

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

ZAKLJUČNA STROKOVNA NALOGA VISOKE POSLOVNE ŠOLE
ANALIZA ELEKTRONSKE PAMETNE KARTICE

Ljubljana, maj 2019

JASMIN TRIČIČ

IZJAVA O AVTORSTVU

Podpisani Jasmin Tričič, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza elektronske pametne kartice, pripravljenega v sodelovanju s svetovalcem prof. dr. Alešem Groznikom

IZJAVLJAM

1. da sem predloženo delo pripravil samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtoric oziroma avtorjev, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;
7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne _____

Podpis študenta: _____

KAZALO

UVOD	1
1 PREDSTAVITEV OBSTOJEČE UREDITVE DOKUMENTOV V SLOVENIJI	2
1.1 Namen in uporaba dokumentov	2
1.1.1 Osebna izkaznica	2
1.1.2 Potni list.....	3
1.1.3 Vozniško dovoljenje	5
1.2 Zaščitni elementi dokumentov	7
1.2.1 Zaščitni elementi osebne izkaznice	7
1.2.2 Zaščitni elementi potnega lista	8
1.2.3 Zaščitni elementi voziškega dovoljenja.....	8
2 PRIKAZ PRAKTIČNEGA PRIMERA BOLJŠE UREDITVE DOKUMENTOV	9
2.1 Predstavitev ureditve dokumentov v Španiji	9
2.1.1 Elektronska pametna kartica v Španiji	10
2.1.2 Biometrični potni list v Španiji.....	11
2.2 Uporaba elektronske pametne kartice	12
2.2.1 Vrste naprav in delovanje sistema	13
2.2.1.1 Povezovanje v vmesne naprave.....	14
2.2.1.2 Brežžična komunikacijska tehnologija.....	15
2.2.2 Proces uporabe elektronske pametne kartice na dostopnih modulih na pametnih mejah Španije	15
2.2.3 Uporaba elektronske pametne kartice v prometu	16
2.2.3.1 Protokol uporabe pametne kartice v prometu	16
2.3 Zaščitni elementi in varnostni mehanizmi.....	18
2.3.1 Infrastruktura javnega ključa pametne kartice.....	20
2.3.2 Zaščitni elementi elektronske pametne kartice.....	21
SKLEP	23
LITERATURA IN VIRI	25

KAZALO SLIK

Slika 1: Osebna izkaznica Republike Slovenije (pojasnila in dodatne zaščite dokumenta) .	3
Slika 2: Potni list republike Slovenije (pojasnila in dodatne zaščite dokumenta)	5
Slika 3: Prednja in zadnja stran voznškega dovoljenja (pojasnila in dodatne zaščite dokumenta)	6
Slika 4: Prednja in zadnja stran starega voznškega dovoljenja (pojasnila in dodatne zaščite dokumenta).....	7
Slika 5: Nacionalni identifikacijski dokument 3.0	10
Slika 6: Španski biometrični potni list s prikazom zaščitnih elementov.....	11
Slika 7: Dostopni moduli na avtomatskem sistemu mejnega upravljanja.....	13
Slika 8: Uporaba preko povezovanja elektronske pametne kartice v vmesne naprave.....	14
Slika 9: Brezžična komunikacijska tehnologija	15
Slika 10: Postopek uporabe elektronske pametne kartice in biometričnega potnega lista na dostopnih moduli na pametnih mejah v Španiji.	16
Slika 11: Izmenjava sporočil za identifikacijo voznika	17
Slika 12: Zgornja in spodnja stran pametne kartice 3.0	22

SEZNAM KRATIC

ang. - angleško

špan. - špansko

aB - (ang. Authority body); Pooblaščen organ

ABC system - (ang. Automated boarder control system); avtomatski sistem mejnega upravljanja

aCert - (ang. Authority's certificate); certifikat organa

Ad hoc networking - (ang. Ad hoc networking); neodvisnost infrastrukture varnostnih omrežij ali ad hoc omrežje

aID - (ang. Authority's ID); identifikacijski dokument organa

aKpri - (ang. authority private key); organov zasebni ključ

aKpu - (ang. authority's public key); javni ključ organa

API - (ang. Application public interface); distribucija aplikacijskega programskega vmesnika

APP - (ang. application software); aplikacija računalniških programov ali sistemov

aVeh - (ang. Authority vehicle); pristojno vozilo

CAN - (ang. Card Access Number); številka dostopa do kartice ali dostop do čipa

CEA - (ang. Electronic Authentication Code); elektronska koda za overjanje

Ch - (ang. SHA challenge); poziv kriptografske razpršilne funkcije

CLI - (špan. imagen láser cambiante); spreminjajoča laserska gravirana slika

CRP - (slo.) Centralni register prebivalstva

CWA or CEN - (ang. Workshop Agreement); certifikat v zaščitni obliki profila referenčnega dokumenta CWA 14169

DGP - (špan. Direction de la Policía or ang. Spanish General Directorate of Police or the Ministry of the Interior); (v tem primeru španski) generalni direktor policije

DGT - (špan. Dirección General de Tráfico); Generalni direktorat prometa

dID - (ang. driver's identity document); identifikacijski dokument voznika

DIREQ - (ang. Driver Identification Request); zahtevek za identifikacijo voznika

dKpri - (ang. drivers private key); voznikov zasebni ključ

dKpu - (ang. driver's public key); javni ključ voznika

DNle - (špan. Documento Nacional de Indentidad); uradna nacionalna identifikacijska kartica

dSignCert - (ang. Driver's sign certificate); voznikov podpisani certifikat

dVeh - (ang. driving vehicle); voznikovo vozilo

EAL 4 - (ang. evaluation assurance level 4); v skladu s skupnimi kriteriji ocenitve stopnje zanesljivosti

EDR - (ang. Event data recorder); snemalnik podatkov o dogodkih

EEA - (ang. European Economic Area); Evropski gospodarski prostor

eID - (ang. electronic identity card); elektronska pametna identifikacijska kartica

EMŠO - (slo.) Enotna matična številka občana je osebna identifikacijska številka državljana v Republiki Sloveniji

ePassport - (ang. Electronic passport or biometric passport); elektronski potni list ali digitalni potni list

ETSI - (ang. European Telecommunications Standards Institute); Evropski odbor za standardizacijo, ki ga potrdi Evropski inštitut za telekomunikacijske standarde

EU - (ang. European Union); Evropska unija

ID - (ang. identity document); identifikacijski dokument

IOS - (ang. iPhone operated systems); Applov prenosni operacijski sistem

ISO - (ang. International Organization for Standardization); mednarodni organ za določanje standardov, ki ga sestavljajo predstavniki različnih nacionalnih organizacij za standardizacijo.

LiPlate - (ang. License Plate); registrske tablice vozila

MRZ - (ang. Machine readable zone); cona računalniškega branja

NFC - (ang. Near Field Communications); komunikacija s sosednjim poljem ali brezžična komunikacijska tehnologija

NIE - (špan. Número de identificación de extranjero); identifikacijska številka imigranta

NIF - (špan. Número de Identificación Fiscal); davčna identifikacijska številka

OCR – (ang. Optical character recognition); optično prepoznavanje znakov

OCSP - (ang. Online Certificate Status Protocol); internetni certificirani protokolni status

On-SiteDiverID - (ang. On-Site Driver identity card,): voznik oziroma uporabnik identifikacijskih pametnih kartic

PAAVE - (ang. Anonymous Authentication in Vehicular Networks); anonimna avtentifikacija v vozilnih omrežjih

PCMCIA - (ang. Personal Computer Memory Card International Association); integrirani vmesnik (primer čitalec kartic)

PIN - (ang. personal identification number); osebna numerična koda

PKCS # 11 - (ang. Public-Key Cryptography Standards); standard javnega ključa za kriptografijo je eden izmed standardov javnega ključa za kriptografijo in se nanaša tudi na programski vmesnik za ustvarjanje ter manipuliranje kriptografskih žetonov

PKI - (ang. Public key infrastructure); infrastrukturo javnega ključa

RFC - (ang. Request for Comments); objava iz tehnološke skupnosti z kodo RFC 3739

RSA - (ang. Rivest–Shamir–Adleman); šifriran kripto sistemski javni ključ

RSU - (ang. Road side unit); računalniška naprava , ki je ob cesti npr.: policijski avto ali radarski stolp

SHA - (ang. Secure Hash Algorithm); to je kriptografska razpršilna funkcija, ki ima vhod in proizvaja 160-bitno (obsega 20-bajtov) razpršeno vrednost, znano kot pretvornik sporočil

Spanish eID - (ang. electronic identity card); Španska elektronska pametna kartica

SSCD - (ang. Secure signature creation device); naprava za ustvarjanje varnega podpisa

TPD - (ang. tamper-proof device); naprava, ki preprečuje vdor nepooblaščenega osebj

UV - (ang. Ultraviolet); ultravijolično

V2I - (ang. vehicle to infrastructure); vozilo do infrastruktura

V2V - (ang. vehicle to vehicle); komunikacija prevoznega sredstva do prevoznega sredstva

VANETs - (ang. Vehicular ad hoc networks): varnostni sistem v mobilnih omrežjih in
ustvarjanje brezžičnega omrežja za izmenjavo podatkov med vozili

vehPos - (ang. Vehicle Position); lokacije vozila

VIZ - (ang. Visual inspection zone); cona vizualne kontrole

ZOIzk – (slo.) Zakon o osebni izkaznici

ZPLD – (slo.) Zakon o potnem listu

Zvoz - (slo.) Zakon o voznikih

UVOD

Osební dokumenti so v prvi vrsti namenjeni dokazovanju identitete posameznika. Gre za javne listine, ki jih izdajo državni organi. Običajno so opremljene s fotografijo in vsebujejo določene podatke o imetniku listine.

Z napredkom tehnologije se ponujajo še številne druge napredne možnosti uporabe osebnih dokumentov in uporabo identifikacije za dostop do različnih storitev javne uprave. Osební dokumenti tako postajajo »moderna orodja upravljanja v sodobni družbi, s katerimi se lahko rešuje različne in spreminjajoče se socialne in politične probleme« (Bennett-Colin & Lyon, 2008, xi).

Tako postajajo osebni dokumenti pomembno orodje, ki ga je smiselno povezati z različnimi državnimi bazami oz. z bazami različnih državnih organov. Tako lahko omogočajo dostop državljanov do zanje pomembnih podatkov, ki pa mora biti varen in vezan na identiteto lastnika dokumenta. Omenjeno pa zahteva preskok od pogleda na dokument, kot zgolj vir identifikacije posameznika, na pogled na dokument kot enoten, biometrično verificiran dostop do informacijskih sistemov države.

Namen naloge je predstaviti dobre prakse glede ureditve osebnih dokumentov in možne izboljšave obstoječega sistema v Republiki Sloveniji, tako z vidika funkcionalnosti, kot tudi varnosti. Raziskovalna vprašanja, ki predstavljajo izhodišče za pripravo diplomske naloge so:

- Kakšna je obstoječa ureditev v Sloveniji na področju osebnih dokumentov?
- Kakšna je uporabna vrednost oziroma funkcionalnost dokumentov ter kako zagotavljajo njihovo varnost?
- Kakšne izboljšave so na tem področju mogoče?
- Ali obstajajo konkretni primeri boljših rešitev?

Cilj te diplomske naloge je predstaviti boljši pristop pri ureditvi osebnih dokumentov na podlagi konkretnega primera, dodatne možnosti uporabe, ki jih to prinaša, ter analizirati zaščitne elemente in varnostne mehanizme v elektronskem svetu.

Tako bom v diplomskem delu najprej na kratko predstavil obstoječo ureditev na področju osebnih dokumentov v Sloveniji, pri čemer se bomo dotaknili ključnih dokumentov, njihovega namena in uporabe. Posebno pozornost bom namenil zaščitnim elementom, ki so namenjeni zagotavljanju varnosti, saj gre za enega ključnih vidikov pri uporabi dokumentov.

V drugem delu bom na praktičnem primeru predstavil možnosti izboljšav obstoječe ureditve v Sloveniji. Izhajal bom iz primera druge evropske države, ki je na tem področju naredila precej korakov naprej in ima tako določene stvari urejene zelo dobro. Govoril bom o Španiji

in nekaterih njenih ključnih dokumentih. Tu bom izpostavil elektronsko pametno kartico, kot dokument prihodnosti, ki lahko nadomesti in hkrati nadgradi različne obstoječe dokumente. Predstavil bom ključne prednosti enotne pametne kartice in načine njene uporabe. Opisal bom tudi, kako na dostopnih modulih uporabljamo pametno kartico ali biometrični potni list na pametnih mejah Španije. Na področju pametne kartice bom predstavil tudi varnostne mehanizme omrežij te kartice.

V zaključku bom opisal svoj pogled na obravnavano področje. Govoril bom o smiselnosti uporabe enotne pametne kartice v Sloveniji in razlogih za njeno uvedbo v prihodnosti. Poleg tega bom izpostavil nekaj področij, kjer bi pametna kartica lahko olajšala vsakodnevno življenje prebivalcev Slovenije, poenostavila poslovanje javne uprave in hkrati omogočila bolj varno uporabo osebnih podatkov.

1 PREDSTAVITEV OBSTOJEČE UREDITVE DOKUMENTOV V SLOVENIJI

V nadaljevanju bom najprej na kratko predstavil obstoječe stanje na področju osebnih dokumentov. Ključni osebni dokumenti v Republiki Sloveniji so: osebna izkaznica, potni list in vozniško dovoljenje. Vsakega izmed omenjenih dokumentov bomo najprej na kratko predstavili, pri čemer bomo govorili o namenu in uporabi dokumenta ter zaščitnih elementih dokumentov.

Vsakega od dokumentov bom predstavil tudi na vzorčni sliki, kjer bom povzel glavne lastnosti dokumenta, njegove značilnosti ter zaščitne elemente dokumenta.

1.1 Namen in uporaba dokumentov

Osnovni namen osebnih dokumentov je izkaz identitete osebe. Vsak državljan je zavezan, da se na zahtevo uradne osebe (pooblaščen po zakonu) identificira z dokumentom, s katerim uradna oseba preveri njegovo istovetnost. V ta namen mora vedno s seboj imeti vsaj enega izmed v nadaljevanju predstavljenih dokumentov.

1.1.1 Osebna izkaznica

Osebna izkaznica je dokument, s katerim državljan Slovenije izkazuje istovetnost. Osebno izkaznico lahko uporabimo za potovanja v Evropske države in znotraj Schengenske meje drugih držav. Če državljan Slovenije nima drugega dokumenta za izkaz istovetnosti organom, mora imeti vsaj osebno izkaznico, ki jo lahko naredi po 18. letu starosti. Državljeni mlajši od osemnajstega leta lahko imajo osebni dokument pri katerem vloži vlogo zakoniti zastopnik (2. in 3. člen Zakon-a o osebni izkaznici (ZOIzk-1), Ur. l. RS, št. 35/2011).

prodajanje, trgovanje ali posojanje potnega lista drugemu in ga uporabljati kot svojega (1., 3. in 4. člen Zakon-a o potnih listinah (ZPLD-1-UPB4), Ur. l. RS, št. 29/2011).

V Sloveniji imamo različne vrste potnih listov: službeni potni list, potni list za vrnitev, potni list, ki se izdaja po mednarodni pogodbi ter diplomatski potni list. V tej diplomi bomo obravnavali samo potni list Republike Slovenije (5. člen ZPLD-1-UPB4).

Za izdajo potnega lista je pristojno ministrstvo za notranje zadeve. Pristojni organ za notranje zadeve Republike Slovenije izda potni list v določenih pogojih: če je državljan polnoleten, ni pravnomočno obsojen zaradi naklepne kaznivega dejanja ter ni v kazenskem postopku zaradi kaznivega dejanja (4. odstavek 12. člen ZPLD-1-UPB4).

Za pridobitev potnega lista uveljavimo vlogo pri pristojnemu organu. Lahko jo vloži državljan, ki je dopolnil 18 let ter tudi državljan, ki sicer še ni dopolnil 18 let, a je sklenil zakonsko zvezo. Za državljana, ki ni poslovno sposoben in je mlajši od 18 let, vloži vlogo za potni list njegov zakoniti zastopnik. Zakoniti zastopnik, priloži fotografijo pristojnemu organu v fizični in digitalni obliki. Digitalno fotografijo državljana hranijo eno leto na elektronskem odložišču organa. Od datuma vložitve fotografije državljana lahko poleg potnega lista naredi druge osebne dokumente najkasneje v 12 mesecih. Dve enaki fotografiji državljana Slovenije morata biti v predpisani obliki potnega lista (22. in 23. člen ZPLD-1-UPB4).

Veljavnosti izdanega potnega lista so sledeče (14. člen ZPLD-1-UPB4):

- državljanom starim nad 18 let izdajo potni list z veljavnostjo 10 let;
- državljanom starim 3 do 18 let izdajo potni list z veljavnostjo 5 let;
- državljanom, ki še niso dopolnili 3 leta izdajo potni list z veljavnostjo do 3. leta starosti.

V primeru, če državljan spremeni kakršnekoli podatke na potnem listu, mora pristojnemu organu za notranje zadeve Republike Slovenije vrniti potni list najkasneje v roku 30 dni. Spremembe so lahko naslednje (20. člen ZPLD-1-UPB4):

- sprememba posameznega ali več podatkov na biografski strani potnega lista;
- sprememba stalnega prebivališča;
- fotografija na potnem listu ne kaže več prave podobe osebe;
- potni list je obrabljen, poškodovan ali ni več uporaben zaradi drugega razloga.

V primeru izgube ali tatvine potnega lista mora imetnik to pristojnemu organu javiti najkasneje v osmih dneh. Zaradi varnosti se ob izgubi ali tatvini potnega lista Republike Slovenije objavijo podatki na portalu e-uprava. Po izročitvi potnega lista, pristojni organ shrani posebne podatke kot evidenco, ki se vzdržuje in vodi v bazi podatkov notranjega ministrstva. Ti posebni podatki so (23. in 30. člen ZPLD-1-UPB4):

- tip in vrsta potnega lista;

- fotografija državljana v digitalni obliki, v kateri je ni mogoče prebrati z napravami za branje biometričnih podatkov;
- registrska in serijska številka potnega lista;
- vročitev potnega lista;
- izgubljeni ali ukradeni potni list;
- prstni odtis oziroma podatki o roki prstnega odtisa itd.

Na Sliki 2 je prikazan potni list Republike Slovenije in njegovi zaščitni elementi, ki jih predstavljamo v naslednjem sklopu.

Slika 2: Potni list republike Slovenije (pojasnila in dodatne zaščite dokumenta)



Vir: Evropski svet - Svet Evropske unije (brez datuma b); Upravna enota Ljutomer RS (brez datuma).

1.1.3 Vozniško dovoljenje

Vozniško dovoljenje je dokument, ki dokazuje istovetnost osebe, hkrati pa osebi dovoljuje voziti prevozno sredstvo določene kategorije. Imetnik vozniškega dovoljenja se lahko usposablja za več kategorij motornih vozil: AM, A1, A2, A, B1, B, BE, C1, C, D1, D, C1E, CE, D1E, DE, F, G. V tej diplomi bomo obravnavali samo kategorijo B motornih vozil, ki zajema osebne avtomobile, namenjene prevozu oseb (23. odstavek 62. člena Zakon-a o voznikih (Zvoz-1), Ur. l. RS, št. 85/2016;).

Tisti lastnik, ki ima v lasti vozniško dovoljenje motornih vozil B kategorije ima opravljen glavni izpit šole vožnje ter pogoj zdravstvenega spričevala in druge metode dodatnih usposabljanj voznika (1. odstavek 1. člena Zvoz-1).

Zdravniško spričevalo za kategorijo B motornih vozil zahteva primerno duševno in telesno stanje voznika za vožnjo motornih vozil. Ministrstvo, ki je pristojno za promet, izvaja strokovni nadzor na podlagi določb in predpisov, ki se nanašajo na vozniški izpit, vozniška dovoljenja, program izobraževanja ter dodatnega usposabljanja (1. odstavek 20. člena in 1. odstavek 88. člen Zvoz-1).

Ministrstvo, ki je pristojno za promet, je javna agencija. Javna agencija izda vozniško dovoljenje osebi, ki izpolnjuje naslednje zahteve oziroma pogoje (1. odstavek 60. člen Zvoz-1):

- je dopolnil predpisano starost za vožnjo motornih vozil,
- je uspešno opravil vozniški izpit,
- je fizično in duševno zmožen voziti prevozno sredstvo, kar dokaže z veljavnim zdravniškim spričevalom,
- ji ni prepovedana izdaja vozniskega dovoljenja, dokler taka prepoved traja v zvezi z varnostnim ukrepom odvzema vozniskega dovoljenja;
- ji vozniško dovoljenje ni začasno odvzeto ali odvzeto za stalno,
- se določeni vrsti motornega vozila ali kategorije ne izvršuje stranska sankcija prepovedi vožnje.

Za izdajo vozniskega dovoljenja lahko uporabijo ustrezno fotografijo, ki jo priloži oseba v fizični ali digitalni obliki. To fotografijo hranijo v evidenci izdanega drugega uradnega identifikacijskega dokumenta ter kaže pravo podobo osebe (7. odstavek 60. člena Zvoz-1).

Novi vozniki dobijo vozniško dovoljenje Republike Slovenije, ki je prikazano na Sliki 3. Vozniki, ki imajo še stara vozniška dovoljenja (v roza barvi), kot so prikazana na Sliki 4, lahko te kadarkoli zamenjajo z novimi najkasneje do 19. januarja 2023 (93. člen Zvoz-1).

Slika 3: Prednja in zadnja stran vozniskega dovoljenja (pojasnila in dodatne zaščitne dokumenta)

Legenda:

1. Priimek imetnika
2. Ime imetnika
3. Datum in kraj rojstva
- 4a. Datum izdaje dovoljenja
- 4b. Datum veljavnosti dovoljenja
5. Serijska številka
7. Podpis imetnika
8. Naslov imetnika
9. Kategorije vozniskega dovoljenja
10. Datum prve izdaje
11. Datum veljavnosti
12. Dodatne informacije / omejitve

Prikazana sta v dokumentu zaščitna elementa v katerem sta dva večslojna laserska zapisa, in sicer podoba imetnika oziroma serijska številka dokumenta

Črno-bela fotografija državljanca RS

VOZNIŠKO DOVOLJENJE REPUBLIKA SLOVENIJA

1. Vzorec
2. Ana
3. 01.01.1979 Ljubljana
4a. 18.01.2023 4b. 18.01.2023 4c. UE Ljubljana
5. 999900403
7. [Podpis]
8. Ljubljana
Beethovnova ulica 003
9. AM, A1, A2, A, B1, B, C1, C1E, F

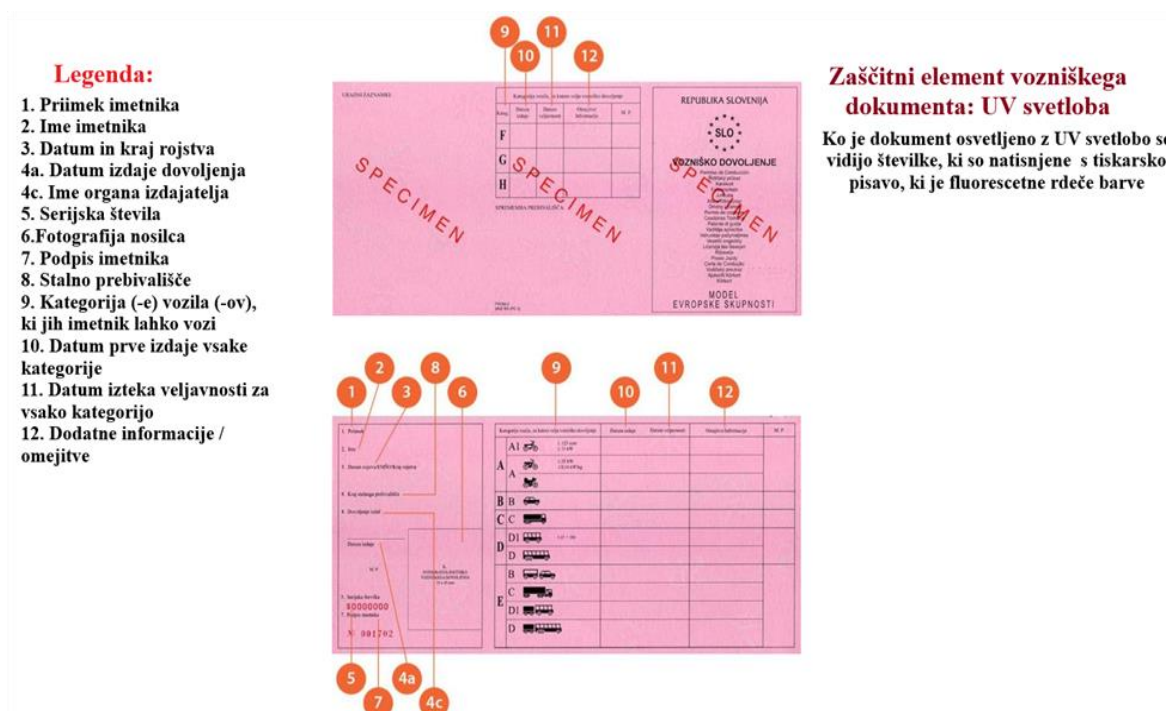
Zaščitni element je tiskarska tehnika v katerem se barva spreminja iz zelene v modro

Prikazan je zaščitni element vozniskega dovoljenja Republike Slovenije v katerem je optično spremenljiv element, ki se pokaže na stranski svetlobi (Kinegram)

Dodatna zaščita dokumenta je stranska svetloba v katerem je na otipni element desno spodaj (stiliziran državni grb) in mat pravokotnik levo zgoraj

13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 00. 01. 02. 03. 04. 05. 06. 07. 08. 09. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 4

Slika 4: Prednja in zadnja stran starega voziškega dovoljenja (pojasnila in dodatne zaščite dokumenta)



Vir: Evropski svet – Svet Evropske unije (brez datuma č)

1.2 Zaščitni elementi dokumentov

Eden izmed ključnih vidikov osebnih dokumentov je njihova varnost, tako z vidika varovanja osebnih podatkov imetnika dokumenta, kot tudi z vidika preprečevanja zlorab in ponarejanja dokumentov. V ta namen so v dokumente vključeni različni varnostni sloji in zaščitni elementi.

Nenehen napredek v tehnologiji predstavlja edinstven izziv pri zagotavljanju varnosti dokumentov. V ta namen dokumentom dodajajo nove varnostne sloje, ki zagotavljajo večjo varnost imetniku dokumenta in otežijo ponarejanje dokumentov.

V nadaljevanju predstavljamo zaščitne elemente obstoječih dokumentov, pri čemer bomo začeli z osebno izkaznico.

1.2.1 Zaščitni elementi osebne izkaznice

Na Sliki 1 so prikazani zaščitni elementi, gre za precej enostavne varnostne sloje, ki temeljijo le na svetlobni zaščiti in laserskih podobah. Prvi zaščitni element predstavljata spremenljivi laserski podobi v zgornjem desnem kotu sprednje strani, ki prikazujeta konjenika in serijsko

številko osebne izkaznice. Naslednji varnostni element je podpis, ki je prikazan v desnem spodnjem kotu prednje strani dokumenta.

Na zadnji strani dokumenta je dodaten zaščitni element v obliki motiva konjenika, kjer se barva spreminja iz zelene v modro. Poleg tega je nad konjenikom še obris mej Republike Slovenije, ki je viden pod svetlobo. Poleg tega so na zadnji strani črke »OI« v Braillovi pisavi, ki jih je mogoče otipati in so vidne pod stransko svetlobo.

1.2.2 Zaščitni elementi potnega lista

Starejši potni iz leta 2006 je vključeval le nekaj enostavnih zaščitnih elementov, ki pa so bili nadgrajeni z novo verzijo potnega lista v 2016. Novi potni list tako vključuje:

- Zaščitni element v obliki tiskarske tehnike na naslovnici notranje strani – lipov list in napis SVN;
- Zaščitni element v tiskarski tehniki s številko dokumenta na hrbtni strani integrirane kartice;
- Integrirana kartica z biografskimi podatki z različnimi zaščitnimi elementi (laserski zapis s podobo obraza imetnika z napisom EU in obrisom Slovenije, kitica himne vidna na stranski svetlobi, kitica himne v obliki spirale, pečat z grbom, oblika Triglava z izbočenimi točkami, lipov list v tiskarski tehniki itd.);
- Zaščitni elementi na notranji strani s podobo obraza imetnika in vodnim znakom konjenika;
- Biometrični čip do katerega je mogoče dostopati s pomočjo optičnega skeniranja zapisa na spodnji strani integrirane kartice (OCR-B).

Kljub nadgradnjam pa potni list še vedno ne vključuje nekaterih naprednih elementov, kot je personaliziran čip, ki je kriptiran z zaščito javnih ključev, ki bi imetnika zavaroval pred spreminjanjem, brisanjem in zlorabami (Upravna enota Ljutomer RS, brez datuma).

1.2.3 Zaščitni elementi voznškega dovoljenja

Starejši voznški izpit je imel zgolj en zaščitni element; fluorescentne rdeče številke vidne z UV svetlobo. Zaščito so izboljšali pri novejšem voznškem dovoljenju, ki je v obliki kartice.

Na sprednji strani ima novo voznško dovoljenje številne varnostne elemente:

- podpis imetnika voznškega dovoljenja,
- list v tiskarski tehniki, pri katerem se barva spreminja iz zelene v modro,
- kinegramski elementi oz. optično spremenljivi elementi, ki se pokažejo na stranski svetlobi.

Varnostni elementi pa so vključeni tudi na hrbtni strani voznškega dovoljenja:

- večslojna laserska zapisa s podobo imetnika in serijsko številko dokumenta,
- otipni element s stiliziranim državnim grbom,
- mat pravokotnik levo zgoraj.

Klub temu, da voziško dovoljenje vključuje številne varnostne elemente, pa so ti večinoma optične narave oz. so vezani na naravno svetlobo. Ne vključuje pa naprednih varnostnih elementov, kot je na primer pametni čip.

2 PRIKAZ PRAKTIČNEGA PRIMERA BOLJŠE UREDITVE DOKUMENTOV

V prejšnjem sklopu smo predstavili trenutno ureditev na področju dokumentov v Sloveniji in nekatere izboljšave glede varnosti dokumentov. Dodatni varnostni elementi seveda pomenijo postopne izboljšave, a ne predstavljajo večjega koraka naprej v smislu funkcionalnosti dokumentov.

Nekatere države na tem področju že imajo zelo zanimive pristope, ki hkrati poskušajo združevati dokumente in jih prenesti v dobo elektronskega poslovanja. Tako na primer uvajajo elektronske pametne kartice, biometrični potni list, infrastrukturo javnega ključa za zagotavljanje varnosti, itd.

Omenjeno omogoča dodatne funkcionalnosti ter nekatere bolj napredne zaščitne elemente. Velika Britanija, Nemčija, Estonija in Španija so le nekatere izmed držav, ki so bolj ali manj uspešno začele razvijati tovrstne sisteme. Tovrstne pobude pa so se začele pojavljati tudi na nivoju Evropske Unije (ABC 4EU, 2018).

V nadaljevanju bom podrobneje predstavil primer Španije, ki je ena izmed redkih držav, ki je že uspešno uvedla sistem pametnih osebnih dokumentov, podprtih z elektronskim poslovanjem, in kjer te dokumente že uporabljajo v številne različne namene.

2.1 Predstavitev ureditve dokumentov v Španiji

Namen prenove ureditve področja osebnih dokumentov je v prvi vrsti informatizacija in združevanje različnih dokumentov. Tako so v Španiji uvedli elektronsko pametno kartico, ki združuje funkcionalnosti različnih dokumentov: osebne izkaznice, voziško dovoljenje, zdravniško kartico, knjižnične kartice, kartice javnega prevoza, itd. Ob tem pa še vedno ostaja potni list, ki je zaradi zakonodajnih omejitev in višje varnosti dokumenta še vedno potreben za potovanje v določene države (Wikipedia, 2019b).

V nadaljevanju tako predstavljamo elektronsko pametno kartico in biometrični potni list. Najprej bomo oba dokumenta na kratko predstavili, potem pa se bomo podrobneje posvetili

predvsem elektronski pametni kartici. Tako bomo predstavili za kaj, kje in kako jo lahko uporabljamo ter predstavili njene zaščitne elemente.

2.1.1 Elektronska pametna kartica v Španiji

Elektronska pametna kartica (ang. eID) ali elektronska osebna izkaznica je nacionalni identifikacijski dokument (špan. DNle – Documento Nacional de Identidad). Kartica ima 60 mesečno certificirano veljavnost in je prisotna v večini komercialnih in administrativnih odnosov. Gre za laminirano ali polikarbonatno kartico, ki navaja ime in priimek imetnika, datum rojstva, naslov, starše, spol, naslov prebivališča, mesto in rojstvo pokrajine ter vsebuje fotografijo in identifikacijsko številko, sestavljeno iz osmih števil. To številko uporabljajo tudi za davčne namene, gre za davčno identifikacijsko številko (špan. NIF-Número de identificación fiscal). Primer nacionalnega identifikacijskega dokumenta 3.0 je prikazan na Sliki 5 (MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía, brez datuma a).

Slika 5: Nacionalni identifikacijski dokument 3.0



Vir: MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía (brez datuma g).

Elektronsko identifikacijsko izkaznico izdajo v pisarnah nacionalne španske policije. Če želi državlján Španije zaprositi za elektronsko pametno kartico, je pogoj, da ima oseba špansko državljanstvo in dovoljenje za španski konzulat. Tujcem, ki zakonito prebivajo v Španiji ali pa nameravajo tam kupiti nepremičnino, izdajo identifikacijsko številko tujca (špan. NIE-Número de identificación de extranjero); (Wikipedia, 2019č; MINISTERIO DEL INTERIOR, brez datuma).

Nacionalni identifikacijski dokument je edini dokument splošne uporabe na vseh področjih nacionalne ravni, vendar pa je obvezna referenca za izdajo drugih dokumentov. Na ta način je mogoče potrditi, da nacionalni identifikacijski dokument uživa popolno sprejetje v španski družbi. Poleg tega ima nacionalni identifikacijski dokument enako podatkovno strukturo kot potni list. Tako lahko opravlja funkcijo potovalnega dokumenta in je njegova uporaba možna na pametnih mejah (ang. ABC systems) na način, ki je povsem enakovreden trenutnemu elektronskemu potnemu listu (MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía, brez datuma a).

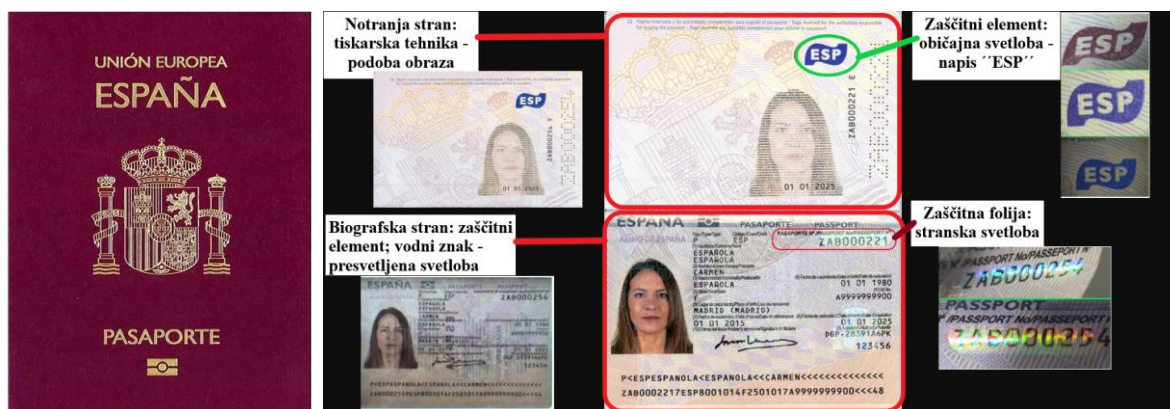
2.1.2 Biometrični potni list v Španiji

Španski potni list je biometrični potni list, znan tudi kot elektronski potni list ali digitalni potni list (ang. ePassport). Je tradicionalni potni list, ki ima vgrajen elektronski mikroprocesorski čip, ki vsebuje biometrične podatke, ki jih je mogoče uporabiti za overovitev identitete imetnika potnega lista.

Potne liste izdajo španskim državljanom zaradi potovanja zunaj Španije. Vsak španski državljan je tudi državljan Evropske unije (ang. EU). Potni list skupaj z nacionalno osebno izkaznico ali elektronsko pametno kartico omogoča proste pravice do gibanja in prebivanja v katerikoli državi Evropske unije in Evropskega gospodarskega prostora (ang. EEA). Zunaj Evropske unije lahko španski državljani potujejo s potnim listom, v nekaterih državah pa potrebujejo poleg potnega lista še vizo (Wikipedia, 2019c).

Potni list uporablja brezkontaktno tehnologijo pametnih kartic, vključno z mikroprocesorskim čipom (računalniškim čipom) in anteno (tako za napajanje do čipa in komunikacijo). Čip je vgrajen na zadnji strani potnega lista. Ključne informacije potnega lista so natisnjene na podatkovni strani potnega lista in shranjene v čipu. Na Sliki 6 je prikazan španski biometrični potni list (ang. ePassport), v katerem so prikazani zaščitni elementi in druge funkcije dokumenta (Wikipedia, 2019a).

Slika 6: Španski biometrični potni list s prikazom zaščitnih elementov



Vir: MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía (brez datuma e); Evropski svet – Svet Evropske unije (brez datuma c).

Mikročip, ki se nahaja na zadnji strani biometričnega potnega lista, vsebuje naslednje podatke o lastniku (MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía, brez datuma e): skenirano sliko lastnika, biografske informacije (vodni znak, zaščitno folijo, podobo obraza) in prstni odtis.

Infrastruktura javnega ključa (ang. PKI) se uporablja za avtentifikacijo elektronsko shranjenih podatkov v čipu potnega lista. Trenutno standardizirana biometrija, ki jo uporabljajo za to vrsto identifikacijskega sistema, je prepoznavanje obraza in/ali prepoznavanje prstnega odtisa.

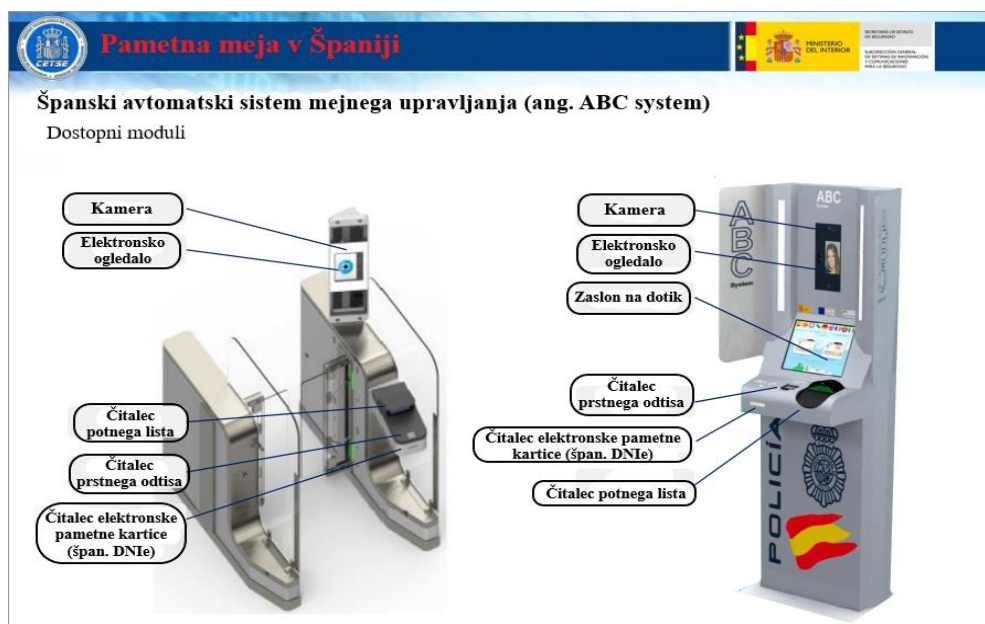
Kot že omenjeno, pa se bomo posvetili predvsem elektronski pametni kartici, ki predstavlja napredno tehnologijo, ki je lahko zelo zanimiva tudi za Slovenijo.

2.2 Uporaba elektronske pametne kartice

Elektronska pametna kartica združuje različne dokumente, s čimer tudi povezuje različne funkcionalnosti. Tako omogoča (Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre, 2017a, str. 19; Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre, 2019b; ECODIARIO.ES, 2015; Wikipedia, 2019b):

- **Identifikacija identitete:** Certifikat o avtoriteti (digitalni podpis) zagotavlja lastniku, da v elektronski komunikaciji vsaki pristojni osebi dokaže svojo identiteto, saj ima certifikat o istovetnosti ter zasebni ključ povezan z njim.
- **Elektronsko podpisovanje dokumentov:** Z uporabo certifikata o podpisu lahko prejemnik oziroma pristojni organ elektronsko podpisanega sporočila preveri pristnost tega podpisa, s čimer dokaže identiteto podpisnika.
- **Potrjevanje integritete dokumenta:** Omogoča preverjanje, da dokument ni spremenil katerikoli zunanji agent. Zagotovitev integritete dokumenta izvajajo s pomočjo različnih funkcij, ki jih uporabljajo v kombinaciji z elektronskim podpisom. Ta shema omogoča identifikacijsko preverjanje, če je bil spremenjen podpis po pošiljanju sporočila.
- **Panelni dostop do administracije:** Aplikacija omogoča dostop do številnih storitev različnih agencij z eno samo prijavo. Na ta način je mogoče dostopati do portala socialnega zavarovanja, generalnega direktorata prometa (globe, kazenske točke), ministrstva za pravosodje (rojstni in poročni list), do katastra nepremičnin, portala davčne agencije, lokalne/mestne uprave, zdravstvenih podatkov, itd.
- **Vozniško dovoljenje:** Elektronska pametna kartica je dokumentna identifikacijska številka za španske državljane. Enako številko uporabljajo za voziško dovoljenje.
- **Potni list:** Nacionalni identifikacijski dokument (špan. DNIE) ima enako podatkovno strukturo kot potni list. V tem smislu lahko pametna kartica (špan. DNIE) opravlja enake funkcije kot potni dokument in omogoča uporabo na dostopnih modulih, ki se imenuje avtomatski sistem mejnega upravljanja (ang. ABC systems). Dostopni modul je prikazan na Sliki 7.

Slika 7: Dostopni moduli na avtomatskem sistemu mejnega upravljanja



Vir: Spanish Ministry of Interior (2017, str. 10).

Poleg tega elektronska pametna kartica omogoča tudi številne druge funkcionalnosti (MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía, brez datuma č):

- urediti nakupe prek interneta s podpisom,
- urediti dokumentacijo v javni upravi kadarkoli in brez čakanja,
- izvesti varne transakcije z bančnimi subjekti,
- dostop do stavbe, kjer delamo,
- varno uporabo našega osebnega računalnika,
- gotovost identitete v pogovoru na internetu.

2.2.1 Vrste naprav in delovanje sistema

Za uporabo elektronske pametne kartice je potrebno imeti določene strojne in programske elemente, ki omogočajo dostop do čipa kartice in s tem uporabo certifikatov, ki jih vsebuje. Elektronska pametna kartica je dokument z dvojnim vmesnikom, v katerem se kartica poveže na dva načina (Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre, 2017a, str. 16-18):

- preko povezovanja elektronske pametne kartice v vmesne naprave;
- preko brezžične komunikacijske tehnologije.

2.2.1.1 Povezovanje v vmesne naprave

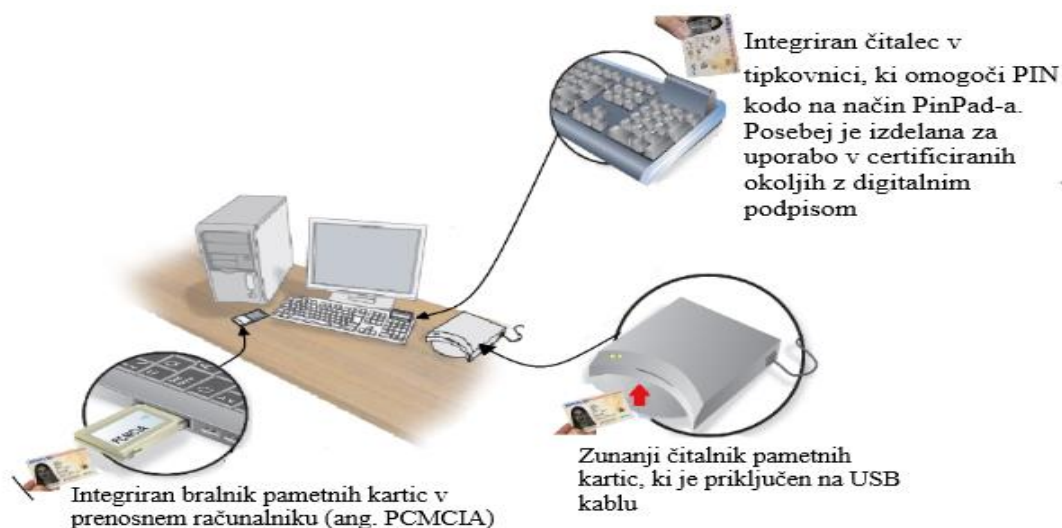
Za povezovanje pametne kartice z drugimi napravami je potrebna primerna strojna in programska oprema. Z vidika strojne opreme je potreben dovolj zmogljiv osebni računalnik (minimalna zahteva Intel Pentium III ali močnejši procesor) in čitalnik pametnih kartic, ki ustreza mednarodnim standardom (ang. ISO-7816). Obstajajo različne izvedbe čitalnikov pametnih kartic: integrirane v tipkovnico, zunanja naprava povezana preko USB ali preko vmesnika integrirano v prenosnem računalniku (ang. PCMCIA), (Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre, 2017a, str. 16).

Minimalne zahteve z vidika programske opreme so: primeren operacijski sistem (Windows 7 ali novejši, Linux ali Mac), internetni brskalnik (Microsoft Internet Explorer, Microsoft Edge, Chrome, Mozilla Firefox), programski gonilniki (gonilniki za čitalnik pametnih kartic) in kriptografski gonilniki ali moduli elektronske pametne kartice (Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre, 2017a, str.17).

Da bi pravilno uporabljali elektronsko pametno kartico, mora biti na njej nameščen kriptografski vmesnik imenovan kriptografski modul. V računalniškem sistemu mora biti nameščen gonilnik imenovan Minidriver ali CardModule v obliki standarda javnega ključa za kriptografijo številka 11 (ang. PKCS#11) oziroma v obliki kriptografskega žetona (Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre, 2017a, str. 17).

Slika 8 prikazuje postopek povezave pametne kartice v vmesne naprave preko integriranega bralnika pametnih kartic (v računalniku ali tipkovnici) oziroma preko zunanjega čitalnika.

Slika 8: Uporaba preko povezovanja elektronske pametne kartice v vmesne naprave



Vir: MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía (brez datuma c).

2.2.1.2 Brezžična komunikacijska tehnologija

Druga možnost za povezovanje elektronske pametne kartice z drugimi napravami je uporaba brezžične komunikacijske tehnologije. V tem primeru se kartice neposredno poveže z drugo elektronsko napravo. To je lahko pametni telefon, tablični računalnik ali čitalnik brezžične komunikacijske naprave (ang. NFC). Naprava mora ustrezati mednarodnemu subjektu za standarde (ang. ISO), (Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre, 2017a, str. 17-18).

Za uporabo pametne kartice je obvezna namestitev aplikacij (ang. APP) na elektronske naprave, ki so dostopne na različnih mestih spletnega portala (na primer: Google Play, Android, IOS, GNU/Linux). Aplikacija (ang. APP), ki uporablja elektronsko pametno kartico se identificira preko vmesnika ali naprave in tako dostopa do določene storitve ali pa omogoča podpisovanje dokumentov. Slika 9 prikazuje uporabo preko brezžične tehnologije (Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre, 2017a, str. 17-18).

Slika 9: Brezžična komunikacijska tehnologija



Vir: Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre (2017a, str. 18).

2.2.2 Proces uporabe elektronske pametne kartice na dostopnih modulih na pametnih mejah Španije

Uporaba elektronske pametne kartice pri prestopu meje omogoča poenostavitev postopkov. Ob povezavi kartice z dostopnim modulom je mogoče avtomatizirati potrebne postopke, s čimer se izboljša varnost in hkrati skrajšajo čakalni časi ob prehodu meje. Hkrati se tako lahko osebje na meji, namesto same verifikacije dokumentov, posveti bolj podrobnemu preverjanju oseb in zagotavljanju varnosti (Spanish Ministry of Interior, 2017, str. 7-8).

Slika 10 prikazuje, kakšne so zahteve v Španiji in kakšen je potek in proces mejnega upravljanja elektronske pametne kartice (špan. DNIE) in biometričnega potnega lista (ang. Epassport) na dostopnih modulih na pametni meji v Španiji (ang. ABC system Spain). (Spanish Ministry of Interior, 2017, str. 11-17).

Slika 10: Postopek uporabe elektronske pametne kartice in biometričnega potnega lista na dostopnih modulih na pametnih mejah v Španiji.



Vir: Spanish Ministry of Interior (2017; str. 8-17).

2.2.3 Uporaba elektronske pametne kartice v prometu

Ena pomembnih prednosti uporabe elektronske pametne kartice, je tudi avtomatizirana identifikacija oseb v prometu, ki prispeva k varnosti cestnega prometa. V nadaljevanju predstavljamo protokol uporabe v cestnem prometu.

Pametna kartica je ena najpreprostejših in najprimernejših načinov avtentifikacije za varno podatkovno komunikacijo v negotovih omrežjih. V njej je opisan protokol za anonimno avtentifikacijo v vozilnih omrežjih (ang. PAAVE). Pametna kartica hkrati uporablja zaščito sporočil v varnostnem sistemu mobilnega omrežja in ustvarjanje brezžičnega omrežja za izmenjavo podatkov med vozili (ang. VANETs). (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 51).

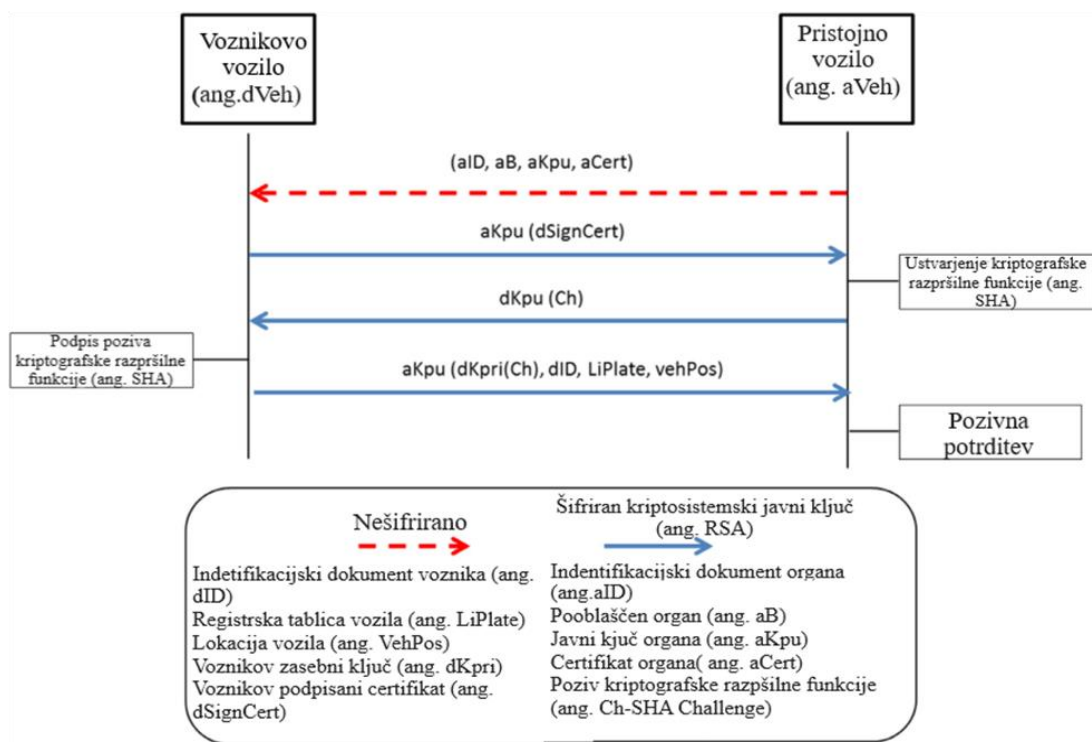
2.2.3.1 Protokol uporabe pametne kartice v prometu

Predlagani protokol temelji na pametni kartici, ki jo zazna računalniška naprava, da se vozilo najprej identificira preko računalniške naprave na cesti; stolpu ali policijskem avtu (ang. RSU) s kriptografskim postopkom javnega ključa, v katerem računalniška naprava deli vozilo s šifriranim ključem; šifriran ključ deli vsa vozila, ki so overjena z isto računalniško napravo na cesti, da lahko anonimno preberejo druga sporočila vozil. Računalniška naprava na cesti je edina subjektivna oseba ali entiteta, ki bi lahko poznala resnično identiteto voznika. Vendar je resnična identiteta vozila omejena na poznavanje vozniškega dovoljenja za identifikacijo voznika ali lastnika. Anonimna avtentifikacija v vozilnih omrežjih ne pojasnjuje ali bi lahko identificirali osebo, ki vozi vozilo, drugače je možno, da voznik ni

lastnik oziroma lastnica vozila (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 51).

Na zahtevo organa je predlagana naslednja shema za identifikacijo pristnih podatkov voznika in vozila. Za jasno razlago sheme voznikov ali uporabnikov pametnih kartic (ang. On-SiteDriverID), najprej predstavimo podatke, ki si jih izmenjujejo med organi, ki ga predstavljajo bodisi kot organ za vozila ali bodisi kot računalniška naprava, ki je ob cesti. Protokol za preverjanje pristnosti voznika ali uporabnika pametnih kartic zajema štiri sporočila med organom in voznikom vozilom. Ta sporočila so opisana na sliki 11.

Slika 11: Izmenjava sporočil za identifikacijo voznika



Vir: Sánchez-García, García-Campos, Reina, Toral & Barrero (2016, str. 54).

Na začetku organ odda sporočilo, ki se imenuje zahteva za identifikacijo voznika (ang. DIREQ). Po prejemu sporočila zahtevka za identifikacijo voznika se bo voznikovo vozilo samodejno odzvalo s protokolom voznika ali uporabnika pametnih kartic, ki se izvaja v vozilu naprave in omogoča enostavno zaznavanje nepooblaščenega dostopa do zaščitene predmeta (ang. TPD), v katerem je integrirana ali združena s špansko elektronsko pametno kartico. Prvič bo naprava, ki preprečuje vdor nepooblaščenega osebjja preverila ali je potrdilo organa veljavno ali potrdilo podpise zaupanja vredna stranka. V njihovih izvedbah so zaupali certifikatom, ki jih je izdal Generalni direktorat policije, saj je isti organ, ki izdaja špansko elektronsko pametno kartico (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 53).

Na odziv pristojnega organa voznikovo vozilo odda sporočilo zahtevka za identifikacijo voznika, ki vsebuje certifikat o podpisu španske pametne kartice. Ta certifikat vsebuje javni

ključ voznika (ang. dKpu) in tudi znak tretje osebe, ki jamči, da javni ključ pripada vozniku. V primeru španske elektronske pametne kartice je tretja stranka španski generalni direktor policije. To sporočilo je poslano s šifriranim javnim ključem organa (ang. aKpu), zato je zagotovljeno, da nihče, razen pristojnega organa, ne bo mogel prebrati certifikata voznika. To ščiti voznika pred poneverbami, ki si prizadevajo predstaviti organ, kjer ne bodo mogli dostopati do voznikovega certifikata ali potrdila, ker nimajo zasebnega ključa organa, potrebnega za dešifriranje certifikata (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 53).

Pristojno vozilo prejme potrdilo o voznikovem podpisu certifikata. Nato organ generira kriptografsko razpršilno funkcijo (ang. SHA-1) z razpršilnim pozivom, v katerem ga šifrira z javnim ključem voznika, ter ga prenese. Ko voznikovo vozilo prejme pozivno sporočilo, ga dešifrira in ga podpiše s svojim zasebnim ključem. Nato voznikova naprava, ki preprečuje vdor nepooblaščenega osebja, sestavi sporočilo s podpisanim pozivom in drugimi nepodpisanimi informacijami o identiteti voznika in vozila.

Ti podatki so sestavljeni iz identifikacijskega dokumenta voznika, registrske tablice vozila (ang. LiPlate) in lokacije vozila (ang. vehPos). Sčasoma voznikova naprava, ki preprečuje vdor nepooblaščenega osebja, podpiše celotno sporočilo javnega ključa organa ter prenese sporočilo.

Po prejemu teh informacij pristojno vozilo dešifrira sporočilo s svojim zasebnim ključem in dešifrira geslo z javnim ključem voznika. Če se prikažejo informacije o vozniku, ki je lastnik vozila lahko organ zaupa identifikacijskemu dokumentu voznika skupaj z registrsko tablico in lokacijo vozila. Ta protokol zagotavlja avtentifikacijo, ki ji ni mogoče nasprotovati. (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 53)

V nadaljevanju bom predstavil enega ključnih vidikov elektronske pametne kartice. Gre za zaščitne elemente oz. varnostne mehanizme pametnih kartic, ter s tem povezano infrastrukturo javnega ključa (certifikati).

2.3 Zaščitni elementi in varnostni mehanizmi

Z intenzivno uporabo interneta so se na področju komuniciranja pojavile nove varnostne grožnje zaradi nedavne rasti mobilnega računalništva. V svetu je veliko povezanih naprav, preko katerih se lahko izmenjujejo informacije preko interneta. Komunikacijo med takšnimi mobilnimi napravami je treba izvajati na varen način tako, da lahko sogovorniki, ki sodelujejo v njem, zaupajo drug drugemu s pomočjo mehanizmov preverjanja pristnosti. Pomembno je tudi zagotoviti celovitost sporočil in zaupnost izmenjanih informacij (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 50).

V splošnih računalniških omrežjih je veliko varnostnih sredstev, ki jih je mogoče uporabiti s cenovno dostopnimi stroški, da bi zagotovili identifikacijo. Metode za preverjanje

pristnosti so pogosto kategorizirane. Velikokrat uporabijo geslo, ali kaj podobnega kot je osebna značilnost, na primer prstni odtis. Oseba pa mora imeti pri sebi osebno izkaznico.

Pametne kartice prinašajo večjo varnost kot pa kartice, ki temeljijo samo na geslih. Prav tako ima pametna kartica kriptografsko zmogljivost in dve funkciji prenosljivosti, kot so lastništvo kartice in pa geslo. Pametna kartica je tudi cenovno dostopnejša od biometrije. (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 50).

Varnostni sistem v avtomobilih omrežja in tudi širši koncept paradigme internetne stvari (ang. Ad hoc networking) zahtevajo nove varnostne mehanizme. Ta omrežja so dovzetna za skupne in popolnoma nove varnostne grožnje. Neodvisnost infrastrukture varnostnih omrežij v avtomobilih je dejstvo vsakega vozlišča, ki deluje kot usmerjevalnik, mobilnost in uporaba brezžičnih komunikacijskih povezav. To so glavni razlogi za takšne nove varnostne grožnje. Kot je navedeno se ad hoc omrežja nanašajo na tehnologijo, ki omogoča omrežno komunikacijo na ad hoc osnovi, zato je težko zagotoviti avtentičnost in zaupnost. Vendar je eden od načinov za vzpostavitev varne komunikacije v ad hoc omrežjih uporaba storitev, overjanje in certificirani servisi (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 51).

Pri protokolih usmerjanja za ad hoc omrežja ni popolne varnostne rešitve, ki zagotavlja varno komunikacijo v vsaki situaciji. Zato je rešitev zelo odvisna od značilnosti dogodka. Pri samem dogodku lahko cestni organi, na primer policija začne ukrepati in prepozna resnično identiteto osebe. Za predlagano varnostno shemo je visok interes saj izboljšuje varnost v sistemu mobilnega omrežja in ustvarjanje brezžičnega omrežja za izmenjavo podatkov med vozili, zlasti v primerih, ko cestni organ zahteva neposreden mehanizem avtentifikacije na kraju samem. Uporaba elektronske identifikacijske kartice za zagotovitev specifičnih varnostnih komunikacij v komunikacijah prevoznega sredstva do prevoznega sredstva (ang. V2V) dopolnjuje trenutne pristope za zavarovanje varnostnega sistema v mobilnih omrežjih in ustvarjanje brezžičnega omrežja za izmenjavo podatkov med vozili (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 50).

Varnostni sistem v mobilnih omrežjih in ustvarjanje brezžičnega omrežja za izmenjavo podatkov med vozili je bila zanimiva tema že od samega začetka avtomobilske komunikacije. Različni dostopi so sledili kot nove varnostne grožnje in kot skupek v zadnjih parih letih. Dostop, ki je odvisen od privatnosti avtomobila se na široko uporablja, kot avtorizacijska garancija med vozili, samo da ne izdaja njene prave identitete. Tako da lahko pravo identiteto vozila pridobijo oziroma zasledijo le državni organi (npr.: policija, oblast); (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 51).

Ta proces zahteva čas, ter konzumira in vključuje pravne osebe (npr.: cestne organizacije, ki zahtevajo identifikacijo – tablice vozila, ter sodnika, ki dovoljuje pravni osebi, da odkrije pravo identiteto voznika na podlagi tablic vozil). Proces je počasen, ker zahteva zaznavo cestne situacije, ki zahteva poznavanje realne identitete vozila. Organom bi koristilo, da

vnaprej vedo pravo identiteto vozila. Pri uporabi identifikacijskih pametnih kartic bi organi lahko prišli, do informacij glede voznikove identitete in prevoznega sredstva na varnejši in hitrejši način; še posebno v situacijah, kot so naloge za nadzor prometa ali nujne primere, ki bi jih uporabljali za izmenjavo podatkov v varnostnem sistemu. (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 50)

Glavni cilj voznikov oziroma uporabnikov identifikacijskih pametnih kartic je ustvarjanje varnega sistema v mobilnih omrežjih in ustvarjanje brezžičnega omrežja za izmenjavo podatkov med vozili. Organom omogoča enostavno in avtomatsko pridobivanje identitete voznikov. S tem se izognejo vključevanju drugih pravnih oseb, na primer sodnika, v proces identifikacije voznika. V nasprotnem primeru bi bil proces zapleten in dolgotrajen. Zato imajo vozniki oziroma uporabniki elektronskih pametnih kartic uporabniško osredotočeno zasnovo s stališča organov, ki brez težav gladko pridobijo identitete voznikov. To preprosto dosežejo z zagonom aplikacije, ki izvaja varnostno shemo voznikov ali uporabnikov pametnih kartic.

Na področju tradicionalnih varnostnih mehanizmov je navedeno, da kombinacija kriptografskih mehanizmov prepreči večino napadov v ad hoc omrežjih (ang. ad hoc networking). Kriptografske mehanizme morajo zavarovati na podlagi ključne javne infrastrukture (ang. PKI) v ad hoc omrežjih. Kar zadeva varnostne mehanizme za varnostni sistem v mobilnih omrežjih in ustvarjanje brezžičnega omrežja za izmenjavo podatkov med vozili je jasno, da je treba podatke zavarovati, saj sporočila vsebujejo pomembne informacije, kot so vozna pot in datum lokacije. Razkrivanje teh informacij, povezano z identiteto voznikov, bi lahko uporabili zlonamerno (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 51).

2.3.1 Infrastruktura javnega ključa pametne kartice

Nacionalne vlade so v zadnjem desetletju spodbudile uporabo te metode preverjanja avtentifikacije, s čimer so izboljšale obstoječe identifikacijske kartice za državljane. Zaenkrat to velja za Španijo, kjer je osebna izkaznica postala pametna kartica, imenovana elektronska identifikacijska kartica. Španska elektronska identifikacija vsebuje osebne podatke v mikročipu, ki jih lahko uporabljajo za namene informacijske varnosti. Španska vlada nenehno spodbuja elektronsko uporabo identifikacijskih kartic in distribucije aplikacijskega programskega vmesnika (ang. API) za razvoj novih storitev, ki temeljijo na tej kartici.

Infrastrukturo javnega ključa omogoča in upravlja španski generalni direktorat policije (špan. DGP). Celoten opis infrastrukturnega javnega ključa je zabeležen v španski elektronski identifikacijski pametni kartici. Uporablja certifikat X.509 in protokol o statusu spletnega potrdila (ang. OCSP). Tako internetni certificirani protokolni status omogoča, da se vsak španski državljan avtentificira zoper katerokoli storitev, ki zahteva identifikacijo z uporabo digitalnega podpisa in tudi drugih varnostnih mehanizmov. Poudariti je treba, da se

napredni digitalni ali elektronski podpis šteje kot rokopisni podpis španskega prava (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 51).

Javni ključ infrastrukture je ena izmed najbolj primernih možnosti za zavarovanje varnostnega sistema v mobilnih omrežjih in ustvarjanje brezžičnega omrežja za izmenjavo podatkov, npr. med vozili. Preverjanje identitete je bistvenega pomena za prepoznavanje osebe, ki je odgovorna za določene prekrške, kot so prometne nesreče ali kršitev v prometu. Kljub temu je bila arhitektura varnostne strojne opreme v varnostnem sistemu mobilnega omrežja in ustvarjanje brezžičnega omrežja za izmenjavo podatkov med vozili zasnovana z dvema glavnima napravama v vozilu. Prvi je snemalnik podatkov o dogodkih (ang. EDR) za evidentiranje kritičnih podatkov o vozilih v izrednih razmerah, druga naprava pa preprečuje vdor nepooblaščenega osebja (ang. TPD), odgovornega za vse kriptografske operacije in shranjevanje zasebnih ključev in certifikatov (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 50).

Pri tem pristopu bodo organi za certifikate (ang. CAs) izdali javno-zasebni ključ za vsako vozilo, hkrati pa bi vsako vozilo imelo seznam anonimnih, vendar certificiranih digitalnih ključev. Ključi, ki se pogosto spreminjajo se vsakokrat zamenjajo z novim certificiranim ključem. To ohrani zasebnost voznikov in jih zaščiti pred več grožnjami, hkrati pa mora organom dovoliti, da razkrijejo informacije vozila za namen odgovornosti voznika. To je znano kot pogojna zasebnost ali pogojna anonimnost. Običajno je potrebna odobritev sodnika, da se razkrije resnična identiteta voznika (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 51).

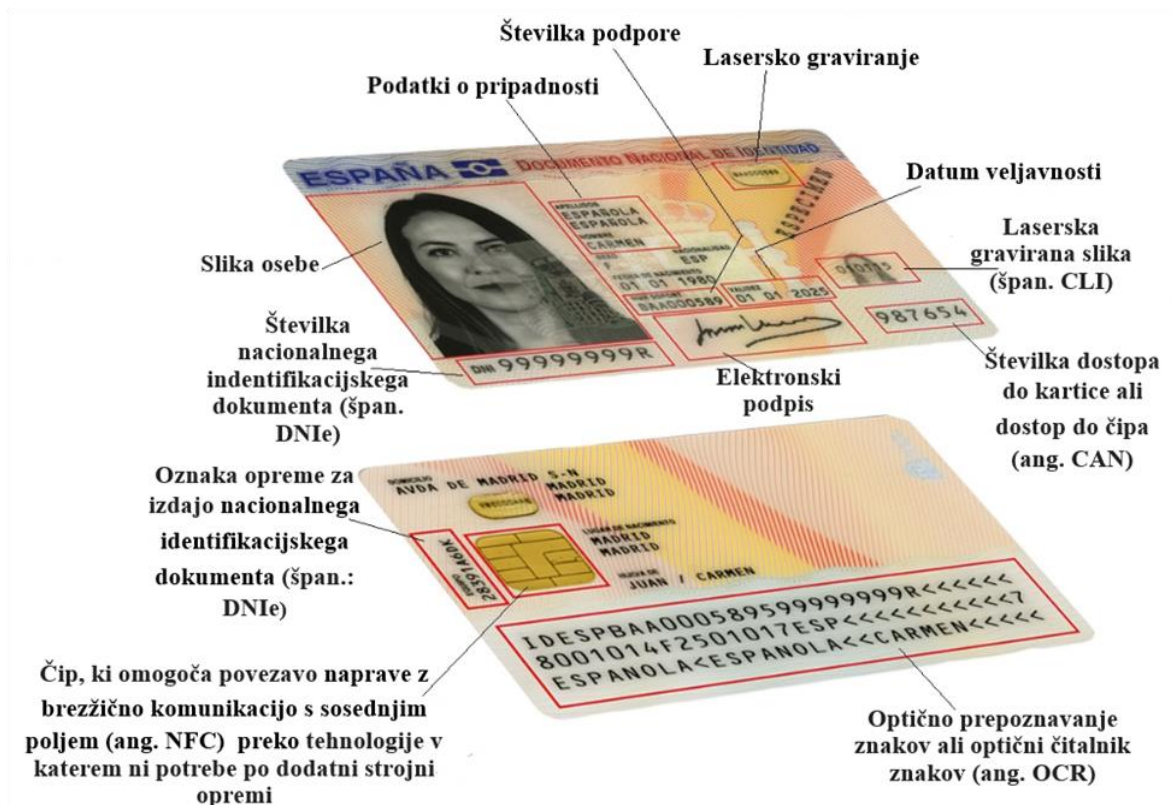
2.3.2 Zaščitni elementi elektronske pametne kartice

Fizično je uradna nacionalna pametna kartica polikarbonatna kartica, ki sledi standardu ISO 7816 za pametne kartice. Vključuje osebne podatke, kot so fotografija, osebni podpis lastnika in druge osebne podatke. V uradni nacionalni pametni kartici je vključenih več varnostnih elementov in jih je mogoče razvrstiti v skladu z njihovimi zmogljivostmi (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 52):

- Prvi nivo (zaznavanje uporabnika in zaščitni elementi): Hologrami, kinegrami in drugi varnostni elementi, ki so vidni na dnevni svetlobi oz. stranski svetlobi.
- Drugi nivo (zaznavanje z uporabo naprav): odzivna UV-črnila, mikro pisanje itd.
- Tretji nivo (laboratorijsko zaznavanje): biometrična primerjava.

Z razliko od večine slovenskih dokumentov, predstavljenih v prejšnjih poglavjih, sta pri španski pametni kartici vključena še dva dodatna varnostna nivoja, drugi in tretji nivo, ki bistveno prispevata k varnosti kartice. Nekateri izmed vključenih varnostnih elementov so prikazani na Sliki 12.

Slika 12: Zgornja in spodnja stran pametne kartice 3.0



Vir: MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía (brez datuma b).

Z vidika dokumentnih podatkov, ki so vključeni v čip pametne kartice, so podatki razdeljeni na tri različne varnostne ravni, ki so dostopne samo za branje (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 52):

- Javno območje (brez omejenega dostopa): organi za certifikate (ang. CA), vmesno potrdilo o izdaji, javni ključi imetnikov, potrdilo komponent.
- Zasebno območje, to je dostop z osebno identifikacijsko številko ali z osebno numerično kodo (ang. PIN): podpis lastnika, overitve identifikacije X.509v3 certifikatov in zasebni ključ imetnika.
- Varnostno območje, ki je dostopno samo prek policijske opreme: elektronske informacije, ki so enake kot bi bile fizično napisane, biometrični podatki in serijska številka naprave.

Uradna nacionalna identifikacijska kartica ali pametna kartica se šteje za napravo za ustvarjanje varnega podpisa (ang. SSCD) v skladu s skupnimi kriteriji ocenitve stopnje zanesljivosti (ang. EAL 4) v certificirani obliki zaščite profila referenčnega dokumenta CWA 14169 (ang. CWA ali CEN Workshop Agreement). Izda ga Evropski odbor za standardizacijo, ki ga potrdi Evropski inštitut za telekomunikacijske standarde (ang. ETSI). Izvedba infrastrukture javnega ključa za nacionalno pametno kartico temelji na standardu X.509 in so ga že izdali in podpisali organi za certificiranje. Če organi za certifikate zaupajo

svojim metodam, potem verodostojnost temelji na organih za certificiranje (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 52).

Uradna nacionalna pametna kartica omogoča potrdilo o podpisu imetnika. Namen potrdila o podpisu je omogočiti državljanom, da imajo možnost digitalnega podpisovanja transakcij in dokumentov, tako da zagotavljajo integriteto sporočil in avtorstvo. Za potrditev podpisa je potrebno, da z napravo za ustvarjanje varnega podpisa vstavite PIN-kodo imetnika preko zaupnega kanala. V Španiji je napredni elektronski podpis enakovreden zakonitemu podpisu, zato mora vsako podpisano nalogo odobriti lastnik (državljan) nacionalne pametne kartice (Sánchez-García, García-Campos, Reina, Toral & Barrero, 2016, str. 52).

SKLEP

V diplomu sem predstavil osebne dokumente, ki jih uporabljamo v Republiki Sloveniji, pri čemer sem izhajal iz dveh ključnih vidikov uporabnosti in varnosti.

Z vidika uporabnosti so obstoječi dokumenti namenjeni predvsem identifikaciji osebe, ne omogočajo pa naprednejših funkcionalnosti, kot so dostop do storitev javne uprave oz. povezovanje z informacijskimi sistemi države.

Pomemben vidik uporabnosti je tudi združevanje različnih funkcij oziroma dokumentov v eni sami kartici. V Sloveniji imamo tako osebno izkaznico, vozniško dovoljenje, zdravstveno kartico, itd. Nimamo pa teh dokumentov združenih v eni pametni kartici, kot smo to videli na primeru Španije.

Če bi imeli vse dokumente v enem, razen potnega lista za mednarodna potovanja, bi imeli manj stroškov in dela z dokumenti, s čimer bi olajšali delo pristojnim organom v Sloveniji, prihranili čas. Še pomembneje, s tem bi bistveno olajšali tudi življenje državljanom.

V elektronski pametni kartici bi lahko imeli enake aplikacije, kot smo jih opisali na primeru Španije. Pametna kartica bi vsebovala biometrične podatke rezidenta v Sloveniji, kot sta prstni odtis ter obraz. Danes ta tehnologija za biometrične podatke že obstaja na pametnih napravah kot so telefoni, tablični računalniki ter osebni računalniki.

Elektronsko pametno kartico, bi lahko uporabljali preko pametnih naprav kot so: pametni telefoni, tablični računalniki, namizni in prenosni računalnik z zunanji napravami. To so naprave, ki berejo elektronsko pametno kartico, to pa bi seveda bila biometrična avtorizacija te elektronske pametne kartice. V biometrično avtorizacijo spadajo prstni odtis ali odčitavanje obraza in zaščitna koda pametnih naprav. Postopek, bi bil tak, da bi elektronsko pametno kartico postavili pod pametno napravo ali v zunanjo napravo, ki je povezana na računalniku. Tako bi dobila pametna naprava avtorizacijo preko prstnega odtisa, odčitavanja obraza ali zaščitne kode, na prenosnem ali namiznem računalniku pa bi imeli samo zaščitno

kodo, s katero bi računalnik izdal lokacijo te naprave kot avtoriteto tega rezidenta v Sloveniji.

Če bi imeli v Sloveniji elektronsko pametno kartico, bi ta lahko združevala: osebni dokument, voziško dovoljenje, zdravstveno kartico, možnost oddaje glasu na volitvah s pomočjo pametne kartice preko računalnika ali druge naprave, vozovnice za javni promet (notranji in mednarodni vozni promet v Sloveniji), knjižnične kartice, itd.

Pomemben vidik pri osebnih dokumentih je identifikacija pri prehodu državnih mej. Tudi tu lahko pametna kartica in biometrični potni list predstavljata pomemben korak naprej, saj omogočata uvedbo avtomatiziranih dostopnih modulov oz. uvedbo pametnih mej v Sloveniji. Kot smo navedli na primeru Španije, to zagotavlja boljšo prehodnost mej, hitrejša postopke, večjo varnost, osebu na meji pa omogoča, da se posveti predvsem dodatnim varnostnim preverjanjem in ne izgublja časa z opravili, ki so lahko avtomatizirana.

Pametna kartica lahko bistveno spremeni tudi postopke in varnost v cestnem prometu, saj državnim organom omogoča hitrejša preverjanja identitete voznika oz. storilca kaznivega dejanja. Tudi tu gre predvsem za poenostavitev postopkov z uvedbo povsem elektronskega poslovanja.

Predlagana pametna kartica omogoča tudi digitalni podpis, s katerim je mogoče enostavno avtentificirati osebo in tako potrditi dokumente, to je dokazati identiteto osebe. V prihodnje bi lahko taka identifikacija služila kot elektronsko dokazilo o istovetnosti osebe pri poslovanju na razdaljo z javno upravo in tudi z gospodarskimi subjekti, npr. pri izposoji avtomobila.

V bližnji prihodnosti bi lahko elektronsko pametno kartico uporabljali tudi kot bančno kartico, s pomočjo pametnega čipa v elektronski pametni kartici. Pametno bančno kartico oziroma pametno kartico bi lahko uporabljali v bankah, hranilnicah, raznih trgovinah, kjer potrebujemo v elektronski pametni kartici token. Token je šifriran program, ki se ga ne da kopirati na druge naprave.

Z vidika varnosti sem predstavil nekatere novejša varnostna elementa, ki so vključeni v slovenske osebne dokumente in napredek glede na prejšnje verzije dokumentov. Tako je novo voziško dovoljenje. Kljub očitnemu napredku na področju varnosti pa gre tu predvsem za varnostne elemente, vezane na svetlobo, in ne vključujejo nekaterih višjih nivojev varnosti, kot smo jih prikazali na primeru španske pametne elektronske kartice.

Poleg tega lahko pametna kartica omogoči tudi nivojske dostope do podatkov, kot smo to videli na primeru Španije z javnim, zasebnim in varnostnim območjem podatkov. Bistveno pa k varnosti pripomore tudi možnost uporabe infrastrukture javnega ključa (certifikati), ki zagotavljajo varno povezovanje z globalno bazo podatkov.

Uporaba pametne kartice pa omogoča tudi nekatere druge zanimive varnostne mehanizme, npr. če bi prišlo do izgube ali kraje kartice bi pametno kartico lahko blokirali. Lastnik elektronske pametne kartice bi obvestil o izgubi ali kraji kartice, pametna kartica pa bi bila blokirana preko pristojnega organa v Sloveniji. Ko bi zaznali prvi stik pametne naprave z internetom ali brezžičnim omrežjem, na primer z mobilnim telefonom ali s tabličnim računalnikom, bi se tako izničili vsi podatki na čipu in javil bi lokacijo izgubljene elektronske pametne kartice. Zlorabo elektronske pametne kartice bi seveda kaznovali.

LITERATURA IN VIRI

1. ABC 4EU. (2018). *Automated Border Control Gates for Europe*. Pridobljeno 2. maja. 2019 iz http://abc4eu.com/docs/Abc4eu_leaflet_19102015.pdf
2. Bennett-Colin, J. & Lyon, D. (2008). *Surveillance, Security and Identification in Global Perspective*. Kraj: London. Routledge Tylor & Francis Group
3. ECODIARIO.ES. (2015, 9. februar). *This is the DNI 3.0 that merges DNI, driving license and health card*. Pridobljeno 15. maja. 2018 iz <https://ecodiario.eleconomista.es/sociedad/noticias/6973690/09/15/Asi-es-el-DNI-30-que-fusionara-a-finales-de-2015-DNI-carne-de-conducir-y-tarjeta-sanitaria.html#>
4. eUPRAVA RS. (brez datuma). *Osebna izkaznica*. Pridobljeno 20. januarja. 2019 iz <https://e-uprava.gov.si/podrocja/osebni-dokumenti-potrdirila-selitev/osebni-dokumenti/osebna-izkaznica.html>
5. Evropski svet - Svet Evropske unije (brez datuma a). PRADO. *Listina: SVN-BO-02001-Osebna izkaznica*. Pridobljeno 19. januarja. 2019 iz <https://www.consilium.europa.eu/prado/sl/SVN-BO-02001/index.html>
6. Evropski svet – Svet Evropske unije. (brez datuma b). PRADO. *Listina: SVN-AO-02004 - Potni list*. Pridobljeno 15. marca. 2018 iz <https://www.consilium.europa.eu/prado/sl/SVN-AO-02004/index.html>
7. Evropski svet – Svet Evropske unije. (brez datuma c). PRADO. *Listina: ESP-AO-05001 - ESPAÑA PASAPORTE*. Pridobljeno 10. decembra. 2018 iz <https://www.consilium.europa.eu/prado/sl/ESP-AO-05001/index.html>
8. Evropski svet – Svet Evropske unije. (brez datuma č). PRADO. *Listina: SVN-FO-02001 - Vozniško dovoljenje*. Pridobljeno 28. januarja. 2019 iz <https://www.consilium.europa.eu/prado/sl/SVN-FO-02001/index.html#sec-feat-1-1>
9. Evropski svet – Svet Evropske unije. (brez datuma d). PRADO. *Listina: SVN-FO-04001 - Vozniško dovoljenje*. Pridobljeno 10. decembra. 2018 iz <https://www.consilium.europa.eu/prado/sl/SVN-FO-04001/index.html>
10. MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía. (brez datuma a). *DNI electrónico - Ideas básicas*. Pridobljeno 18. oktobra. 2018

iz

https://www.dnielectronico.es/PortalDNIE/PRF1_Cons02.action?pag=REF_100&id_menu=1

11. MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía. (brez datuma b). *Electronic DNI - DNI 3.0 Description*. Pridobljeno 29. oktobra. 2018 iz https://www.dnielectronico.es/PortalDNIE/PRF1_Cons02.action?pag=REF_103&id_menu=1
12. MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía. (brez datuma c). *DNI electronico - Que hace falta para utilizarlo*. Pridobljeno 29. oktobra. 2018 iz https://www.dnielectronico.es/PortalDNIE/PRF1_Cons02.action?pag=REF_300&id_menu=15
13. MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía. (brez datuma č). *Documento Nacional de Identidad electrónico*. Pridobljeno 31. oktobra. 2018 iz https://sede.policia.gob.es/portaCiudadano/sede/inf_dni.html
14. MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía. (brez datuma d). *DNI electronico - Para que se puede utilizar*. Pridobljeno 8. novembra. 2018 iz https://www.dnielectronico.es/PortalDNIE/PRF1_Cons02.action?pag=REF_280&id_menu=15
15. MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía. (brez datuma e). *PASAPORTE - Cómo es el pasaporte español*. Pridobljeno 10. decembra. 2018 iz https://www.dnielectronico.es/PortalDNIE/PRF1_Cons02.action?pag=REF_1080&id_menu=55
16. MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía. (brez datuma f). *Resources – Video*. Pridobljeno 31. oktobra. 2018 iz https://www.dnielectronico.es/PortalDNIE/PRF1_Cons02.action?pag=REF_3003&id_menu=51
17. MINISTERIO DEL INTERIOR, Dirección General de la Policía & Cuerpo Nacional de Policía. (brez datuma g). *DNI electronico- Diferencias DNIE y DNI 3.0*. Pridobljeno 5. oktobra. 2018 iz https://www.dnielectronico.es/PortalDNIE/PRF1_Cons02.action?pag=REF_038&id_menu=1
18. MINISTERIO DEL INTERIOR. (brez datuma). *Número de Identidad de Extranjero (NIE)*. Pridobljeno 22. november. 2018 iz <http://www.interior.gob.es/web/servicios-al-ciudadano/extranjeria/ciudadanos-de-la-union-europea/numero-de-identidad-de-extranjero-nie->
19. Ministrstvo za notranje zadeve Republike Slovenije. (2019). *EMŠO – Enotna matična številka občana*. Pridobljeno 19. januarja. 2019 iz http://www.mnz.gov.si/mnz_zasvasosebni_in_tajni_podatki/emso/

20. Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre. (2017a, 27.oktober). *GUIA DE REFERENCIA DEL DNIE CON NFC*. Pridobljeno 29. oktobra. 2018 iz https://www.dnielectronico.es/PDFs/Guia_de_Referencia_DNIE_con_NFC.pdf
21. Real Casa de la Moneda-Fabrica Nacional de Moneda y Timbre. (2019b). *Panel acceso a la Administración, - login único DNIE*. Google Play - Google store. Pridobljeno 1. novembra. 2018 iz <https://play.google.com/store/apps/details?id=com.dnieloginwidget>
22. Sánchez-García, J., García-Campos, J. M., Reina, D. G., Toral, S. L. & Barrero, F. (2016). *On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks*. *Future Generation Computer Systems* 64, str. 50-60. Pridobljeno 10. aprila. 2018 iz <http://dx.doi.org.nukweb.nuk.uni-lj.si/10.1016/j.future.2016.04.024>
23. Spanish Ministry of Interior. (2017, 26. oktober). *Smarter borders in Spain*. Pridobljeno 14. novembra. 2018 iz <https://www.icao.int/Meetings/TRIP-Symposium-2017/Presentations/BELDA.pdf>
24. Upravna enota Ljutomer RS. (brez datuma). *Biometrični potni list RS*. Pridobljeno 16. marca. 2018 iz http://www.upravneenote.gov.si/fileadmin/pageuploads/ue-ljutomer/pdf/Novice/biometricni_potni_listi.pdf
25. Wikipedia. (2019a, 10.maj). *Biometric passport*. Pridobljeno 25. novembra. 2018 iz https://en.wikipedia.org/wiki/Biometric_passport
26. Wikipedia. (2019b, 15.maj). *DNI (Spain)*. Pridobljeno 23. novembra. 2018 iz [https://es.wikipedia.org/wiki/DNI_\(Espa%C3%B1a\)#DNI_electr%C3%B3nico](https://es.wikipedia.org/wiki/DNI_(Espa%C3%B1a)#DNI_electr%C3%B3nico)
27. Wikipedia. (2019c, 20.maj). *Spanish passport*. Pridobljeno 25. novembra. 2018 iz https://en.wikipedia.org/wiki/Spanish_passport
28. Wikipedia. (2019č, 20.marec). *Documento Nacional de Identidad (Spain)*. Pridobljeno 22. novembra. 2018 iz [https://en.wikipedia.org/wiki/Documento_Nacional_de_Identidad_\(Spain\)](https://en.wikipedia.org/wiki/Documento_Nacional_de_Identidad_(Spain))