ŠOLSKI CENTER VELENJE

ELEKTRO IN RAČUNALNIŠKA ŠOLA

Trg mladosti 3, 3320 Velenje

MLADI RAZISKOVALCI ZA RAZVOJ SAŠA REGIJE

RAZISKOVALNA NALOGA

ALTERNATIVNE UPORABE BIOMETRIČNIH OSEBNIH IZKAZNIC

Tematsko področje:

Računalništvo

Avtor:

Anže Maj Blagus

Mentor:

Samo Železnik, inž.

Velenje, 2022/2023

Raziskovalna naloga je bila opravljena na ŠC Velenje, na Elektro in računalniški šoli, 2023.

Mentor: Samo Železnik, inž.

Datum predstavitve: marec 2023

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

ŠD Elektro in računalniška šola Velenje, šolsko leto 2022/2023

KG osebna izkaznica/eMRTD/biometrična osebna izkaznica

AV BLAGUS, Anže

SA ŽELEZNIK, Samo

KZ 3320 Velenje, Trg mladosti 3

ZA ŠC Velenje, Elektro in računalniška šola, 2023

LI 2022/2023

IN ALTERNATIVNE UPORABE BIOMETRIČNIH OSEBNIH IZKAZNIC

TD Raziskovalna naloga

OP

IJ SL

JI sl/en

AI V tej raziskovalni nalogi sem raziskoval uporabo in delovanje novih biometričnih osebnih izkaznic, ki so jih upravne enote v Sloveniji začele izdajati 28. marca leta 2022. Te izkaznice so naprednejše kot navadne osebne izkaznice, saj vsebujejo čip, ki omogoča elektronsko potrjevanje identitete, digitalno podpisovanje z uporabo kvalificiranih potrdil in elektronsko avtentikacijo. V teoretičnem delu raziskovalne naloge sem predstavil tehnologije, ki so osnova za delovanje biometričnih osebnih izkaznic, njihovo delovanje ter uporabo pri novih izkaznicah. Predstavil sem tudi tehnologije, ki sem jih uporabil za izdelavo aplikacije v drugem delu raziskovalne naloge ter mobilno aplikacijo eOsebna, ki jo je vzporedno z novimi biometričnimi izkaznicami država izdala za uporabo prav teh. V praktičnem delu sem izdelal aplikacijo, ki prikaže uporabo novih izkaznic na praktičnem primeru ter opisal njeno delovanje.

KEY WORDS DOCUMENTATION

ND Elektro in računalniška šola, šolsko leto 2020/2021

CX identification card/eMRTD/travel document/biometric travel documents

AU BLAGUS, Anže

AA ŽELEZNIK, Samo

PP 3320 Velenje, Trg mladosti 3

PB ŠČ Velenje, Elektro in računalniška šola, 2023

PY 2022/2023

TI ALTERNATIVE USES OF BIOMETRIC IDENTIFICATION CARDS

DT RESEARCH WORK

NO

LA SL

AL sl/en

AB In this research work, I explored the uses and functionality of the new biometric identity cards, which the Slovenian government began to issue on March 28, 2022. The new biometric ID cards have a chip that allows for electronic identification, digital signing, and electronic authentication. In the theoretical part of the work, I presented the technologies behind the operation of biometric identity cards, their inner workings, and use in the new cards. I also explained the technologies that I used to implement the applications in the second part of the research assignment. In the practical part, I created an application that demonstrates the use of the new cards on a practical example and described its operation.

KAZALO KRATIC

angl. – angleško

MRTD – (angl. Machine readable travel document); strojno berljive potovalne listine
MRZ – (angl. Machine readable zone); strojno berljivo območje
GPS – (angl. Global Positioning System); globalni sistem za določanje položaja
ISO - (angl. International Organization for Standardization); Mednarodna organizacija za standardizacijo
ML - (angl. Machine Learning); strojno učenje
PIN - (angl. Personal identification number); osebna identifikacijska številka
PUK - (angl. Personal unblocking key); osebni ključ za deblokiranje
SOD - (angl. Document Security Object); varnostni objekt za dokumente

KAZALO VSEBINE

KAZALO SLIK

KAZALO KODE

1 UVOD

Osebe izkaznice so preprost način identifikacije, ki se je v preteklosti izkazal za zadovoljivega, toda z razvojem tehnologije se je pojavila možnost izboljšave. Z 28. marcem leta 2022 so upravne enote po Sloveniji začele izdajati biometrične osebne izkaznice, ki poleg delovanja kot navadna osebna izkaznica, ponujajo dodatne funkcionalnosti prek čipa, ki je v njih. V sklopu te raziskovalne naloge sem se odločil raziskati možnosti uporabe teh izkaznic tudi zunaj področja identifikacije.

1.1 Hipoteze raziskovalne naloge

Zastavil sem naslednje hipoteze:

1. Biometrične osebne izkaznice podpirajo komunikacijo z namenskimi aplikacijami.
2. Biometrične osebne izkaznice je mogoče uporabiti za namene poleg identifikacije.
3. Mogoče je preveriti, da so podatki na biometrični osebni izkaznici veljavni in resnični.
4. Na biometrične osebne izkaznice ni mogoče pisati neresničnih podatkov.

2 PREGLED OBJAV

V tem poglavju so predstavljene tehnologije, standardi in koncepti, ki so bili uporabljeni tekom raziskovanja in izdelave aplikacije za to raziskovalno nalogo.

2.1 Biometrične osebne izkaznice

Biometrične osebne izkaznice so v primerjavi z navadnimi vizualno spremenjene in varnostno nadgrajene. Vsebujejo vse elemente navadne osebne izkaznice (osebne podatke, številko izkaznice, potrebne simbole), poleg pa tudi nove elemente, ki so bolj podrobno opisani v nadaljevanju.
Nove biometrične osebne izkaznice bo mogoče uporabljati tudi v sistemu zdravstvenega zavarovanja. [1]

2.1.1 QR-koda

QR koda (ang. Quick Response code) je dvodimenzionalna koda, ki vsebuje informacije v obliki črnih kvadratov, ki so razporejeni v matriki na beli podlagi. QR koda je podobna črtni kodi, vendar ima večjo kapaciteto za shranjevanje podatkov. Primer QR kode vidimo na: Slika 1.

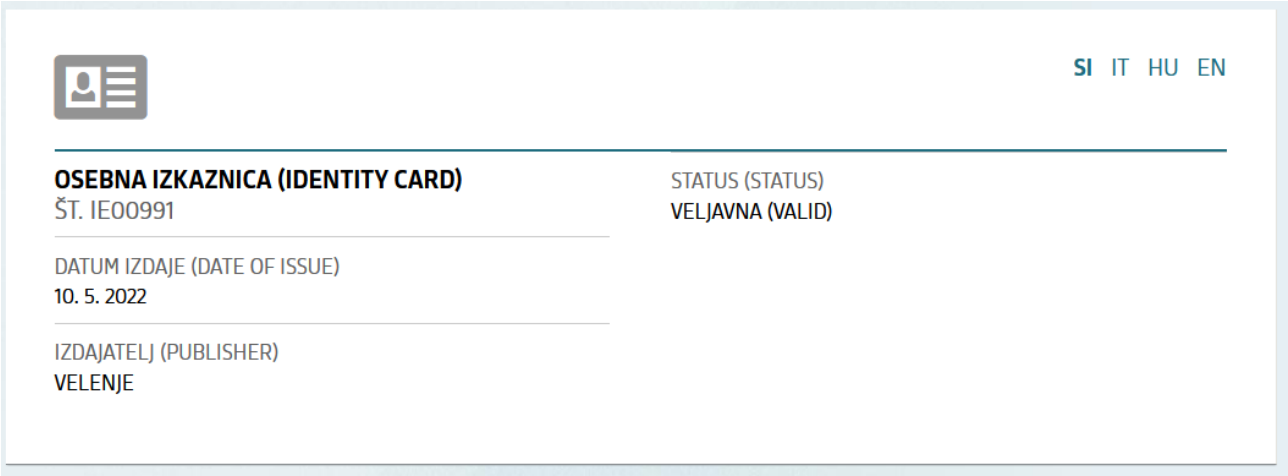
Slika 1: Primer QR kode

QR kodo lahko preberemo s pomočjo mobilne naprave, ki ima vgrajeno kamero in ustrezno aplikacijo za branje QR kod. Ko uporabnik s kamero mobilne naprave usmeri na QR kodo, aplikacija prebere kodo in dekodira vsebino, ki je shranjena v njej Vsebina QR kode se lahko razlikuje od spletnih naslovov, besedilnih sporočil, telefonskih številk,

GPS koordinat, e-poštnih naslovov in drugih podatkovnih zapisov.

Na novi biometrični izkaznici je natisnjena QRkoda, ki omogoča preverjanje veljavnosti izkaznice na portalu eUprava. Ob skeniranju nam portal prikaže naslednje podatke (vidne tudi na: Slika 2):

- številko osebne izkaznice
- datum izdaje osebne izkaznice
- mesto izdaje
- status veljavnosti



Slika 2: Podatki o izkaznici na portalu eUprava

2.1.2 Čip

V novo osebno izkaznico je vgrajen čip tipa NXP P71 z operacijskim sistemom JCOP 4 podjetja NXP. Na čipu so shranjeni biometrični podatki in sicer slika obraza in dva prstna odtisa, kvalificirano potrdilo za elektronski podpis ter dve sredstvi elektronske identifikacije (z visoko in nizko ravnjo zanesljivosti).

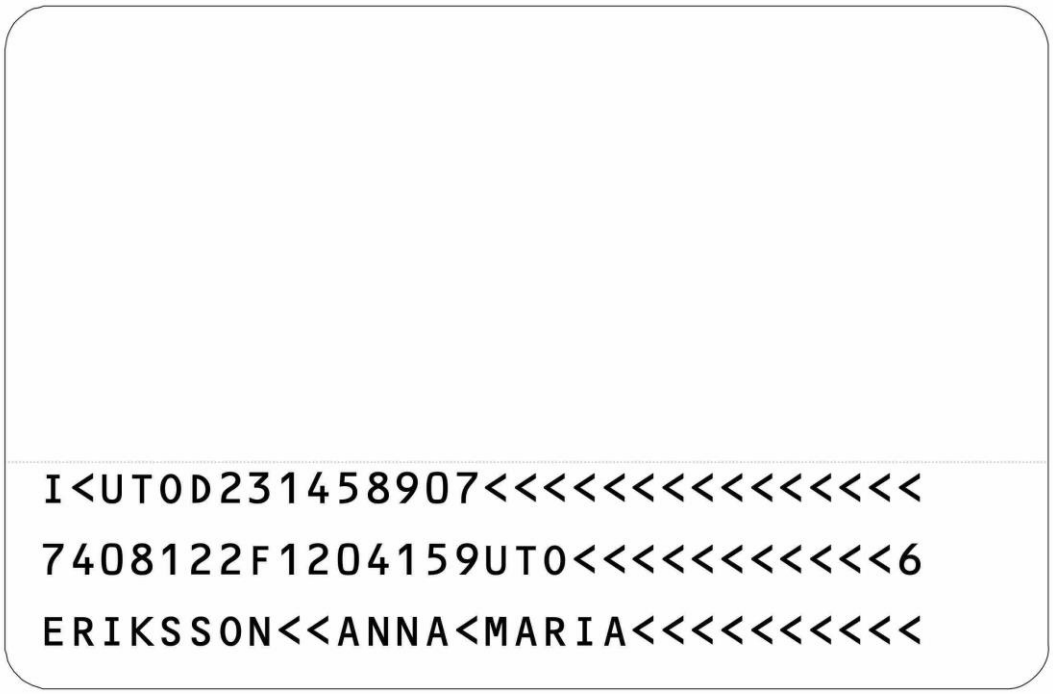
Posameznikova fotografija je na čipu shranjena v formatu JPEG2000, prstna odtisa pa v formatu WSQ (Wavelet Scalar Quantization). Podrobnejši pregled formata njihovega shranjevanja prstih odtisov je izven obsega te naloge.

Kvalificirano potrdilo za elektronski podpis in potrdilo visoke ravni zanesljivosti sta

zaščitena z uporabniškim geslom, ki ga uporabnik nastavi z začetnim geslom (visoka raven zanesljivosti), dostop do elektronske identifikacije z nizko ravnjo pa je mogoč brez posebne avtentikacije (z nizko ravnjo zanesljivosti). [2]
Za pregled biometričnih podatkov je sistem avtentikacije ločen in sicer zahteva naslednje podatke: številko osebnega dokumenta, datum poteka dokumenta ter datum rojstva.
Po avtentikaciji s čipom je na voljo datoteka SOD (angl. Security Object for the Document), ki vsebuje povzetke (angl. hashes) vseh dokumentov na čipu, ki so digitalno podpisani z državnim ključem. S tem je zagotovljena pristnost vseh podatkov na čipu in onemogočeno spreminjanje prav teh, torej so biometrični podatki na čipu verodostojni in resnični.

2.1.3 Machine Readable Travel Documents

Standard Machine Readable Travel Documents (MRTD) je mednarodni standard za izdajanje potnih listov in ostalih dokumentov, ki ga določa Mednarodna organizacija civilnega letalstva (ICAO). MRTD določa način zapisa podatkov, kot so: tip dokumenta, ime, številka dokumenta, datum rojstva, spol, datum izdaje dokumenta, datum poteka dokumenta. Ti podatki so zapisani v MRZ – strojno berljivem območju (angl. Machine Readable Zone), kar omogoča standardizirano branje in procesiranje teh podatkov z uporabo računalnikov.



Slika 3: Primer MRZ

MRZ na osebnih izkaznicah je zgrajen iz 3 vrstic. Naslednja razlaga temelji na primeru iz: Slika 3.

Prva vrstica vsebuje tip dokumenta (»I«), državo, ki je dokument izdala (»UTO« – Utopija), številko dokumenta (»D23145890«) ter kontrolno vrednost (»7«).

Druga vrstica vsebuje datum rojstva (»740812« – 12.8.1974), kontrolno vrednost (»2«), spol osebe (»F« – ženski), datum poteka dokumenta (»120415« – 15.4.2012) še eno kontrolno vrednost (»9«) ter državljanstvo osebe (»UTO«).

Zadnja vrstica vsebuje ime in priimek osebe.

Deseti del standarda MRTD ga razširi in doda določila za elektronske biometrične dokumente. Določa način shranjevanja biometričnih in ostalih podatkov ter standarde, ki določajo komunikacijo s čipom (ISO/IEC 7816-4 in ISO/IEC 7816-8). [3] [4]

2.1.4 Java Card

Čip in operacijski sistem na njem, ki sta uporabljena v novih biometričnih osebnih izkaznicah sledita specifikaciji Java Card. To je tehnologija, ki omogoča ustvarjanje aplikacij za pametne kartice, torej v okoljih, kjer je količina spomina in procesorske moči zelo mala.

Ponuja podnabor programskega jezika Java, ki omogoča razvoj aplikacij, kot so identifikacijske kartice, bančne kartice, kartice za vstop na območja z omejenim dostopom, prevozne kartice in aplikacije za ostale namene. [5]https://www.oracle.com/java/technologies/java-card/javacard1.html

2.1.5 ISO 7816

Standard ISO 7816 je razdeljen na več delov, v nadaljevanju je povzetih prvih pet:

1. Fizične karakteristike, ki definirajo dimenzije kartic, njihovo odpornost na statično elektriko, elektromagnetno sevanje in mehanični stres, prav tako pa lokacijo magnetičnega pasu na kartici.
2. Dimenzije in lokacije kontaktov, ki definirajo lokacijo, namen in električne značilnosti kovinskih kontaktov na kartici.
3. Električni signali in prenosni protokoli, ki definirajo napetostne in tokovne zahteve, ki jim morajo slediti kontakti, najbolj pomembno pa protokola (T=0 in T=1) za komunikacijo s čipom.
4. Ukazi za izmenjavo, ki določajo standardne ukaze za izmenjavo podatkov s čipom. Ti ukazi omogočajo dostop do podatkov na čipu, varnost in prenos podatkov.
5. Sistem številčenja in postopek registracije aplikacijskih identifikatorjev, ki postavi standard za t.i. aplikacijske identifikatorje.

[6]

APDU History

Cla...	INS	P1	P2	P3/...	Len	Data (Hex)	SW	Response (verbose)	Data Out (Hex)	Data Out (String)	Full Response (Hex)
00	B0	00	00	00	00		69 86	Command not allowed (no c...			69 86
00	84	00	00		08		90 00	No further qualification	CB 87 30 2E 2E 1A 10 F0	..0.....	CB 87 30 2E 2E 1A 10 F0 90 ...
00	84	00	00		10		90 00	No further qualification	F1 F7 2B 52 8A 5E C4 19 61 ...	..+R.^..a$<|....	F1 F7 2B 52 8A 5E C4 19 61 ...
00	B2	00	00		10		6A 86	Incorrect parameters P1-P2			6A 86
00	CA	00	00		10		69 82	Security status not satisfied			69 82

Slika 4: Komunikacija s čipom

Primer komunikacije med čitalcem in kartico vidimo na: Slika 4.

2.2 Tehnologije za aplikacijo

V tem poglavju so opisane tehnologije, ki se tičejo izdelave aplikacije, ki deluje z novimi biometričnimi osebnimi izkaznicami.

2.2.1 NFC

NFC (Near Field Communication) je skupek komunikacijskih protokolov, ki omogoča bližnji dvosmerni prenos podatkov med napravami, ki se nahajajo v bližini ena druge (na razdalji do 4 cm).

Uporabljen je za razne namene, vse od brezkontaknega plačevanja na blagajni do deljenja kontaktov med telefoni.

Za komunikacijo uporablja visokofrekvenčno polje (1,56 MHz). Komunikacija poteka med dvema napravama, »pobudnikom« ter »tarčo«. Pobudnik ustvari radiofrekvenčno polje, ki napaja tarčo, kar omogoča, da je lahko tehnologija NFC uporabljena tudi v napravah, ki nimajo lastnega napajanja.

2.2.2 Java

Java je visokonivojski, objektno orientiran programski jezik, ki je bil razvit v 90. letih prejšnjega stoletja pri podjetju Sun Microsystems (sedaj v lasti Oracle Corporation). Java se izvaja na virtualnem stroju Java (Java Virtual Machine – JVM), kar omogoča, da so Java aplikacije prenosljive na različne platforme, kot so Windows, Mac OS X, Linux in celo vgrajeni sistemi, kot so čipi na pametnih karticah.

2.2.3 JMRTD

JMRTD (Java Machine Readable Travel Documents) je odprtokodna knjižnica za

programski jezik Java, ki omogoča branje in pisanje MRTD (Machine Readable Travel Documents).
Omogoča razvoj aplikacij za branje in pisanje podatkov iz biometričnih potnih listov in osebnih izkaznic, kot so fotografije in prstni odtisi. Knjižnica podpira različne protokole (Basic Access Control – BAC, Extended Access Control – EAC), ki zagotavljajo varno komunikacijo med bralnikom in čipom. Poleg tega podpira tudi različne standardizirane formate, kot so ISO 7816, ISO 14443 in ISO 19794, kar omogoča splošno uporabo za MRTD različnih držav.

2.2.4 Regularni izrazi

Regularni izrazi (tudi regex ali regexp) so zapisi, ki opisujejo vzorce znakov, ki se ujemajo s skupino besedilnih nizov. Regex se uporabljajo za iskanje in/ali zamenjavo določenih vzorcev znakov v besedilnih nizih.

Sestavljeni so iz znakov, ki predstavljajo določene vrste znakov ali znakovne skupine (npr. črke, številke, posebni znaki, itd.), kot tudi posebnih znakov, ki predstavljajo določene vzorce (npr. začetek ali konec besede, določeno število ponovitev, itd.).

Uporaba regularnih izrazov se pogosto uporablja v programiranju, urejevalnikih besedil in drugih aplikacijah, kjer je potrebno iskati, filtrirati ali zamenjati besedilne nize po določenem vzorcu.

Najpreprostejši primer uporabe regularnih izrazov je iskanje določene besede v besedilnem nizu. Na primer, če imamo besedilni niz "Danes je lep sončen dan", lahko uporabimo regex "sončen" za iskanje besede "sončen" v tem besedilnem nizu.

Mogoče je uporabiti tudi znake; kot na primer »*«, ki pomeni, da se prejšnji znak ponovi 0 ali večkrat ter ».«, ki nadomešča katerikoli znak. Recimo, da imamo besedilni niz "aaabbbccc". Če želimo poiskati vse vzorce, ki se začnejo z a in se končajo s c, lahko uporabimo regex "a.*c". Ta regex išče besedilne nize, ki se začnejo z a, vmes lahko

vsebujejo katerikoli znak (označen z zvezdico *) in se končajo s c.

2.2.5 ML Kit

ML Kit je knjižnica za strojno učenje (ang. machine learning), ki jo je razvilo podjetje Google. Knjižnica je namenjena razvijalcem mobilnih aplikacij, ki želijo v svoje aplikacije vključiti funkcionalnosti strojnega učenja, kot so prepoznavanje besedila, obrazov, objektov, barv in drugih elementov.

2.3 Obstoječe rešitve

V tem poglavju je opisanih nekaj aplikacij in programov, ki že delujejo z biometričnimi osebnimi izkaznicami.

2.3.1 Aplikacija eOsebna

Mobilna aplikacija eOsebna je bila izdana vzporedno z novimi osebnimi izkaznicami in omogoča:

- aktivacijo osebne izkaznice
- spremembo kode PIN
- odklepanje osebne izkaznice s kodo PUK
- pregled podatkov na izkaznici

2.3.2 IDProtect Client

Programska oprema IDProtect Client je namenjena uporabi nove osebne izkaznice s čitalnikom pametnih kartic na namiznih računalnikih. Podpira branje digitalnih potrdil iz osebne izkaznice, spreminjanje PIN kode kartice ter odklepanje kartice s kodo PUK.
Povzeto po [7].

2.3.3 ReadID Me

ReadID Me je zaprtokodna aplikacija podjetja Inverid, ki omogoča branje biometričnih podatkov iz osebnih izkaznic in potnih listov.
Deluje tako, da najprej z uporabo kamere prebere MRZ, potem pa se s prebranimi podatki

avtenticira s čipom (preko NFC) in prikaže prebrane podatke iz osebne. [8]

3 MATERIALI IN METODE DELA

Osnoven povod za izdelavo te raziskovalne naloge je bila ideja, da bi se izdelala uporabna aplikacija, ki bi bila sposobna preko NFC komunicirati z novimi biometričnimi izkaznicami.

Zaradi tega sem se najprej lotil raziskave obstoječih rešitev.

3.1 Izdelava aplikacije

Za problem oz. razlog za izdelavo aplikacije sem si izbral identifikacijo ob vozniškem izpitu, prav tako pa kot dodatno funkcionalnost beleženje ur med vožnjo v avtošolah. Ta problem bi res demonstriral uporabo in zmožnosti tehnologije.

3.1.1 Branje MRZ

Kot je bilo povedano v poglavju 2.1.2, se je pri branju biometričnih podatkov potrebno s čipom najprej avtenticirati in sicer s podatki o številki dokumenta, datumom poteka ter datumom rojstva osebe. Ročen vnos teh podatkov je v večini okoliščin, kjer bi uporabljali osebno izkaznico, nepraktičen, zato uporabimo strojno branje MRZ, kjer so vsi ti podatki zapisani.

Za branje MRZ uporabimo Googlovo knjižnico ML Kit, bolj podrobno TextRecognizer modul, s katerim iz kamere pridobimo tekst. Ta tekst po pridobitvi obdelamo s spodaj naštetimi regularnimi izrazi za posamezne vrstice v MRZ:

1. ([A-Z]{1})([A-Z<]{1})([A-Z<]{3})([A-Z0-9<]{9})([0-9]{1})([A-Z0-9<]{15})
2. ([0-9]{6})([0-9{1}])([MF]{1})([0-9]{6})([0-9]{1})([A-Z<]{3})([A-Z0-9<]{11})([0-9]{1})
3. ([A-Z]+)(<[A-Z]+){0,}<<([<]{0,})([A-Z]+)(<[A-Z]+){0,}(<.+){0,}

S tem preverimo, da se tekst, ki smo ga pridobili ujema s formatom MRZ, torej smo uspešno prebrali MRZ. Iz njega zatem izluščimo podatke, ki jih potrebujemo za BAC avtentikacijo, torej številko dokumenta, datum rojstva ter datum poteka dokumenta.

Slika?

3.1.2 Avtentikacija s čipom

Ko iz MRZ preberemo potrebne podatke, se je potrebno s čipom avtenticirati.

V aplikaciji se uporablja knjižnica JMRTD, ki olajša komunikacijo s čipom po določenih standardih in protokolih.

Za avtentikacijo potrebujemo tudi PACE varnostne informacije, katere najprej pridobimo iz kartice, za tem pa izvedemo BAC avtentikacijo. Ta proces je viden v: Koda 1.

```
BACKeySpec bacKey = new BACKey(passportNumber, birthDate, expirationDate);
(...)
CardAccessFile cardAccessFile = new CardAccessFile(
        service.getInputStream(PassportService.EF_CARD_ACCESS));
Collection<SecurityInfo> securityInfoCollection = cardAccessFile.getSecu-
rityInfos();
for (SecurityInfo securityInfo : securityInfoCollection) {
    if (securityInfo instanceof PACEInfo) {
        PACEInfo paceInfo = (PACEInfo) securityInfo;
        service.doPACE(bacKey, paceInfo.getObjectIdentifier(),
                PACEInfo.toParameterSpec(paceInfo.getParameterId()), null);
        paceSucceeded = true;
    }
}
```

Koda 1: BAC avtentikacija

3.1.3 Branje podatkov

Po avtentikaciji lahko iz kartice preberemo naslednje podatke:

- ime in priimek osebe
- spol osebe
- datum rojstva
- datum poteka osebne izkaznice
- številko dokumenta
- narodnost
- državo izdaje
- frontalno sliko osebe

Tudi branje naredimo z uporabo knjižnice JMRTD, in sicer beremo iz raznih, preddefiniranih dokumentov. V: Koda 2, na primer, vidimo branje MRZ podatkov (ki so

shranjeni tudi na čipu). Na enak način (iz drugih dokumentov) se preberejo še ostali podatki, vključno s sliko.

```
CardFileInputStream dg1In = service.getInputStream(PassportService.EF_DG1);
DG1File dg1File = new DG1File(dg1In);

MRZInfo mrzInfo = dg1File.getMRZInfo();
personDetails.setName(mrzInfo.getSecondaryIdentifier().replace("<", "
").trim());
personDetails.setSurname(mrzInfo.getPrimaryIdentifier().replace("<", "
").trim());
personDetails.setPersonalNumber(mrzInfo.getPersonalNumber());
personDetails.setGender(mrzInfo.getGender().toString());
personDetails.setBirthDate(DateUtil.convertFromMrzDate(mrzInfo.getDateOfBir
th()));
personDetails.setExpiryDate(DateUtil.convertFromMrzDate(mrzInfo.getDateOfEx
piry()));
personDetails.setSerialNumber(mrzInfo.getDocumentNumber());
personDetails.setNationality(mrzInfo.getNationality());
personDetails.setIssuerAuthority(mrzInfo.getIssuingState());
```

Koda 2: Branje kopije podatkov MRZ iz čipa

3.1.4 Uporaba podatkov

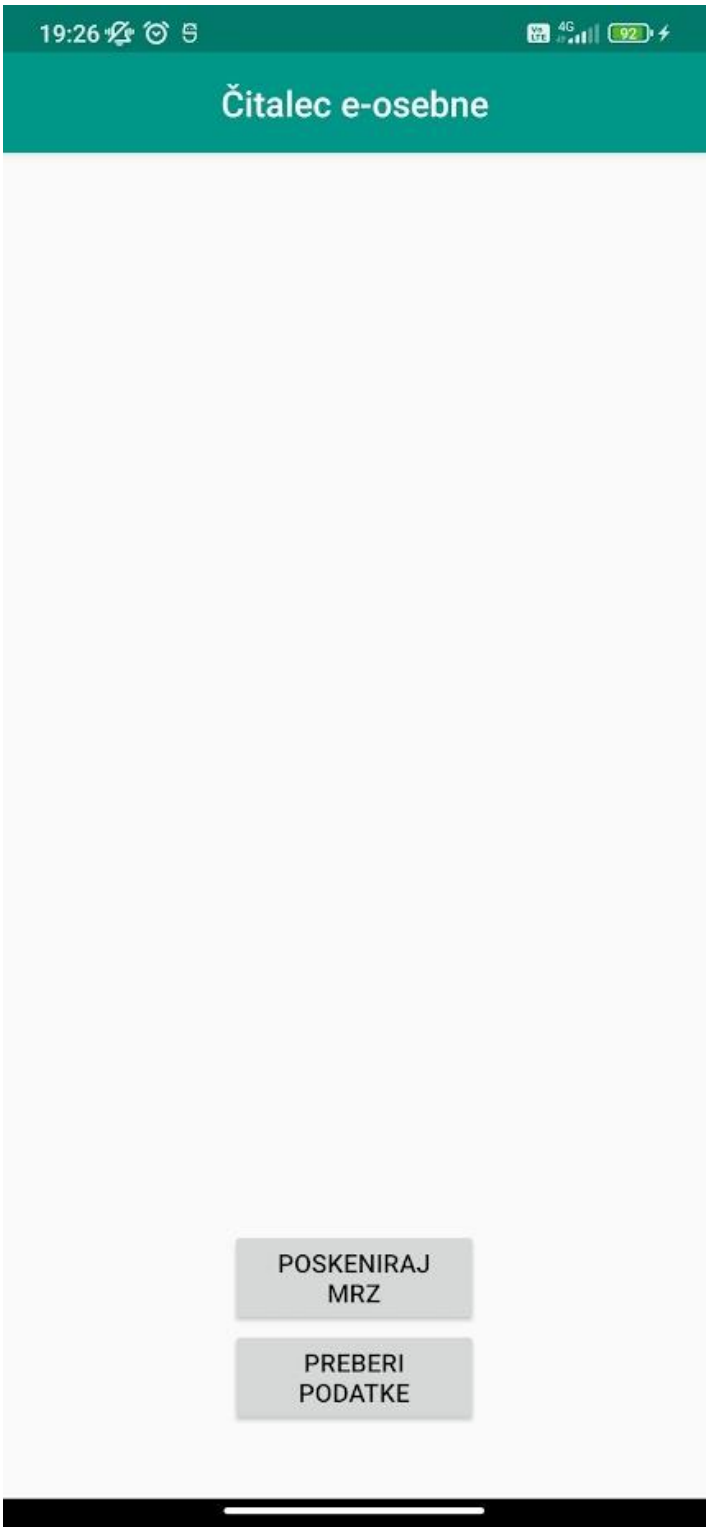
Po branju, ustvarimo povzetke (hashe) prebranih podatkov in jih primerjamo s hashi v t.i. SOD datoteki. Če so enaki, vemo, da so podatki verodostojni.

Zatem lahko podatke prikažemo in omogočimo uporabniku, da preveri verodostojnost dokumenta, ki mu je bil podan.

3.2 Prikaz delovanja aplikacije

V tem poglavju je predstavljeno delovanje aplikacije.

Po odprtju vidimo prvi ekran, prikazan na: Slika 5.

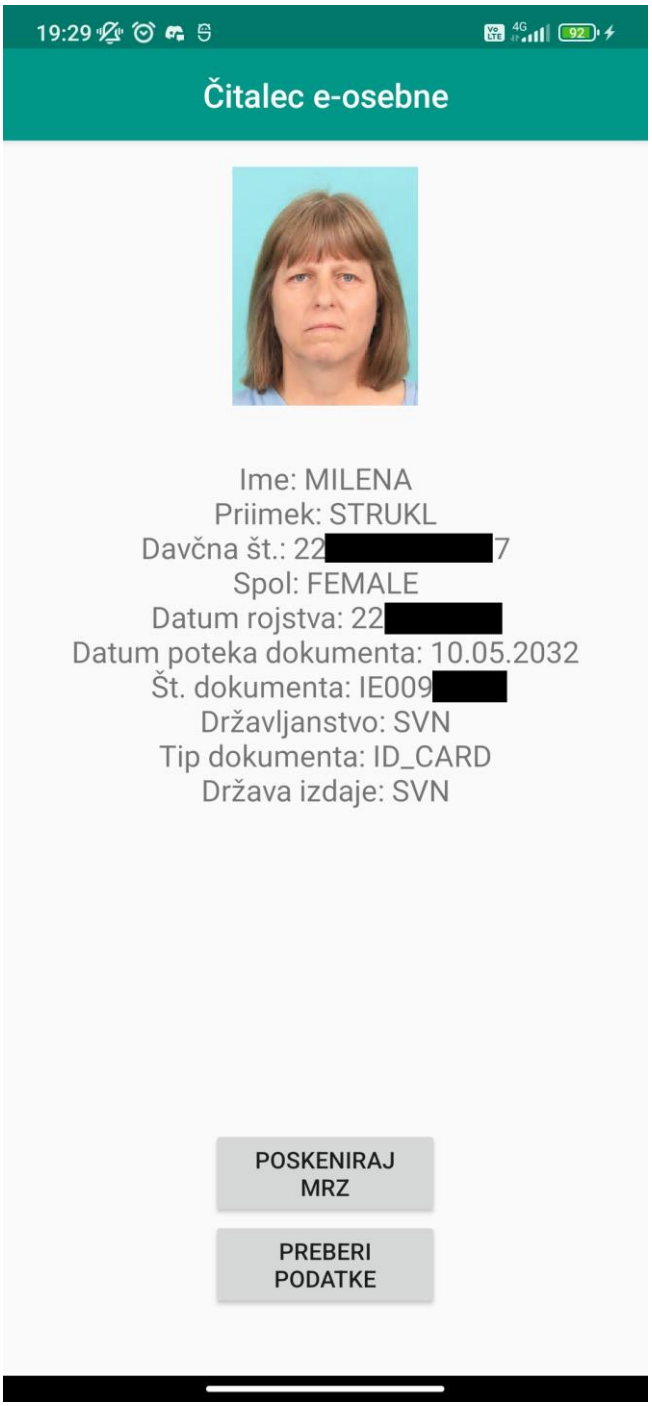


Slika 5: Prvi zaslon aplikacije

Po kliku na gumb »Poskeniraj MRZ« se nam odpre kamera, ki takoj ob zaznavanju pravilnega MRZ, to javi in se ponovno odpre 1. zaslon. Čitalec je viden na: Slika 6.

Slika 6: Čitalec MRZ

Zatem prislonimo k telefonu osebno izkaznico in po nekaj sekundah se nam izpišejo podatki, vidni na: Slika 7.



Slika 7: Prikaz podatkov

4 REZULTATI IN RAZPRAVA

1. **Biometrične osebne izkaznice podpirajo komunikacijo z namenskimi aplikacijami.**

To hipotezo sem potrdil, saj sem namensko aplikacijo tudi izdelal. Na spletu je dovolj informacij o standardih ter protokolih, na katerih delujejo biometrične osebne izkaznice, prav tako pa obstoječih knjižnic, da je mogoče izdelati namensko aplikacijo za lastno uporabo.

2. **Biometrične osebne izkaznice je mogoče uporabiti za namene poleg identifikacije.**

To hipotezo sem delno potrdil in delno ovrgel, saj bi za namene poleg identifikacije bili uporabni digitalni podpisi ter certifikati, dokumentacije za ta del delovanja biometričnih osebnih izkaznic pa nisem našel dovolj, da bi jo lahko potrdil.

3. **Mogoče je preveriti, da so podatki na biometrični osebni izkaznici veljavni in resnični.**

To hipotezo sem potrdil, saj je celotno delovanje poteka avtentikacije ter branja podatkov narejeno na tak način, da je mogoče preveriti njihovo veljavnost in resničnost. Vsi podatki na kartici so podpisani s privatnim ključem države, ki je zaupanja vreden, zato so spremembe nemogoče oz. vidne.

4. **Na biometrične osebne izkaznice ni mogoče pisati neresničnih podatkov.**

To hipotezo sem potrdil, saj pisanje neresničnih podatkov na čip ni mogoče, saj tega čip ne podpira oz. zahteve za pisanje podatkov zavrne. Pisanje po prvem (tovarniškem) nalaganju podatkov ni mogoče.

5 ZAKLJUČEK

To raziskovalno nalogo sem začel izdelovati brez kakršnegakoli predznanja na področju pametnih kartic in tehnologij.Mee je pa to področje zelo zanimalo. Tekom izdelave sem se pogosto poglobil v specifične standarde in tehnologije, prav tako pa sem njihovo

delovanje preizkusil. S tem sem dobil dejansko razumevanje teh tehnologij in vzporedno še izdelal to raziskovalno nalogo.

Bolj sem se poglobil v del izkaznic, ki ima opravka z biometričnimi podatki, ne pa prav veliko v del z digitalnimi potrdili, ki je pravzaprav bolj zanimiv za resnično uporabo. V nadaljevanju bi ta del definitivno bolj raziskal in se poglobil v njegovo delovanje.

6 POVZETEK

V tej raziskovalni nalogi sem raziskoval uporabo in delovanje novih biometričnih osebnih izkaznic, ki so jih upravne enote v Sloveniji začele izdajati 28. marca leta 2022. Te izkaznice so naprednejše kot navadne osebne izkaznice, saj vsebujejo čip, ki omogoča elektronsko potrjevanje identitete, digitalno podpisovanje z uporabo kvalificiranih potrdil in elektronsko avtentikacijo. V teoretičnem delu raziskovalne naloge sem predstavil tehnologije, ki so osnova za delovanje biometričnih osebnih izkaznic, njihovo delovanje ter uporabo pri novih izkaznicah. Predstavil sem tudi tehnologije, ki sem jih uporabil za izdelavo aplikacije v drugem delu raziskovalne naloge ter mobilno aplikacjo eOsebna, ki jo je vzporedno z novimi biometričnimi izkaznicami država izdala za uporabo prav teh. V praktičnem delu sem izdelal aplikacijo, ki prikaže uporabo novih izkaznic na praktičnem primeru ter opisal njeno delovanje.

7 ZAHVALA

Za pomoč pri izdelavi raziskovalne naloge se zahvaljujem:

- mentorju g. Samotu Železniku za nasvete in pomoč pri izdelavi raziskovalne naloge
- gospe dr. Nataši Meh Peer, prof. za lektoriranje raziskovalne naloge
- mami Mileni Štrukl, ki je s posojo svoje osebne izkaznice pripomogla k testiranju in raziskovanju delovanja biometričnih osebnih izkaznic

8 VIRI IN LITERATURA

[1] „Biometrična osebna izkaznica,“ [Elektronski]. Available: https://www.gov.si/teme/biometricna-osebna-izkaznica/. [Poskus dostopa 25 1 2023].

[2] „Brošura e-osebna,“ [Elektronski]. Available: https://www.gov.si/assets/ministrstva/MNZ/SOJ/Novice/2022/Biometricna-osebna-izkaznica/Brosura-BOI.pdf. [Poskus dostopa 21 2 2023].

[3] „ICAO,“ [Elektronski]. Available: https://www.icao.int/publications/documents/9303_p10_cons_en.pdf. [Poskus dostopa 25 1 2023].

[4] „MRTD,“ [Elektronski]. Available: https://docs.regulaforensics.com/fundamentals/machine-readable-travel-documents/. [Poskus dostopa 21 2 2023].

[5] „Java Card,“ [Elektronski]. Available: https://www.oracle.com/java/technologies/java-card/javacard1.html. [Poskus dostopa 21 2 2023].

[6] „Standardi za pametne kartice,“ [Elektronski]. Available: https://www.q-card.com/about-us/smart-card-standards/page.aspx?id=1461. [Poskus dostopa 21 2 2023].

[7] „Programska oprema IDProtect Client,“ [Elektronski]. Available: https://www.si-trust.gov.si/sl/eoi/programska-oprema-idprotect-client/. [Poskus dostopa 21 2 2023].

[8] „ReadID Me App,“ [Elektronski]. Available: https://www.inverid.com/readid-me-app. [Poskus dostopa 21 2 2023].