technologie dosahují vzájemné součinnosti (dodržování standardů a kompatibility), tudíž jsou vzájemně interoperabilní. [28]

„Národní bod je informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému. Správcem národního bodu je Správa základních registrů. Samostatná součást národního bodu plní úlohu uzlu podle přímo použitelného předpisu Evropské unie upravujícího rámec interoperability. Správce národního bodu zajistí, aby národní bod splňoval požadavky stanovené přímo použitelným předpisem Evropské unie upravujícím rámec interoperability.“ [24]

Portál národního bodu (eidentita.cz)

Portál národního bodu pro identifikaci a autentizaci představuje nástroj pro prokázání totožnosti uživatele elektronických služeb. Národní bod je zřízen zákonem č. 250/2017 Sb. o elektronické identifikaci. Aktivací elektronických funkcí v eOP vznikne příslušný profil občana v národním bodu. [30]

Občan může po přihlášení pomocí Národní identitní autority (NIA) a ověření totožnosti spravovat své údaje, které mohou být předány kvalifikovaným poskytovatelům. Vždy však jejich výdej je podmíněn souhlasem občana. [30]

Přihlašovací stránku portálu NIA s výběrem možností identifikace je vidět na Obr. 5.

Obr. 5 – Přihlašování pomocí NIA

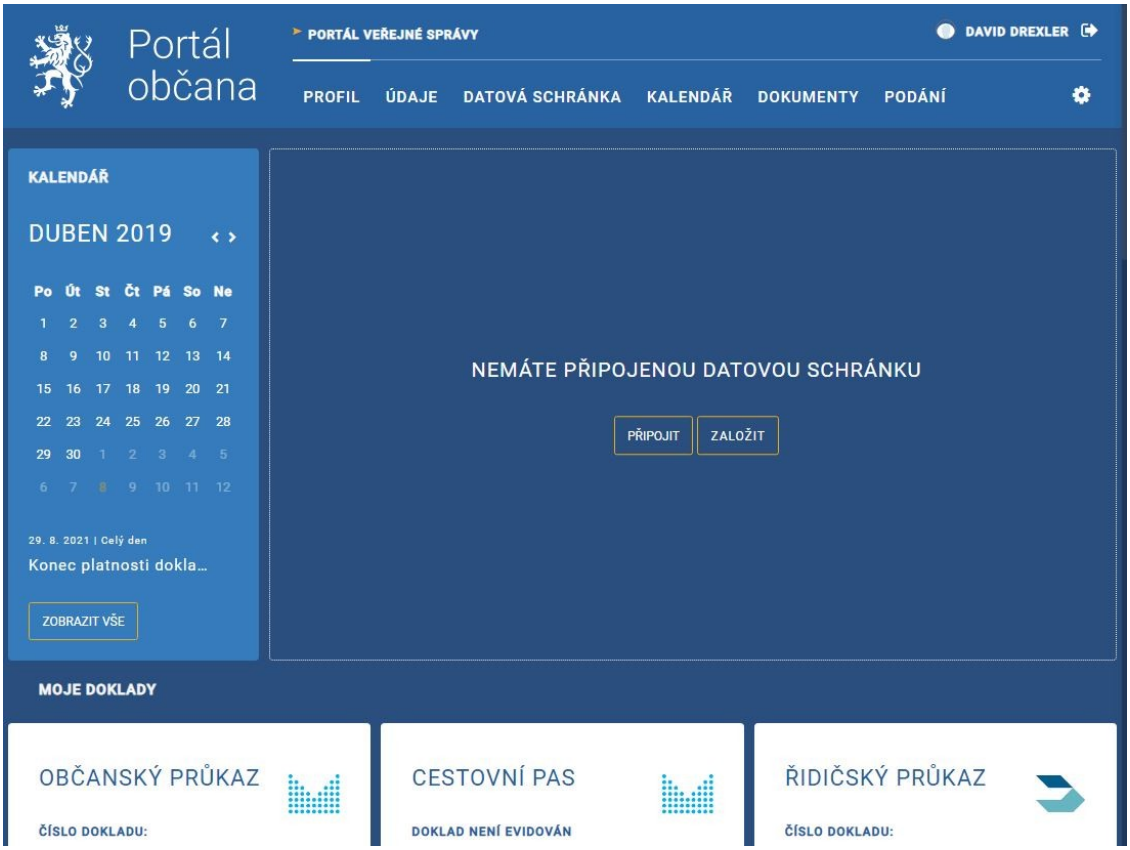
Portál občana (obcan.portal.gov.cz)

Přihlášeným uživatelům umožní přijímat a posílat datové zprávy, spravovat údaje ze základních registrů, prohlížet kalendář s nadcházejícími událostmi, ukládat nebo spravovat doklady a dokumenty či podávat žádosti. [31]

Další dostupné služby v Portálu občana:

- Rychlí přístup k portálům eRecept, ČSSZ, Finanční správy ČR, OZP a portálům občana měst Pelhřimov, Říčany a Chotěboř.
- Twitter kanál Portálu občana - aktuální informace z oficiálního kanálu.
- Náhled do katastru nemovitostí - přehledy čísel listů vlastnictví nemovitostí a jednoduší přístup k informacím o nemovitostech v aplikaci Nahlížení do Katastru nemovitostí.
- Výstup ze živnostenského rejstříku - seznam podnikatelských subjektů žadatele, potvrzení o neexistenci zápisu, výpis subjektu obsahující údaje z veřejné i neveřejné části živnostenského rejstříku.
- Elektronické podání ve formátu Jednotného registračního formuláře.
- Zobrazení dat z Centrálního registru řidičů ČR - aktuální data o řidičském oprávnění občana, průkazu či průkazu o profesní způsobilosti. Zobrazení poslední změny a stavu bodového konta.

Webové rozhraní a úvodní stránka po přihlášení do Portálu občana je vidět na Obr. 6.



Obr. 6 – Úvodní stránka Portálu občana po přihlášení

Portál eRecept (pacient.erecept.sukl.cz)

Umožňuje přístup pacientů, lékařům a zdravotním pojišťovnám k elektronickým receptům. Vytváří statistické přehledy pro Ministerstvo zdravotnictví a Policii České republiky. [32]

ePortál ČSSZ (eportal.cssz.cz)

Pojištěncům nabízí nahlížení na údaje evidované v databázi ČSSZ, odesílání online žádostí či elektronické vyplnění a podání tiskopisů. Formou internetové služby nabízí přístup ke službám 24 hodin denně. [33]

Elektronické služby finanční správy ČR (adisepo.mfcr.cz)

Portál slouží ke komunikaci s finanční správou a získání informací z daňového řízení. [29]

Přihlášení pomocí NIA je určena pouze pro fyzické osoby. Údaje získané přihlášením pomocí eOP je možné využít k načtení vybraných položek ve formuláři pro odeslání aplikací EPO. [34]

Informační systém datových schránek (mojedatovaschranka.cz)

Datové schránky slouží ke komunikaci s orgány veřejné moci a to zasílat a přijímat elektronickou poštu a dokumenty. [29]

Vitakarta – portál OZP (ozp.cz)

Umožňuje se přihlásit k online portálu VITAKARTY a využívat elektronických služeb nabízený klientům Oborové zdravotní pojišťovny zaměstnanců bank, pojišťoven a stavebnictví. [35]

Portál občana města Pelhřimov (obcan.mupe.cz), **Portál občana města Říčany** (obcan.ricany.cz), **Portál občana města Chotěboř** (portal.chotebor.cz/portal)

Portál občana města Pelhřimov, Říčany a Chotěboř umožňují přihlášení za pomocí eOP s cílem on-line komunikace s příslušným městským úřadem. Pro přihlášené uživatele je možno vyřizovat jednotlivé agendy přes internet a využívat možností např. předvyplnění elektronický formulářů, zjištění stavu plateb místních poplatků či průběh právě vyřizovaných žádostí. I nepřihlášenému návštěvníkovy portálu jsou poskytovány nejrůznější informace týkající se dané obce. [36] [37] [38]

5 KÓDY PRO OCHRANU OBČANSKÉHO PRŮKAZU

S aktivováním čipu v eOP je spojeno několik číselných kódů, které slouží pro ochranu elektronických funkcí občanského průkazu. [39]

- **Deblokační osobní kód (DOK)**
- **Identifikační osobní kód (IOK)**
- **Personal Identification Number (PIN)**
- **PIN Unblocking Key (PUK)**
- **PIN pro kvalifikované elektornické podpisy (QPIN)**

Tab. 1 uvádí hlavní funkce a využití těchto kódů.

Tab. 1 – Funkce a využití kódů eOP

Kód	**Funkce**	**Využití**
DOK	Odblokování IOK	Zřídka
IOK	Schvalování elektronické identifikace a prvotní nastavení PUK	Každá identifikační operace
PIN	Schvalování operací s kryptografickými klíči a certifikáty (vytváření klíčů, autentizace atd.)	Správa certifikátů či přihlášení certifikátem
PUK	Nastavení či odblokování PIN a QPIN	Zřídka
QPIN	Schvalování kvalifikovaného elektronického podpisu	Vytváření kvalifikovaného elektronického podpisu

Dalším číselným kódem je **bezpečností osobní kód (BOK)**, který však není přímo spjatý s elektronickým čipem občanského průkazu. Slouží zejména při osobním prokazování totožnosti. Zvolení jeho hodnoty je povinností při převzetí, i když si občan neaktivuje elektronické funkce občanského průkazu. Používá se zřídka v případě, kdy jsou pochybnosti při shodě podoby držitele s průkazovou fotografií. [39]

Občan může odmítnout zadání hodnot DOK a IOK při převzetí občanského průkazu v případě, že nechce aktivovat jeho elektronické funkce. PUK, PIN a QPIN slouží pro funkce elektronického podepisování, a proto pokud jej držitel eOP nechce používat, nemusí je nastavovat. [39]

5.1 Ochrana kódů

Zejména z bezpečnostních důvodů je pro každý kód nastaveno omezení počtu chybných hodnot a minimální délka (počet číslic), který daný kód musí obsahovat. [39] V Tab. 2 jsou uvedeny počty chybných zadání do zablokování a rozsah délek jednotlivých kódů.

Tab. 2 – Omezení přístupových kódů

Kód	Počet chybných pokusů	Délka (min/max)
DOK	10	4 – 10
IOK	3	4 – 10
PUK	5	8 – 15
PIN	3	5 – 15
QPIN	3	5 – 15
BOK	3	4 – 10

Všechny kódy jsou tzv. osobní, a tudíž žádný z nich nesmí občan nikomu sdělovat. Pokud dojde k prozrazení kódu je nutné, změnit jeho hodnotu (pomocí originálního softwaru) nebo zablokovat identifikační funkci eOP prostřednictvím Správy základních registrů. Po zablokování nelze dále využívat ani znovu aktivovat elektronické funkce a je nutné zažádat o nový občanský průkaz. Všechny kódy kromě BOK lze kdykoliv změnit po přihlášení v příslušné obslužné aplikaci na PC. [39] Přehled kde a jak lze prvotně nastavit či odblokovat jednotlivé kódy je uveden v Tab. 3.

Tab. 3 – Nastavení a odblokování přístupových kódů

Kód	Prvotní nastavení	Odblokování
DOK	Úřad spolu s IOK	Úřad spolu s IOK
IOK	Úřad spolu s DOK	Úřad spolu s DOK nebo PC po zadání DOK
PUK	PC po zadání IOK	Nelze
PIN	PC po zadání PUK	PC po zadání PUK
QPIN	PC po zadání PUK	PC po zadání PUK
BOK	Úřad	Úřad

5.2 Hlediska členění přístupových kódů

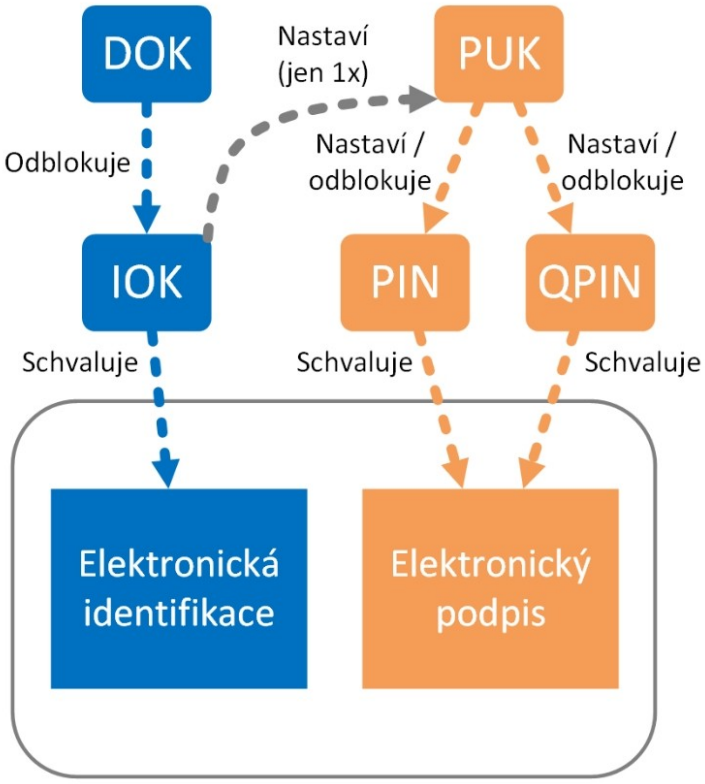
Z jednoho hlediska lze rozdělit kódy pro:

- **schvalování operací** *(IOK, PIN, QPIN)* – používány při běžných úkonech a práci s elektronickými funkcemi občanského průkazu.
- **odblokování nebo nastavení jiných kódů** *(DOK, PUK)* – nutné k odblokování některých schvalovacích kódů, když opakovaně zadáváme nesprávné hodnoty. [39]

Z dalšího hlediska lze kódy dělit dle funkce:

- **elektronické identifikace** *(DOK, IOK)*
- **elektronického podpisu** *(PUK, PIN, QPIN*) - pro aktivování funkcí elektronického podpisu je nutné nejdříve aktivovat identifikační funkci, nastavením IOK. [39]

Hierarchii a členění přístupových kódů ilustruje Obr. 7.



Obr. 7 – Hierarchie a členění přístupových kódů [39]

6 ČTEČKY KARET

Pro práci s elektronickými funkcemi občanského průkazu je nezbytné připojení čtecího zařízení, do nějž je občanský průkaz vložen. Čtečka karet může být součástí zařízení (klávesnice, vlastní slot) či jako externí hardware. [40] [41]

K zajištění vyšší bezpečnosti se doporučuje použít čtečku s integrovanou klávesnicí. Nehrozí tak odcizení zadávaných hodnot kódů prostřednictvím PC. [42]

Nevýhodou čteček s integrovanou klávesnicí je obvykle vyšší pořizovací cena oproti čtečkám bez klávesnice. Čtečky s displejem mohou také špatně zobrazovat názvy zadávaných kódů, proto se doporučuje řídit pokyny, které zobrazuje aplikace v PC. Je také doporučeno dbát při výběru čtečky s klávesnicí na zajištění třídy Class 2 **Secure PIN Entry (SPE)**, která by měla být uvedena v technických specifikacích dané čtečky. [40]

6.1 Čtečky karet pro připojení k PC

Doporučené parametry čtečky čipových karet:

- Soulad s normou ISO 7816
- CCID (Chip Card Interface Device)
- Zajištění kompatibility s operačním systémem připojeného zařízení
- Podpora PC/SC
- Microsoft Windows Hardware Quality Labs (WHQL)
- Podpora Plug and Play (automatická instalace ovladačů) [40]

Funkčnost čtečky lze jednoduše otestovat pomocí obslužných aplikací eObčanka identifikace či Správce karty. Pakliže některá z aplikací nekomunikuje s čtečkou karet, ohlásí tuto skutečnost uživateli. [40]

Další možností jak ověřit funkčnost čtečky je použít příkaz spuštěný z příkazové řádky operačního systému. [40]

- **MS Windows** – *certutil -scinfo*
- **Linux** – *pcsc_scan* (součást balíčku *pcsc-tools*)
- **macOS** – *pcstest* [40]

Server Živě.cz testoval, které čtečky čipových karet spolehlivě fungují s eOP na operačních systémech Windows 7 a 10.

Testováním redakce Živе.cz prošli tato zařízení:

- *Gemalto Safe Net Reader CT1100*
- *Gemalto IDBridge CT710*
- *USB Contact Smart Chip Card*
- *+ID*
- *Cherry TC 1100*

V Tab. 4 jsou uvedeny jednotlivé čtečky, jejich cena a výhody a nevýhody.

Tab. 4 – Ověřené čtečky čipových karet pro PC dle serveru Živě.cz

Název	**Cena**	**Výhody**	**Nevýhody**
Gemalto SafeNet Reader CT1100	2104 Kč	• bezdrátové použití • kompaktní rozměry a nízká hmotnost • možnost použití s kabelem	• vysoká cena • nutnost nabíjení • pomalejší
Gemalto IDBridge CT710	956 Kč	• vestavěná klávesnice • hardwarové provedení	• vyšší cena • nutnost ruční instalace ovladačů na Windows 10
USB Contact Smart Chip Card	160 Kč	• nízká cena • velikost • poddajný kabel	• potenciální bezpečnostní riziko (neověřený zdroj nákupu)
+ID	490 Kč	• malé rozměry a nízká hmotnost • zajímavý design	• obavy z fyzické výdrže čtečky • nejasnost v zasunutí průkazu • vyšší cena z důvodu designu
Cherry TC 1100	359 Kč	• funkčnost jinak žádné	• poněkud vyšší cena z důvodu jednoúčelovosti čtečky

Vůbec nejdražší čtečkou v testu byla Gemalto SafeNet Reader CT1100 viz. Obr. 8. Za cenu 2104 Kč, však nabízí i Bluetooth k spárování čtečky s mobilním zařízením. Druhou nejdražší čtečku od stejného výrobce Gemalto IDBridge CT710 viz. Obr. 9 si může zákazník koupit za cenu 956 Kč. Čtečka nabídne vestavěnou klávesnici s displejem pro vyšší bezpečnost. Čtečka s označením USB Contact Smart Chip Card viz. Obr. 10 byla zakoupena za velmi nízkou cenu 160 Kč ze zahraničního webu eBay.com z neověřeného zdroje.

Testeři se však shodli, že riziko bezpečnosti u této čtečky je přijatelné. Dalším zařízením byla čtečky s označením +ID viz. Obr. 11, která vyniká svým designem a malými rozměry. Posledním zařízením v testu byla čtečka Cherry TC 1100 viz. Obr. 12. Čtečka ničím nevyniká ani nezaostává oproti ostatním, redaktoři však usoudili, že za cenu kolem 350 Kč je cena poněkud vyšší s ohledem na jednoúčelovost zařízení.

Obr. 8 – Gemalto Safe Net Reader CT1100 [43]

Obr. 9 – Gemalto IDBridge CT710 [43]

Obr. 10 – USB Contact Smart Chip Card [43]

Obr. 11 – +ID [43]

Obr. 12 – Cherry TC 1100 [43]

6.2 Čtečky karet pro připojení k mobilnímu zařízení

Každá čtečka se k mobilnímu zařízení připojuje přes Bluetooth. Pro první identifikaci je potřeba čtečku spárovat s mobilním zařízením. Pro párování není nutné instalovat do mo-

bilního zařízení další software ani párovat čtečku v operačním systému. Vždy je nutné mít nainstalovanou mobilní aplikaci eObčanka, kterou lze získat v oficiálních obchodech pro Android a iOS. Přes tuto aplikaci probíhá následné párování. [41]

Podmínky pro mobilní zařízení:

- kompatibilní verze operačního systému
- mobilní aplikace eObčanka nainstalovaná v zařízení
- zapnuté Bluetooth [44]

Podmínky pro čtečku karet:

- kompatibilní čtečka karet
- zapnuté Bluetooth
- vzdálenost mezi čtečkou a mobilním zařízením nepřesahující 10 metrů [44]

Pro práci s eOP a mobilní aplikací jsou podporovány pouze tři čtečky.

Kompatibilní čtečky s mobilní aplikací:

- *ACS ACR 3901 U-S1*
- *Feitian bR301 BLE – c45 /černá varianta/*
- *Gemalto Safe Net Reader CT1100*

Tab. 5 uvádí cenu, dostupnost v ČR a kompatibilitu s operačním systémem podporovaných čteček mobilních zařízení.

Tab. 5 – Cena, dostupnost v ČR a kompatibilita podporovaných čteček

Název	**Cena**	**Dostupnost v ČR**	**Kompatibilita**
ACS ACR 3901 U-S1	cca 1300 Kč	Ano - omezeně	• Android 4.3 a vyšší • iOS 5.0 a vyšší
Feitian bR301 BLE – c45 /černá varianta/	$85	Ne	• Android • iOS
Gemalto SafeNet Reader CT1100	cca 2100 Kč	Ano - omezeně	• iOS

Čtečka ACS ACR 3901 U-S1 viz. Obr. 13 podporuje obě mobilní platformy, avšak na českém trhu je její dostupnost omezená. Prodejci jí nabízí v cenové hladině okolo 1300 Kč. Další čtečkou podporující jak Android i iOS je Feitian bR301 BLE – c45 /černá varianta/

viz. Obr. 14. Výrobce pod stejným označením (bR301 BLE) nabízí dvě čtečky, podporována je pouze čtečka s bluetooth low energy (černá varianta). Zařízení není dostupné v ČR, na oficiálních stránkách výrobce se prodává za cenu 85 amerických dolarů. Poslední podporovanou čtečkou je již zmiňovaná SafeNet Reader CT1100 viz. Obr. 8, u které však chybí kompatibilita s operačním systémem Android. Na webu info.eidentita.cz je také avizováno, že výrobce oznámil ukončení distribuce ke konci roku 2018. [41] [45] [46]

Obr. 13 – ACS ACR 3901 U-S1 [41]

Obr. 14 – Feitian bR301 BLE – c45 [41]

7 PODPŮRNÉ APLIKACE

Pro práci s elektronickým průkazem a využívání jeho funkcí je nutné do zařízení stáhnout a nainstalovat obslužnou aplikaci eObčanka. Aplikace je dostupná pro PC a pro mobilní zařízení. [47]

7.1 Aplikace pro PC

Pro práci s občanským průkazem na PC je nutné připojit zařízení k internetu, nainstalovat obslužné aplikace eObčanka a připojit čtečku čipových karet s nainstalovanými ovladači. Instalační balíček lze stahovat na portálu info.eidentita.cz v sekci „Ke stažení“. Instalaci v PC lze provést pouze pod oprávněním správce operačního systému. [48] [44]

Aplikace eObčanka je dostupná pro tyto platformy a verze operačních systémů:

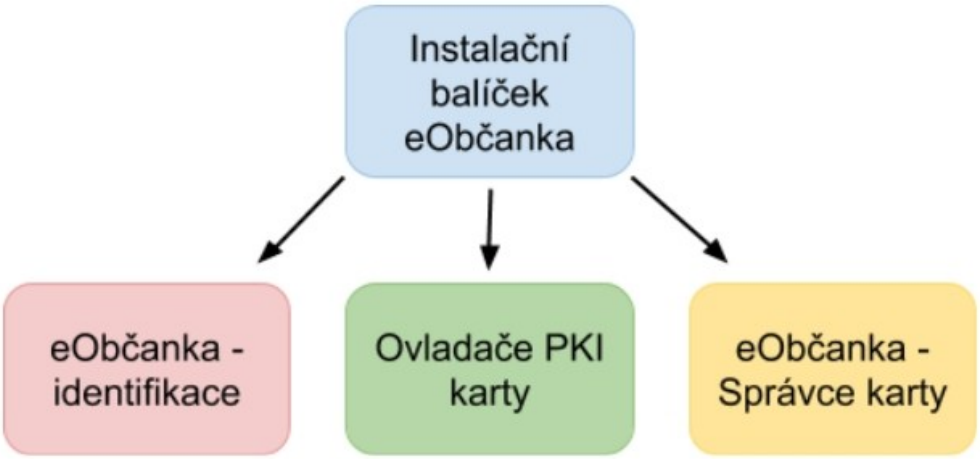
- MS Windows 7 a vyšší
- MS Windows Server 2008 R2 až MS Windows Server 2016
- Ubuntu Linux 17.10
- Ubuntu Linux 18.04 LTS
- OS X 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave [48] [49]

Před instalací by si měl uživatel ověřit, zda pochází software z důvěryhodného zdroje, že neobsahuje škodlivý software a používá originální aplikaci. To lze ověřit pomocí elektronického podpisu (otisku - hashe) instalačního balíčku. Toto ověření provádí operační systémy MS Windows a macOS před instalací automaticky. Operační systém Linux však toto ověření neprovádí. Proto další možností je porovnání otisku instalačního balíčku s hodnotou otisku na oficiálních stránkách pro stažení instalačních balíčků. [50]

Do zařízení se po instalaci instalačního balíčku uloží kompletní softwarová podpora:

- eObčanka – identifikace
- Ovladače čipové karty pro práci s certifikáty
- eObčanka – Správce karty [48]

Ilustrační schéma instalovaných jednotlivých komponent aplikace lze vidět na Obr. 15.



Obr. 15 – Instalované komponenty aplikace eObčanka [48]

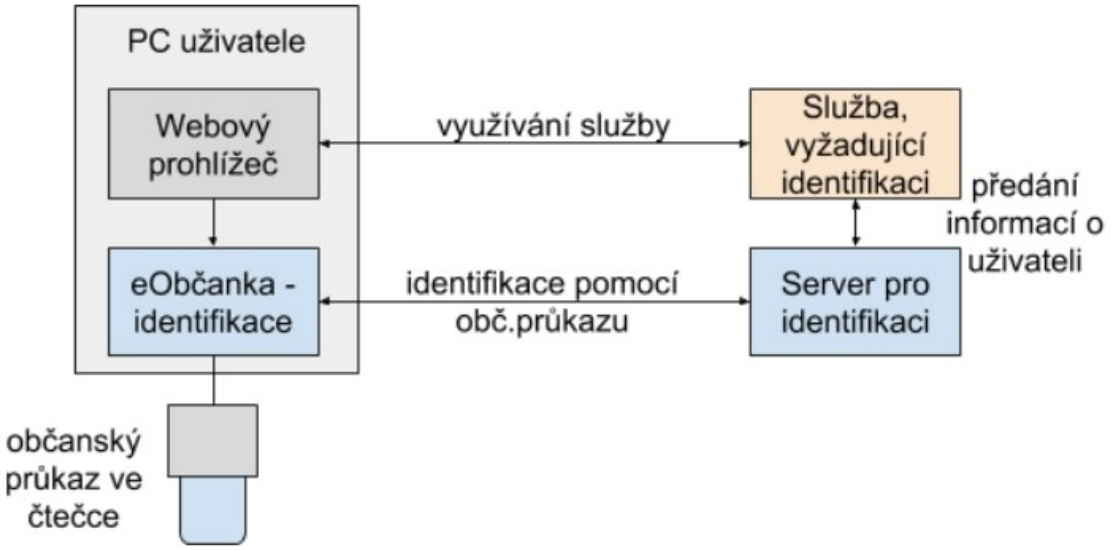
7.1.1 eObčanka – identifikace

Umožňuje zpřístupnit uživateli identifikační funkce eOP pro vzdálenou identifikaci k online službám. Aplikace zajišťuje interakci s uživatelem a zprostředkovává komunikaci mezi serverem a elektronickým čipem průkazu. [51]

Zjednodušený proces identifikace uživatele:

- Uživatel chce využít služeb vyžadující identifikaci. Provozovatel této služby požaduje prokázání uživatelovi totožnosti.
- Před zahájením identifikace uživatel nainstaluje do svého zařízení obslužnou aplikaci pro elektronickou identifikaci.
- Pomocí webového prohlížeče se uživatel připojí k webovým stránkám poskytovatele služby. Webová stránka osahuje možnost přihlášení pro ověření totožnosti uživatele. Uživatel je přesměrován na portál eidentita.cz. Uživatel si zvolí možnost identifikace pomocí eOP.
- Webová stránka spustí aplikaci eObčanka – identifikace.
- Uživatel je vyzván k vložení eOP do čtečky. Zadáním správného IOK schválí držitel použití průkazu pro identifikaci.
- K ověření totožnosti aplikace komunikuje s národním bodem pro identifikaci a autentizaci. V případě úspěšného ověření totožnosti vyzve portál uživatele k udělení souhlasu s odesláním údajů poskytovateli služby, kterou uživatel požaduje. Souhlasem se informace odešlou poskytovateli, který poskytne požadovanou službu uživateli. [52]

Výše popsaný proces lze znázornit pomocí schématu na Obr. 16.



Obr. 16 – Proces elektronické identifikace pomocí eOP [52]

Aplikace umožňuje v případě problémů využít pokročilého mechanismu diagnostiky prostředí, která vyhledá a nabídne řešení daného problému. Spuštěním diagnostického režimu začne aplikace automaticky provádět kontrolu, ve které se zaměřuje na tři hlavní oblasti:

- Aplikace a operační systém – kontrola verze OS a aplikace.
- Čtečka karet a čip občanského průkazu – kontrola čtečky, ovladačů a dostupnosti eOP.
- Dostupnost internetu a serveru pro identifikaci – kontrola internetového připojení a připojení k serveru. [52]

Jestliže je zjištěna v některé oblasti diagnostiky chyba, zobrazí se uživateli popis chyby a návod jak problém odstranit. Některé problémy však dokáže vyřešit aplikace automaticky a nepotřebuje součinnost uživatele. [52]

7.1.2 eObčanka – Správce karty

Aplikace umožňuje např.:

- zobrazení informací o certifikátech v čipu,
- zobrazení kryptografických klíčů v čipu,
- import nebo smazání certifikátu,
- nastavení, odblokování či změna přístupových kódů,
- diagnostiku. [53]

Aplikace se po spuštění snaží vyčíst prostřednictvím připojené čtečky dostupné informace uložené na čipu eOP. Tento průběh lze přerušit a kdykoli opakovat. Po načtení se zobrazí uživateli stromová struktura s informacemi. Tyto objekty jsou reprezentovány příslušným symbolem a textem:

- Čtečka – název čtečky.
- Karta – číslo dokladu.
- Přístupový kód – název kódu.
- Kryptografický klíč – identifikátor klíče.
- Certifikát – jméno držitele certifikátu. [53]

7.1.3 Ovladače pro podporu práce s certifikáty

Většina operací prováděných ovladači probíhá na pozadí. Pro integraci čteček do operačního systému se dodržují technické standardy. Dodržením těchto standardů aplikacemi třetích stran lze eOP využívat v běžně používaných aplikacích pro kryptografické operace. [54] [55]

Standardy:

- **CryptoAPI** – využití kryptografického rozhraní v MS Windows.
- **PKCS#11** – použití u aplikací využívající vlastní kryptografii. Podpora platforem MS Windows, Linux a macOS.
- **tokenID** – použití u nativních aplikací macOS. [54]

Ovladače pro standardy CryptoAPI a tokenID se nemusí konfigurovat. Použití PKCS#11 je však nutné nakonfigurovat pro příslušné aplikace třetích stran. [55]

Funkce ovladačů:

- Použití certifikátů – elektronické podepisování a přihlašování do webových stránek.
- Správa certifikátů – čtení informací o certifikátech, vytváření, zápis či mazání certifikátů a kryptografických klíčů.
- Práce s přístupovými kódy – kontrola či změna hodnot, zablokování kódu, zobrazení okna pro zadání kódu atd. [54] [55]

7.2 Aplikace pro mobilní zařízení

Mobilní aplikace eObčanka umožňuje pouze elektronickou identifikaci a autentizaci pomocí mobilního zařízení. Pro účely podepisování je vytvořeno mobilní SDK (Software

Development Kit), které je určeno pro aplikace třetích stran. Podpisové SKD umožňuje zabezpečit přístup k podpisovým funkcím eOP. Ministerstvo vnitra na speciálních stránkách githubu poskytuje veškerou dokumentaci a SDK ke stažení. [56]

Pro využití elektronické identifikace je nutné pro mobilní zařízení zajistit:

- připojení k internetu (wi-fi, datové připojení),
- instalaci mobilní aplikace eObčanka,
- spárování aplikace s Bluetooth čtečkou čipových karet. [57]

Aplikace eObčanka je dostupná pro tyto platformy a verze mobilních operačních systémů:

- Android 4.4.4 a vyšší
- iOS 10.0 a vyšší [58]

Aplikaci pro platformu Android lze stáhnout z oficiálního obchodu Google Play. Příslušná aplikace pro zařízení s iOS je dostupná v App Store. Stažení a instalace u obou platforem probíhá standardním způsobem. Je doporučováno aplikaci ihned po instalaci vyzkoušet. Při prvním spuštění se zobrazí průvodce, který seznámí uživatele s funkcemi aplikace. Průvodce lze přeskočit. Po skončení průvodce je aplikace připravena na připojení čtečky a provedení identifikace. [57]

Z bezpečnostního hlediska provádí mobilní aplikace kontrolu na „root“ (Android) a „jailbreak“ (iOS). Pakliže aplikace zjistí, že nesplňuje mobilní zařízení požadavky na bezpečný běh, dojde k zamezení autentizace. [58]

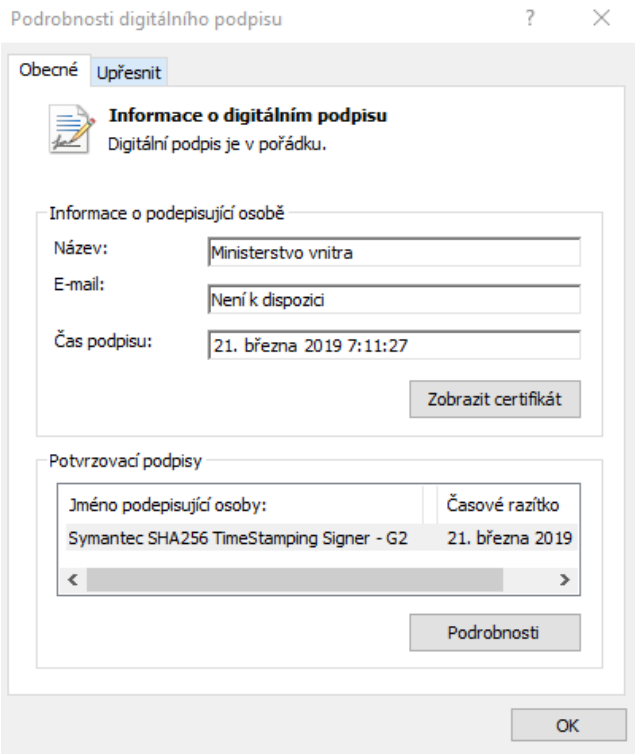
8 ANALÝZA PODPŮRNÝCH APLIKACÍ

Analýza podpůrných aplikací, ověření identifikačních funkcí, porovnání PC a mobilní verze aplikace proběhlo na platformě Windows 10 a Android 8.1. K testování funkčnosti byla použita čtečka čipových karet ACS ACR 3901 U-S1 a eOP s novým čipem vydaný po 1. 7. 2018 s aktivovanou identifikační funkcí.

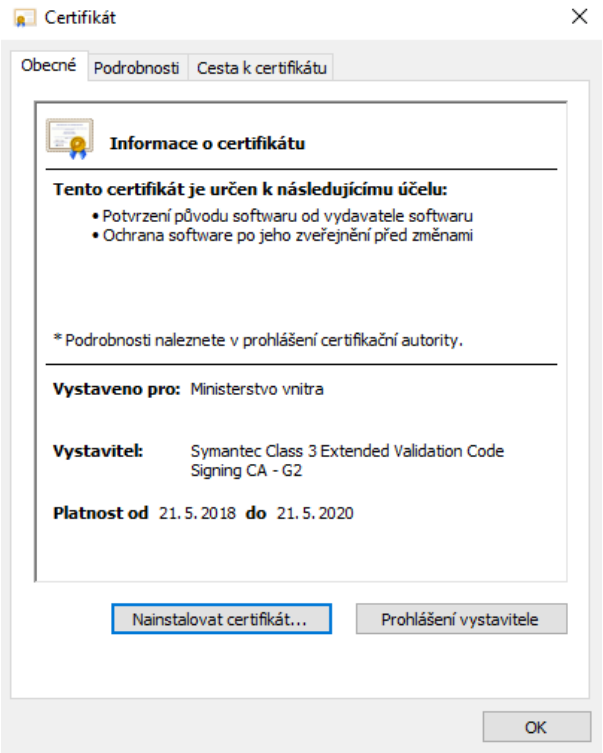
8.1 Aplikace eObčanka na MS Windows

Prvním krokem je stažení aktuální verze v současnosti s označením 3.1.1.19123 softwaru eObčanka pro MS Windows. Z oficiálních stránek ke stažení byla vybrána aplikace v 64 bitové verzi dle typu operačního systému. Instalační soubor o velikosti 16,2 MB má po stažení do příslušné složky název *eObcanka_x64.exe*. Po spuštění souboru pod opraveným správce systém Windows automaticky provedl ověření původu instalačního balíčku. Software musí být elektronicky podepsán Ministerstvem vnitra na základě důvěryhodného certifikátu. Systém automaticky vyrozuměl o této skutečnosti příslušným dialogem.

Zda je soubor podepsán lze zjistit i zobrazením vlastností souboru a na kartě Digitální podpis. V seznamu podpisů ověřit podrobnosti o digitálním podpisu. Na Obr. 17 jsou vidět informace o digitálním podpisu. Zde je vše v pořádku. Podepisující osobou je Ministerstvo vnitra a podpis je opatřen platným certifikátem s časovým razítkem od společnosti Symantec. Podrobnosti o certifikátu lze vidět na Obr. 18.



Obr. 17 – Podrobnosti digitálního podpisu instalačního balíčku eObčanka



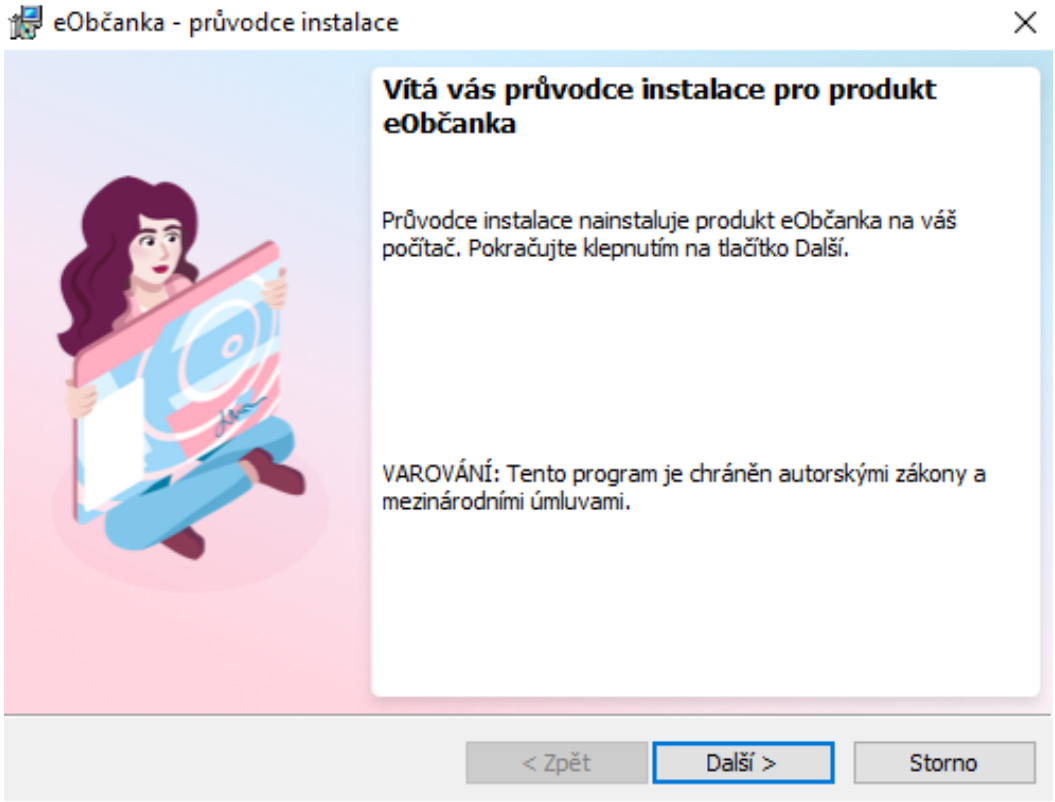
Obr. 18 – Certifikát instalačního balíčku eObčanka

K ověření integrity instalačního balíčku je možné porovnat HASH souboru s hodnotou uvedenou na oficiálních stránkách ke stažení. Hodnotu otisku pomocí algoritmu SHA-1 či SHA-256 vypočítáme v našem případě zadáním příkazu do příkazového řádku následovně:

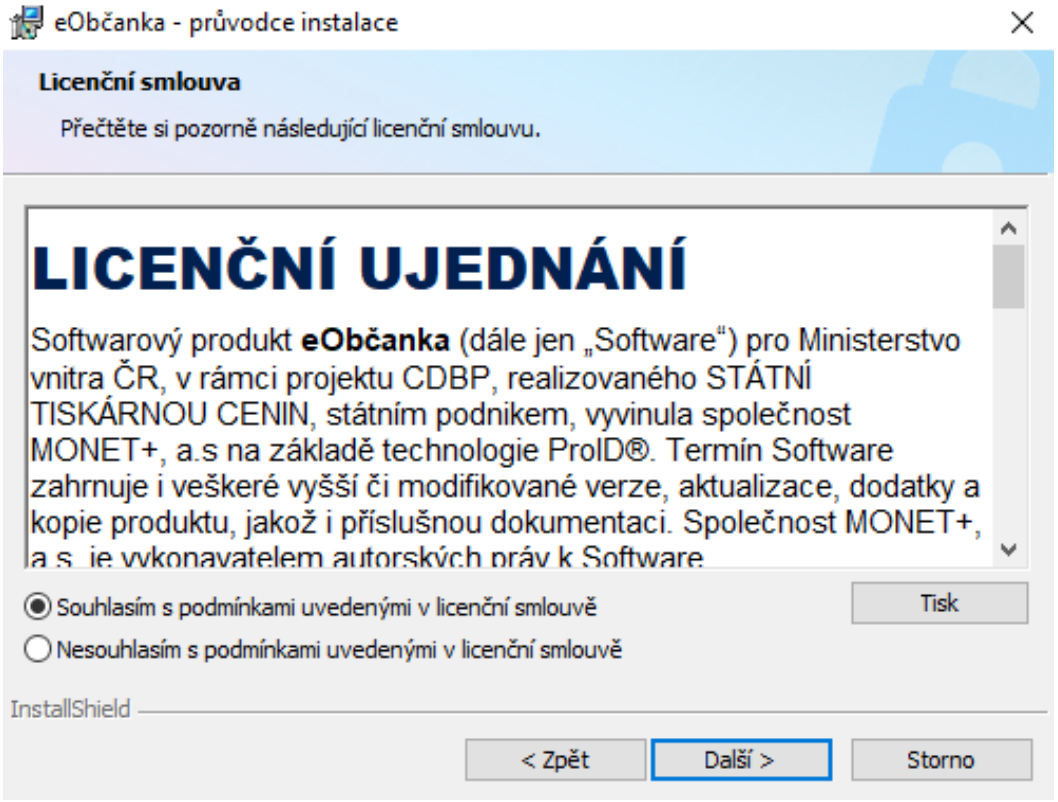
- *certutil -hashfile C:\Users\David\Downloads\eObcanka_x64.exe SHA1*
- *certutil -hashfile C:\Users\David\Downloads\eObcanka_x64.exe SHA256*

Vypočítané hodnoty otisků u obou algoritmů jsou shodné s uvedenými hodnotami na oficiálních stránkách ke stažení.

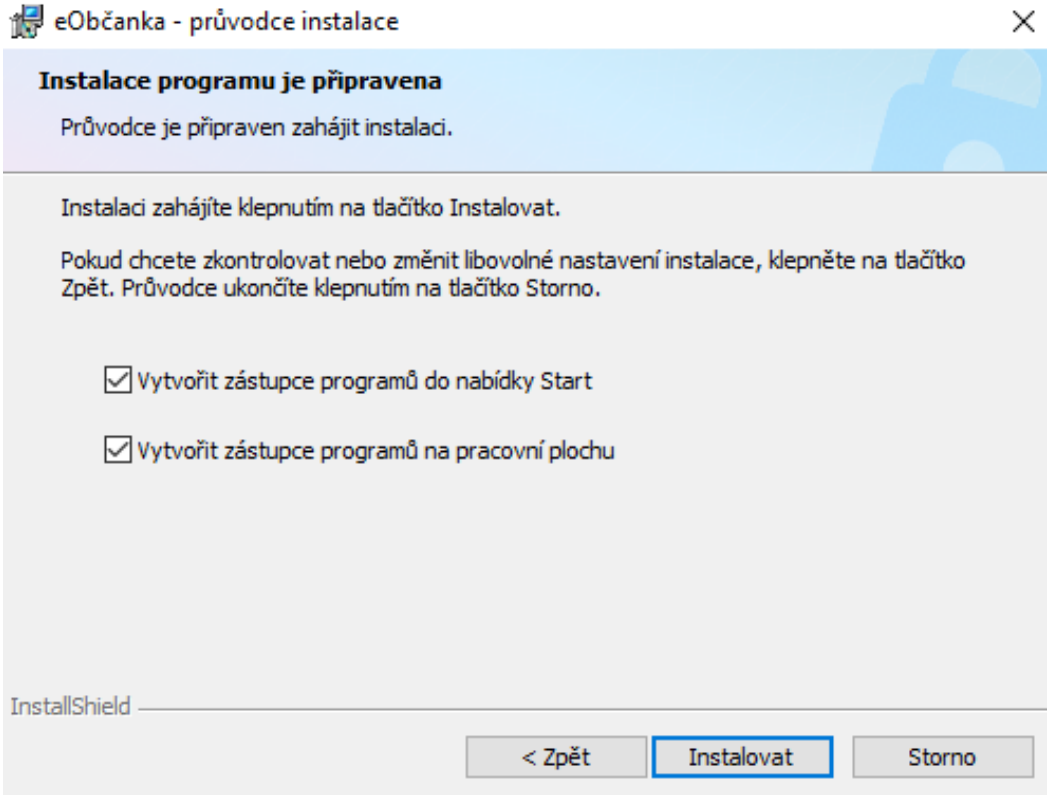
Po ověření původu instalačního balíčku lze přistoupit k samotné instalaci aplikace eObčanka. Spustí se průvodce instalace produktu eObčanka viz. Obr. 19. Jednoduchý průvodce provedl celou instalací počínaje nutností odsouhlasení licenčních ujednání k softwaru viz. Obr. 20, volbou zda se mají vytvořit zástupci programů v nabídce Start a na pracovní ploše jak je vidět na Obr. 21. Průvodce po kliknutí na tlačítko Instalovat automaticky nainstaluje bez výběru umístění jednotlivé součásti balíčku. Průběh instalace lze vidět na Obr. 22.



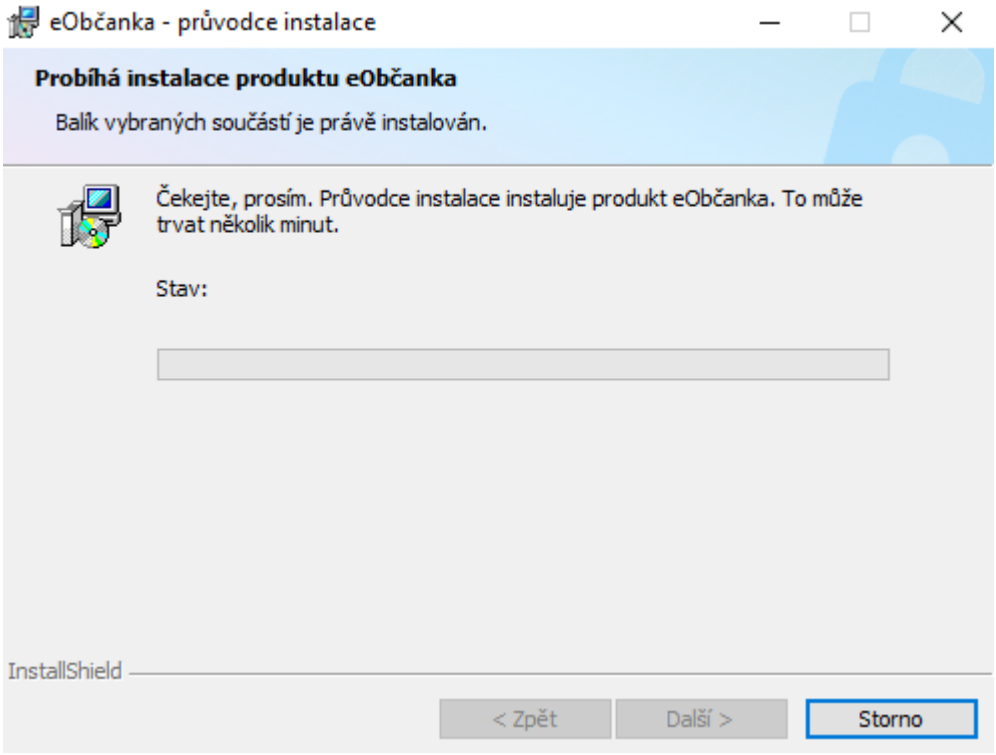
Obr. 19 – Průvodce instalace eObčanka



Obr. 20 – Licenční ujednání aplikace eObčanka

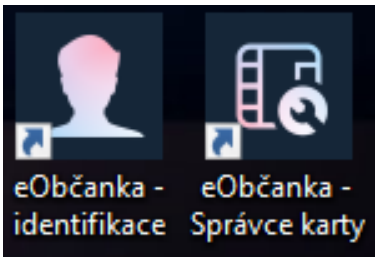


Obr. 21 – Vytvoření zástupců aplikace eObčanka

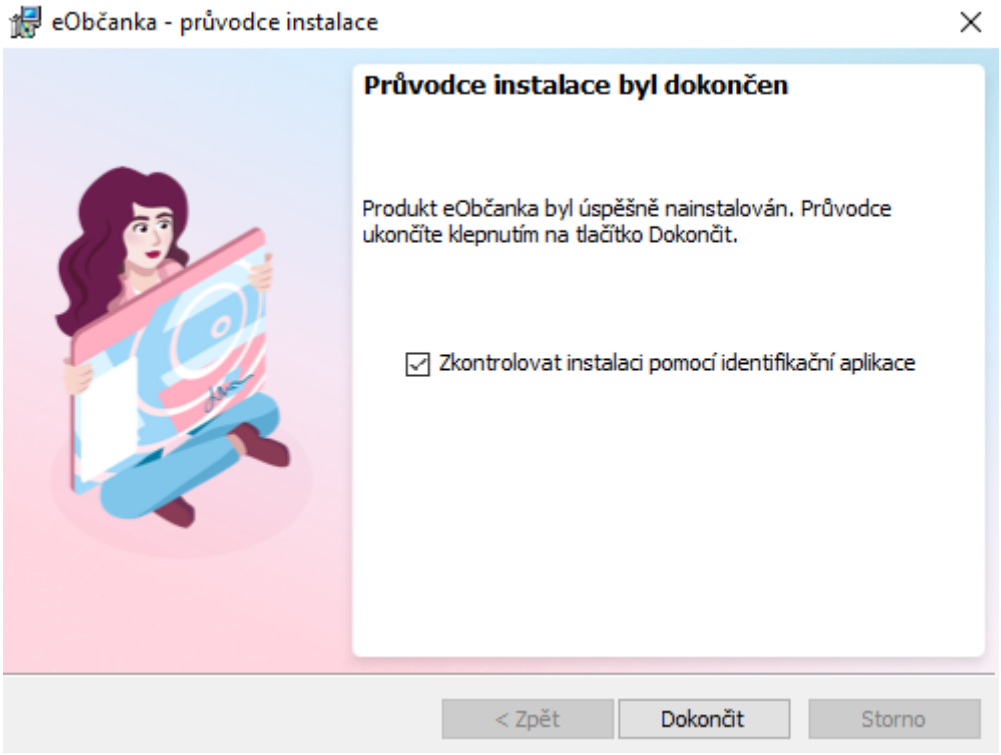


Obr. 22 – Průběh instalace aplikace eObčanka

Po úspěšné instalaci byly vytvořeny ikony zástupců na pracovní ploše aplikací eObčanka – identifikace a eObčanka – Správce karty, které jsou vidět na Obr. 23. Na Obr. 24 volbou „Zkontrolovat instalaci pomocí identifikační aplikace“ a potvrzením tlačítkem dokončit se spustí diagnostická funkce aplikace eObčanka - identifikace.



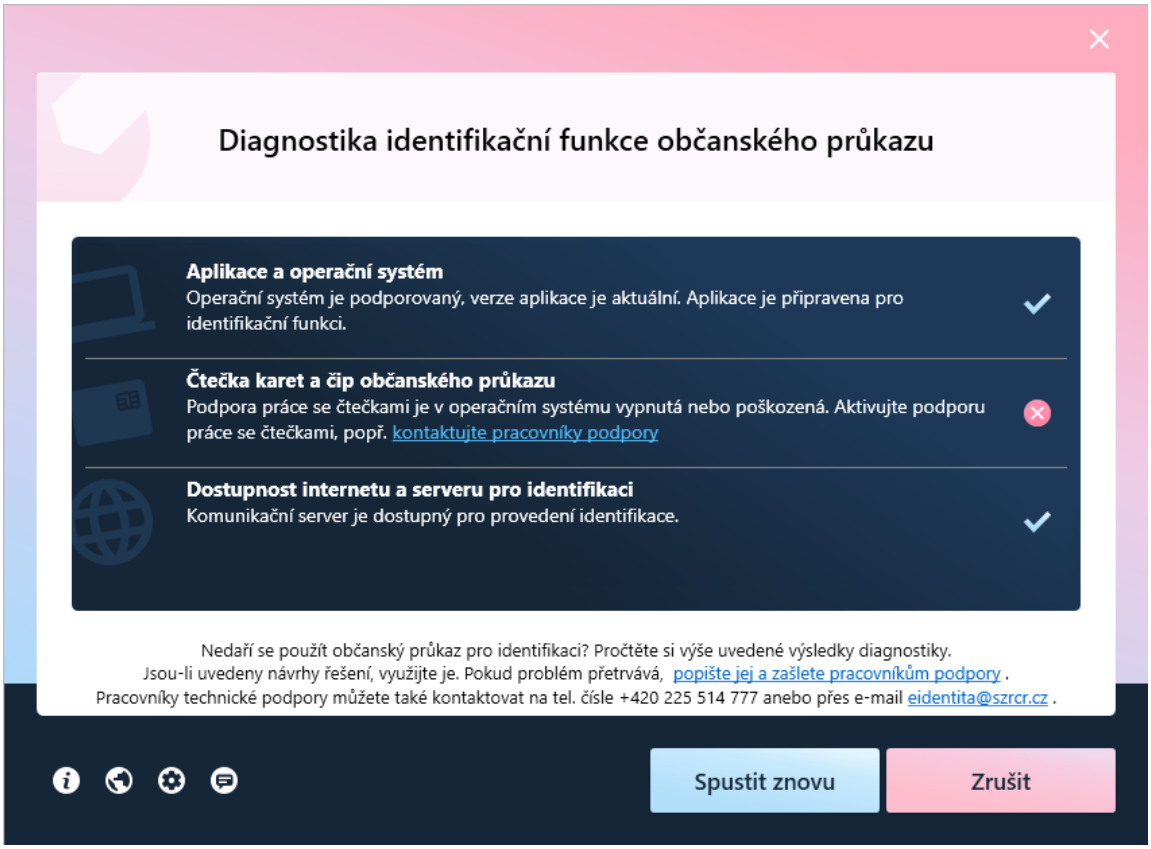
Obr. 23 – Zástupci aplikací na pracovní ploše



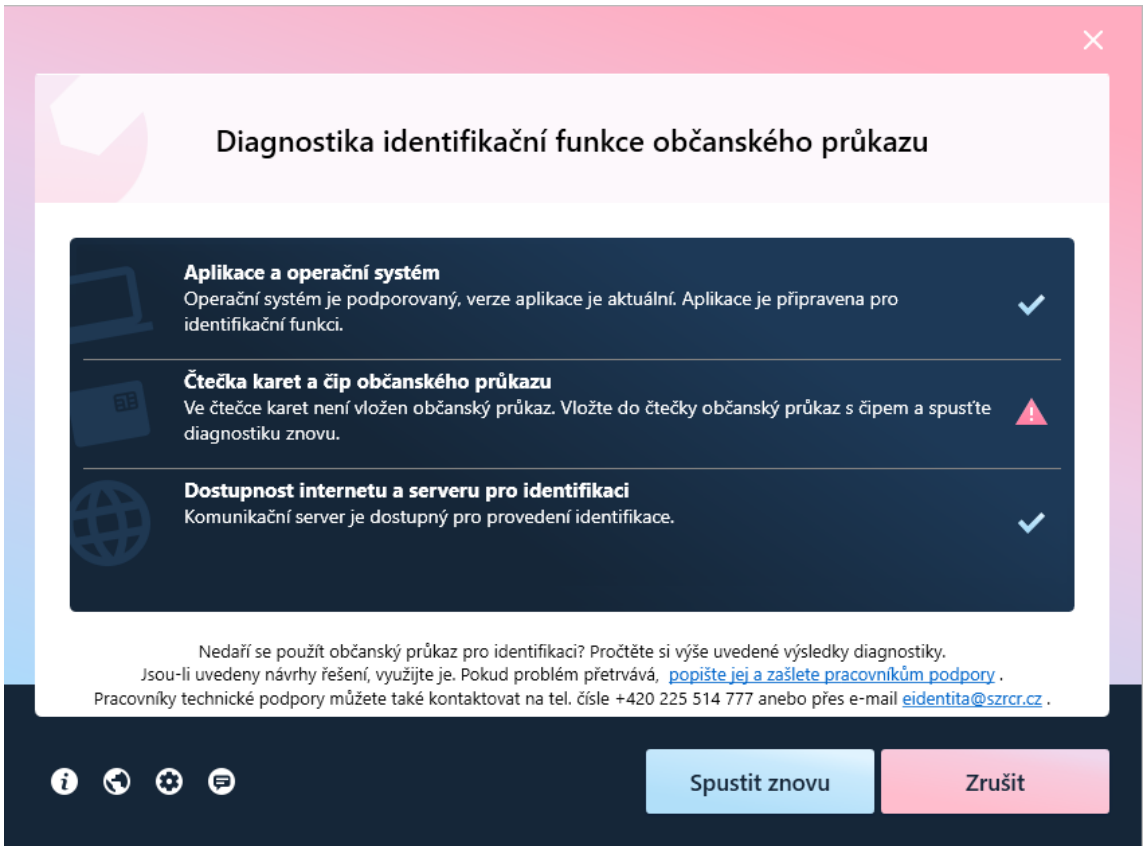
Obr. 24 – Dokončení instalace aplikace eObčanka

Po ukončení diagnostika aplikace zobrazila, ve které oblasti nastala chyba. Na Obr. 25 je vidět, že v oblasti Čtečky karet a čipu občanského průkazu nastala chyba. Ta nastala z důvodu nepřipojení čtečky k PC. Po připojení čtečky čipových karet a spuštění nové diagnostiky tlačítkem „Spustit znovu“ hlásí aplikace upozornění ve stejné oblasti, že do čtečky karet nebyl vložen občanský průkaz viz. Obr. 26. Po vložení eOP do čtečky a opětovném spuštění diagnostiky už nenastal žádný problém a je možné provádět identifikační funkce jak je vidět na Obr. 27.

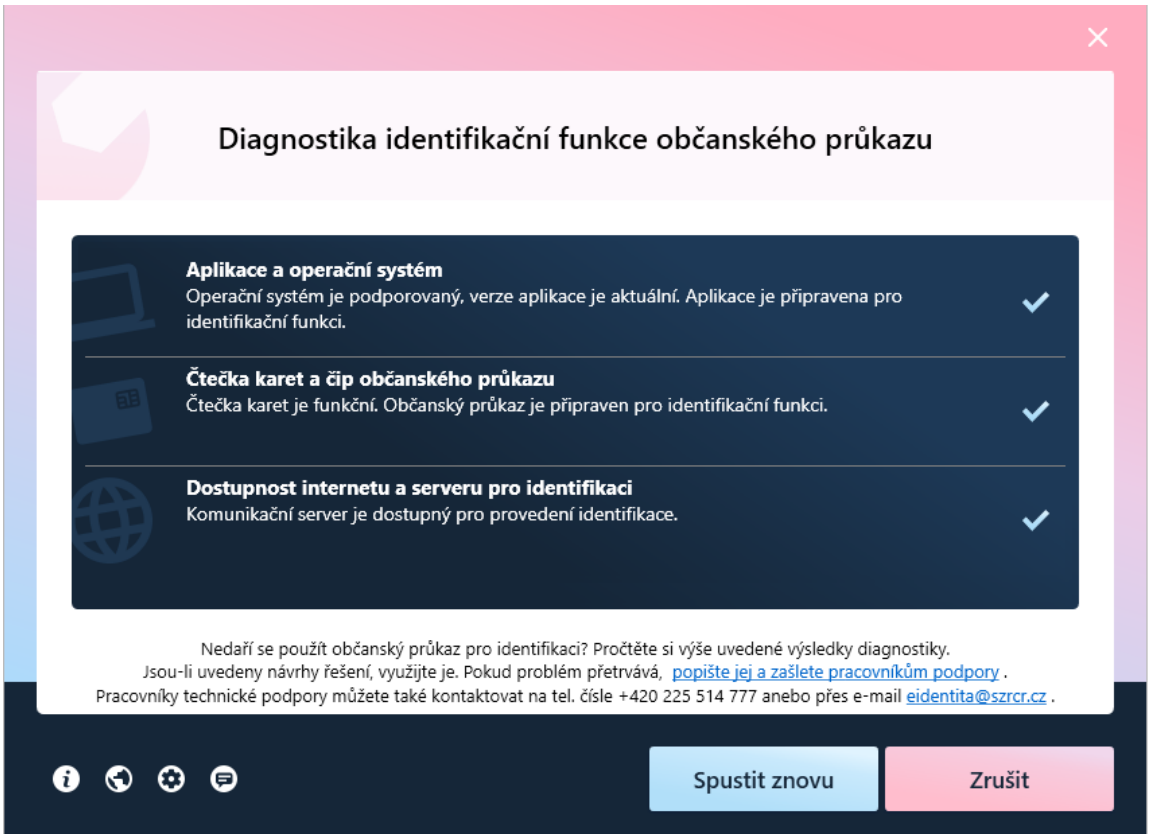
Ovladače ke čtečce karet ACS ACR 3901 U-S1 po připojení k PC byly automaticky nainstalovány. Zařízení nepotřebovalo žádné konfigurace ani ruční stažení a instalaci ovladačů.



Obr. 25 – Diagnostika identifikační funkce - nepřipojená čtečka



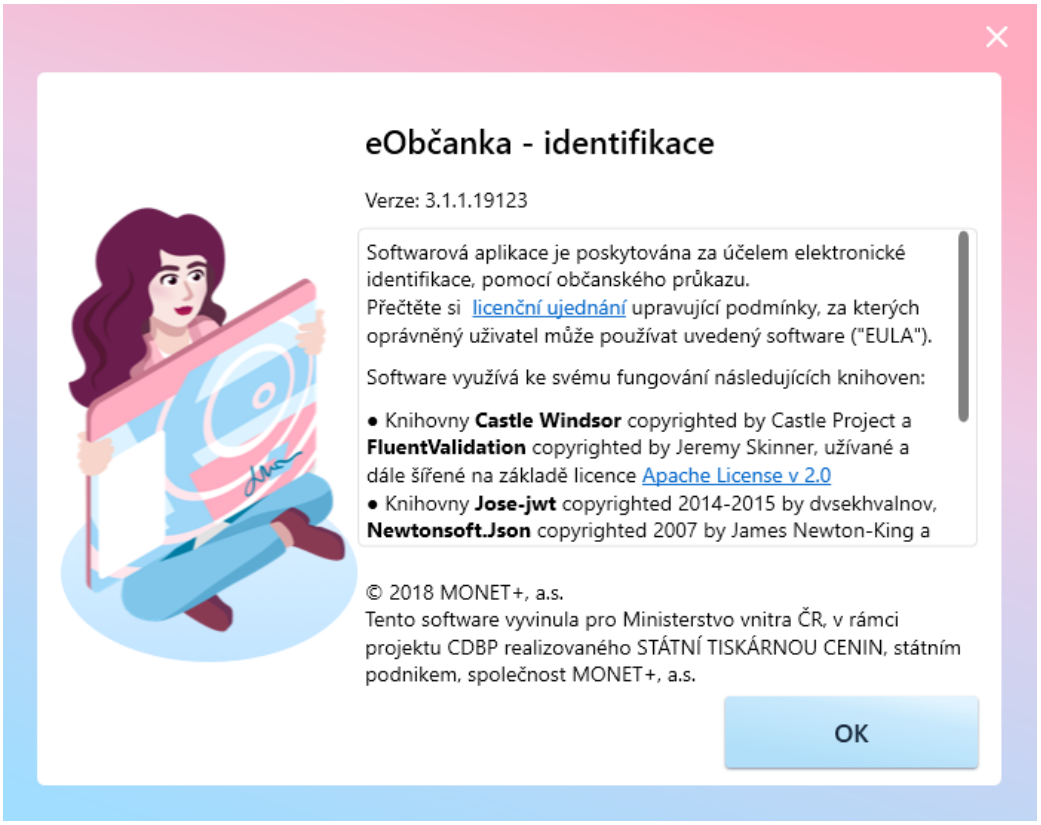
Obr. 26 – Diagnostika identifikační funkce - není vložen eOP



Obr. 27 – Diagnostika identifikační funkce - úspěšná diagnostika

V dolním levém rohu aplikace eObčanka – identifikace jsou umístěny ikony, které vedou k zobrazení dále k:

- **O aplikaci** – obsahuje účel aplikace, odkaz na licenční ujednání, využívané knihovny, vydavatele softwaru viz. Obr. 28.
- **Informace o identifikační funkci** – odkazuje na webové stránky info.eidentita.cz popisující jak se identifikovat pomocí občanského průkazu na PC.
- **Nastavení aplikace** viz. Obr. 29 – povolení či zakázání následujících nastavení:
  - Automatické ukončování aplikace po úspěšném dokončení identifikace
  - Zapisování provozních záznamů
  - Zapisování podrobných provozních záznamů
  - Zahájení identifikace (automaticky) po vložení občanského průkazu do čtečky
  - Deaktivace použití interní klávesnice čtečky
- **Odeslat problém pracovníkům podpory** – formulář umožňující odeslání zprávy o problému pracovníkovi podpory. Okno aplikace pro odeslání formuláře je vidět na Obr. 30.

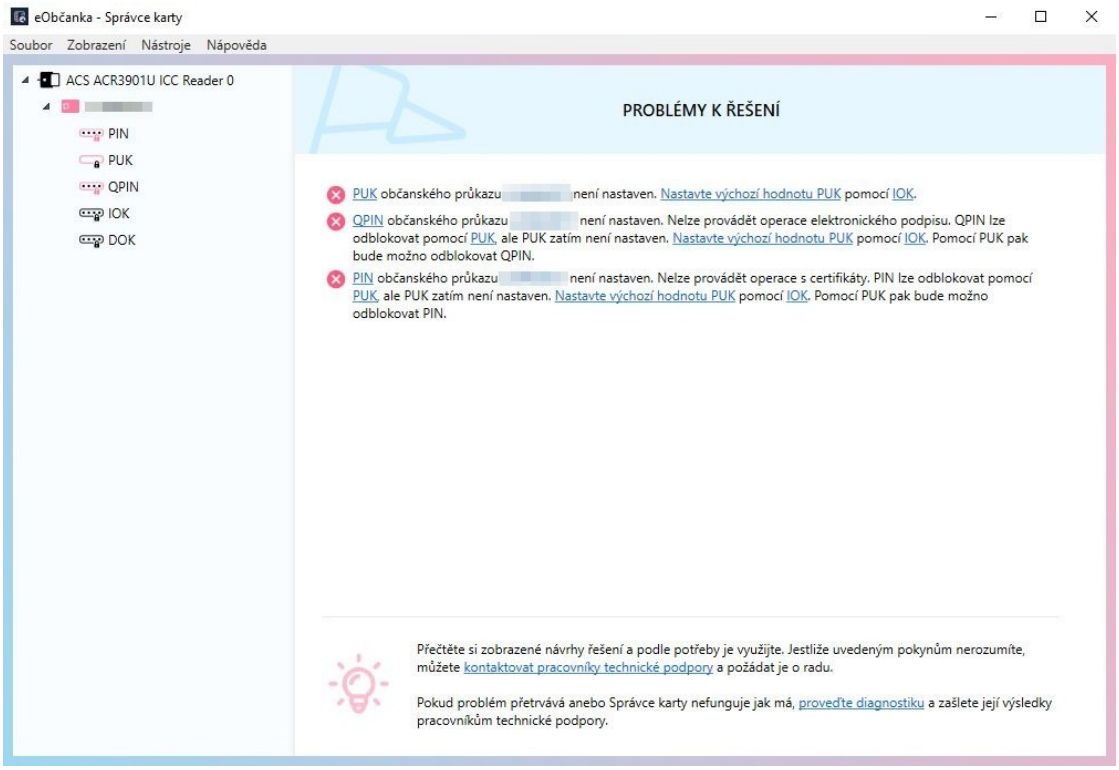


Obr. 28 – O aplikaci eObčanka - identifikace

Obr. 29 – Nastavení aplikace eObčanka - identifikace

Obr. 30 – Formulář podpory aplikace eObčanka - identifikace

Spuštěním aplikace eObčanka – Správce karty došlo k automatické detekci čtečky a případně vloženého eOP. Čtečka v tomto případě nebyla připojena a aplikace nahlásila chybu. Po připojení čtečky a vložení eOP do čtečky, lze buď znovu spustit aplikaci nebo v již otevřeném okně stisknout klávesu F5 pro obnovení. Tlačítko pro obnovu lze také nalézt v menu Zobrazení → Obnovit. Program automaticky začal načítat informace z čipu eOP. Nalezenou čtečku a občanský průkaz zobrazil v levé části okna, jako objekty ve stromu informací. V pravé části se následně zobrazují detailní informace či problémy k řešení. Jak lze vidět na Obr. 31 aplikace úspěšně detekovala čtečku i občanský průkaz. Formou symbolů s textovým popisem zobrazila název čtečky, číslo občanského průkazu (z důvodu ochrany údajů je číslo eOP nečitelné) a jednotlivé přístupové kódy. V pravé části okna nahlásila informace o skutečnosti, že kódy PUK, QPIN a PIN nejsou nastaveny. Z informací lze vyčíst podrobné vysvětlení s příslušnými odkazy.

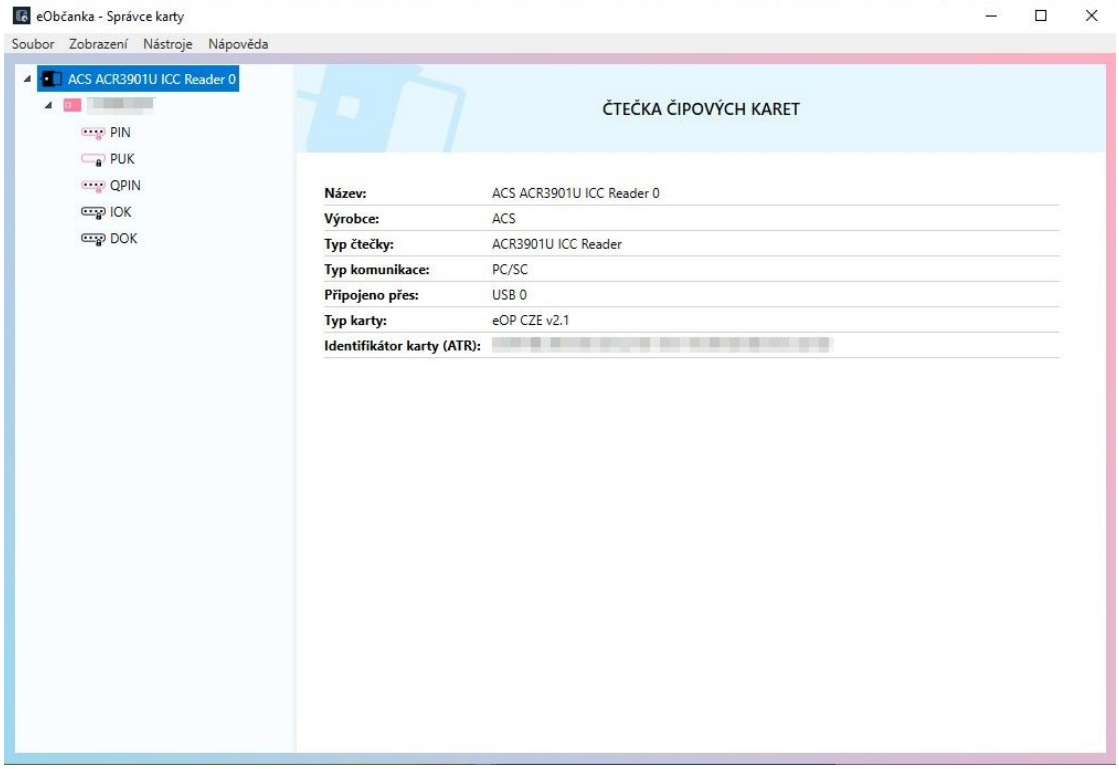


Obr. 31 – Okno aplikace eObčanka – Správce karty

Menu aplikace eObčanka – Správce karet nabízí možnosti:

- **Soubor** – obsahuje tlačítko pro ukončení programu.
- **Zobrazení** – volba standardního či rozšířeného zobrazení a obnovit (F5).
- **Nástroje**
    - Zobrazit diagnostiku – provede diagnostický test a zobrazí informace o nalezených čtečkách, čipových kartách, klíčů a certifikátech. Diagnostické informace lze uložit, kopírovat do schránky a odeslat pracovníkům podpory.
    - Uložit diagnostiku – uložení diagnostických informací do paměti PC v textovém dokumentu (*.txt).
    - Problémy k řešení – zobrazí problémy k řešení.
    - Nastavení – nastavení aplikace zda zapisovat provozní záznamy a podrobné provozní záznamy.
- **Nápověda** – zobrazí informace o aplikaci nebo otevře PDF soubor s uživatelskou příručkou programu.

Označením objektu v levé části okna se zobrazily jeho informace. Na Obr. 32 lze vidět informace o připojené čtečce karet jako název, výrobce, typ čtečky, typ komunikace, připojení, typ vložené karty a identifikátor karty.



Obr. 32 – Informace o čtečce v aplikaci eObčanka – Správce karty

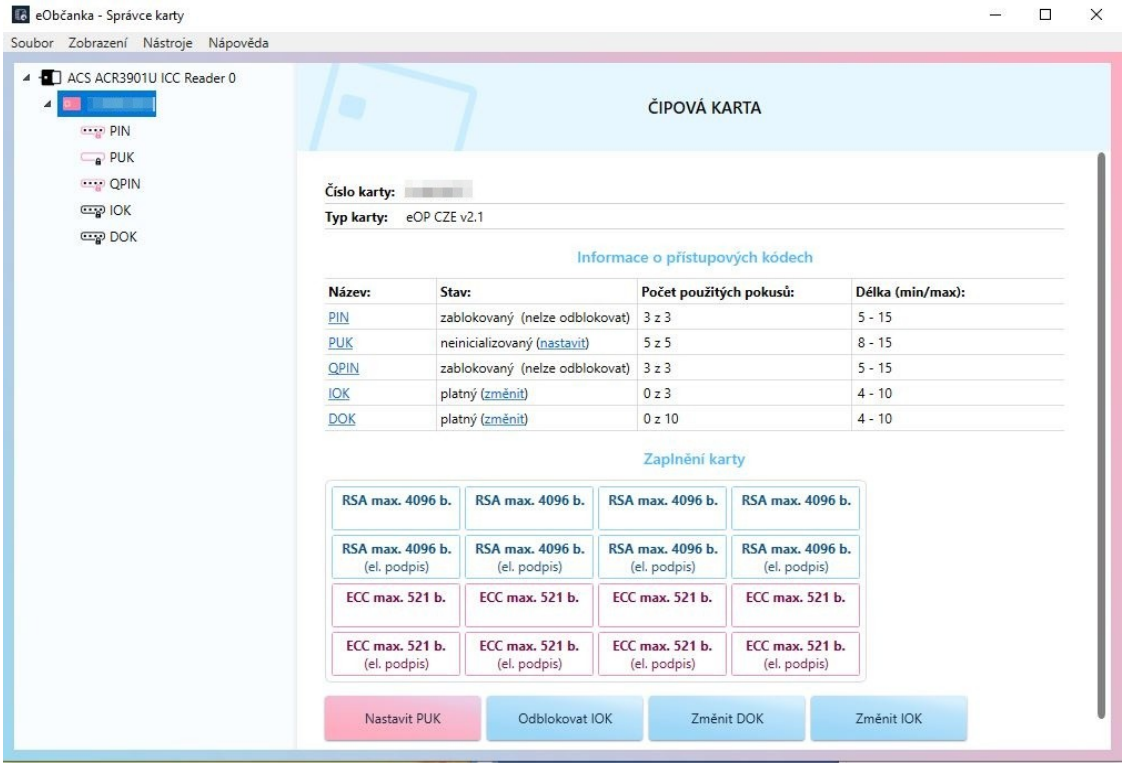
Obr. 33 zobrazuje informace o čipové kartě. Z okna informací o čipové kartě lze vyčíst číslo karty, typ karty, informace o přístupových kódech a zaplnění karty. Pomocí tlačítek akcí lze nastavit PUK, odblokovat IOK, změnit DOK a IOK.

Typ karty s hodnotou *eOP CZE v2.1* označuje občanský průkaz, který byl vydán po datu 1. 7. 2018. Občanské průkazy s čipem vydané před tímto datem mají označení *eOP CZE v1.0*. [55]

V tabulce informací o přístupových kódech lze sledovat jednotlivé kódy jejich stav, počet použitých pokusů a jejich minimální a maximální délku.

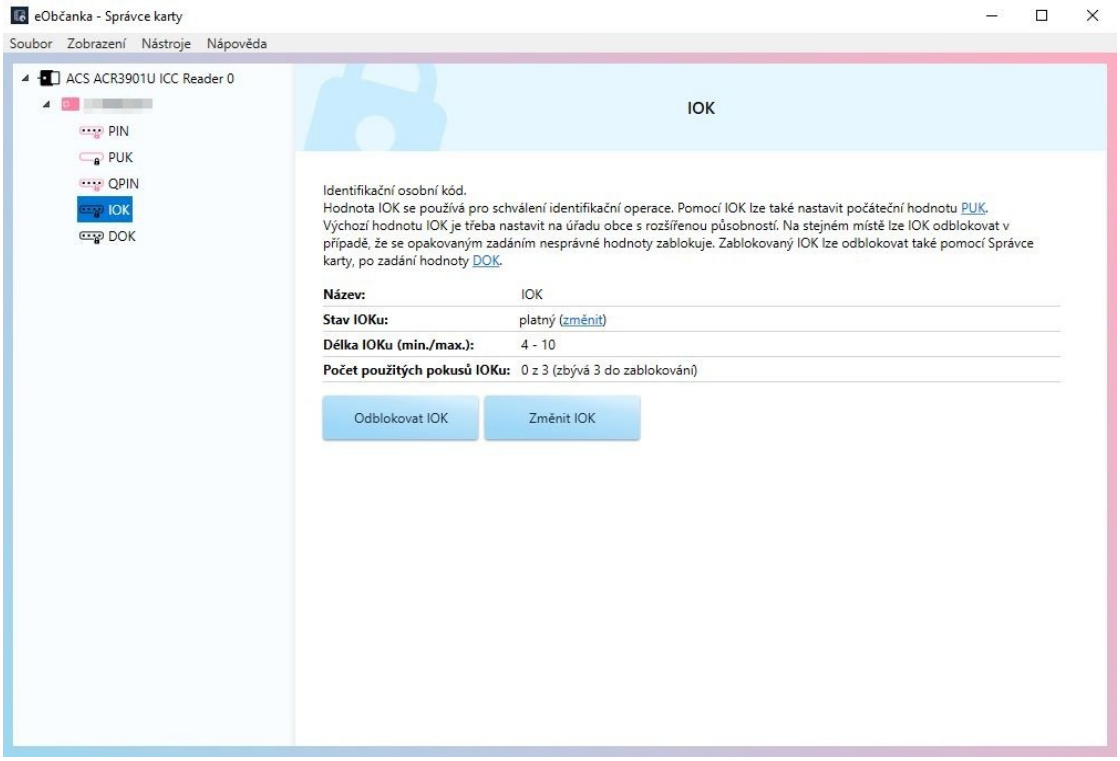
V přehledu o zaplnění čipu karty je zobrazen stav zaplnění jednotlivých kontejnerů pro uložení kryptografických klíčů a certifikátů. V žádném z vyobrazených kontejnerů nejsou nahrána data. Prázdný kontejner má proto bílou barvu. Po zaplnění se příslušný kontejner vybarví. Jednotlivé reprezentace kontejneru mimo jiné zobrazují informaci o algoritmu klíče (RSA či ECC), délce klíče či účelu klíče. Kontejnery klíčů určené pro podepisování

mají uvedeno v popisu *(el. podpis)*. Zobrazením tooltipu po najetí kurzoru myši na vybraný kontejner lze zjistit další informace. [55]



Obr. 33 – Informace o čipové kartě v aplikaci eObčanka – Správce karty

Výběrem jednoho z přístupových kódů se zobrazí jeho podrobné informace. Na Obr. 34 lze vidět okno s informacemi o kódu IOK, jeho stav, minimální a maximální délku a počet použitých pokusů s informací o zbývajících pokusech než dojde k zablokování. Tlačítky akcí lze odblokovat IOK či změnit jeho hodnotu.



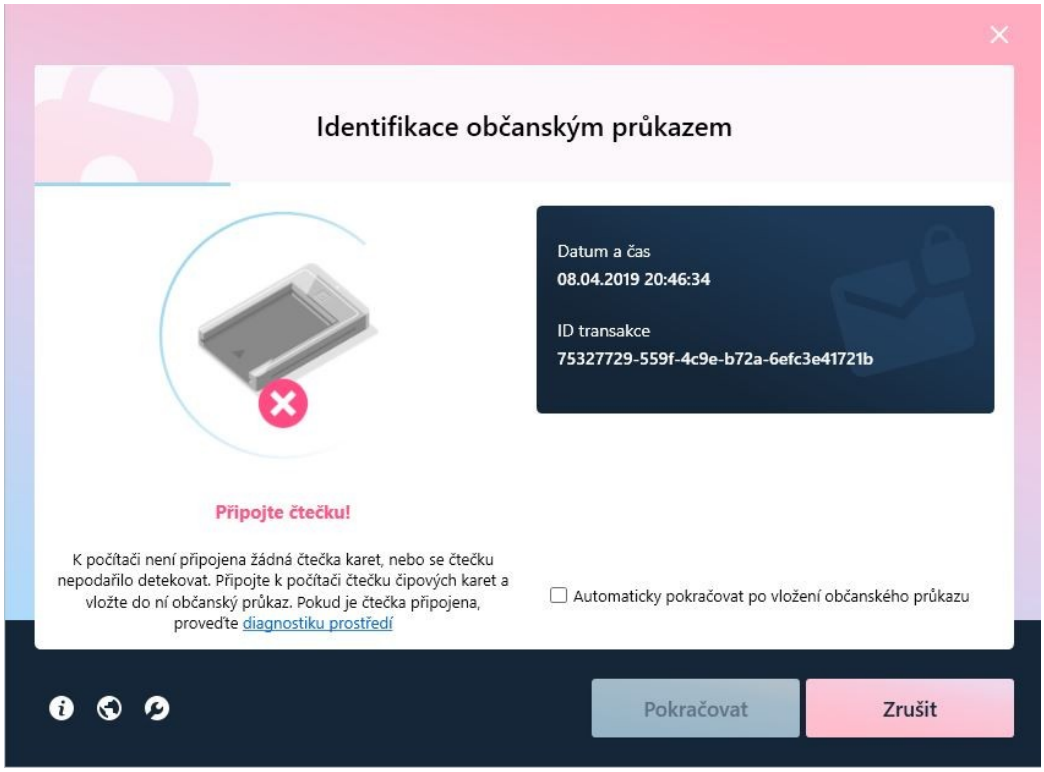
Obr. 34 – Informace o IOK v aplikaci eObčanka – Správce karty

8.1.1 Identifikace pomocí eOP na PC

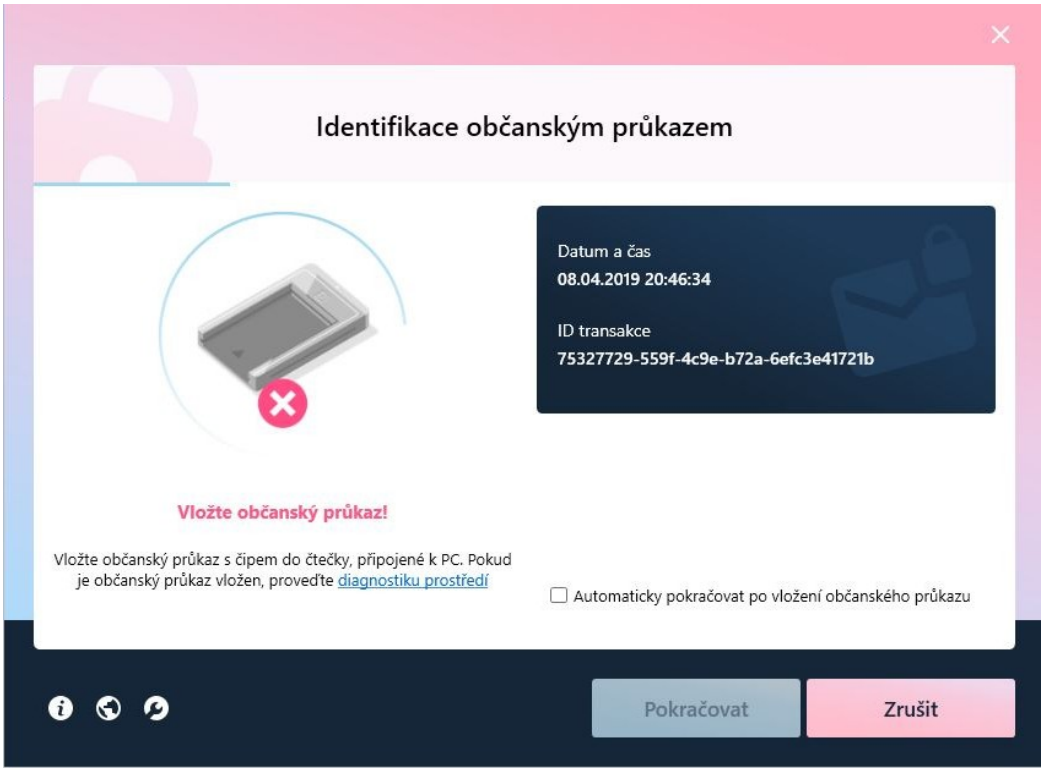
Pro otestování přihlašování ke kvalifikovanému poskytovateli byl vybrán Portál občana a ePortál ČSSZ.

Přes oficiální stránky Portálu veřejné správy se lze přihlásit do Portálu občana za pomocí ověření prostřednictvím prostředků e-identity nebo se přihlásit datovou schránkou.

Identifikace pomocí eOP probíhá přes webové stránky NIA k tomu určeným. Stránka po potvrzení o přihlášení začala spouštět přihlašovací komponentu. Webový prohlížeč vyzval k potvrzení, zda má být spuštěna obslužná aplikace eObčanka – identifikace. Potvrzením systém spustil příslušnou aplikaci, která začala vyhledávat připojenou čtečku. V okně pro identifikaci občanským průkazem se zobrazují i informace o ID transakce, datu a času. Pokud čtečku není možné detekovat, aplikace vyzvala o její připojení viz. Obr. 35. Stejnou skutečnost oznámí i pro nevložený občanský průkaz viz. Obr. 36.



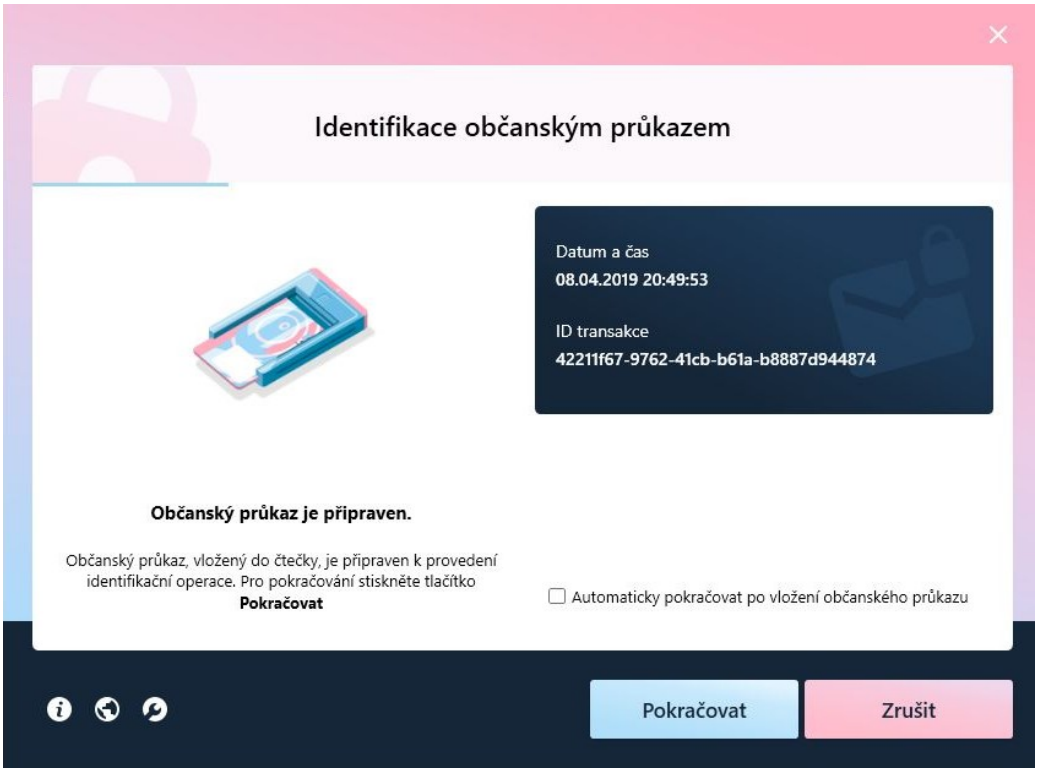
Obr. 35 – Oznámení o nepřipojení čtečky v aplikaci eObčanka - identikace



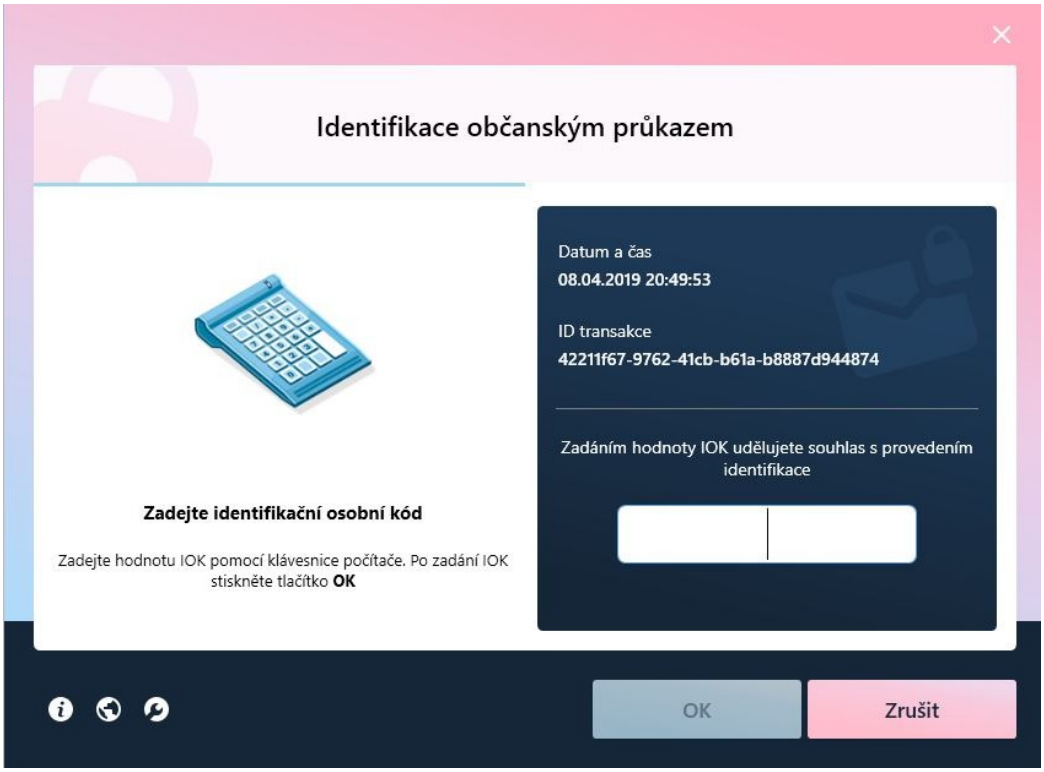
Obr. 36 – Oznámení o nevložení eOP v aplikaci eObčanka - identifikace

Pokud aplikace úspěšně detekuje čtečku s vloženým občanským průkazem, vyzve k dalšímu pokračování a to zadání IOK viz. Obr. 37. Aplikace rozpoznala použití čtečky

karet bez integrované klávesnice a upozornila na zadání kódu z klávesnice počítače viz. Obr. 38.



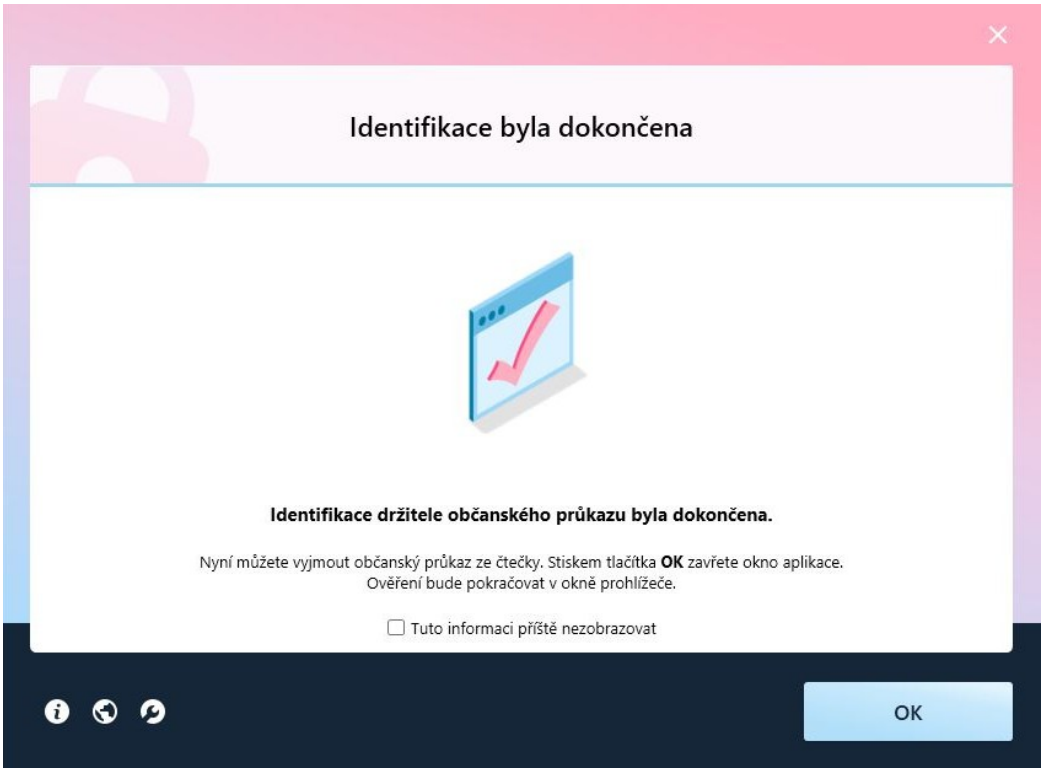
Obr. 37 – Oznámení o vložení eOP v aplikaci eObčanka - indentifikace



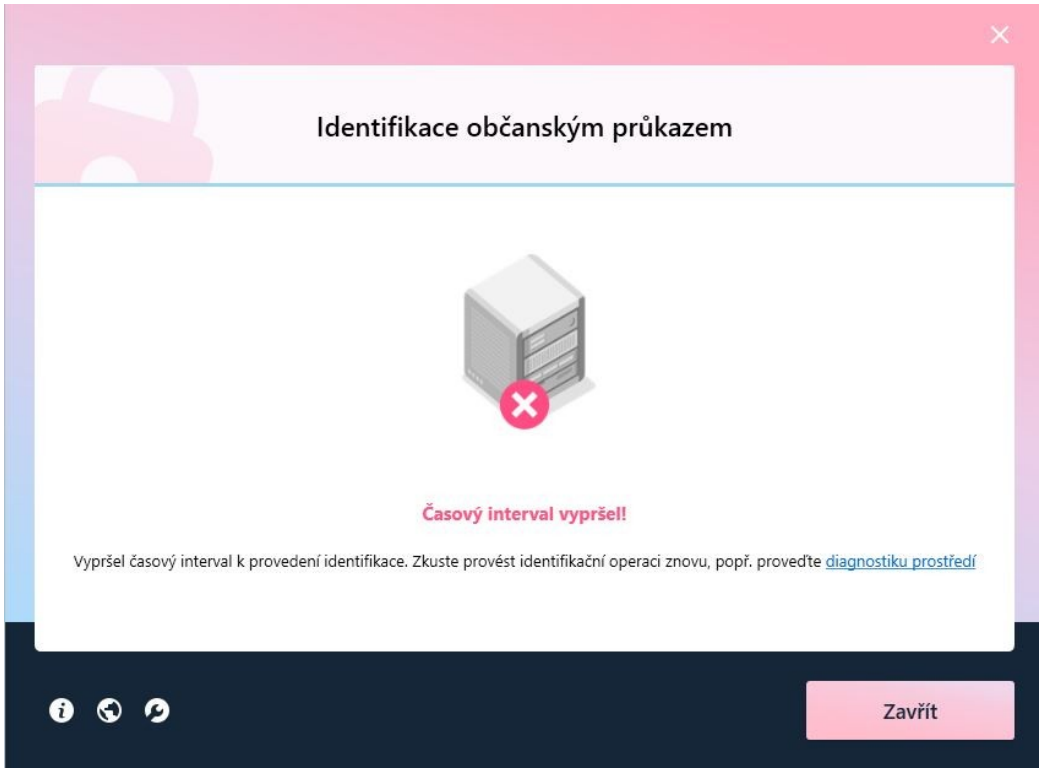
Obr. 38 – Zadání IOK v aplikaci eObčanka - identifikace

Ověřením správné hodnoty kódu došlo k úspěšnému dokončení identifikace. Tuto informaci lze příště přeskočit, zatržením příslušené možnosti. Tlačítkem OK se zavřelo okno aplikace a další práce probíhala v prohlížeči viz. Obr. 39.

Nutno podotknout, že pro celou operaci identifikace je vymezen určitý časový interval. Překročením tohoto intervalu dojde k přerušení identifikačních operací a je nutné celý proces opakovat znovu. Příslušné upozornění se zobrazí v aplikaci jak je vidět na Obr. 40 i na stránkách NIA. Z tohoto důvodu je dobré mít již připojenou čtečku s vloženým eOP před zahájením identifikace.



Obr. 39 – Oznámení o dokončení identifikace v aplikaci eObčanka - identifikace



Obr. 40 – Vypršení časového limitu v aplikaci eObčanka - identifikace

Portál pro identifikaci vyzval o udělení souhlasu pro výdej údajů pro kvalifikovaného poskytovatele viz. Obr. 41. U údajů typu příjmení, jméno, datum a místo narození je umožněno odmítnout souhlas. Lze zobrazit hodnoty volitelných údajů a rozhodnout zda udělit poskytovateli trvalý, jednorázový či neudělit souhlas o výdeji vybraných údajů.

Obr. 41 – Udělení souhlasu o poskytování údajů

Po udělení souhlasu došlo k předání informací a přesměrování zpět na Portál občana, kde bylo nutné souhlasit s žádostí o poskytování údajů ze základních registrů a agendových informačních systémů. Po tomto kroku již bylo umožněno využít funkcí Portálu občana.

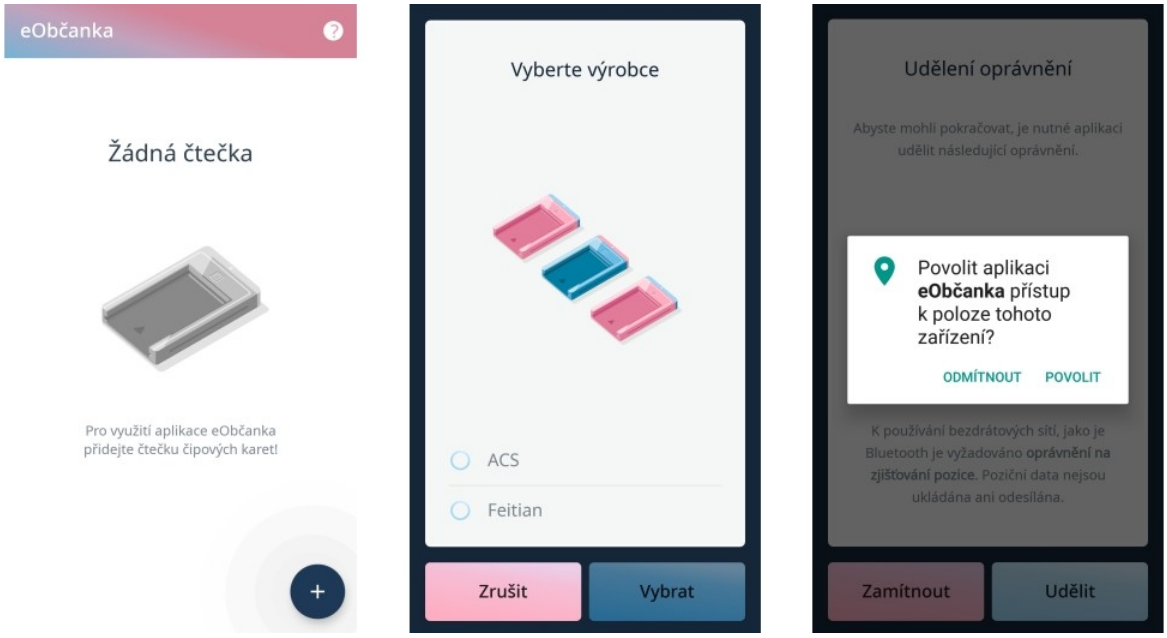
Přihlášení do ePortálu ČSSZ proběhlo přes příslušnou přihlašovací stránku zcela bez problému a stejným způsobem jako u Portálu občana. Pomocí identifikace prostřednictvím NIA, využitím identifikační funkce eOP a udělením souhlasu s poskytováním příslušných údajů došlo k úspěšnému přihlášení.

8.2 Aplikace eObčanka pro Android

Mobilní aplikace eObčanka pro Android je dostupná v oficiální distribuci přes obchod Google Play. Verze aplikace je 1.0.0 (2827) s datem vydání 31. 10. 2018. Po stažení a instalaci do mobilního přístroje využila 17,52 MB místa v příslušné paměti. Aplikace může požadovat oprávnění v oblastech polohy, telefon a úložiště zařízení.

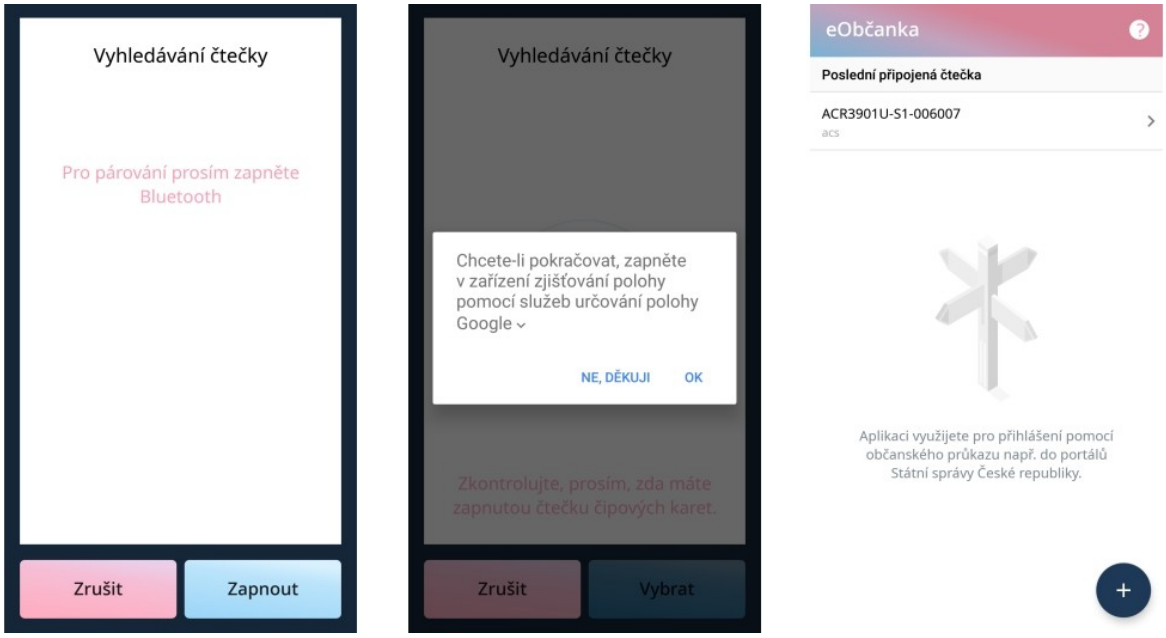
Tapnutím na příslušnou ikonu se spustí aplikace s prvotním tutoriálem, který ve čtyřech krocích seznámil se základními informace o využití, nutnosti vlastnit čtečku karet a aktivací IOK.

Dalším krokem bylo přidání čtečky čipových karet. Aplikace k tomuto vyzvala jak je vidět na Obr. 42. Na platformě Android lze v současnosti využívat pouze dvě čtečky. Aplikace nabídla výběr příslušných výrobců viz. Obr. 42. Pro párování čtečky byla zvolena čtečka od ACS. Následně aplikace oznámila, že je nutné udělit oprávnění na zjišťování pozice. Toto oprávnění je nutné k využívání bezdrátových sítí, jako je Bluetooth. Poziční data nejsou v tomto případě ukládána ani odesílána. Potvrzením výzvy se zobrazilo dialogové okno s povolením oprávnění viz. Obr. 42.



Obr. 42 – Přidání čtečky (vlevo), výběr výrobce čtečky (uprostřed) a oprávnění k poloze (vpravo) v mobilní aplikaci eObčanka

Pokud nebylo v zařízení zapnuto Bluetooth, aplikace upozornila a nabídla možnost jej zapnout jak je vidět na Obr. 43. Aplikace začala vyhledávat aktivní čtečku karet od zvoleného výrobce. Pokud čtečka není aktivní nelze jí vyhledat a aplikace upozorní na možnost, že je nutné čtečku zapnout. Pokud není zapnuto zjišťování polohy, zobrazí se dialog pro jeho zapnutí viz. Obr. 43. Aplikace vyhledala příslušnou čtečku a zobrazila její označení. Následně nabídla možnost nastavit si její vlastní název. Připojená čtečka se přidala od seznamu čtečích zařízení, kde je možné zjistit další informace viz. Obr. 43.



Obr. 43 – Výzva k zapnutí Bluetooth (vlevo), zjišťování polohy (uprostřed) a seznam připojených čteček (vpravo) v mobilní aplikaci eObčanka

V informacích o čtecím zařízení je možné zjistit:

- **Jméno zařízení** – vlastní pojmenování čtečky s možností editace
- **Typové označení výrobce**
- **MAC adresa**
- **Status** – upozornění zda je zařízení připojené
- **Občanský průkaz** – upozornění zda je vložen eOP
- **Stav baterie** – procento nabití baterie čtečky
- **Logo výrobce**

Přes tlačítko „Připojit“ lze zapnout Bluetooth mobilního zařízení a tlačítkem „Zapomenout“ odstranit čtečku ze seznamu.

Při ukončení a novém spuštění aplikace se zobrazí seznamu spárovaných čteček. V pravém horním rohu po tapnutí na ikonu otazníku, lze vyvolat nápovědu. Tato možnost byla i při prvním spuštění při přidání čtečky.

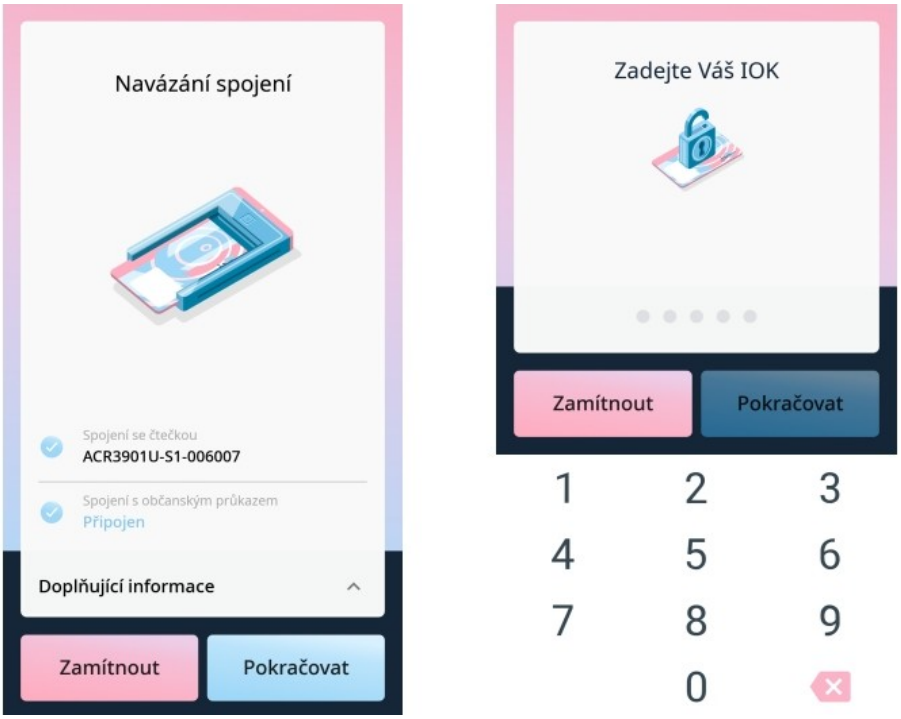
Nápověda aplikace nabízí:

- **Časté dotazy** – seznam důležitých otázek s odpověďmi
- **Tutorial** – spuštění úvodního tutoriálu
- **Zákaznická podpora** – kontakt s odkazy na pracovníky zákaznické podpory
- **O aplikaci** – informace o verzi aplikace, účelu či vývojáři softwaru

8.2.1 Identifikace pomocí eOP na mobilním zařízení

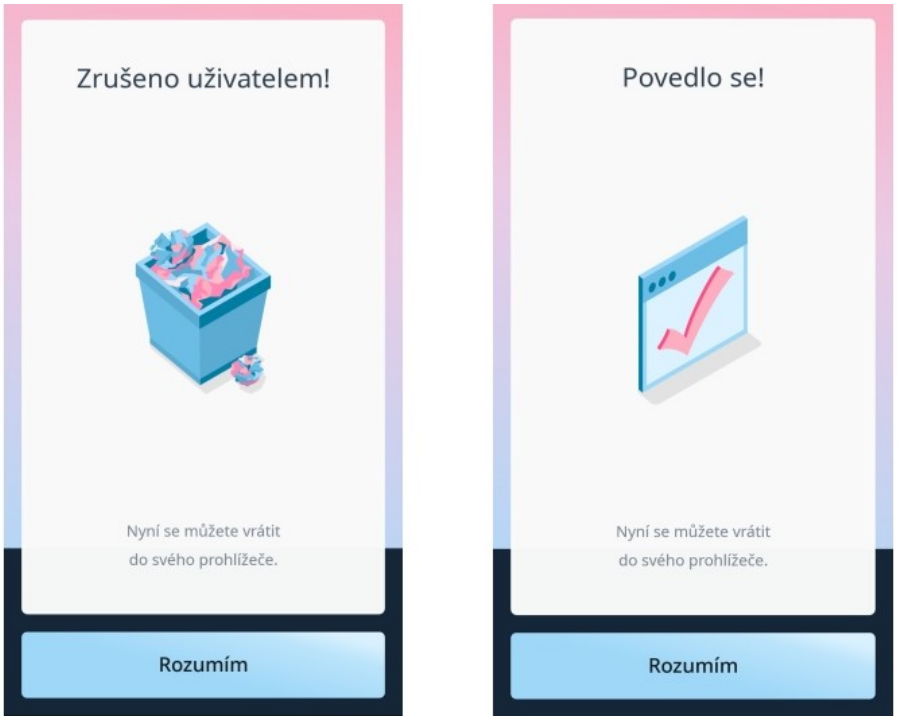
Pro požadavek identifikace byl znovu vybrán Portál občana. Přes webovou stránku pro přihlášení do portálu byla přesměrována komunikace na stránky NIA. Zde jak v předchozím případě došlo k potřebné identifikaci. Stránky NIA při požadavku na identifikaci pomocí eOP automaticky spustilo mobilní aplikaci nainstalovanou v telefonu.

Aplikace automaticky navazuje spojení se čtečkou karet. Pokud není spuštěno zjišťování polohy, zobrazil se dialog o jeho zapnutí. Se čtečkou nelze navázat spojení také z důvodu vypnutého Bluetooth. To je nutné spustit na obou stranách. Po navázání spojení se čtečkou je nutné vložení eOP do čtečky. Na Obr. 44 je vidět úspěšné spojení se čtečkou a eOP. V tuto chvíli lze zjistit i doplňující informace a to datum, čas a ID transakce. Tlačítkem pokračovat došlo k požadavku na zadání IOK viz. Obr. 44.



Obr. 44 – Spojení se čtečkou (vlevo) a zadání IOK (vpravo) v mobilní aplikaci eObčanka

V tomto i předchozím kroku je možné zamítnout proces identifikace pomocí příslušeného tlačítka. Oznámení o zrušení procesu je vidět na Obr. 45. Po zadání správné hodnoty IOK došlo k úspěšné identifikaci viz. Obr. 45 a vrácení uživatele na webovou stránku NIA pro udělení souhlasu o poskytování údajů. Udělením potřebných souhlasů (lze i trvale a přeskočit tento krok) je komunikace přesměrována na Portál občana již jako přihlášený uživatel.



Obr. 45 – Zrušení procesu (vlevo) a úspěšná identifikace (vpravo) v mobilní aplikaci eObčanka

8.3 Srovnání aplikací pro PC a mobilní zařízení

Z předchozích kapitol a analýzy aplikací lze nastínit výhody a nevýhody aplikace eObčanka pro PC a mobilní zařízení.

Výhody aplikace pro PC:

- Kompatibilita s mnoha čtečkami
- Obsahuje aplikaci eObčanka - Správce karty
- Možnost práce s certifikáty a elektronickými podpisy
- Lze provádět nastavení, změny a odblokování bezpečnostních kódů
- Možnost různých nastavení aplikací
- Podpora pro řešení problému formou odeslání formuláře s možností připojení souborů s diagnostikou a pracovními záznamy aplikace
- Jednoduchá instalace
- Uživatelsky a graficky přívětivé prostředí

Nevýhody aplikace pro PC:

- Možnost stažení a instalace nebezpečné aplikace
- V některých případech nutnost ruční instalace ovladačů čtečky

Výhody aplikace pro mobilní zařízení

- Velmi jednoduchá instalace
- Oficiální distribuce přes Google Play či App Store
- Jednoduché, uživatelsky a graficky přívětivé prostředí
- Není nutné instalovat ovladače čteček

Nevýhody aplikace pro mobilní zařízení

- Podpora pouze tří čteček čipových karet z toho jen dvě pro Android
- Cena a dostupnost čteček
- Nutnost vlastnit kompatibilní čtečku s technologií Bluetooth
- Nelze pracovat s certifikáty a elektronickými podpisy
- Nelze nastavit, změnit ani odblokovat bezpečnostní kódy

Srovnáním výhod a nevýhod lze říci, že pro uživatele bude v současnosti přívětivější využití eOP a jeho aplikací na PC. Za stěžejní lze považovat dostupnost a cenu čteček čipových karet. Aplikace pro PC nabízí více možností a je tudíž i nepostradatelnou součástí pakliže uživatel bude chtít pracovat s některým z přístupových kódů nebo využít funkcí pro elektronické podepisování. Obě aplikace nabízí uživatelsky přátelské prostředí s jednoduchou instalací a intuitivním ovládáním.

9 VYHODNOCENÍ A DISKUSE

Následující vyhodnocení se opírá o dosažené poznatky a zprávy. Má za cíl provést diskusi nad vhodností eOP. Za podstatné výsledky této práce lze považovat zjištění, že veřejná správa České republiky má zaručený nástroj pro identifikaci a autentizaci občana, se kterým lze provádět úkony v rámci eGovernmentu u nás, ale i v zahraničí. Interoperabilitou, jak je nazývána schopnost technologií vzájemné součinnosti splňují nové občanské průkazy cíle z nařízení eIDAS. Bylo vytvořeno legislativní i technologické prostředí pro vytváření služeb pro elektronické transakce využívající eOP. Nové občanské průkazy jsou vhodnými nástroji pro toho, kdo chce využívat služeb eGovernmentu či využívat např. elektronické podpisy. Tyto požadavky však sebou nesou určité znalosti a dovednosti v oblasti informačních a komunikačních technologií. Uživatel si musí uvědomit, že pracuje se svými citlivými údaji, které mohou být v prostředí počítačů a internetu zneužity neoprávněnými subjekty. Měl by proto své chování přizpůsobit i těmto skutečnostem. Technologie spjaté s eOP zaručují bezpečností ochranu, avšak vždy záleží na daném uživateli, který s touto technologií pracuje. V současné době se lze přihlašovat pomocí eOP k nejméně devíti portálům. Přihlašování vždy směřuje přes portál národní bodu, jehož úkolem je i předání údajů o uživateli, ke kterým dal souhlas. V souvislosti se službami, které kvalifikovaní poskytovatelé po přihlášení nabízí, mohou vznikat i omezení. Za takové lze považovat např. vlastnění datové schránky. Aplikace vytvořené pro práci s elektronickými funkcemi občanského průkazu jsou dostupné pro nejpoužívanější operační systémy na PC i na mobilním zařízení. Všechny aplikace jsou uživatelsky přívětivé a funkční.

Dle nedávných zpráv počet vydaných eOP ke dni 31. března 2019 bylo bezmála 902 tisíc. Počet přihlášení k Portálu občana je k začátku dubna téměř 154,5 tisíc. Polovina přihlášení proběhlo přes datovou schránku, čtvrtina pře eOP a čtvrtina formou jednorázového přihlášení kombinující jméno, heslo a SMS. Změny by měla přinést novela zákona o elektronických úkonech a autorizované konverzi dokumentů. Novela počítá s možností pomocí eOP zřídit datovou schránku bez nutnosti osobní návštěvy a podání písemné žádosti. Zájem o datovou schránku pro fyzickou osobu se zvyšuje. V současnosti se jich eviduje něco přes 154,5 tisíc. [59]

Jedním z důvodů nevyužívání služeb eGovernmentu je technologická bariéra. Pro mnoho lidí je použití např. eOP obtížné. K masovému využívání eOP zřejmě zabrání i zpráva, že se připravuje možnost přihlášení za pomocí bankovní identity. To by velmi zjednodušilo

proces identifikace vůči službám veřejné správy. Nutné je však nejdříve přijmout příslušná legislativní opatření. [60] [61]

V rámci akce Hackathon, který měl za cíl ověřit bezpečnost projektu eOP a otevřít jej pro veřejnost vyplynulo, že *„funkcionality eObčanky nepřesahují úroveň datových schránek, chybí logické struktury a řešení poskytuje jen omezenou kompatibilitu s produkty dostupnými na českém trhu. Ke svému provozu vyžaduje eObčanka pořízení hardwarové čtečky čipových karet, což omezuje dostupnost veřejné služby.“ „Účastníci hackathonu potvrdili, že zásadním negativem nových elektronických průkazů je uzavřenost systému a absence jakékoli dokumentace.“* [62]

Z výše uvedených zpráv lze usuzovat, že s narůstajícím počtem vydaných eOP se zvýší i počet přihlášení k elektronickým službám veřejné správy. S přibývajícími službami a možnostmi eOP může být pro některé občany vhodnější využití eOP, před alternativními formami přihlášení. Stále však datová schránka je mnohdy používanější formou. Za stávající bariéry pro uživatele lze považovat technologickou náročnost či hardwarové požadavky. Hrozbou pro eOP mohou být i nové formy přihlášení.

V praxi výsledky této práce jsou přínosné zejména pro držitele nového občanského průkazu, který chce využívat jeho elektronických funkcí. Čtenáře seznámí se základními pojmy, službami eOP a praktickými ukázkami aplikací na PC i v mobilním zařízení. Práce neřeší práci s elektronickými podpisy a certifikáty za pomocí nového eOP.

Další možné směry využívání moderních technologií vidím v průzkumu uživatelské přívětivosti a také v schopnosti tyto technologie používat lidmi s různou vzdělanostní strukturou, s lidmi s různou technologickou dostupností těchto nástrojů a také s ohledem na věk a měnící se fyzické schopnosti lidí.

ZÁVĚR

Občanský průkaz s novým čipem umožňuje nejvyšší míru autentizace vůči poskytovatelům především veřejné správy. Celý proces vydávání a elektronické identifikace se pojí s platnou legislativou jak na území České republiky v podobě příslušných zákonů tak na evropském trhu. Stát vytvořil platformu, která splňuje přísné nařízení eIDAS pro zapojení našeho občana do vzájemné interoperabiliti elektronických identit v EU. V současné době se pomocí eOP lze připojit k nejméně 9 portálům a využívat jejich služeb.

S ochranou elektronických dat v eOP a proti jejich případnému zneužití neoprávněnou osobou se pojí i bezpečností kódy. Mezi tyto kódy patří DOK, IOK, PIN, PUK a QPIN. Pro využívání elektronické identifikace jsou však nutné pouze první dva zmíněné (DOK a IOK). Pro každý z kódů jsou nastaveny limity jak v chybném počtu zadání tak i jeho délky.

Pro práci s eOP je nutné pořídit si čtečku čipových karet. Na trhu je v současnosti dostatek zařízení, které lze využít k propojení s PC. Ceny se odvíjí od funkcí či samotnému zpracování čtečky. Na výběr jsou čtečky s klávesnicí či bez ní. Pro vyšší bezpečnost jsou doporučovány čtečky s integrovanou klávesnicí. Pro připojení k mobilnímu zařízení je nutné si pořídit čtečku s technologií Bluetooth. Kompatibilní čtečky s mobilní aplikací jsou pouze tři modely. Avšak jejich dostupnost je pro občana, který by chtěl využít možnosti přihlásit se přes mobilní zařízení k požadovaným službám, značně omezená. Také cena těchto čteček může být pro mnoho lidí až příliš vysoká.

Aby bylo, možné využívat elektronických funkcí eOP je nutné mít nainstalovanou obslužnou aplikaci eObčanka. Aplikace je dostupná pro PC i jako mobilní aplikace. Aplikace pro PC je dostupná pro Windows, macOS i Linux. Instalační balíček eObčanka pro PC obsahuje softwarovou podporu v podobě ovladačů pro práci s certifikáty, aplikaci pro vzdálenou identifikaci k online službám a aplikaci pro správu karty. Mobilní aplikace je dostupná pro platformu Android a iOS. Aplikace obsahuje bezpečností prvky i průvodce pro připojení čtečky či provedení identifikace.

Funkčnost aplikací a ověření identifikačních funkcí byla testována na operačním systému Windows 10 a mobilním zařízením s verzí Android 8.1. Byla použita čtečka čipových karet ACS ACR 3901 U-S1, která nabízí podporu pro obě uvedené platformy. Samozřejmostí byl i občanský s novým čipem vydaný po 1. 7. 2018 a aktivovanou identifikační funkcí.

U aplikace eObčanka na Windows byl úspěšně ověřen zdroj instalačního balíčku. Instalace jednotlivých komponent do PC proběhla bez problému. Aplikace eObčanka - identifikace určená pro identifikaci nabízí mimo průvodce i nástroje pro diagnostiku identifikačních funkcí občanského průkazu či možnost kontaktování a odeslání provozních souborů pracovníkovi podpory. Aplikace pro správu karty je nepostradatelnou součástí, kterou lze spravovat jednotlivé bezpečnostní kódy a pracovat s kryptografickými klíči a certifikáty umožňující např. elektronické podepisování.

Aplikace pro mobilní zařízení s operačním systémem Android je dostupná přes oficiální obchod Google Play. Tato aplikace je určená pouze pro identifikaci z mobilního zařízení. Nabízí mimo jiné průvodce pro párování čtečky, informace o čtecím zařízení či nápovědu s užitečnými informacemi.

Práce s podpůrnými aplikacemi na obou platformách lze považovat za velmi přívětivou. Identifikační funkce byla ověřena přihlášením k Portálu občana a ePortálu ČSSZ. Požadavek pro identifikaci správně směřoval přes webové stránky NIA k tomu určeným. Identifikace proběhla na PC i na mobilním zařízení úspěšně.

Z výše získaných poznatků lze usoudit, že elektronizace a identifikace občana vůči státní správě České republiky jde správným směrem. Stát je na začátku cesty k plné elektronizaci svých služeb a má k tomu dostatečně silný nástroj v podobě zaručené identifikace a autentizace uživatele online služeb. Do budoucna se dá určitě počítat s rozšiřování jednotlivých služeb, které bude možné využít. Za bariéru lze považovat nutnost někdy i vyšších technologických dovedností od případného uživatele. Nedostatky lze pozorovat u mobilní platformy, kde jsou především vysoké pořizovací náklady na čtečky karet a jejich nedostupnost v ČR. Také nutnost koupit si čtečku čipových karet může být faktorem nevyužití funkcí eOP.

SEZNAM POUŽITÉ LITERATURY

[1] ROSMAN, Pavel a Ladislav BUŘITA. *Informatika pro ekonomy a manažery*. Vyd. 3., upr. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011. ISBN 978-80-7454-125-4.

[2] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, 2011. CZ.NIC. ISBN 978-80-904248-3-8.

[3] KRHOVJÁK, Jan a Václav MATYÁŠ. Autentizace a identifikace uživatelů. *Zpravodaj ÚVT MU*. 2007, (1), 1-5. ISSN 1212-0901.

[4] ROSMAN, Pavel. *Informatika pro ekonomy*. Vyd. 4., nezměn. Zlín: Univerzita Tomáše Bati ve Zlíně, 2008. ISBN 978-80-7318-738-5.

[5] Jak na Internet - Počítačová hesla. *Https://www.jaknainternet.cz/* [online]. Praha: CZ.NIC, 2019 [cit. 2019-03-25]. Dostupné z: https://www.jaknainternet.cz/page/1178/pocitacova-hesla/

[6] Nebojte se Internetu Bezpečná hesla - Nebojte se Internetu. *Nebojte se Internetu Viděli jste v televizi...* [online]. Praha: CZ.NIC, 2019 [cit. 2019-03-25]. Dostupné z: https://www.nebojteseinternetu.cz/page/3448/bezpecna-hesla/

[7] PUDIL, Roman. Single sign-on vs. synchronizace hesel. *Computerworld*. 2012, **2014**(19), 26.

[8] Biometric authentication (What is biometrics?) | 2019 Review - Gemalto. *Gemalto World leader in Digital Security* [online]. Gemalto NV, 2019 [cit. 2019-04-04]. Dostupné z: https://www.gemalto.com/govt/inspired/biometrics

[9] Biometrická data (Biometric Data) - ManagementMania.com. *Sociální síť pro business - ManagementMania.com* [online]. Wilmington: MANAGEMENTMANIA.COM LLC, c2011-2016 [cit. 2019-04-04]. Dostupné z: https://managementmania.com/cs/biometricka-data-biometric-data

[10] 10 biometrických technologií, které vás identifikují | VTM.cz. *VTM.cz – věda, technika, zajímavosti, budoucnost* [online]. Praha: CZECH NEWS CENTER a.s., 2019 [cit. 2019-04-04]. Dostupné z: http://vtm.e15.cz/aktuality/10-biometrickych-

technologii-ktere-vas-identifikuji

[11] Úvod do kryptografie. *EARCHIVACE* [online]. Česká republika: eArchivace, 2014 [cit. 2019-03-07]. Dostupné z: http://www.earchivace.cz/technologie/uvod-do-kryptografie/

[12] Encryption: Everything You Need to Know About Cryptography. *Mobile and Unity Software Development Company | Crysberry* [online]. Crysberry, 2018 [cit. 2019-03-07]. Dostupné z: https://crysberry.com/blog/facts-about-encryption-cryptography

[13] Symetrická kryptografie – Wikisofia. *Wikisofia* [online]. Praha: Univerzita Karlova v Praze, 2013 [cit. 2019-03-07]. Dostupné z: https://wikisofia.cz/wiki/Symetrick%C3%A1_kryptografie

[14] JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-731-8456-7.

[15] Proudová šifra. *Czech DBpedia – Česká DBpedia = strojově čitelná česká Wikipedie* [online]. Praha: Vysoká škola ekonomická v Praze, 2014 [cit. 2019-03-07]. Dostupné z: https://cs.dbpedia.org/page/Proudov%C3%A1_%C5%A1ifra

[16] Asymetrická kryptografie. *Univerzitní informační systém MENDELU* [online]. Brno, b.r. [cit. 2019-03-07]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7027

[17] Algoritmy kryptologie – Wikisofia. *Wikisofia* [online]. Praha: Univerzita Karlova v Praze, 2013 [cit. 2019-03-07]. Dostupné z: https://wikisofia.cz/wiki/Algoritmy_kryptologie

[18] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2., podstatně přeprac. a rozš. vyd., V nakl. Leges vyd. 1. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6.

[19] How Pretty Good Privacy works, and how you can use it for secure communication. *FreeCodeCamp.org* [online]. freeCodeCamp.org, b.r. [cit. 2019-03-08]. Dostupné z: https://medium.freecodecamp.org/how-does-pretty-good-privacy-work-3f5f75ecea97

[20] EIDAS: Elektronické značky a pečetě a rekviem za datovou zprávu - Lupa.cz.

Lupa.cz - server o českém Internetu [online]. Praha: Internet Info, c1998–2019 [cit. 2019-03-05]. Dostupné z: https://www.lupa.cz/clanky/eidas-elektronicke-znacky-a-pecete-a-rekviem-za-datovou-zpravu/

[21] BUDIŠ, Petr. *Elektronický podpis a jeho aplikace v praxi*. Olomouc: ANAG, 2008. Právo (ANAG). ISBN 978-80-7263-465-1.

[22] Občanský průkaz s čipem. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/

[23] 328/1999 Sb. Zákon o občanských průkazech. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Zlín: AION CS, c2010-2018 [cit. 2018-11-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/1999-328

[24] 250/2017 Sb. Zákon o elektronické identifikaci. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Zlín: AION CS, c2010-2018 [cit. 2018-11-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-250

[25] 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Zlín: AION CS, c2010-2018 [cit. 2018-11-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297

[26] 111/2009 Sb. Zákon o základních registrech. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Zlín: AION CS, c2010-2018 [cit. 2018-11-29]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-111

[27] Nařízení eIDAS – Cíle, nástroje, důsledky. In: *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, 2018 [cit. 2018-11-29]. Dostupné z: www.mvcr.cz/soubor/1-eidas-narizeni-eidas-cile-nastroje-dusledky.aspx

[28] Interoperabilita - ManagementMania.com. *Sociální síť pro business - ManagementMania.com* [online]. Wilmington: MANAGEMENTMANIA.COM LLC, c2011-2016 [cit. 2018-11-29]. Dostupné z: https://managementmania.com/cs/interoperabilita

[29] Kde je možné se přihlásit. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/sep/

[30] Portál národního bodu. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/portal/

[31] Portál občana - Přihlášení. *Portál veřejné správy* [online]. Praha: Ministerstvo vnitra, 2018 [cit. 2018-11-29]. Dostupné z: https://obcan.portal.gov.cz/prihlaseni

[32] Přihlásit. *Státní ústav pro kontrolu léčiv* [online]. Praha: Státní ústav pro kontrolu léčiv, 2010 [cit. 2018-11-29]. Dostupné z: https://pacient.erecept.sukl.cz/suklerp/Account/Login?ReturnUrl=%2fsuklerp%2fPacient%2f

[33] ČSSZ - ePortál. *ČSSZ - ePortál* [online]. Praha: Česká správa sociálního zabezpečení, 2018 [cit. 2018-11-29]. Dostupné z: https://eportal.cssz.cz/web/portal/uvodem

[34] Daňový portál : Vstupní stránka - expert. *Daňový portál* [online]. Praha: Generální finanční ředitelství, 2018 [cit. 2018-11-29]. Dostupné z: http://adisepo.mfcr.cz/adistc/adis/idpr_pub/epo2_info/podani_nia.faces

[35] VITAKARTA, mVITAKARTA a VITAKARTA+ | Oborová zdravotní pojišťovna. *Vítejte | Oborová zdravotní pojišťovna* [online]. Praha: Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví (207), 2019 [cit. 2019-03-28]. Dostupné z: https://www.ozp.cz/pro-klienty/vitakarta-online

[36] *Úvodní strana | Portal Občana* [online]. Česká Lípa: DATRON, a.s., 2019 [cit. 2019-03-28]. Dostupné z: https://obcan.mupe.cz/obcan/

[37] O portálu Občana | Portal Občana. *Úvodní strana | Portal Občana* [online]. Česká Lípa: DATRON, a.s., 2019 [cit. 2019-03-28]. Dostupné z: https://obcan.ricany.cz/obcan/o_portalu_obcana

[38] EPortál | VERA, spol. s.r.o. *Chotěboř: Titulní stránka* [online]. Praha: WEBHOUSE, s.r.o., 2012 [cit. 2019-04-01]. Dostupné z:

https://portal.chotebor.cz/portal/mujportal.html

[39] Kódy pro ochranu občanského průkazu. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/OchranneKody.aspx

[40] Čtečky karet pro připojení k PC. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/CteckyKaret.aspx

[41] Čtečky karet pro připojení k mobilnímu telefonu. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/CteckyMobil.aspx

[42] Podmínky použití občanského průkazu se strojově čitelnými údaji a s kontaktním elektronickým čipem pro účely elektronické identifikace a doporučená bezpečnostní opatření - Ministerstvo vnitra České republiky. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, 2018 [cit. 2018-11-29]. Dostupné z: https://www.mvcr.cz/clanek/podminky-pouziti-obcanskeho-prukazu-se-strojove-citelnymi-udaji-a-s-kontaktnim-elektronickym-cipem-pro-ucely-elektronicke-identifikace-a-doporucena-bezpecnostni-opatreni.aspx?q=Y2hudW09Mg%3d%3d

[43] Ověřené čtečky, které fungují s eObčankami: testujeme a doplňujeme – Živě.cz. In: *Živě.cz – O počítačích, IT a internetu* [online]. Praha: CZECH NEWS CENTER, 2018 [cit. 2018-11-29]. Dostupné z: https://www.zive.cz/clanky/eobcanka-ctecka/sc-3-a-194572/default.aspx#part=1

[44] Informační portál k národnímu bodu. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/Download/

[45] Bluetooth Reader | FEITIAN. *Security Hardware and Solution Provider for PKI token,One Time Password (OTP),Software Protection Dongle,Smart Card,Reader and Mobile Solution for Payment | FEITIAN* [online]. Beijing: FEITIAN Technologies, 2018 [cit. 2018-11-29]. Dostupné z: https://www.ftsafe.com/onlinestore/product?id=15

[46] EObčanka dostala aplikace pro Android, Linux a macOS. K telefonu potřebujete speciální čtečku – Živě.cz. In: *Živě.cz – O počítačích, IT a internetu* [online]. Praha: CZECH NEWS CENTER, 2018 [cit. 2018-11-29]. Dostupné z: https://www.zive.cz/clanky/eobcanka-dostala-aplikace-pro-android-linux-a-macos-k-telefonu-potrebujete-specialni-ctecku/sc-3-a-195741/default.aspx

[47] Jak začít využívat identifikační funkci občanského průkazu. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/IdentifikaceJakZacit.aspx

[48] Zprovoznění aplikací eObčanka na PC. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/InstalacePC.aspx

[49] Instalace aplikací eObčanka v prostředí macOS. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2019-03-25]. Dostupné z: https://info.eidentita.cz/eop/InstalacemacOS.aspx

[50] Ověření integrity a původu instalačního balíčku. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/IntegritaPuvodSW.aspx

[51] UzivatelskaPrirucka_Identifikace_Windows.pdf. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/download/UzivatelskaPrirucka_Identifikace_Windows.pdf

[52] Elektronická identifikace pomocí občanského průkazu. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/Identifikace.aspx

[53] Aplikace eObčanka - Správce karty. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/SpravceKarty.aspx

[54] Ovladače pro podporu práce s certifikáty. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/OvladaceKarty.aspx

[55] UzivatelskaPrirucka_SpravceKarty_Windows.pdf. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/Download/UzivatelskaPrirucka_SpravceKarty_Windows.pdf

[56] SDK pro podepisování z mobilních aplikací. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2019 [cit. 2019-04-09]. Dostupné z: https://info.eidentita.cz/eop/MobilniSDK.aspx

[57] EObčanka pro Android a iOS. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/Download/UzivatelskaPrirucka_eObcanka_Mobil.pdf

[58] Zprovoznění aplikace eObčanka na mobilním telefonu. *Elektronická identita - informační web* [online]. Praha: Správa základních registrů, 2018 [cit. 2018-11-29]. Dostupné z: https://info.eidentita.cz/eop/InstalaceMobil.aspx

[59] Portál občana nově upozorní na propadající doklady. Řidiči se podívají na své body | info.cz. *Info.cz - Česko, svět, politika, zpravodajství, analýzy, události, byznys* [online]. Praha: CZECH NEWS CENTER a.s., c2001-2019 [cit. 2019-05-08]. Dostupné z: https://www.info.cz/pravo/portal-obcana-nove-upozorni-na-propadajici-doklady-ridici-se-podivaji-na-sve-body-41270.html

[60] Přes 5,5 milionu Čechů bude moci mít ”digitální občanku” pro komunikaci s úřady, vznikne z bankovních dat | Hospodářské noviny (IHNED.cz). *Hospodářské noviny - byznys, politika, názory (IHNED.cz)* [online]. Praha: Economia, a.s., c1996-2019 [cit. 2019-05-09]. Dostupné z: https://domaci.ihned.cz/c1-66544770-pres-5-5-milionu-cechu-bude-moci-diky-digitalni-obcance-komunikovat-s-urady-online-k-prihlasovani-pouziji-bankovni-identitu

[61] Ke komunikaci se státem i uzavírání smluv bude stačit pouhé přihlášení k internetovému bankovnictví | eGOVERNMENT NETWORK NEWS. *EGOVERNMENT NETWORK NEWS* [online]. Manchester – Salford: AVERIA LTD., b.r. [cit. 2019-05-09]. Dostupné z: https://www.egov-nn.com/ke-komunikaci-se-statem-i-uzavirani-smluv-bude-stacit-pouhe-prihlaseni-k-internetovemu-bankovnictvi/

[62] Hackathon odkryl nedostatky u projektu eObčanka. *EGOVERNMENT NETWORK NEWS* [online]. Manchester – Salford: AVERIA LTD., b.r. [cit. 2019-05-09]. Dostupné z: https://www.egov-nn.com/hackathon-odkryl-nedostatky-u-projektu-eobcanka/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
BOK	Bezpečnostní osobní kód
CCID	Chip Card Interface Device
ČSSZ	Česká správa sociálního zabezpečení
DES	Data Encryption Standard
DNA	Deoxyribonucleic Acid
DOK	Deblokační osobní kód
DSA	Digital Signature Algorithm
ECC	Eliptic Curve Cryptography
eIDAS	eID And Signature
eOP	Elektronický občanský průkaz
IDEA	International Data Encryption Algorithm
IOK	Identifikační osobní kód
MAC	Media Access Control
NIA	Národní identitní autorita
OZP	Oborová zdravotní pojišťovna
PC	Personal Computer
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PUK	PIN Unblocking Key
QPIN	PIN pro kvalifikované elektornické podpisy
RC	Ron's Code, Rivest Cypher
SDK	Software Development Kit
SHA	Secure Hashing Algorithm
SIM	Subscriber Identity Module

SMS	Short message service
SSO	Single sign-on
USB	Universal Serial Bus
WHQL	Microsoft Windows Hardware

SEZNAM OBRÁZKŮ

Obr. 1 – Činnosti autentizačního protokolu [1] 11
Obr. 2 – Princip symetrického šifrování [1] 15
Obr. 3 – Princip asymetrického šifrování [1] 17
Obr. 4 – Ověření pravosti digitálního podpisu [1] 18
Obr. 5 – Přihlašování pomocí NIA 27
Obr. 6 – Úvodní stránka Portálu občana po přihlášení 28
Obr. 7 – Hierarchie a členění přístupových kódů [39] 32
Obr. 8 – Gemalto Safe Net Reader CT1100 [43] 35
Obr. 9 – Gemalto IDBridge CT710 [43] 35
Obr. 10 – USB Contact Smart Chip Card [43] 36
Obr. 11 – +ID [43] 36
Obr. 12 – Cherry TC 1100 [43] 36
Obr. 13 – ACS ACR 3901 U-S1 [41] 38
Obr. 14 – Feitian bR301 BLE – c45 [41] 38
Obr. 15 – Instalované komponenty aplikace eObčanka [48] 40
Obr. 16 – Proces elektronické identifikace pomocí eOP [52] 41
Obr. 17 – Podrobnosti digitálního podpisu instalačního balíčku eObčanka 45
Obr. 18 – Certifikát instalačního balíčku eObčanka 45
Obr. 19 – Průvodce instalace eObčanka 46
Obr. 20 – Licenční ujednání aplikace eObčanka 47
Obr. 21 – Vytvoření zástupců aplikace eObčanka 47
Obr. 22 – Průběh instalace aplikace eObčanka 48
Obr. 23 – Zástupci aplikací na pracovní ploše 48
Obr. 24 – Dokončení instalace aplikace eObčanka 49
Obr. 25 – Diagnostika identifikační funkce - nepřipojená čtečka 50
Obr. 26 – Diagnostika identifikační funkce - není vložen eOP 50
Obr. 27 – Diagnostika identifikační funkce - úspěšná diagnostika 51
Obr. 28 – O aplikaci eObčanka - identifikace 52
Obr. 29 – Nastavení aplikace eObčanka - identifikace 52
Obr. 30 – Formulář podpory aplikace eObčanka - identifikace 53
Obr. 31 – Okno aplikace eObčanka – Správce karty 54
Obr. 32 – Informace o čtečce v aplikaci eObčanka – Správce karty 55

Obr. 33 – Informace o čipové kartě v aplikaci eObčanka – Správce karty 56
Obr. 34 – Informace o IOK v aplikaci eObčanka – Správce karty 57
Obr. 35 – Oznámení o nepřipojení čtečky v aplikaci eObčanka - identikace 58
Obr. 36 – Oznámení o nevložení eOP v aplikaci eObčanka - identifikace 58
Obr. 37 – Oznámení o vložení eOP v aplikaci eObčanka - indentifikace 59
Obr. 38 – Zadání IOK v aplikaci eObčanka - identifikace 59
Obr. 39 – Oznámení o dokončení identifikace v aplikaci eObčanka - identifikace 60
Obr. 40 – Vypršení časového limitu v aplikaci eObčanka - identifikace 61
Obr. 41 – Udělení souhlasu o poskytování údajů 61
Obr. 42 – Přidání čtečky (vlevo), výběr výrobce čtečky (uprostřed) a oprávnění k poloze (vpravo) v mobilní aplikaci eObčanka 63
Obr. 43 – Výzva k zapnutí Bluetooth (vlevo), zjišťování polohy (uprostřed) a seznam připojených čteček (vpravo) v mobilní aplikaci eObčanka 64
Obr. 44 – Spojení se čtečkou (vlevo) a zadání IOK (vpravo) v mobilní aplikaci eObčanka 65
Obr. 45 – Zrušení procesu (vlevo) a úspěšná identifikace (vpravo) v mobilní aplikaci eObčanka 66

SEZNAM TABULEK

Tab. 1 – Funkce a využití kódů eOP 30
Tab. 2 – Omezení přístupových kódů 31
Tab. 3 – Nastavení a odblokování přístupových kódů 31
Tab. 4 – Ověřené čtečky čipových karet pro PC dle serveru Živě.cz 34
Tab. 5 – Cena, dostupnost v ČR a kompatibilita podporovaných čteček 37