Prikaz koncepta nove informacijsko komunikacijske usluge e-ID

Kostervajn, Vinko

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:394928

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Vinko Kostervajn

PRIKAZ KONCEPTA NOVE INFORMACIJSKO KOMUNIKACIJSKE USLUGE e-ID

DIPLOMSKI RAD

Zagreb, 2015.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

PRIKAZ KONCEPTA NOVE INFORMACIJSKO KOMUNIKACIJSKE USLUGE e-ID

CONCEPT PREVIEW OF THE NEW INFORMATION AND COMMUNICATION SERVICE e-ID

Mentor: prof. dr. sc. Dragan Peraković

Student: Vinko Kostervajn, 0135217545

Zagreb, 2015.

SAŽETAK

e-ID (elektronički identitet) je način za ljude da se elektroničkim putem dokaže da su to oni za koga tvrde da jesu i na taj način dobe pristup raznim uslugama. Usluga e-ID omogućava građanima korištenje elektroničkih usluga od raznih davatelja usluga koji nude svoje elektroničke usluge putem središnjeg državnog portala. Tako npr. građani mogu kod kuće isprintati razne dokumente bez potrebnog odlaska u odabrane institucije, tvrtke i sl. Uslugom e-ID cjelokupan identitet korisnika bio bi svrstan u jedno, što znači da bi svi podaci korisnika bili na jednom mjestu. Poslovnim korisnicima ova usluga omogućuje pouzdanu potvrdu identiteta i mogućnost evidencije svojih korisnika. SWOT analizom će se prikazati prednosti i nedostaci usluge e-ID.

Identifikacija korisnika vrši se putem elektroničke osobne iskaznice koja služi kao jedinstveni identifikacijski dokument, što znači da korisnik ne mora više koristiti ostale iskaznice, nego bi elektronička osobna zamijenila više njih. Elektronička osobna iskaznica predstavlja pametnu karticu (eng. *Smart Card*) koja sadrži NFC (*Near Field Communication*) tehnologiju kratkog dometa koja omogućuje beskontaktne transakcije.

KLJUČNE RIJEČI: elektronički identitet, pametna kartica, NFC tehnologija, SWOT analiza, arhitektura usluge, vrijednosni lanac

SUMMARY

e-ID (electronic identity) is a way for people to prove electronically that they are who they say they are and thus gain access to a panel of services. Service e-ID enables citizens to use electronic services of various service providers who offer their services through a central electronic state portal. For example, citizens can at home print a variety of documents without visiting selected institutions, companies, etc. With service e-ID entire user identity would fall into one, which means that all user data is on one place. To business users, this service provides assurance of the identity and the ability to register their customers. SWOT analysis will show the advantages and disadvantages of service e-ID.

User identification performs through electronic ID card that serves as a unique identification document, which means that the user doesn't have need to use other cards, so electronic ID card will replace them. Electronic identity card is a smart card that contains the NFC (Near Field Communication) short-range technology that allows contactless transactions.

KEYWORDS: electronic identity, smart card, NFC technology, SWOT analysis, architecture of service, value chain

Sadržaj:

1. Uvod 1

2. Pojam informacijskog sustava 3

2.1. Funkcija informacijskog sustava u poslovnom sustavu 4

2.2. Elementi informacijskog sustava 4

3. Osobni identifikacijski dokumenti u Republici Hrvatskoj 7

3.1. Osobna iskaznica 7

3.2. Potrebna dokumentacija 8

3.3. Elektronički nosač podataka, vrste i rok važenja 8

3.4. Izdavanje nove osobne iskaznice 9

3.5. Iznimke kod izdavanja osobne iskaznice osobi s invaliditetom 10

3.6. Nestanak osobne iskaznice ili sumnja u zlouporabu 10

4. Razvoj i mogućnosti primjene pametne kartice 11

4.1. Pojam pametne kartice 11

4.2. Građa kartice 12

4.3. Način rada pametne kartice 13

4.4. Uporaba pametnih kartica 13

4.5. Vrste pametnih kartica 13

5. Ekosustav informacijsko komunikacijske usluge e-ID 19

5.1. Istraživanje i razvoj nove usluge e-ID 21

5.2. Vrijednosni lanac usluge e-ID 23

5.3. Tržišni segment 27

5.4. Arhitektura informacijsko komunikacijske usluge e-ID 27

5.5. Proces prijave korisnika u sustav usluge e-ID 32

6. SWOT analiza uvođenja usluge e-ID 36

7. Sigurnosni aspekti korištenja usluge e-ID 41

7.1. Osnove kriptografije 41

7.2. Digitalna vjerodajnica 43
7.3. Razlika između elektroničkog i digitalnog potpisa 44
7.4. Infrastruktura javnog ključa..... 48
7.5. Ispitivanje sigurnosti primjene informacijsko komunikacijske usluge e-ID 49
7.6. Krađa identiteta 51
7.7. Sigurnost osobne iskaznice..... 52
8. Scenarij kupnje ulaznice za nogometne utakmice HNS-a 55
9. Analiza ankete ispitanih korisnika..... 56
10. Zaključak 67
Popis literature..... 68
Popis kratica..... 71
Popis slika 72
Popis tablica 73
Popis grafikona..... 73

1. Uvod

U današnje se vrijeme ljudi susreću sa raznim vrstama iskaznica sasvim nepotrebno koje općenito služe za identifikaciju korisnika. Identifikacija se koristi kako bi se olakšali komercijalni i državni poslovi. Pojedinci mogu koristiti tradicionalne identifikacijske oblike transakcija licem u lice koji postaju sve manje korisni za poslovanje na Internetu. Kako bi se riješio problem Internet poslovanja, mnoge vlade stvaraju sustav nacionalne elektronske identifikacije (e-ID) koji omogućuje korisnicima da svoj identitet dokažu elektronskim putem nekom informacijskom sustavu. Nacionalni elektronički identifikacijski sustavi nude razne pogodnosti za pojedince, poduzeća i vladu. Takav sustav može pomoći u smanjenju krađe identiteta i omogućiti pojedincima sigurnosno rukovanje aplikacijama raznih davatelja usluga. Tvrtke na taj način mogu bolje iskoristiti upravljanje identitetom za komuniciranje sa svojim kupcima na Internetu, npr. autentifikacije korisnika za online aplikacije ili provjera starosti svojih kupaca.

Usluga e-ID koja će biti razrađena kroz rad, omogućuje korištenje elektroničkih usluga koje nude razni davatelji usluga putem središnjeg državnog portala, te omogućuje uporabu jedinstvenog identifikacijskog dokumenta u zamjenu za više njih. Elektronička osobna iskaznica (e-iskaznica) popraćena je NFC (*Near Field Communication*) tehnologijom koja omogućuje beskontaktne transakcije, te je takav način funkcionalnosti čini pametnom karticom.

Materija rada izložena je kroz 10 poglavlja:

1. Uvod,
2. Pojam informacijskog sustava,
3. Elektronička osobna iskaznica RH,
4. Razvoj i mogućnosti primjene pametnih kartica,
5. Ekosustav informacijsko komunikacijske usluge e-ID,
6. SWOT analiza uvođenja usluge e-ID,
7. Sigurnosni aspekti korištenja usluge e-ID,
8. Scenarij kupnje ulaznice za nogometne utakmice HNS-a,
9. Analiza ankete ispitanih korisnika,
10. Zaključak.

Drugo poglavlje opisuje informacijski sustav i njegove elementi zbog razumijevanja samog sustava i arhitekture usluge e-ID.

U trećem poglavlju bit će opisana elektronička osobna iskaznica koja se koristi trenutno u Republici Hrvatskoj. Uz funkcionalnost same iskaznice opisana je potrebna dokumentacija i način izdavanja iskaznice, koje su iznimke prilikom izrade iskaznice, te na koji način prijaviti nestanak osobne iskaznice.

U četvrtom poglavlju za razumijevanje same primjene e-iskaznice opisane su vrste pametnih kartica, način primjene istih, pojam pametnih kartica, te njihova građa i dimenzije.

Peto poglavlje opisuje ekosustav usluge e-ID. Definiranjem ekosustava odredit će se vrijednosni lanac i sudionici u sustavu nove usluge, a prikazom arhitekture pojasnit će se funkcionalnosti e-iskaznice i informacijskog sustava, te koje sve iskaznice bi bile uključene u dokument.

U šestom poglavlju SWOT analizom prikazat će se snage i slabosti takve usluge koje predstavljaju sadašnjost temeljenu na prošlosti. Dok će prilike i prijetnje predstavljati budućnost temeljenu na prošlosti i sadašnjosti. Na temelju SWOT analize prikazale bi se prednosti i nedostaci usluge.

Sedmo poglavlje opisuje sigurnosne aspekte korištenja usluge e-ID. Za način predstavljanja sigurnosnih aspekta zadužena je grana kriptografije i vrste kriptografskih sistema. Uz navedeno bit će objašnjena infrastruktura javnog ključa (PKI – *Public Key Infrastructure*), te na koji način PKI digitalno potpisuje vjerodajnice. Na sigurnost usluge djeluju razne prijetnje te će biti opisano ispitivanje sigurnosti primjene usluge, način krađe identiteta i elementi zaštite osobne iskaznice.

U osmom poglavlju opisan je način korištenja usluge e-ID na primjeru kupnje ulaznice za nogometne utakmice Hrvatskog nogometnog saveza.

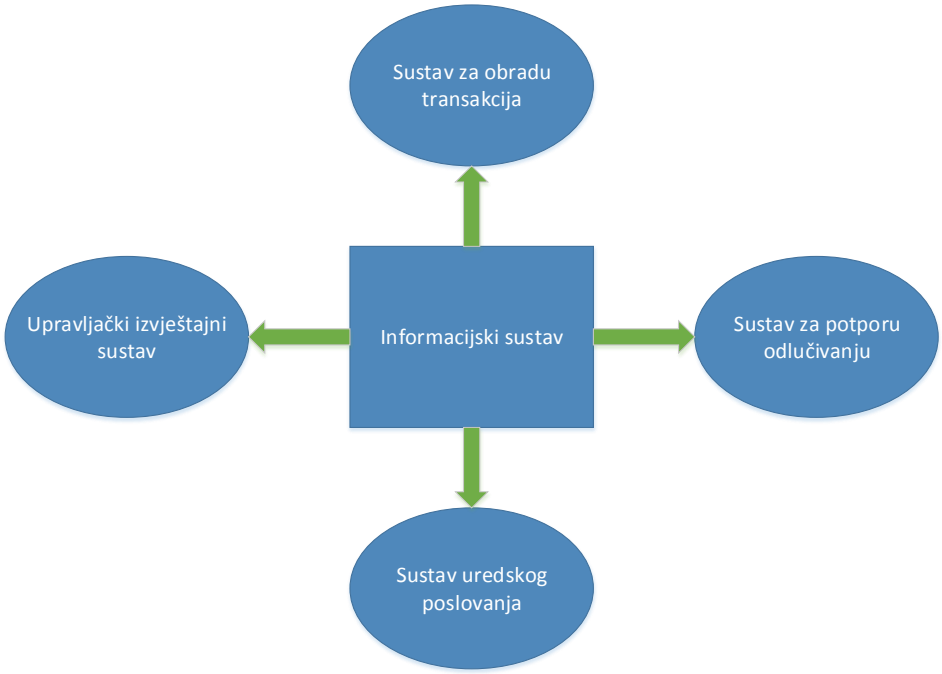
Deveto poglavlje opisuje rezultate ankete provedene u razdoblju između 2. i 10. rujna 2015. Rezultatima je prikazana zainteresiranost korisnika za korištenje nove informacijsko komunikacijske usluge e-ID.

2. Pojam informacijskog sustava

Informacijski sustav (IS) u strogoj definiciji je sustav koji prikuplja, pohranjuje, čuva, obrađuje, i isporučuje potrebne informacije na način da su dostupne svim članovima neke organizacije koji se njima žele koristiti te imaju odgovarajuću autorizaciju. No kraća, ali daleko složenija definicija glasi da je IS dio poslovnog sustava koji daje podatkovnu sliku procesa iz realnog sustava. To vrši modelom podataka, modelom procesa i modelom izvršitelja, [38].

- model podataka definira podatke koji se koriste u poslovnom sustavu.
- model procesa definira procese iz poslovnog sustava te opisuje funkcije po kojima se ti procesi mijenjaju.
- model izvršitelja definira sve koji su uključeni u izvršavanje procesa poslovnog sustava.

Kao dio IS-a, čovjek/pojedinac formalizira poslovno okruženje u podatke, procedure, algoritme, informacije i znanja te usklađujući primjenu informacijskih tehnologija i programske podrške, ispunjava poslovne funkcije i zadatke (dostavljanje i čuvanje podatka neophodnih za odlučivanje, održanje procesa te razvoj i neprekidnost poslovanja).



Slika 1. Dijelovi informacijskog sustava, [18].

Cilj je informacijskog sustava pribaviti informacije potrebne pri izvođenju poslovnog procesa i upravljanju poslovnim sustavom. Uobičajeni su dijelovi informacijskog sustava (Slika 1) sustav za obradu transakcija, upravljački izvještajni sustav, sustav za potporu odlučivanju i sustav uredskog poslovanja, a elementi informacijskog sustava prikazani su u nastavku, [19].

2.1. Funkcija informacijskog sustava u poslovnom sustavu

Informacijski sustav djeluje unutar nekog poslovnog sustava omogućavajući mu da komunicira unutar sebe i sa okolinom. Cilj informacijskog sustava je opskrbiti poslovni sustav sa svim potrebnim informacijama, potrebnim pri izvođenju poslovnog procesa i upravljanju poslovnim sustavom. Mnogobrojni pozitivni rezultati nastaju primjenom IS-a. Između ostalog ističu se uloge IS-a kao: pokretača poslovanja, osnovnog sredstva privređivanja, sredstva za stjecanje prednosti i razlikovanje, sredstva za unapređenje poslovanja, osnovnog podsustava organizacije, itd.

Informacijskim sustavom čovjek/pojedinac formalizira poslovno okružje u podatke, procedure, algoritme, informacije i znanja te usklađujući primjenu IT-a i programsku podršku, ispunjava poslovne funkcije i zadatke (dostavljanje i čuvanje podatka neophodnih za odlučivanje, održanje procesa te razvoj i neprekidnost poslovanja). Pri tom se IS u velikoj mjeri oslanja na ICT (informacijsko-komunikacijsku tehnologiju) te njihovom primjenom obrađuje, prenosi, pohranjuje, dohvaća i objavljuje informacije i podatke kojima se opisuje tijek, stanja i procesi poslovnog sustava.

Informacijski sustav djeluje unutar nekog poslovnog sustava, omogućavajući mu da komunicira unutar sebe i sa svojom okolinom. Slika prikazuje djelovanje informacijskog sustava unutar poslovnog sustava. U poslovni sustav ulaze i izlaze materijalni (materijal, sirovina, energija) i informacijski tokovi. Informacijski sustav preuzima informacije, obrađuje ih i prerađene prezentira poslovnom sustavu ili okolini. Informacijski je sustav dakle podsustav poslovnog sustava, [19].

2.2. Elementi informacijskog sustava

2.2.1. Hardware

Hardware spada pod materijalnu osnovicu koju čine informacijske tehnologije, npr. računala, radne stanice, modemi, fizičke linije za komunikaciju, itd. Hardware je

najniža razina računarskog sustava. Čine je svi dijelovi od koje je načinjen računalni sustav:

- svi mehanički dijelovi
- magnetski, električni i elektronički sastavni dijelovi
- naprave i uređaji (kućište, pogonski motor diska, magnetska vrpca, disk, poluvodička memorija, izvori električnog napajanja, integrirani sklopovi)

Hardware je osnovica računalnog sustava u koju spadaju:

- CPU - sastavljena od elektroničkih komponenti i nema mehaničkih dijelova
- glavne memorije kao osnovnog uređaja za pohranu podataka koja se također sastoji od el. komponenti i ne sadrži mehaničke dijelove
- ulazno-izlaznih uređaja (tipkovnica, zaslon, pisači, veze, sabirnice ...) i obično se sastoje od el. komponenti i različitih mehaničkih dijelova
- vanjska memorija koja se također sastoji od el. dijelova i različitih mehaničkih komponenti
- komunikacijski uređaji, [19].

2.2.2. Software

U *software* spada sva programska podrška koja se koristi pri radu tog sustava, te predstavlja skup svih programa koji se koriste u IS-u. Može se definirati kao onaj dio sustava koji postoji, ali ne u fizičkom obliku nego u obliku informacija pohranjenih na računalu. Sistemski software čine programi koji promatrano zajedno predstavljaju skup programa koji služe za kontrolu i rad strojne podrške pri računalnoj obradi podataka.

Software se dijeli na:

- aplikativni (korisnički programi) - skup korisničkih programa potrebnih za rješavanje raznih problemskih situacija koji proizlaze iz domene zadataka informacijskog sustava
- sistemski (sustavni programi) – skup strojno orijentiranih programa s funkcijom upravljanja i kontrole strojnog sustava u cilju sinkronizacije rada s aplikativnom podrškom, [19].

2.2.3. Lifeware

U *lifeware* ubrajamo "živu" komponentu IS-a. Odnosi se na zaposlenike, timove, njihovo znanje i sve osobe uključen u djelovanje IS-a. Čovjek je osnovna komponenta IS-a jer kao njegov dio čovjek/pojedinac formalizira poslovno okružje u podatke, procedure, algoritme, informacije i znanja te usklađujući primjenu IT-a i programsku podršku, ispunjava poslovne funkcije i zadatke (dostavljanje i čuvanje podatka neophodnih za odlučivanje, održanje procesa te razvoj i neprekidnost poslovanja), [19].

2.2.4. Orgware

Pod pojmom "orgware" se podrazumijeva organizacija tehničke opreme IS-a (hardware), programske opreme IS-a (software) i ljudi-izvršitelja poslova u IS-u u skladnu cjelinu, [19].

2.2.5. Netware

Netware je mrežna komponenta IS-a, tj. komunikacijska infrastruktura bazirana na informacijskim tehnologijama. Jedan od primjera su računalne mreže koje predstavljaju sustave povezanih računala. U mrežnom okruženju računala razmjenjuju podatke, dijele vlastite izvore, omogućavaju komunikaciju, paralelni rad, kreiranje virtualne organizacije itd.

Za ostvarenje računalne mreže potrebna je odgovarajuća softverska i hardverska podrška, a nazivamo je netware ili podrška za mrežu, [19].

2.2.6. Dataware

Dataware su svi sadržaji u informacijskom sustavu kojima se opisuju činjenice iz realnog svijeta i poslovnog sustava na koji se odnose a organizirani i oblikovani tako da budu razumljivi i da se mogu koristiti u poslovanju za donošenje odluka i ostvarivanje ciljeva i zadataka, [19].

3. Osobni identifikacijski dokumenti u Republici Hrvatskoj

3.1. Osobna iskaznica

Osobna iskaznica je elektronička javna isprava kojom dokazujete vaš identitet, hrvatsko državljanstvo, spol, datum rođenja i prebivalište u Hrvatskoj te je obavezna isprava za starije od 18 godina s prijavljenim prebivalištem u Hrvatskoj.

Pravo na hrvatsku elektroničku osobnu iskaznicu imaju svi hrvatski državljani bez obzira na godine života i bez obzira imaju li ili nemaju prebivalište u Hrvatskoj. Ako nemaju prebivalište u Hrvatskoj, upisat će se podatak o prebivalištu u inozemstvu i u tom slučaju osobna iskaznica ne služi kao dokaz prebivališta.

Zahtjev za izdavanje podnosi se policijskoj upravi ili postaji nadležnoj prema prebivalištu podnositelja, a osoba koja uz prebivalište ima prijavljeno i boravište, zahtjev može predati i u policijskoj upravi ili postaji nadležnoj prema mjestu boravišta. Oni s prebivalištem u inozemstvu, zahtjev podnose u bilo kojoj policijskoj upravi ili postaji, [20].



Slika 2. Osobna identifikacijska iskaznica RH, [16].

3.2. Potrebna dokumentacija

Prilikom podnošenja zahtjeva za izdavanje osobne iskaznice potrebno je:

- izvršiti uplatu ovisno o odabranom postupku izdavanja,
- dati na uvid ranije izdanu osobnu iskaznicu ili drugu javnu ispravu kojom se može provjeriti identitet i hrvatsko državljanstvo podnositelja zahtjeva (ranije izdana javna isprava s fotografijom, a identitet djece koja ne posjeduju osobne isprave potvrđuju roditelji svojom izjavom),
- priložiti jednu fotografiju u boji dimenzija 3,5 cm x 4,5 centimetra,
- potpisati Ugovor o davanju usluga certificiranja, [20].

3.3. Elektronički nosač podataka, vrste i rok važenja

Osobna iskaznica sadrži elektronički nosač podataka (čip) na koji se uz podatke ispisane u vizualnoj zoni kartice osobne iskaznice, mogu pohraniti jedan ili dva certifikata, i to:

- identifikacijski certifikat koji se koristi za elektroničku potvrdu identiteta i autentifikaciju prilikom pristupa elektroničkim uslugama,
- potpisni certifikat koji se koristi kao podrška naprednom elektroničkom potpisu i zamjenjuje vlastoručni potpis sukladno zakonu kojim je reguliran elektronički potpis.

Digitalni certifikati pohranjuju se ovisno o dobi:

- eOI izdana djeci do navršenih pet godina ne sadrži identifikacijski niti potpisni certifikat,
- eOI izdana djeci od navršenih pet do navršenih 18 godina sadrži identifikaciji certifikat,
- eOI izdana osobama od navršenih 18 do navršenih 65 godina sadrži identifikacijski i potpisni certifikat,
- osobe s navršenih 65 godina mogu po vlastitoj želji ishoditi osobnu iskaznicu s ili bez identifikacijskog i potpisnog certifikata.

Elektronička osobna iskaznica s aktivnim identifikacijskim certifikatom služi za prijavu u sustav e-Građani i druge e-usluge.

Uz potpisni certifikat, elektronička osobna iskaznica služi za obavljanje aktivnosti vezanih za ovjeru dokumenata elektroničkim potpisom kao valjanom zamjenom za vlastoručni potpis. Rok važenja osobnih iskaznica i certifikata koje sadrži je pet godina. Iznimno, osobna iskaznica koja je izdana osobi s navršenih 65 godina nema roka važenja.

Osoba s navršenih 65 godina koja ishodi osobnu iskaznicu koja sadrži certifikate, protekom roka važenja certifikata (pet godina) može nastaviti koristiti osobnu iskaznicu, ali njome neće moći obavljati elektroničku potvrdu svojeg identiteta niti će joj ona moći služiti za izradu naprednog elektroničkog potpisa. Ako će osoba s navršenih 65 godina nakon isteka roka važenja certifikata htjeti i dalje koristiti osobnu iskaznicu za osiguranje elektroničke potvrde svojeg identiteta te za izradu naprednog elektroničkog potpisa (kao elektroničku ispravu), morat će podnijeti zahtjev za izdavanje nove osobne iskaznice, [20].

3.4. Izdavanje nove osobne iskaznice

Prilikom zamjene osobne iskaznice kojoj je istekao rok važenja potrebno je priložiti staru osobnu iskaznicu koja se poništava i vraća. Ako podnositelju zahtjeva nije već izdana osobna iskaznica ili putovnica Hrvatske, potrebno je službenoj osobi dati na uvid domovnicu i izvadak iz matice rođenih ili rodni list. Osoba čije se ime i prezime sastoji od više riječi, koje se zbog broja slova koja sadrže ne mogu upisati u prostor za upis imena i prezimena, u obrazac osobne iskaznice upisat će se one riječi osobnog imena koje je osoba izjavom pred matičarom odredila za uporabu u pravnom prometu.

Iznimno, prilikom podnošenja zahtjeva za izdavanje osobne iskaznice nije potrebno priložiti fotografiju ukoliko je podnositelju zahtjeva u proteklih pet godina izdana putovnica ili osobna iskaznica koja sadrži OIB, za čije je izdavanje priložena fotografija, a izgled osobe nije značajno promijenjen.

Elektronička osobna iskaznica u redovnom postupku izdaje se u roku od 30 dana od dana podnošenja zahtjeva:

- cijena eOI koje se izdaju djeci do navršenih 5 godina koje ne sadrže certifikate je 60 kuna,
- cijena eOI koje se izdaju djeci od navršenih 5 godina i punoljetnim osobama koje sadrže jedan ili dva certifikata je 79,50 kuna,

- cijena eOI koje se izdaju osobama s navršenih 65 godina koje ne sadrže certifikate je 49,50 kuna.

Elektronička osobna iskaznica u ubrzanom postupku za sve podnositelje zahtjeva izdaju se u roku od 10 dana od dana podnošenja zahtjeva po cijeni od 195 kuna, a iskaznice u žurnom postupku za sve podnositelje zahtjeva izdaju se u roku od tri radna dana od dana podnošenja zahtjeva po cijeni od 500 kuna.

Osoba je dužna preuzeti izrađenu osobnu iskaznicu u roku od 90 dana od dana proteka roka za izdavanje osobne iskaznice, [20].

3.5. Iznimke kod izdavanja osobne iskaznice osobi s invaliditetom

Prilikom podnošenja zahtjeva za izdavanje osobne iskaznice osoba je dužna dati otisak papilarnih linija lijevog i desnog kažiprsta. Ako osoba nema kažiprst ili je vrh kažiprsta ozlijeđen, uzima se otisak srednjeg ili nekog drugog prsta, a ako nema jedne ruke uzima se otisak kažiprsta i srednjeg ili nekog drugog prsta druge ruke. Otisci papilarnih linija se ne uzimaju ako to zbog medicinskih razloga, koji nisu privremeni, nije moguće.

Fotografija koja se prilaže zahtjevu za izdavanje osobne iskaznice treba vjerno prikazivati osobu koja podnosi zahtjev, bez pokrivala za glavu. Iznimno se može uzeti fotografija na kojoj je osoba fotografirana s pokrivalom za glavu ako pokrivalo nosi iz medicinskih razloga, pod uvjetom da pokrivalo ne prekriva obraze, bradu i čelo.

Također iznimno, slijepe osobe koje nose tamne naočale mogu priložiti fotografije na kojima su fotografirane s tamnim naočalama, te im se na njihov zahtjev izdaje osobna iskaznica na kojoj se na poleđini nalazi oznaka za osobnu iskaznicu „OI“ na Brailleovom pismu, [20].

3.6. Nestanak osobne iskaznice ili sumnja u zlouporabu

Osoba je dužna bez odgode najbližoj policijskoj upravi ili postaji prijaviti nestanak, sumnju u zlouporabu ili pronalazak osobne iskaznice.

Ako je osobna iskaznica nestala ili pronađena u inozemstvu, osoba je dužna njezin nestanak ili pronalazak prijaviti najbližoj diplomatskoj misiji/konzularnom uredu Republike Hrvatske koji je o tome dužan bez odgode obavijestiti policijsku upravu ili postaju koja je osobnu iskaznicu izdala, [20].

4. Razvoj i mogućnosti primjene pametne kartice

4.1. Pojam pametne kartice

Pametna kartica je mala kartica ili sličan uređaj s ugrađenim integriranim kružnim čipom. Obično izgledaju kao kreditne kartice, iako može poprimit različite oblike. Ono što čini kartice pametnim je ugrađen čip koji je snažan kao mini računalo te se može programirati za različite aplikacije.

Čip omogućuje pametnoj kartici pohranu i sigurnosni pristup podacima i aplikacijama, te sigurnu razmjenu podataka između čitača i drugih sustava. Tehnologija pametne kartice omogućuje visok stupanj razine sigurnosti i zaštite privatnosti, što čini pametnim karticama idealne za rukovanje osjetljivih informacija kao što su identitet osobe, zdravstvene informacije i sl., [4].

Mnoge vlasti planiraju uvesti, ili su već uvedeni elektronski čitljivi uređaji koji se obično koriste kao sredstva identifikacije, kao što su osobna iskaznica, putovnica, te vozačka dozvola. Namjera je općenito napraviti jednostavniju potvrdu identiteta, praktičnu uporabu te pouzdan način procesiranja informacija kako bi se poboljšala sigurnost dodajući dimenziju težeg načina krivotvorenja dokumenata. Međutim postoje neke nedoumice da sigurnost u stvari može biti ugrožena takvim dokumentima, te osobna privatnost i sloboda može biti povrijeđena neprimjetno ilegalnim skeniranjem.

Tri su važne i nezavisne dimenzije prostora malih identifikacijskih uređaja: da li je uređaj sposoban aktivnom računanju ili sadrži samo podatke na sebi (pametan ili ne); da li je uređaj sposoban komunicirati na neku udaljenost ili je potreban fizički kontakt (kontaktno ili beskontaktno); da li uređaj sadrži samostalno napajanje ili je napajan od strane čitača (aktivno ili pasivno). Svaki uređaj sadrži neki iznos kapaciteta za pohranu podataka, a mnogim, čak i onim bez napajanja, moguće je mijenjati podatke u tijeku normalne uporabe.

Uređaji su često ugrađeni u većim karticama tipa kreditne kartice, što uzrokuje pogrešnu predodžbu o njihovim veličinama. Uređaj obično koristi površinu od 10 četvornih milimetara na samoj kartici, te su izrazito tanki, [5].

4.2. Građa kartice

Većina pametnih kartica je napravljena od slojeva različitih materijala ili podloga, što prilikom njihovog spajanja kartici omogućuje specifične funkcionalnosti. Tipični primjeri kartica danas su izrađeni od PVC-a (polovinil klorid), poliestera ili polikarbonata. Slojevi kartica prvo su tiskani, a zatim prešani velikim pritiskom. Slijedeći korak izrade je rezanje pomoću kalupa, te nakon toga slijedi ugradnja čipa i dodavanje podataka na karticu. Ukupne komponente, uključujući software i plastiku, mogu sadržavati do 12 zasebnih stavki, sve to u jednom paketu koji se pojavljuje korisniku kao jednostavna kartica, [21].



Slika 3. Figurativno prikazana pametna kartica kroz slojeve, [21].

Pametne kartice najčešće dolaze u tri formata:

- ID-0 (85.6mm x 54mm x 0.76mm),
- ID-00 (66mm x 33mm x 0.76mm),
- ID-000 (25mm x 15 mm x 0.76mm).

ID-0 je format kreditnih kartica, a ID-000 je format GSM SIM kartica. Format ID-0 je najčešći te ga, osim kod kreditnih kartica susrećemo kod osobnih iskaznica, [14].

4.3. Način rada pametne kartice

Pametna kartica se spaja na čitač kartica putem izravnog fizičkog kontakta ili putem udaljenog, beskontaktnog radio-frekvencijskog sučelja. Tipična kontaktna kartica ima plastično „tijelo“, čip unutar tijela i kontaktnu ploču koja je obično pozlaćena, te je vidljiva na površini kartice. Za rad, pametna kartica se umetne u čitač pametnih kartica, koji dodiruje kontaktnu ploču. Naredbe, podaci i status kartice se prenosi preko fizičkih kontaktnih točaka.

Beskontaktne pametne kartice izgledaju isto kao kontaktne, ali bez kontaktne ploče. Komuniciraju s čitačem kroz beskontaktno radio-frekvencijsko sučelje. Za rad, beskontaktna pametna kartica nalazi se u neposrednoj blizini čitača te se naredbe i podaci prenose bez ikakvog fizičkog dodira, [4].

4.4. Uporaba pametnih kartica

Pametne kartice trenutno se koriste za mnoge aplikacije po cijelom svijetu, uključujući:

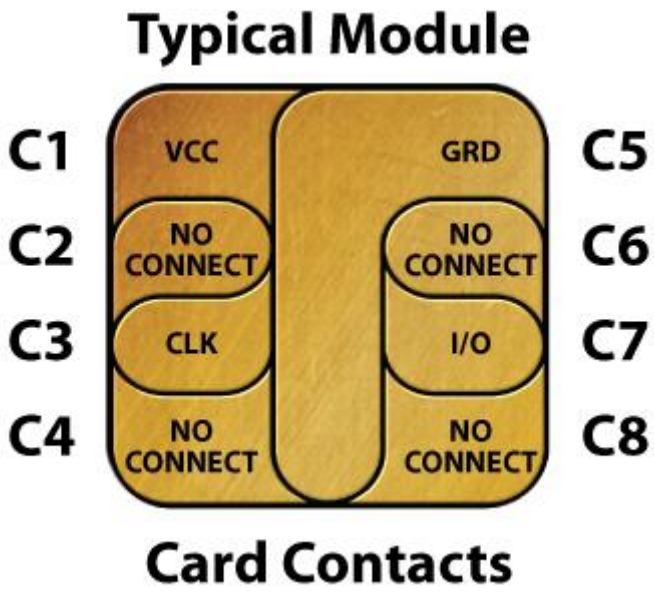
- identifikacijske aplikacije: identifikacijski dokumenti zaposlenika za fizički pristup zgradama, sigurnosni računalni i mrežni pristup, elektronička osobna iskaznica, elektronička putovnica, elektronička vozačka dozvola, kartice za provjeru autentičnosti osobe i sl.,
- zdravstvene aplikacije: građanske zdravstvene iskaznice, te iskaznice pacijenata, kartice prijenosnog medicinskog zapisa i sl.,
- platne aplikacije: kontaktne i beskontaktne kreditne i debitne kartice, tranzitne kartice za plaćanje i sl.,
- telekomunikacijske aplikacije: identifikacijski moduli kod mobilnog pretplatnika, kartice za plaćanje telefonskih poziva i sl., [4].

4.5. Vrste pametnih kartica

4.5.1. Kontaktne kartice

Kontaktne kartice su najčešći tipovi pametnih kartica. Električni kontakti nalaze se na vanjskoj strani kartice te se spajaju na čitač kartica kada je kartica umetnuta. Priključak je vezan na zatvoreno kućište čipa na kartici, [21].

Kontaktne kartice imaju dodirnu površinu oko jednog kvadratnog centimetra koja obuhvaća nekoliko pozlaćenih kontaktnih polja. Polja osiguravaju električnu povezanost kada je kartica umetnuta u čitač, koji se koristi kao komunikacijski medij između pametne kartice i sučelja (npr. računalo) ili mobilnog uređaja. Kartice ne sadrže bateriju, već se napajanje koristi od strane čitača, [22].



Slika 4. Kontaktni čip pametne kartice, [21].

Osnovno obilježje kontaktnih pametnih kartica je čip. Čip je krhak i podložan vanjskim uvjetima kao što su torzija i savijanje. Zbog toga je čip ograničen na veličinu od 25mm2. Pametna kartica ima 8 kontaktnih točaka:

- C1 - Vcc kontakt dovodi se napajanje; naponska razina je 3V ili 5V s maksimalnim odstupanjem od 10%,
- C2 - RST (eng. *reset*) kontakt služi za resetiranje mikroprocesora,
- C3 - CLK (eng. *clock*) je signal vremenskog vođenja,
- C5 - GND (eng. *ground*) kontakt se koristi kao referentna naponska razina; najčešće je to nulta razina,
- C6 - Vpp kontakt je opcionalan i koristi se samo kod starih tipova kartica koje su zahtjevale korištenje dvije programske razine; niža razina označavala je pasivno stanje, viša razina se koristila za pisanje u EEPROM; današnji mikrokontroleri koriste ugrađenu strujnu pumpu,

- C7 - I/O (eng. *Input/Output*) kontakt služi za komunikaciju između kartice i vanjskog svijeta i obratno,
- C4 i C8 - RFU (eng. *Reserved for Future Use*) kontakti su rezervirani za buduća proširenja, [14].

Povećana razina procesorske snage, fleksibilnosti i memorije će zatražit veći trošak. Kartice pojedinačnih funkcija općenito su najisplativije rješenje. Odabir odgovarajuće pametne kartice određuju se prema potrebama korisnika uključujući razinu sigurnosti, vrednovanje troškova, te funkcionalnosti u odnosu na troškove drugih hardverskih elemenata, [21].

4.5.2. Memorijske kartice

Memorijske kartice ne mogu upravljati datotekama i nemaju procesorsku snagu za upravljanje podacima. Sve memorijske kartice komuniciraju sa čitateljima kroz sinkrone protokole. U memorijskim karticama sve se čita i bilježi na fiksnim adresama kartice. Prije projektiranja kartica potrebno je odrediti da li terminali, tj. čitači podržavaju komunikacijske protokole koje sadrži čip. Tri su primarna tipa memorijske kartice:

- kartice s običnom memorijom,
- zaštićene kartice,
- kartice pohranjene vrijednosti, [21].

4.5.2.1. Obične memorijske kartice

Obične memorijske kartice imaju jednostavan način pohranjivanja podataka i nemaju mogućnost obrade istih. Često su napravljene sa I2C[1] ili *flash* serijskim poluvodičem, te spadaju u najniži cjenovni rang. Ove kartice se ne mogu identificirati od strane čitača, tako da računalni sustav mora znati kakav tip kartice se stavlja u čitač. Kartice se lako kopiraju i ne mogu se pratiti od strane identifikatora kartica, [21].

4.5.2.2. Zaštićene memorijske kartice

Zaštićene memorijske kartice imaju u sebi ugrađenu logiku za kontrolu pristupa memoriji kartice. Ponekad nose i naziv „Inteligentne memorijske kartice“, te mogu zaštititi cijeli niz memorije. Također se karticama može ograničiti pristup na pisanje i čitanje, što se obično štiti lozinkom ili sistemskim ključem. Kartice se mogu

[1] I2C ("Inter-Integrated Circuit"), omogućuje dobru podršku za komunikaciju sa različitim sporijim periferijskim jedinicama u sistemima gdje se potreba za njihovim korištenjem javlja povremeno.

podijeliti u logičke dijelove za planiranu multi-funkcionalnost, te ih nije lako kopirati i razmnožavati, ali može biti razbijena šifra od strane hakera (*eng. Hacker*). Oni obično mogu popratiti identifikator na kartici, [21].

4.5.2.3. Kartice pohranjene vrijednosti

Kartice pohranjene vrijednosti dizajnirane su za specifične potrebe skladištenja neke vrijednosti. Mogu biti jednokratne i kartice na koje se može dodavati vrijednost. Prilikom proizvodnje, na karticu se ugrađuje trajna mjera sigurnosti, te može sadržavati lozinku i logiku koja je teško kodirana u čip od strane proizvođača. Za jednostavne aplikacije, kao što su telefonske kartice, čip ima 60 ili 12 memorijskih stanica, jedna za svaku telefonsku jedinicu. Memorijska stanica je svaki put izbrisana kada je telefonska jedinica koristi. Nakon što se sve memorijske jedinice iskoriste, kartica postaje beskorisna i može se baciti. Ovaj proces može biti obrnut u slučaju punjive kartice, [21].

4.5.3. CPU/MPU Mikroprocesorske multifunkcionalne kartice

Mikroprocesorske multifunkcionalne kartice imaju na kartici dinamičke mogućnosti obrade podataka. Izdvajaju memoriju u različite neovisne dijelove ili datoteke dodijeljene specifičnim funkcijama ili aplikacijama. Unutar kartice nalazi se mikroprocesor ili mikrokontroler koji upravlja dodjelom memorije i omogućuje pristup datotekama. Čip koji se nalazi na kartici sličan je onima u osobnim računalima, te upravlja podacima u organiziranim strukturama datoteka preko operativnog sustava kartice (eng*. COS – Card Operating System*).

Za razliku od drugih operativnih sustava, ovaj softver kontrolira pristup korisničke memorije na kartici. Ova sposobnost dopušta različite funkcije ili aplikacije na kartici, omogućujući tvrtkama izdavanje i održavanje raznolikosti proizvoda preko kartice. Primjer za to je debitna kartica koja omogućuje pristup zgradama sveučilišnog kampusa. Multifunkcionalne kartice daju korist izdavačima za promoviranje svojih proizvoda. Naime, tehnologija omogućuje sigurnu identifikaciju korisnika i omogućava ažuriranje informacija, bez zamjene instalirane baze, čime se pojednostavljuje promjene programa i smanjuju troškovi. Za korisnike multifunkcionalnih kartica to znači veće povjerenje i sigurnost, te u konačnici, integracija više kartica koje služe u mnogo svrha.

Postoje mnoge konfiguracije čipova u ovoj kategoriji, uključujući i one koji podržavaju funkcije kriptografske strukture javnih ključeva (*eng. PKI – Public key infrastructure*). Te vrijedi pravilo kartica – što više funkcija, veća cijena, [21].

4.5.4. Beskontaktne kartice

Beskontaktne kartice su pametne kartice koje koriste radiofrekvenciju između kartice i čitača bez fizičkog umetanja kartice u čitač. Umjesto toga, kartica se stavlja s vanjske strane, tj, prislanja se na čitač, te na taj način se iščitavaju podaci. Ove kartice funkcioniraju s ograničenjem memorije i komuniciraju na 125MHz. Druga vrsta ograničene kartice je Gen2 UHF kartica koja radi na frekvenciji između 860 i 960 MHz.

Prve kartice koristile su se na transportnim aplikacijama gdje nije bilo potrebe za velikom vrijednosti, te sigurnost nije bila toliko bitna. Komuniciraju na 13,56MHz, te su u skladu s normama ISO 14443. Ove kartice često su zaštićeni tipovi memorije. Dobile su popularnost u maloprodajnim aktivnostima jer mogu ubrzati transakcije (npr. Visa i MasterCard), za razliku od tradicionalnih pametnih kartica.



Slika 5. NFC pametna kartica i čitač, [38].

Prednost kontaktnih kartica u odnosu na beskontaktne kartice je ta što su kontaktne kartice manje osjetljive na torzije i savijanja. Također, kod beskontaktne kartice, postoji potencijalna opasnost da se bez znanja vlasnika presretnu podaci ili izvedu neke kartične transakcije. Zbog sigurnosnih razloga transakcije beskontaktnih pametnih kartica traju kraće nego transakcije kontaktnih kartica, pa se zbog toga pri transakciji s beskontaktnim karticama prenesu manje količine podataka, [14].

4.5.5. Multimodalne komunikacijske kartice

Ove kartice imaju više metoda komunikacije, te uključuju ISO7816, ISO14443 i UHF gen2. Kako je kartica napravljena određuje da li je hibridna ili ima dvostruko sučelje. Termin ove kartice također uključuje kartice koje imaju magnetsku traku ili barkod kao način komunikacije, [21].

4.5.6. Više komponentne kartice

Više komponentne kartice rađene su za određena tržišna rješenja. Na primjer, postoje kartice gdje je izrađen senzor za otisak prsta ili kartica koja generira jednokratnu zaporku i prikazuje podatke za korištenje online bankarstva. Vrijednosne kartice imaju magnetsku prugu na kojoj se mogu podaci mijenjati, te svaka od ovih tehnologija je specifična za posebnog dobavljača koji posluje na različite načine, [21].

4.5.7. Hibridne kartice

Kartica sa dvostrukim sučeljem koja uključuje beskontaktno i kontaktno sučelje na istoj kartici. Primjer je kartica javnog prijevoza u Portu zvana Andante, koja sadrži čip koji funkcionira beskontaktno ili kontaktno, ovisno o potrebama (ISO/IEC 14443 Type B), [22].

5. Ekosustav informacijsko komunikacijske usluge e-ID

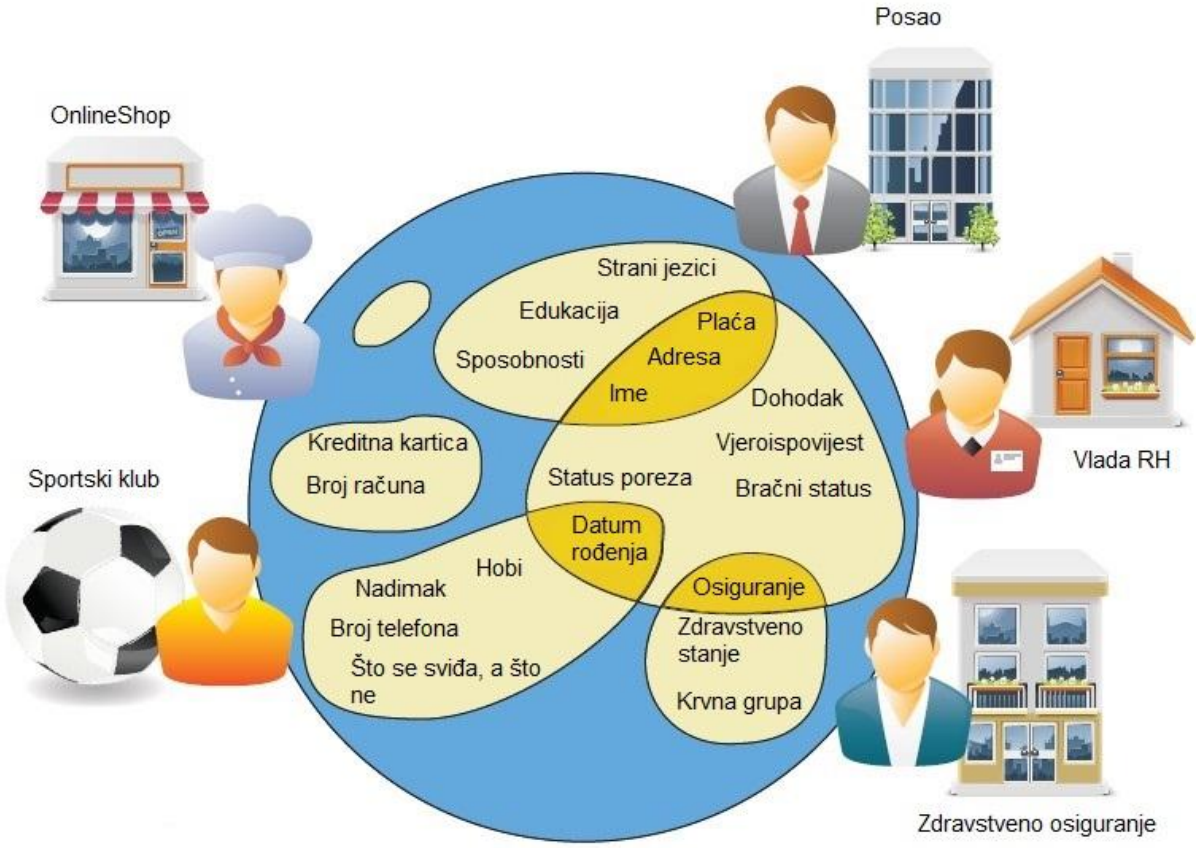
Elektronički identitet (e-ID) je način za ljude da se elektroničkim putem dokaže da su to oni za koga tvrde da jesu i na taj način dobe pristup raznim uslugama. Sposobnost za povezivanje skupa podataka za korisnika, te djelotvorno i sigurno rukovanje korisničkim podacima, zahtijeva neophodan broj različitih interakcija. Elektronički identitet razlikuje se od digitalne iskaznice, čak i ako bi se u nekim slučajevima dva koncepta mogli konvergirati, [23].

U pogledu elektroničkog identitet jedna osoba može biti uključena u više sektora (npr. Oporezivanje, socijalna sigurnost, obrazovanje, banka, telefonske usluge i sl.), a također često ispunjava različite uloge (građana, državnog službenika, odvjetnika, „oca“ i sl.), ovisno o kontekstu. Svim podacima treba upravljati na odgovarajući način. Suočavanje sa bogatim sadržajem informacija pohranjenih u elektroničkom identitetu, zahtijeva odgovarajuće zakonske odredbe u pogledu zaštite podataka i osobne kontrole osobnim podacima pojedinaca, što će biti opisano u poglavlju sigurnosni aspekti korištenja usluge e-ID.

Korisnikov identitet može se prikazati kao skup atributa, ili općenitije, skup informacija koje jedna stranka[2] zna o korisniku. Dakle, jedan identitet postoji samo u vezi sa strankom jer različite stranke znaju različite stvari o istom korisniku. Svaki korisnik ima različit identitet, moguće i više identiteta sa svakom strankom kojom komunicira. Da se provjeri autentičnost atributa, stranka može izvesti provjeru identiteta na samom atributu korisnika (Npr. zahtjevaju od korisnika da osigura fizički dokument) ili se osloniti na specijaliziranog izdavatelja koji provjerava sam identitet korisnika, [6].

Na primjer, na slici, Marko ima mnogo različitih atributa, od kojih podskupovi čine Markove (ime uzeto za primjer) različite identitete koji komuniciraju online s ljudima i institucijama. Identiteti dijele jedinstveni atribut koji može biti povezan; primjerice, njegov broj socijalnog osiguranja može se povezati preko svojeg identiteta sa atributima u zdravstvenom osiguranju dok se ostali identiteti ne mogu povezati. Marko bi trebao biti u mogućnosti upravljati svojim identitetom na isti način kako i uspijeva u „svijetu baziranom na papirima“.

[2] Strankom su nazvane sve državne i zdravstvene institucije, tvrtke i poduzeća, banke, te male institucije tipa nogometni klub gdje se može implementirati usluga e-ID.



Slika 6. Atributi elektroničkog identiteta u infrastrukturi, [6].

Takvo upravljanje korisničkim identitetom zahtjeva dva osnovna mehanizma: jedan za prijenos ovjerenih atributa od izdavatelja do oslanjajuće stranke i jedan za provjeru autentičnosti korisnika u utvrđenom identitetu. Prijašnji mehanizam bitan je za obavljanje pouzdanih elektroničkih transakcija i zahtjeva za kriptografiju. Potonji mehanizam može u načelu biti realiziran s jednostavnim korisničkim imenom i lozinkom, ali to daje loše sigurnosne garancije. Doista, lozinke su jako osjetljive na nasumično pogađanje, nagađanje tj. krađu identiteta i napada socijalnim inženjeringom. Nesigurnost lozinke utječe previše na privatnost. Za ublažavanje nedostataka, mnogi davatelji usluga prikupljaju više irelevantnih informacija (npr. lokacija ili povijest transakcija) o korisnicima kako bi mogli analizirati te podatke za otkrivanje sumnjivog ponašanja i potencijalne povrede. Dakle, za jači kriptografski mehanizam potrebno je uključiti kriptografiju javnog ključa što je opisano pod poglavljem sigurnosni aspekt korištenja usluge e-ID.

U svijetu baziranom na papirima prijenos atributa i autentifikacije su često stavljene u jedan mehanizam. Na primjer, vozačka dozvola prenosi atribut „Čovjeku je dopušteno voziti auto“ od izdavatelja do bilo koje za to zadužene stranke, te stranka vidi sliku na vozačkoj dozvoli i provodi mehanizam autentifikacije.

Kod ostvarivanja prijenosa atributa i autentifikacije u digitalnom svijetu, oponašajući rješenja bazirana na papirima, kako se često događa, nije dovoljno. Umjesto toga, u obzir se uzimaju različite okoline: digitalni podaci se jednostavno kopiraju i gotovo je nemoguće virtualno kontrolirati jednom kad su pušteni. Dakle, bilo koje stvaranje i omogućavanje podataka mora slijediti princip minimizacije. Kada korisnik prenosi atribute od izdavatelja do oslanjajuće stranke, nijedna stranka ne bi trebala biti u mogućnosti saznati bilo koju informaciju koju već prijenosni atribut nije pokazao, čak i ako stranke surađuju.

Naravno, sustav upravljanja identitetom koji se pridržava takvih načela ne može eliminirati svu svjetsku digitalnu opasnost. Komunikacija i pohranjene informacije trebaju uvijek biti kriptirane. Osjetljivi podaci trebaju biti popraćeni sa pravilima korištenja: tko ih može koristiti, za koju svrhu će se koristiti i kada ih izbrisati, [6].

5.1. Istraživanje i razvoj nove usluge e-ID

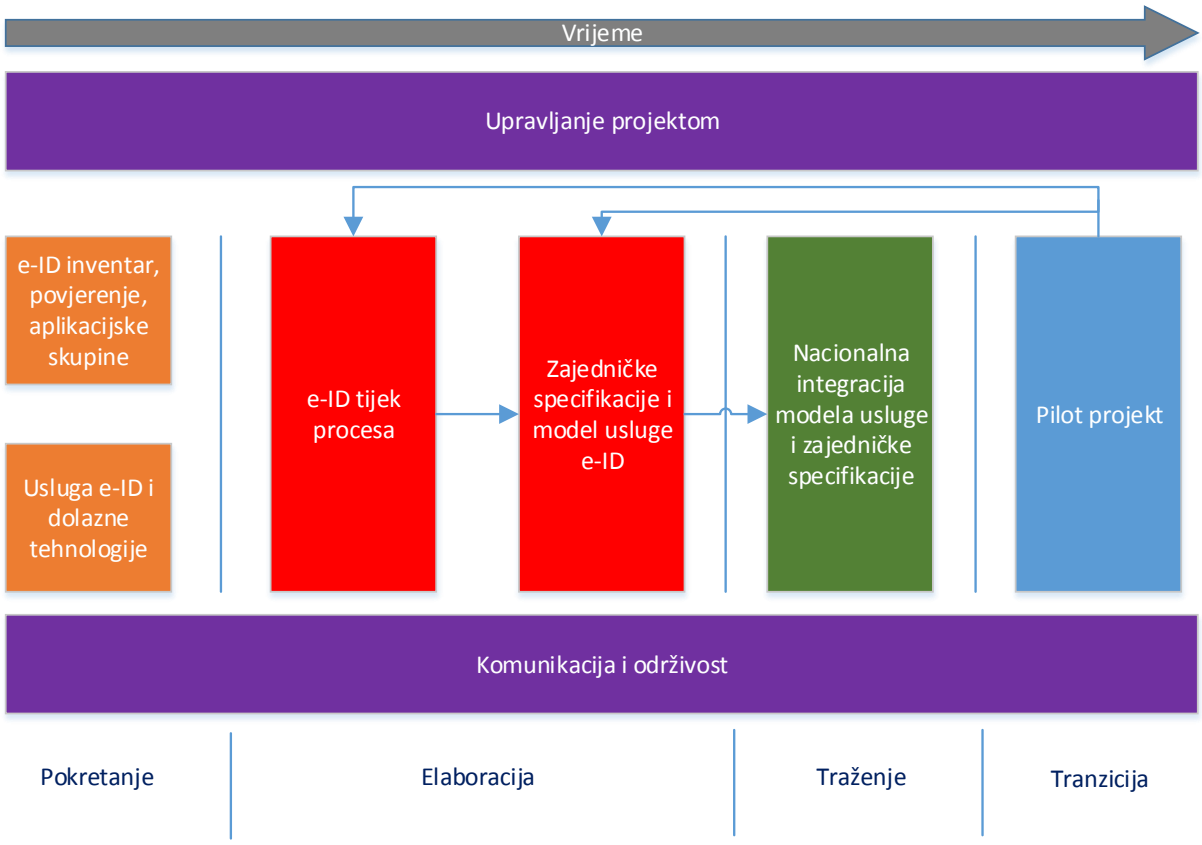
Istraživanje se opisuje kao aktivan, ustrajan i sustavan proces proučavanja s ciljem otkrivanja, tumačenja i pojašnjavanja činjenica. Ovo intelektualno proučavanje provodi se s ciljem stvaranja višeg znanja o događajima, ponašanju, te primjenjivim teorijama i zakonima. Termin istraživanje se također koristi pri opisivanju cijelog skupa informacija o određenoj temi, a obično se vezuje uz znanost i znanstvenu metodu istraživanja. Istraživanja se financiraju od strane javnih ustanova, dobrotvornih organizacija, te privatnih skupina i poduzeća.

Označava sustavno stvaranje novih spoznaja i vrijednosti, otvara nova pitanja, te generira nove ideje, nova rješenja i alternative, a obuhvaća:

- točno određivanje onoga što se želi znati,
- određivanje od koga se želi prikupiti podatke,
- izbor načina prikupljanja podataka,
- odabir načina obrade rezultata, [24].

Proces istraživanja teče u smjeru od početka istraživanja nove usluge prema kraju, a može se podijeliti u 4 faze:

- pokretanje
  - postavlja se pitanje o novoj usluzi,
  - temeljem pitanja generiraju se ideje i vizije,
- elaboracija
  - proces u kojem se prelazi s vizija na ciljeve,
- traženje
  - traže se rješenja, stvaraju alternative,
  - analiziraju se rizici pojedinih rješenja,
- tranzicija
  - ocjenjuje se napredak, kvaliteta istraživanja, te da li treba pokrenuti razvoj nove usluge, [17].

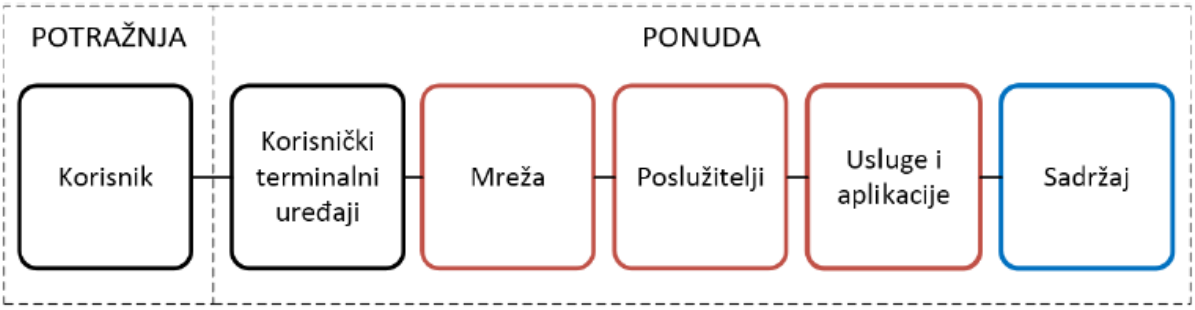


Slika 7. Istraživački proces e-ID usluge, [25].

5.2. Vrijednosni lanac usluge e-ID

Vrijednosni lanac opisuje različite proizvode i usluge te njihove odnose. Svaka karika lanca dodaje novu vrijednost prije negoli rezultat svojih aktivnosti preda sljedećoj karici u lancu. Osnovni vrijednosni lanac informacijsko komunikacijske tehnologije obuhvaća sljedeće elemente:

- korisnik – građani,
- korisnička oprema,
- mreža,
- poslužitelj,
- usluge i aplikacije,
- sadržaj, [1].



Slika 8. Vrijednosni lanac informacijsko komunikacijske usluge, [17].

Za razumijevanje odnosa na tržištu potrebno je poznavati informacijsku i komunikacijsku tehnologiju te pripadajući joj vrijednosni lanac (eng. *value chain*), s definiranom ponudom i potražnjom. Vrijednosni lanac uključuje korisnika koji, služeći se svojom opremom, putem mreže komunicira s drugim korisnicima ili pristupa poslužiteljima za različite usluge i primjene, uključujući i informacijske sadržaje dostupne korisnicima. Kako je riječ o dijelovima vrijednosnog lanca koji sve povezuju, međunarodno normiranje i standardizacija na području informacijske i komunikacijske tehnologije preduvjet su za globalnu primjenu opreme i transparentnost usluga, [1].

Vrijednosni lanac će u daljnjem tekstu biti objašnjen za tvrtku e-ID d.o.o. koja omogućuje uslugu e-ID za sve građane Republike Hrvatske. Usluga e-ID općenito omogućuje pristup korisnika različitim davateljima usluga preko web aplikacije, tj. uslugama koje davatelji nude. Tvrtka e-ID d.o.o. omogućuje identifikacijski i autentifikacijski sustav (IAS) pomoću kojeg je moguća identifikacija i autentifikacija

korisnika za različite davatelje usluga, te na taj način sustav daje potvrdu davatelju o valjanosti korisničkih podataka.

5.2.1. Korisnik

Korisnik općenito predstavlja potrošača neke usluge ili aplikacije, te pristupa mreži. U vrijednosnom lancu, korisnici predstavljaju građane koji koriste uslugu elektroničkog identiteta. Korisnici mogu biti segmentirani na fizičke (privatne) i pravne osobe, te se način korištenja usluge može podijeliti na dva načina, tj. dvije vrste sudjelovanja u vrijednosnom lancu. Jedna strana koja može sudjelovati u korištenju elektroničkog identiteta je osoba sa osobnim identifikacijskim dokumentom koja pristupa usluzi, a druga strana (davatelj usluge) koristi uslugu na način dobivanja korisničkih podataka, tj. autorizacije korisnika. Na primjer, dolazak korisnika u ljekarnu, prislanjanjem osobne iskaznice na čitač, zaposlenik u ljekarni vidi podatke o osobi za koje ima pristup, te izdaje poslani recept od strane zdravstvene ustanove. Na taj način korisnik pristupa usluzi, a ljekarna pristupa usluzi na način dobivanja podataka o korisniku.

Usluga e-ID pruža pogodnosti za sve sudionike uključene u vrijednosni lanac. Korisnik ima veliku prednost u smislu pristupa i dostupnosti usluge zbog mogućeg korištenja na računalima, tabletima i pametnim mobilnim terminalnim uređajima. Posebnu pozornost vrijedi naglasiti da je usluga *userfrendly*, što znači da je maksimalno prilagođena korisnicima. Usluga e-ID ovisi o drugim davateljima usluga, te se na temelju njih i njihovog sadržaja formira dostupnost i prilagodljivost usluge, [7].

5.2.2. Korisnička oprema

Korisničkom opremom (eng. *user equipment*) naziva se uređaj kojim raspolaže krajnji korisnik (eng. *end-user*), [1]. U tom slučaju osobni identifikacijski dokument, tj. elektronička osobna iskaznica te različiti pristupni uređaji npr. računala, tableti i pametni mobilni terminalni uređaji predstavljaju korisničku opremu. Za čitanje podataka sa osobne iskaznice potrebna je mrežna i komunikacijska oprema, tj. NFC čitači i računalna oprema, te programsko sučelje (eng. *software*) odnosno program preko kojeg funkcionira usluga.

Usluga e-ID također omogućuje integraciju aplikacija i programskih sučelja u novu *cloud* infrastrukturu, što će zauzvrat pružiti pogodnosti za davatelje usluga. Na

taj način će biti omogućeno da koriste provjerenu autorizaciju bez potrebe za ulaganjem u tehnologije i ispunjavanje uvjeta zakonskih obveza. To će također pružiti nove poslovne prilike za aplikacije i davatelje usluga te određivanje novog tržišnog segmenta potrošača, koji su izbjegavali korištenje takvih usluga zbog pitanja povjerenja ili zabrinutosti zbog privatnosti.

5.2.2.1. Uređaji u javnim institucijama

Uređaji postavljeni u javnim institucijama predstavljaju računalne uređaje na kojima građani mogu uz prislanjanje e-iskaznice dobiti pristup dokumentima vezanim za instituciju u kojoj je uređaj postavljen. Ti uređaji će služiti ako osoba dođe na lokaciju da može predati zahtjev za dokumentom i podići ga na šalteru institucije.

5.2.3. Mreža

Tvrtka e-ID d.o.o. nema svoju vlastitu mrežu već za prijenos i dobivanje podataka koristi mrežu telekomunikacijskog davatelja usluge. Za pristupanje usluzi e-ID potreban je pristup internetu, a omogućen je preko različitih telekomunikacijskih davatelja usluga.

Internet je javno dostupna globalna paketna podatkovna mreža koja zajedno povezuje računala i računalne mreže korištenjem istoimenim protokolom (internet protokol = IP). To je "mreža svih mreža" koja se sastoji od milijuna kućnih, akademskih, poslovnih i vladinih mreža koje međusobno razmjenjuju informacije i usluge kao što su elektronička pošta, chat i prijenos datoteka te povezane stranice i dokumente World Wide Weba, [26].

5.2.4. Poslužitelj

Tvrtka e-ID d.o.o. predstavlja informacijsko tehnološki sustav središnje identifikacije i autentifikacije korisnika elektroničkih javnih usluga.

Tvrtka predstavlja vlasnika poslužiteljske infrastrukture i kao takva raspolaže računalnim i komunikacijskim sustavima s odgovarajućim memorijskim kapacitetom i kapacitetom obrade za potrebe svojih korisnika, [17].

5.2.5. Usluge i aplikacije

5.2.5.1. Davatelj usluge

Usluga je svaka samostalna gospodarska djelatnost koja se uobičajeno obavlja za naknadu, ukoliko nije obuhvaćena pravnim propisima vezanim uz slobodu kretanja roba, kapitala i osoba.

Davatelj ili pružatelj usluge je svaka fizička osoba koja je državljanin Republike Hrvatske ili državljanin države ugovornice EGP-a ili svaka pravna osoba sa sjedištem u Republici Hrvatskoj ili državi ugovornici EGP-a koja nudi ili pruža uslugu, [27].

Davatelji usluge mogu biti sve stranke tj. sve institucije, tvrtke, poduzeća i sl. koje žele kao vrstu identifikacije korisnika koristiti uslugu e-ID. Davatelji imaju pristup središnjem državnom portalu preko kojeg oni kao takvi mogu pružiti različite elektroničke usluge. Infrastruktura omogućuje jednostavnu integraciju postojećih identifikacijskih usluga u univerzalnu autentifikacijsku uslugu. Posebnim naglaskom na analizu rizika privatnosti, sudionici će dobiti povećanu svijest o rizicima od strane visoke sigurnosti elektroničkog identiteta.

Davatelji usluga ne moraju izdavati svoj vlastiti dokument za potrebe svojih korisnika već koriste elektroničku osobnu iskaznicu izdanu od strane Ministarstva unutarnjih poslova.

5.2.5.2. Davatelj aplikacijske usluge

Davatelj aplikacijske usluge brine se za upravljanje ponudom aplikacija prema krajnjem korisniku te prodaje aplikacija na komercijalnim principima. [prezentacija]. Davatelji usluga brinu o svojim aplikacijama koje služe za pristup korisnika raznim elektroničkim uslugama.

5.2.6. Sadržaj

5.2.6.1. Vlasnik sadržaja

Vlasnik sadržaja je sam davatelj usluge. On omogućuje pristup uslugama koje nudi. Većina poduzeća i ustanova prisutnih na Internetu u ulozi je vlasnika sadržaja (eng. *content owner*) koji raspolaže informacijom u izvornom obliku. Sadržaj se korisnicima može ponuditi besplatno ili uz naplatu, a vlasništvo sadržaja podrazumijeva autorska i komercijalna prava. Vlasnik sadržaja je ujedno i davatelj sadržaja, čija je uloga omogućavanje sadržaja, [1].

5.2.6.3. Omogućavatelj sadržaja

Omogućavatelj sadržaja je tvrtka e-ID d.o.o. jer omogućuje korisniku prikaz svih dostupnih davatelja usluga, te usluga koje oni kao takve nude. Priprema izvornu informaciju za daljnje oblikovanje, objavljivanje, obradu, pohranu i pretraživanje, [17].

5.3. Tržišni segment

Tržišnim segmentom ustanovljuje se ciljano tržište za uslugu e-ID. Tržište se dijeli na segmente (eng. *Market segment*) unutar kojih pojedine skupine korisnika imaju homogene potrebe te između njih ne postoji preklapanje potreba. Najčešće se analiziraju potrebe određenog tržišnog segmenta. Ponekad se usluge razvijene za cjelokupno tržište prilagođavaju potrebama određenog tržišnog segmenta, [1].

Usluga elektroničkog identiteta s obzirom na način pristupa usluzi može se podijeliti na fizičke i pravne osobe. Tržišni segment usluge e-ID obuhvaća sve korisnike tj. građane jer svi posjeduju identifikacijski dokument s kojim se potvrđuje njihov identitet. Tržišni segment mora biti usmjeren na potrebu korisnika. Na primjer, ako je korisniku potrebna medicinska pomoć, ulaskom u bolnicu, elektroničkim identitetom identificira se korisnik te mu se nudi potrebna pomoć, što znači da tržišni segment ne označava ciljano tržište nego općenitu potrebu svih građana.

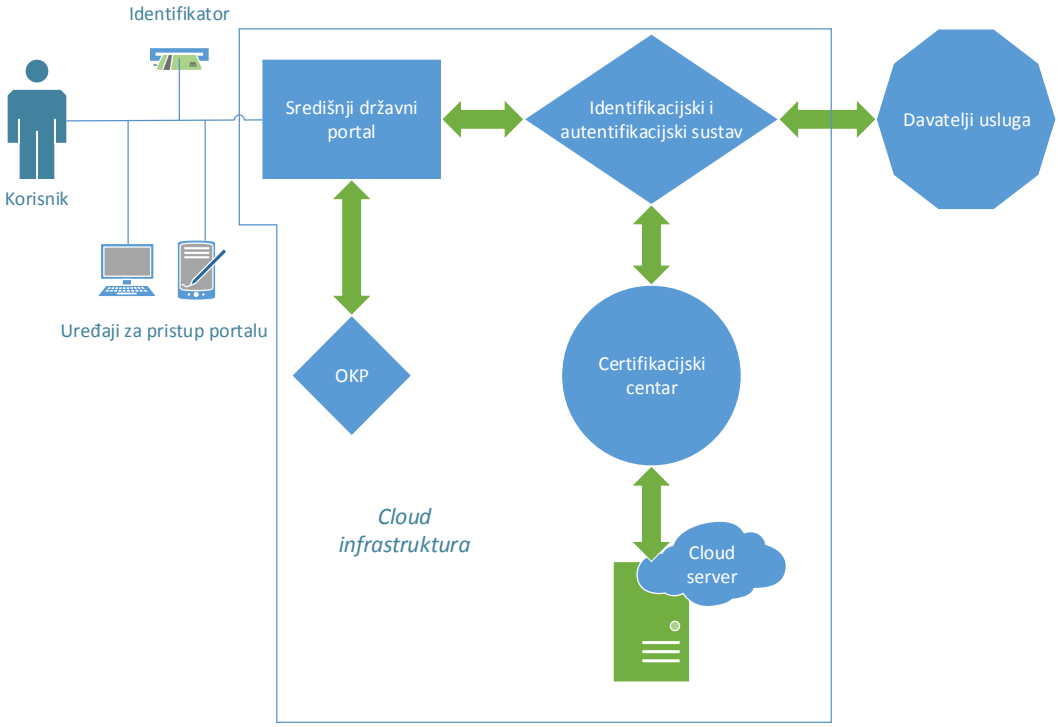
5.4. Arhitektura informacijsko komunikacijske usluge e-ID

Arhitektura informacijsko komunikacijske usluge e-ID opisuje općenitu funkcionalnost same usluge, te na koji način korisnik dolazi do određenih davatelja usluga. Uz arhitekturu opisan je način registracije novih korisnika na središnji državni portal, te njihov zahtjev za određenom uslugom. Također je opisan način identifikacije već registriranih korisnika.

Arhitektura usluge (Slika 9) sastoji se od:

- korisnika,
- identifikatora,
- pristupnih uređaja,
- središnjeg državnog portala,
- osobnog korisničkog pretinca,
- identifikacijskog i autentifikacijskog sustava (IAS),
- certifikacijskog centra,

- *cloud* infrastrukture,
- *cloud* servera,
- davatelja usluga.



Slika 9. Arhitektura informacijsko komunikacijske usluge e-ID

5.4.1. Korisnik

Kao što je objašnjeno pod poglavljem 5.2.1. korisnik predstavlja osobu koja pomoću identifikatora i raznih pristupnih uređaja pristupa samoj usluzi e-ID. Identifikator korisnika je elektronička osobna iskaznica sa NFC tehnologijom. Korisnik može pristupiti usluzi na računalu, tabletu, pametnom mobilnom uređaju ili bilo kojem drugom uređaju koji ima pristup internetu te mogućnost otvaranja web aplikacija.

5.4.2. Identifikator - Elektronička osobna iskaznica usluge e-ID (e-iskaznica)

e-iskaznica predstavlja identifikator kod usluge e-ID. Na temelju identifikatora korisnik/građanin identificira sebe kao legitimnu osobu za pristup svojim podacima i uslugama. Identifikator omogućuje identificiranje korisnika od strane davatelja usluga jednostavnim prislanjanjem iskaznice na čitače. Za razliku od elektroničke osobne iskaznice RH, ova iskaznica posjeduje NFC tehnologiju beskontaktnih transakcija što znači da ne sadrži čip za kontaktne transakcije.

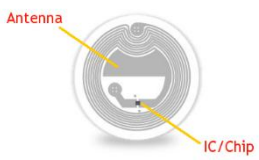
e-iskaznicu mogu podići osobe sa važećim osobnim identifikacijskim brojem, što znači da osobe od 15 godina na dalje mogu koristiti potpunu funkcionalnost usluge. Djeca do 5 godina koriste iskaznice koja ne sadrže certifikate te je rok važenja 5 godina. e-iskaznica za djecu od 5 do 15 godina sadrže identifikacijske certifikate koji omogućavaju potvrdu identiteta u postupcima vezanim uz obrazovanje. Rok važenja svih vrsta iskaznica je 5 godina.

5.4.2.1. NFC (Near Field Communication)

NFC je radio tehnologija kratkog dometa koja omogućuje komunikaciju između dva NFC1. uređaja. Do komunikacije dolazi kada se kompatibilni NFC uređaji nalaze u rasponu manjem od 13 cm ili se jednostavno dodirnu. Frekvencija na kojoj djeluje je 13,56 MHz i brzina prijenosa podataka iznosi 424 Kbit/s. U komunikaciju moraju biti uključeni dva uređaja. Prvi uređaj naziva se inicijator (eng. *initiator*) koji je aktivan uređaj i odgovoran za pokretanje komunikacije, dok se drugi naziva meta uređaj (eng. *target device*) te odgovara na zahtjeve inicijatora. Komunikacija započinje kada aktivni uređaj dolazi u blizinu meta uređaja, generira magnetsko polje na 13,56 MHz i napaja meta uređaj, [8].

NFC tehnologija privukla je mnogo pozornosti tijekom posljednjih nekoliko godina, te brzo napreduje. Broj aplikacija u kojima se koristi NFC tehnologija je velik, uključujući i aplikacije kao što su sigurnosno plaćanje, upravljanje pristupom, te industrija maloprodaje između ostalog. Nadalje, NFC je zamišljen kao potencijalna tehnologija za Internet stvari (eng. *Internet of Things*).

Kod usluge e-ID korisnik pristupa usluzi sa elektroničkom osobnom iskaznicom. NFC čitači omogućuju čitanje podataka sa iskaznice pomoću NFC oznake (Slika 10), te se korisnički podaci šalju prema aplikacijskom programskom sučelju koje zatraži pristup bazi podataka koja je smještena na *cloud* serverima.



Slika 10. NFC oznaka (eng. Tag), [28].

5.4.3. Središnji državni portal

Središnji državni portal je jedinstveno mjesto za pristup javnim informacijama na internetskoj stranici, što znači da predstavlja web aplikaciju tj. aplikacijsko sučelje za pristup korisnika uslugama koje nude davatelji. Središnji državni portal služi za informiranje i objedinjavanje informacija državnih institucija i davatelja usluga kako bi građani na što jednostavniji način došli do traženih informacija. Uveden je da bi se na jednom mjestu olakšao pristup informacija te povećala transparentnost istih. [egrađani] Korisnik pristupa središnjem državnom portalu uz pomoću elektroničke osobne iskaznice. Novi korisnik mora dati zahtjev za izradom pristupnog računa, tj. registracijom novog korisnika ukoliko koriste staru osobnu iskaznicu. Prilikom preuzimanja nove, korisnici dobivaju pristupne podatke, te su automatski registrirani na portal.

5.4.4. Osobni korisnički pretinac

Osobni korisnički pretinac (OKP) svakom korisniku usluge e-ID omogućava primanje osobnih službenih poruka (e-poruka) vezanih za javne usluge, postupke (odnosno njihov tijek) i osobne statuse te njihov pregled, upravljanje i pohranu. Službene poruke stvaraju i dostavljaju javne institucije. OKP služi za primanje poruka i pregled dostupnih elektroničkih usluga, [15].

Građanima RH OKP omogućuje da na jednom mjestu:

- na siguran i povjerljiv način primaju, pregledavaju, prate i upravljaju svim svojim službenim komunikacijama s javnim sektorom,
- budu informirani o važnim situacijama i događajima vezanim za osobna zakonska prava i obveze te o korištenju osobnih podataka u javnom sektoru.

Davateljima elektroničkih usluga omogućuje:

- da neposredno, jednostavno, automatizirano, sigurno, pouzdano i ekonomično dostavljaju službenu korespondenciju svojim korisnicima bez nužnosti da sami razvijaju i održavaju svoja rješenja.

5.4.5. Identifikacijski i autentifikacijski sustav

Identifikacijski i autentifikacijski sustav je informacijsko tehnološki sustav središnje identifikacije i autentifikacije korisnika javnih elektroničkih usluga. Prilikom

pristupanja korisnika nekoj od usluga, sustav vrši provjeru identiteta korisnika na način da daje zahtjev certifikacijskom centru. Na temelju odgovora, IAS odlučuje o pravovaljanosti identiteta korisnika, te vrši daljnje preusmjeravanje prema davatelju usluge.

5.4.6. Certifikacijski centar

Certifikacijski centar (eng. Certification Authority – CA) je pravni subjekt koji obavlja poslove izdavanja vjerodajnice, [15]. Autentifikacija vjerodajnice obavlja se na poslužitelju certifikacijskog centra koji daje potvrdu pravovaljanosti identiteta korisnika. Certifikacijski centar smatra se trećom stranom kojoj se vjeruje. Davatelji usluga u certifikacijskom centru daju zahtjev u kojem se određuje koji atributi identiteta korisnika su potrebni za korištenje e-usluge. Svaki davatelj usluga bira atribute, naravno, ako certifikacijski centar dopušta prikaz pojedinih koji su zahtijevani.

5.4.7. Cloud infrastruktura

Cloud[3] *computing* općenito prikazuje model računarstva u kojem se usluge postavljaju na Internet i korisnici im pristupaju prema određenim uvjetima. Malo složenija definicija kaže da je oblak skup računala i programa na koje se postavlja usluga koja se pruža preko Interneta, a računarstvo u *cloud-u* obuhvaća *cloud* i usluge koje se postavljaju na *cloud*, [11].

Podaci koji se nalaze na *cloud-u* smješteni su na udaljenim serverima. Prilikom promjene različitih lokacija, korisnik uvijek ima pristup podacima koji su smješteni na serverima, što znači da korisnik ne mora biti povezan, tj. imati direktan pristup nekom serveru.

Kod usluge e-ID, *cloud* infrastruktura omogućuje integraciju aplikacijskog programskog sučelja (API – *Application Programming Interface*) sa samim serverima na kojima se nalaze korisnički podaci. Usluga e-ID omogućuje prilagođavanje sučelja raznim strankama u različitu korist. Stranke svoje programsko sučelje povezuju na *cloud* servere, tako da je programu moguće pristupiti s više lokacija. Da bi pristup *cloud* serverima bio realiziran, stranka kod koje je zatražen pristup mora biti povezana na Internet mrežu.

[3] Cloud - oblak

Usluga e-ID funkcionira kao *SaaS* (eng. *Software as a Service* – softver kao usluga). Korisniku je omogućeno korištenje dostupnih aplikacija koje se nalaze u infrastrukturi *cloud-a*. aplikacije su dostupne s različitih klijentskih uređaja uz pomoć klijentskog sučelja (npr. Web preglednik). Pri tome korisnik ne provjerava pozadinsku infrastrukturu, uključujući mrežu, servise, operacijske sustave, pohranu podataka ili čak individualne aplikacijske mogućnosti. Jedina moguća iznimka su specifične korisničke konfiguracijske postavke. Odnosno, *SaaS* je tehnološka platforma koja omogućuje dostupnost aplikacija putem Interneta u obliku usluga koje se unajmljuju prema potrebi, umjesto da se kupuju kao zasebni program koji treba instalirati na kućnim uređajima (računalima i sl.) ubrzan je trend prijelaza na taj poslovni model, koji davateljima usluga omogućuje najam tekstualnih, tabličnih, kalendarskih ili drugih programa prema potrebi, čime se izbjegava trošak kupovine, instalacije, nadogradnje i održavanja programa na uređajima. Ovaj model *cloud computinga* dostavlja jednu aplikaciju preko korisničkog preglednika tisućama korisnika koji koriste arhitekturu predviđenu za mnoštvo zakupa. S korisničke strane to znači da nema dodatnog ulaganja u poslužitelje ili programske licence, a davateljima usluga troškovi su mali u odnosu na tradicionalnu uslugu držanja datoteka na poslužitelju, [11].

5.4.8. Cloud serveri

Cloud serveri služe za pohranu svih atributa identiteta korisnika. Certifikacijski centar prilikom dobivanja zahtjeva o identitetu korisnika, povlači podatke o korisniku sa *cloud* servera. Identitet korisnika je nadalje sažet u digitalnu vjerodajnicu koju certifikacijski centar digitalno potpisuje i prosljeđuje. Identifikacijski i autentifikacijski sustav zatim dostavlja identitet korisnika davatelju usluga, gdje davatelji odlučuju o prihvaćanju ili neprihvaćanju atributa identiteta korisnika.

5.4.9. Davatelj usluge

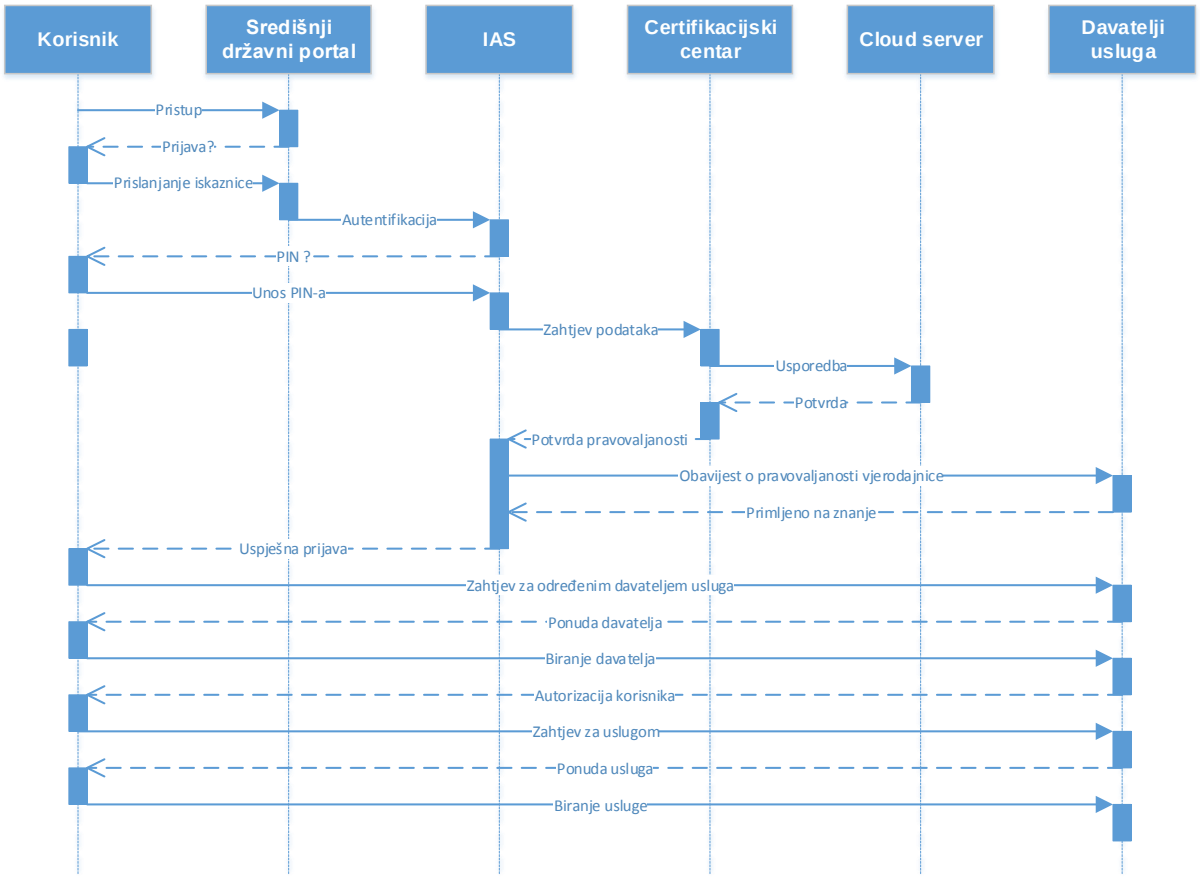
Davatelj usluga pruža e-uslugu autentificiranim korisnicima. Davatelj e-usluge korisnika smatra autentificiranim ukoliko korisnik posjeduje dokaz da je autentifikacijski poslužitelj uspješno potvrdio pravovaljanost identiteta korisnika.

5.5. Proces prijave korisnika u sustav usluge e-ID

Korisnik pristupa raznim terminalnim uređajima tipa računalo, tablet, smartphone i sl. Identifikator koji koristi za autentifikaciju je elektronička osobna iskaznica. Pristupni uređaji trebaju sadržavati NFC čitače za čitanje identifikatora. U

današnje vrijeme većina smartphone-a i tableta podržava NFC tehnologiju, tako da je moguće pristupiti putem istih. Za pristup na računalu, korisnik mora imati dodatni čitač koji se u većini slučajeva spaja na USB port, ili samo računalo sadrži ugrađeni čitač.

Identifikacija se vrši na stranici prijave središnjeg državnog portala, te samu identifikaciju vrši identifikacijski i autentifikacijski sustav. Prilikom prislanjanja iskaznice na čitač, korisnika zatraži potvrdu PIN-om, te IAS prosljeđuje zahtjev prema certifikacijskom centru, gdje centar uspoređuje podatke koje drži pohranjene u svojoj bazi podataka. Nakon što se obavi provjera, certifikacijski centar obavještava IAS o pravovaljanosti ili nepravovaljanosti vjerodajnice. Kod potvrde pravovaljanosti vjerodajnice, IAS iz evidencije OIB-a dohvaća definirane identifikacijske podatke o korisniku te hi prosljeđuje e-usluzi. E-usluga nakon odobrenog pristupa autorizira korisnika za daljnji rad u okviru e-usluge.



Slika 11. Proces prijave na središnji državni portal

Identifikacijski i autentifikacijski sustav predstavlja sučelje između korisnika i CA elementa. Glavna funkcija IAS elementa jest identifikacija i autentifikacija korisnika u ime CA elementa te dostavljanje vjerodajnice generirane od strane CA elementa korisniku. Nakon autentifikacije IAS element šalje digitalno potpisani zahtjev za vjerodajnicom odgovarajućem CA elementu. Kao odgovor, CA element vraća odgovarajuću vjerodajnicu. Primljenu vjerodajnicu IAS element prosljeđuje davatelju usluga. Kako sudjeluje kod generiranja vjerodajnica, IAS element isto tako sudjeluje i kod njihovog opoziva. Ukratko bi se dalo reći da IAS element obnaša funkcije infrastrukture javnih ključeva u ime korisnika kojem služi.

5.5.1. Jednostruka autentifikacija

Jednostruka autentifikacija (eng. *Single Sign On)* predstavlja prijavu samo jednom autentifikacijom vjerodajnice za potrebe prijava na više različitih e-usluga između kojih postoji neka poveznica. IAS omogućuje jednostruku autentifikaciju po pojedinoj aktivnoj sjednici IAS-a. Odnosno, nakon uspješne prijave putem IAS-a korisnik može nastaviti prijave na druge e-usluge sve dok traje sjednica IAS-a. Prilikom prekida trajanja sjednice, korisnik će biti upućen na ponovno ukucavanje PIN-a, nakon čeka će korisnik biti ponovo autoriziran za korištenje pojedinih e-usluga, [15].

Prednosti korištenja SSO su:

- povećana produktivnost korisnika. Omogućuje da korisnici unose autentifikacijske podatke samo na jednom mjestu za sve usluge koje koriste u jednom trenutku,
- autentifikacija je bazirana na jedinstvenoj bazi sigurnosnih podataka
- propagiranje sigurnosnih atributa kroz sustav
- korisnik pamti samo jedan identifikator za sve aplikacije,
- administratori održavaju centralizirani repozitorij korisnika za cijeli sustav,
- reducirani troškovi uvođenja i održavanja,
- jednostavnije razvijanje novih aplikacija. SSO pruža jedinstveno autentifikacijsko sučelje. Programeri ne moraju brinuti o autentifikaciji. Mogu pretpostaviti da je korisnik uspješno autentificiran kada dođe zahtjev za aplikacijom i zajedno s njim korisnički podaci,

- ostvarenje SSO rješenja može se provesti u koracima, prvo na jednom dijelu aplikacija da bi onda krenuli na preostali dio. Nije potrebno napraviti ogroman skok.

Problemi koji se javljaju sa SSO rješenjima uključuju sljedeće:

- promjena postojećih aplikacija. Ostvarenje SSO rješenja može biti komplicirana, dugotrajna, skupa za promjenu postojećih aplikacija.
- računala bez nadzora. Npr. ako se korisnik uspješno prijavi, te se udalji od računala ili drugih pristupnih uređaja i ostavi ih bez nadzora. Iako je generalno pitanje sigurnosti, u SSO sučelju je posebno opasno jer su svi autorizirani resursi kompromitirani.
- jedna točka napada. Sve aplikacije koriste usluge jednog poslužitelja, koji je glavna meta zlonamjernih korisnika, [10].

5.5.2. Jednostruka odjava

Jednostruka odjava (eng. *Single Sign Out*) predstavlja način odjave sa svih uslužnih poslužitelja (davatelja usluga) samo jednom odjavom korisnika. Jednostruka odjava se može obaviti samo sa onih uslužnih poslužitelja koji su ugradili ovu funkcionalnost.

Ukoliko davatelj e-usluge ne podržava ovu funkcionalnost, odjava se obavlja na stranicama svake e-usluge pojedinačno. Proces odjave sa uslužnog poslužitelja je uvijek u nadležnosti davatelja e-usluge. IAS preporučuje ugradnju funkcionalnosti jednostruke odjave za sve e-usluge, zbog mogućnosti zaborava svih posjećenih e-usluga, [15].

6. SWOT analiza uvođenja usluge e-ID

Analiza okruženja ili okoline podrazumijeva istraživanje svih važnijih karakteristika kako vanjskog tako i unutarnjeg okruženja sa svrhom identifikacije strateških čimbenika koji će odrediti budućnost poduzeća. Analiza okruženja i identifikacija strateških čimbenika može se sagledati kao potpora odlučivanju u procesu formulacije strategije, [29].

Najjednostavnija metoda za analizu okruženja je SWOT. SWOT analiza je strategijski instrument pomoću kojeg se dinamički sučeljavaju snage/slabosti poduzeća s prilikama/prijetnjama okruženja radi identificiranja šansi/rizika za opstojnost poduzeća. SWOT analiza (akronim od *strenghts* – snage, *weakneses* – slabosti, *opportunities* – prilike i *threats* – prijetnje) dijagnostički je i prognostički instrument, koji omogućuje i olakšava planiranje mjera za pojačanje snaga i razgradnju slabih mjesta, ishodište u procesu strategijskog upravljanja, prvi je korak u definiranju postojeće i poželjne pozicije poduzeća. Najveći je doprinos pokušaj cjelovite vizualizacije pozicije poduzeća. Riječ je o multi-dimenzionalnom postupku, koji podrazumijeva primjenu induktivnog i deduktivnog, intuitivnog i umreženog načina mišljenja. Rezultati primjene SWOT analize prikazuju se uobičajeno u SWOT matrici ili matrici šansi/rizika, u kojoj su zastupljene i kvantitativna i kvalitativna dimenzija. SWOT analiza provodi se prema analitičko dijagnostičkom modelu analize potencijala, pomoću kojeg je moguće istraživati i stvarati sud o potencijalima poduzeća te na temelju identificiranih prilika i opasnosti okruženja utjecati na razgradnju slabosti i jačanje snaga poduzeća, [39].

Kako se radi o novoj usluzi postoje određene prednosti i snage koje pomažu iskoristiti sile u okruženju. Prednost usluge e-ID za razliku od ostalih davatelja slične usluge je u tome što omogućava identifikaciju korisnika jedinstvenim identifikacijskim dokumentom e-iskaznica koja predstavlja elektroničku osobnu iskaznicu. Takva iskaznica stoji kao jedinstveni identifikator i može se koristiti u zamjenu za više različitih iskaznica, npr. zdravstvena iskaznica i dopunsko osiguranje, iskaznica javnog prijevoza, identifikacijske iskaznice zaposlenika i sl. Time se smanjuje potreba davatelja usluga za izdavanjem raznih iskaznica, te povećava učinkovitost jedne identifikacijske iskaznice korisnika.

Tablica 1. Prikaz SWOT analize informacijsko komunikacijske usluge e-ID

Snage	Slabosti
• jedna identifikacijska iskaznica u zamjenu za više njih • smanjenje opterećenja prilikom pristupanja administraciji • tehnička podrška u elektroničkom informacijskom sustavu • poboljšanje sigurnosti identiteta korisnika i podataka vezanih za identitet • poboljšanje nacionalne sigurnosti • povećanje administrativne učinkovitosti • smanjenje troškova • ograničavanje mogućnosti za prijevaru • jedan sustav sa dostupnim svim elektroničkim uslugama • pouzdanost • jednostavnost • brzina dobivanja podataka i dokumenata • *Single Sign On/Out* • konkurentnost davatelja e-usluga	• troškovi i naknade za implementaciju usluge • smanjenje interoperabilnosti (međusobno djelovanje i funkcioniranje više sustava) • pravne poteškoće • privatnost • sigurnost podataka
Prilike	**Prijetnje**
• ulaganje u inovacije • proširenje asortimana usluga • prostor za nove davatelje usluga • novi oblik poslovanja davatelja usluga sa korisnicima	• izravna ili neizravna konkurencija • vanjski i unutarnji faktor koji utječe na ugrožavanje sustava usluge e-ID • mogućnost krađe identiteta • namjerna ili nenamjerna povreda identiteta korisnika • nelegitimno i needucirano zaposleno osoblje

Usluga e-ID generira razne pogodnosti za pojedince, poduzeća i vladu, uključujući lakše trgovanje u digitalnoj ekonomiji, omogućujući usluge e-vlade i poboljšanje sigurnosti za sve *online* transakcije.

Mnoge vrste transakcija e-ekonomije postaju učinkovitije sa uslugom e-ID. Usluga omogućuje pojedincima autentifikaciju za elektroničke usluge, sigurno komuniciranje i stvaranje pravno obvezujućih elektroničkih potpisa. Tvrtke mogu koristiti funkcije upravljanja identitetom sa svojim klijentima, kao što je autentifikacija

korisnika na *online* aplikacije. Građani imaju korist od elektroničkih informacijskih sustava koji omogućuju *Single Sign On,* što im omogućuje korištenje jedne potvrde identiteta za više elektroničkih usluga različitih davatelja. Korisnici e-iskaznice mogu bolje zaštititi svoju privatnost na internetu ograničavajući količinu informacija koju dijele s drugima. Korištenje usluge e-ID omogućuje brojne usluge privatnog sektora koji ovise o znanju identiteta korisnika. E-iskaznica može također poslužiti kao digitalni novčanik za kupnju proizvoda ili usluga, osobno ili *online*.

Usluga e-ID također omogućava olakšanje mnogih usluga e-vlade. Vlada može pojednostaviti mnoge usluge kao što je pružanje državne beneficije, koja ovisi o znanju identiteta korisnika. Vlada može bolje ponuditi inovativne usluge, poput Internet glasovanja, koje zahtjeva autentifikaciju na daljinu. Građani usluge e-ID mogu ispuniti i potpisati elektroničke dokumente s bilo kojeg mjesta koje ima pristup internetu, čime se eliminira dugotrajno čekanje u državnim institucijama i uredima javnih bilježnika. Isto tako tvrtke mogu sigurno komunicirati s vladom *online* u vezi aktivnosti kao što je plaćanje poreza ili traženje dozvola. Uporaba sigurne elektroničke komunikacije eliminira potrebu prepisivanja podataka iz papirnatih obrazaca, čime se smanjuju pogreške i vrijeme obrade istih. Vlada dobiva mnoge koristi od povećane učinkovitosti, primjerice uklanjanjem duplih unosa podataka, smanjenje troškova vezanih uz nepotrebne papirologije, uključujući troškove tiskanja, skladištenja i prijevoza.

Konačno, sustav usluge e-ID može poboljšati sigurnost online transakcija i spriječiti prijevare i krađe identiteta. Usluga e-ID može stvoriti veće povjerenje i odgovornost u ekosustavu identiteta. Sustav usluge e-ID omogućava multi-faktor autentifikacije što znači da korisnik mora imati identifikacijsku ispravu i PIN da bi mogao potvrditi ulaz u sustav ili neku transakciju. Time je omogućena sigurnost identiteta korisnika. Većina današnjih informacijskih sustava ne koristi multi-faktor autentifikacije gdje dolazi do povrede sigurnosti primjenom različitih korisničkih imena i lozinki, jer se općenito ljudi mogu prijavljivati na raznim javnim lokacijama (računalima), gdje postoji mogućnost pamćenja podataka za prijavu u sustav. Način za povredu identiteta također može biti korištenje jedne lozinke za sve račune, pri čemu se otkrivanjem lozinke može pristupit svim računima, što nije sigurno. Korisnici znaju koristiti više lozinki za različite račune, ali da bi lakše zapamtili, koriste slabe i

jednostavne lozinke, a uporabom jedne e-iskaznice i PIN-a, korisnici dobivaju veći poticaj za korištenje istih.

Jedinstvenim identifikacijskim dokumentom, tj. elektroničkom osobnom iskaznicom mogu se opisati neke prednosti koje sama iskaznica nudi u smislu zadovoljavanja zahtjeva, ciljeva i dizajnerskih odluka:

- prednosti za korisnika - e-ID autentifikacija treba predstavljati lakšu online autentifikaciju dajući građanu veću kontrolu i odgovornost. Elektronička osobna iskaznica predstavlja identifikacijsku shemu građana za Internet i smanjuje korisničke probleme sa kreiranjem raznih korisničkih imena, lozinki i drugih vjerodajnica. Kontrolirano puštanje odabranih podataka elektroničkog identiteta uslugama smanjuje nekontrolirano prikupljanje informacija povezanih identiteta preko davatelja usluga i računa.
- prednosti davatelja usluga - vlada izdaje iskaznice koje mogu pružiti pouzdanu autentifikaciju i visoko kvalitetni zapis podataka. Iskaznice se mogu koristiti ne samo za opću autentifikaciju nego i za ispunjavanje zakonskih uvjeta za identifikaciju. Usluge koje prihvaćaju e-ID dobivaju identifikacijsku informaciju bez pogrešaka, potvrđenu od strane vlade, kao original i pripada stvarnoj osobi. Kroz uslugu e-ID, postojeći davatelji usluge dobivaju više povjerenja u autentifikaciju, te nove usluge postaju ostvarive.
- autentifikacija - e-ID funkcija ne osigurava transakcije, već pruža samo autentifikaciju. Kartica omogućuje povjerenje centrima za instalaciju ključeva i certifikata za elektronički potpis. Funkcija e-ID može se koristiti za dobivanje certifikata online.
- smanjenje podataka - cijeli e-ID sustav je osmišljen po principu *need-to-know* (treba znati), pod kontrolom vlade. Davatelji usluga će biti ovlašteni za pristup podacima samo u mjeri u kojoj oni mogu pokazati potrebu za njima.
- nema centraliziranih baza podataka - infrastruktura javnog ključa i proizvodnja kartica jedine su centralizirane komponente e-ID infrastrukture. Ne postoje centralizirane baze podataka, te se podaci za izradu kartice brišu naknadno.

- kontradiktornost pretpostavke - dizajn utječe na smanjenje prijetnji na privatnost, kao što su napadi na protokole, ključeve ili ostale tehničke mogućnosti za povredu identiteta. Protokoli i upravljanje ključevima dizajnirano je na način da se izbjegnu bilo kakve povrede identiteta.
- držanje korisnika pod kontrolom - za sve online aplikacije korisnik mora ukucati PIN da bi potvrdio pristup bilo kojim podacima ili funkcijama. Oni mogu ograničiti skup podataka dostavljen davatelju usluga, samo što onda davatelj odlučuje da li korisnik može pristupiti usluzi ili ne, [9].

7. Sigurnosni aspekti korištenja usluge e-ID

Sigurnost mreža, usluga i transakcija u informacijskom sustavu usluge e-ID bitna je za stvaranje povjerenja u različite oblike osobnog komuniciranja i elektroničkog poslovanja. Prijetnja u ekosustavu usluge definira se kao okolnost, stanje ili događaj koji može naškoditi osobnu ili mrežnim i računalnim resursima u obliku uništavanja, razotkrivanja ili promjene podataka, prijevare, zlouporabe i uskrate usluge. Zadovoljavanje sigurnosnih zahtjeva omogućuje brzo identificiranje prijetnje sigurnosti te prikladan odgovor. Za sigurnost prijenosa podataka putem Internet mreže zadužena je infrastruktura javnog ključa (PKI – *Public Key Infrastructure*), digitalna vjerodajnica, digitalni potpis, te metode kriptiranja, [1].

7.1. Osnove kriptografije

Podaci koji se mogu pročitati i razumjeti nazivaju se jasnim tekstom. Metode za skrivanje značenja i pretvaranje sadržaja jasnog teksta u nerazumljivi oblik nazivaju se metodama kriptiranja. Kriptiranjem jasnog teksta dobiva se nerazumljiv skup podataka koji se naziva kriptiranim tekstom. Postupak pretvorbe kriptiranog teksta u jasni tekst naziva se dekriptiranje. Postupcima kriptiranja i dekriptiranja podataka bavi se grana računarstva koja se naziva kriptografijom, [2].

Kriptografija je znanost koja omogućuje spremanje i prijenos osjetljivih informacija kroz nesigurne računalne mreže kao što je Internet. Primjena kriptografskih postupaka omogućuje prijenos informacije nesigurnom računalnom mrežom na način da informaciju koja se prenosi ne može pročitati nitko osim onoga kome je namijenjena, [12].

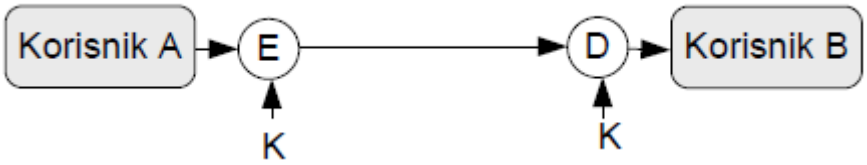
Svrha kriptografskih postupaka je osiguravanje šest sigurnosnih zahtjeva koji su nužni za sigurnu komunikaciju:

- povjerljivost,
- raspoloživost,
- vjerodostojnost,
- autentifikacija,
- autorizacija,
- neporecivost.

Povjerljivost ili tajnost osigurava da informacije u sustavu smiju biti dostupne samo ovlaštenim korisnicima. Raspoloživost osigurava da su informacije uvijek dostupne ovlaštenim korisnicima usprkos mogućim neočekivanim i nepredvidljivim događajima. Vjerodostojnost osigurava da informacije u sustavu mogu mijenjati samo ovlašteni korisnici. Jednoznačno prepoznavanje ovlaštenog korisnika osigurano je pomoću autentifikacije. Mehanizmom autorizacije se ovlaštenim korisnicima dozvoljava pristup samo do onih sadržaja do kojih imaju prava pristupa. Neporecivost predstavlja zaštitu od opovrgavanja prethodno počinjenog djela, [12].

7.1.1. Simetrična kriptografija

Simetrična kriptografija, poznata i pod nazivom kriptografija tajnim ključem, najpoznatiji je i najstariji poznati oblik kriptografije, [1]. Ključ kriptiranja KE i ključ dekriptiranja KD su jednaki i predstavljaju tajni ključ koji znaju samo sudionici sigurne komunikacije. Na slici 12 je prikazan primjer komunikacije između korisnika A i korisnika B koji koriste simetričnu kriptografiju, [12].



Slika 12. Simetrična kriptografija, [12].

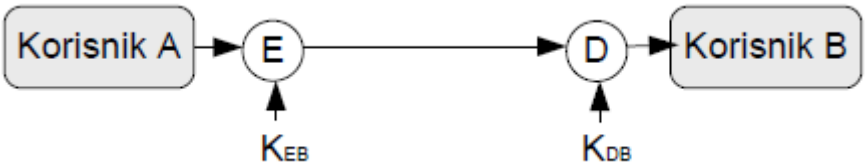
7.1.2. Asimetrična kriptografija

Asimetrična kriptografija, poznata i pod nazivom kriptografija javnim ključem, objavljena je 1976. godine od strane dvaju znanstvenika, Whitfielda Diffiea i Martina Hellmana. Za razliku od simetrične, asimetrična kriptografija koristi dva različita ključa od kojih se jedan koristi za kriptiranje i drugi za dekriptiranje. Asimetrični algoritmi zasnivaju se na matematičkom problemu faktorizacije velikih prirodnih brojeva na proste faktore.

Svaki sudionik u sigurnoj komunikaciji posjeduje jedinstveni par ključeva koji se nazivaju javni ključ *p* i privatni ključ *d*. Javni ključ je javno dostupan svima i služi za kriptiranje. Privatni ključ je poznat samo njegovom vlasniku i služi za dekriptiranje poruka. Određivanje javnog ključa na osnovi poznatog privatnog ključa je jednostavno, dok je određivanje privatnog ključa na osnovi poznatog javnog ključa

matematički izrazito zahtjevna operacija koja je praktički neizvediva, čak i uz primjenu najsuvremenije računalne opreme. Upravo to svojstvo predstavlja osnovu sigurnosti asimetričnih algoritama.

Na slici 13 prikazan je princip rada asimetričnog kriptografskog algoritma. Korisnik A koristeći javni ključ K_{EB} korisnika B kriptira poruku te je pošalje korisniku B. Kako samo korisnik B zna svoj privatni ključ K_{DB}, jedino on može dekriptirati primljenu poruku. Koristeći svoj privatni ključ, korisnik B dekriptira poruku i pročita njen sadržaj.



Slika 13. Asimetrična kriptografija, [12].

Asimetrični algoritmi su zbog svoje matematičke složenosti sporiji u odnosnu na simetrične algoritme pa se zbog toga ne koriste za kriptiranje većih količina podataka. Uglavnom se koriste za razmjenu tajnog ključa simetrične kriptografije te za stvaranje digitalnih potpisa, [12].

7.1.3. Sažimanje poruke

Sažetak poruke osigurava sigurnosni zahtjev vjerodostojnosti poruke. Kriptografski sažetak izrađuje se jednosmjernom funkcijom koja iz poruke proizvoljne duljine izračunava sažetak stalne duljine. Funkcija sažimanja je jednosmjerna, što znači da je izračunavanje sažetka poruke vrlo jednostavno i brzo, dok je dobivanje izvorne poruke na osnovi poznatog sažetka zbog velike računalne složenosti praktički neprovedivo, [12].

7.2. Digitalna vjerodajnica

Digitalna vjerodajnica je skup podataka kojim se korisnik predstavlja određenom entitetu, a služi kao dokaz za provjeru elektroničkog identiteta korisnika vjerodajnice za pristup uslužnim poslužiteljima pružatelja elektroničkih usluga (e-usluga). Vjerodajnica je nešto što korisnik zna ili/i posjedujete (npr. korisničko ime/lozinka, digitalni certifikat i sl.). Korisnik vjerodajnicu treba pažljivo čuvati i nikome je ne smije povjeravati, [15].

Digitalna vjerodajnica (eng. *Digital Certificate*) je digitalno potpisani dokument koji povezuje javni ključ s osobom kojoj pripada. Uvedena je iz razloga što sudionici u komunikaciji moraju doznati ključeve svojih sugovornika. Osim toga, moraju biti uvjereni da sugovornici nisu uljezi koji se lažno predstavljaju. Zamisao digitalne vjerodajnice predložio je L. Kohnfelder 1978. godine. Da bi se osigurala vjerodostojnost digitalne vjerodajnica, ona se digitalno potpisuje, čime potpisnik jamči njezin integritet. Potpisnik digitalne vjerodajnice naziva se certifikacijski centar (eng. Certification Authority - CA). Certifikacijski centar je ustanova ili tijelo kojoj svi korisnici vjerodajnica vjeruju i čiji javni ključ, koji se koristi za provjeru potpisa na vjerodajnici, mora biti pouzdano ispravan. Digitalna vjerodajnica može tvoriti temelj elektroničkog identiteta, pružajući istu ili čak bolju sigurnost za oslanjajuće stranke poštujući privatnost korisnika.

Svaki građanin koji se putem IAS-a prijavi vjerodajnicom uključenom u IAS, imat će jedinstveni elektronički identitet kojim će se koristiti u pristupu elektroničkim javnim uslugama, odnosno u elektroničkoj komunikaciji s javnim sektorom, [15].

Digitalna vjerodajnica sadrži određene podatke o njegovom vlasniku (trenutno važeći standard je X.509 v3), među kojima su:

- ime vlasnika certifikata
- vlasnikov javni ključ
- nadnevak do kada važi javni ključ
- ime CA koji je izdao certifikat
- jedinstveni serijski broj
- dodatne podatke za identifikaciju

Kada se formira neka digitalna vjerodajnica, CA ga na kraju digitalno potpiše svojim tajnim ključem, tako da se njegov sadržaj može pročitati korištenjem CA javnog ključa, ali se ne može neovlašteno mijenjati, [30].

7.3. Razlika između elektroničkog i digitalnog potpisa

Mnogo puta dolazi do zabune i upotrebljava se jedan od izraza bilo elektronički ili digitalni potpis, a da se u stvari radi o onom drugom. Razlika je bitna i sasvim jasna i potrebno je razlikovati ta dva pojma.

Elektronički potpis je općeniti izraz neutralan na tehnologiju i način izvedbe koji obuhvaća sve metode kojima se može potpisati elektronička informacija. Kada neka institucija želi uvesti potpisivanje elektroničkih informacija odnosno elektronički potpis, obično se definiraju zahtjevi za elektronički potpis. Potom se raspravlja i odlučuje koja implementacija je najprihvatljivija, što može biti npr. digitalni potpis.

Digitalni potpis je izvedba elektroničkog potpisa, temeljen na asimetričnoj kriptografiji i funkcijama sažimanja, [31].

7.3.1. Elektronički potpis

Elektronički potpis je općeniti izraz neutralan na tehnologiju i način izvedbe koji obuhvaća sve metode kojima se može potpisati elektronička informacija. Za elektronički potpis mogu se definirati zahtjevi kao što su očuvanje integriteta potpisanih informacija, neporecivost potpisivanja i identifikaciju potpisnika. U okviru elektroničkog potpisa ne govori se o načinu izvedbe traženih zahtjeva dakle korisnicima se ostavlja na izbor odabir najpovoljnije ili najpouzdanije tehnologije za izvedbu koja će odgovarati zahtjevima za elektronički potpis. U hrvatskoj je 24. siječnja 2002. proglašen zakon o elektroničkom potpisu. Prema tom zakonu definicija elektroničkog potpisa je sljedeća: Elektronički potpis - znači skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta. Također definiran je i napredan elektronički potpis, [32].

Napredan elektronički potpis je elektronički potpis koji:

- je povezan isključivo s potpisnikom,
- nedvojbeno identificira potpisnika,
- nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika,
- sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka.

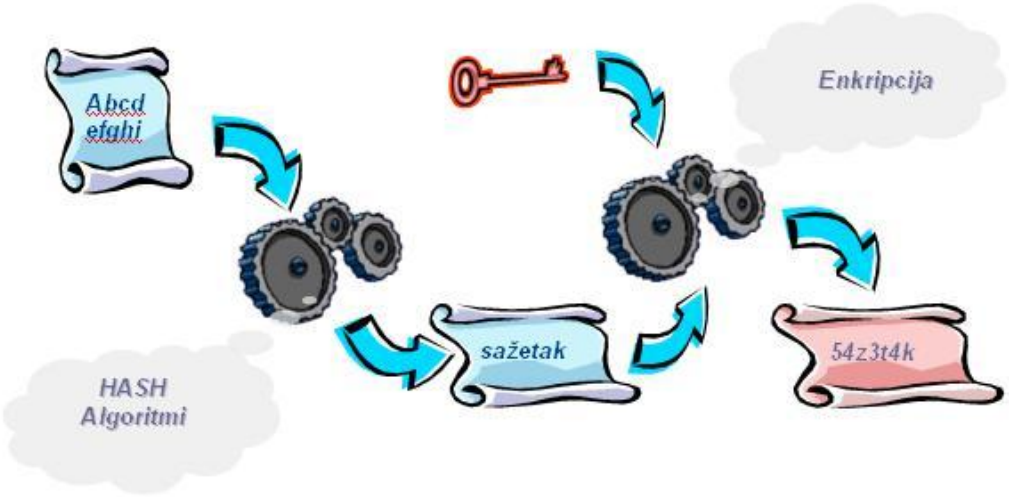
Prema tome napredan elektronički potpis ima istu pravnu snagu i zamjenjuje vlastoručni potpis, odnosno vlastoručni potpis i otisak pečata. Elektroničkim potpisom i njegovom formalno pravnom valjanošću Hrvatska se može uključiti u svjetske gospodarske i tržišne procese e-poslovanja, [32].

7.3.2. Digitalni potpis

Jedna od najpoznatijih implementacija elektroničkog potpisa je digitalni potpis koji je zasnovan na asimetričnoj kriptografiji i algoritmima sažimanja. Dokumenti koji se potpisuju često su veće količine informacija. Asimetrična kriptografija zahtjeva određenu računalnu moć za kriptiranje informacija. U ovisnosti o računalnoj moći i duljini informacije koja se želi kriptirati traje postupak kriptiranja. Prema tome trajanje asimetrične kriptografije nad velikom količinom podataka bi trajalo predugo. Idealna pomoć pri tom problemu su funkcije sažimanja. Digitalni potpis definiran je kao asimetrično kriptirani sažetak informacije privatnim ključem.

Digitalni potpis = E{Q(M), Sa)},gdje je:

- M: informacija
- E: asimetrična funkcija kriptiranja
- Q: funkcija sažimanja
- Sa: privatni ključ



Slika 14. Proces digitalnog potpisa, [33].

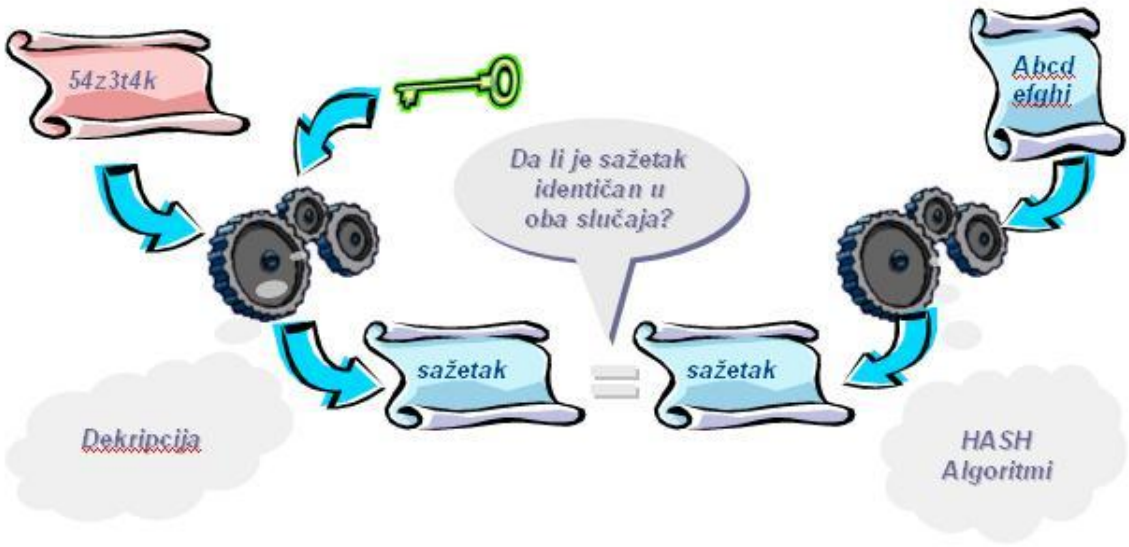
Digitalni potpis osigurava integritet elektroničke informacije, neporecivost i identifikaciju potpisnika, no ne i tajnost. Provjerom potpisa dokazuje se integritet informacije i identificira se potpisnika. Ako je informacija izmijenjena nakon što je bila potpisana to će se detektirati provjerom potpisa, [13].

7.3.2.1. Provjera digitalnog potpisa

Provjera digitalnog potpisa - Q(m')=D{E[Q(m),Sa],Pa} ,gdje je:

- D: asimetrična funkcija dekriptiranja
- Pa: javni ključ
- Q(m') sažetak originalne poruke
- Napravi se sažetak primljene poruke Q(m)

Usporedbom Q(m) i Q(m') provjerava se integritet informacije i identifikacija potpisnika. Dakle Q(m) i Q(m') moraju biti identične, u protivnom ili je informacija naknadno izmijenjena ili je autor nije potpisao ili oboje.



Slika 15. Provjera digitalnog potpisa, [33].

7.3.2.2. Digitalni potpis u praksi

Za primjenu digitalnog potpisa u praksi nedostaje važna karakteristika digitalnog potpisa, a to je autentifikacija potpisnika. Uzmimo za primjer da osoba A pošalje digitalno potpisanu informaciju osobi B. Osoba B po primitku digitalno potpisane informacije može provjerom potpisa provjeriti integritet informacija, ali nikako ne može znati da je osoba A ta za koju se predstavlja. Da bi autentifikacija potpisnika bila moguća treba postojati treća povjerljiva strana. Dakle mora postojati netko kome će se vjerovati. Treća strana naziva se certifikacijski autoritet odnosno certifikator. Opis jedne od mogućih infrastruktura koja, između ostalog, omogućava autentifikaciju je Infrastruktura javnog ključa (eng. Public Key Infrastructure - PKI) , [33].

7.4. Infrastruktura javnog ključa

Komunikacija kojom se razmjenjuju poruke povjerljivog sadržaja kao što je kod usluge e-ID razmjena osobnih podataka mora zadovoljavati nekoliko osnovnih zahtjeva. Prvi zahtjev je autentifikacija, odnosno mogućnost da primatelj poruke pouzdano utvrdi identitet pošiljatelja poruke. Drugi zahtjev je vjerodostojnost, odnosno mogućnost da primatelj poruke utvrdi da li se na putu od odredišta do cilja poruka mijenjala i da li je stigla cjelovita. Treći zahtjev je neporecivost, odnosno sprječavanje pošiljatelja poruke u opovrgavanju činjenice da je on poslao poruku. Četvrti zahtjev je povjerljivost kojim se osigurava tajnost sadržaja poruke za svakoga kome poruka nije namijenjena.

Infrastruktura javnih ključeva zadovoljava sve gore navedene zahtjeve te time omogućuje korisnicima da kroz nesigurnu javnu mrežu, kao što je mreža Internet, sigurno razmjenjuju podatke, novac i druge osjetljive informacije. Koristeći pritom asimetričnu kriptografiju i digitalne vjerodajnice. Infrastruktura javnih ključeva predstavlja osnovu na kojoj se grade aplikacije i mrežne sigurnosne komponente.

Infrastruktura javnog ključa (PKI) složeni je sustav koji objedinjuje certifikate, certifikacijsku centar (certifikator), bazu certifikata i opozvanih certifikata, korisnike certifikata, te sve njihove međusobne interakcije. Prije svega PKI je sustav koji omogućuje autentifikaciju. Koristeći simetričnu i asimetričnu kriptografiju osigurava brojne usluge uključujući povjerljivost podataka, njihov integritet te upravljanje ključevima, odnosno certifikatima, [12].

Infrastruktura javnog ključa omogućuje:

- zaštitu privatnosti komunikacije osiguravajući komunikaciju od presretanja i neovlaštenog čitanja,
- osiguranje integriteta elektroničke komunikacije onemogućavajući izmjene podataka tijekom njihovog prenošenja mrežom
- potvrđivanje identiteta stranaka koje sudjeluju u komunikaciji,
- osiguranje neporecivosti sudjelovanja bilo koje stranke u komunikaciji, [34].

7.5. Ispitivanje sigurnosti primjene informacijsko komunikacijske usluge e-ID

Na sigurnost usluge e-ID mogu utjecati razne prijetnje. Prijetnja je općenito pojava koja ima potencijal uzrokovati gubitak ili štetu. Mogu se svrstati u četiri skupine:

- prirodne prijetnje,
- nenamjerne prijetnje (nesreća),
- prijetnje ljudi s atribucijom nenamjernosti,
- prijetnje ljudi s atribucijom namjernosti,
    - aktivni ljudski napadi,
    - pasivni ljudski napadi, [3].

Razne prijetnje mogu prerasti u ranjivost. Ranjivost je mogućnost da prijetnja postane realnost tj. opisuje se kao stanje, nedostatak ili slabost u sustavu koja se može iskoristiti da bi se uzrokovala šteta ili gubitak, [17].

Prirodne prijetnje mogu se opisati kao geofizičke nesreće, vremenske neprilike, sezonski fenomeni i sl. koji za uzrok imaju uništenje ili oštećenje uređaja, gubitak ili degradacija mreže, prekid komunikacije što podrazumijeva obustavu protoka podataka. Prirodne prijetnje mogu biti požari, potresi, poplave, ispad napajanja (grmljavina) i sl.

Nenamjerne prijetnje se mogu javiti prilikom transporta, u industriji, utjecajem okoline, te na samim uređajima. Takva vrsta prijetnje dolazi iznenadno, a rezultat je uništenje uređaja te mrežnih uređaja i informacija, gubitak mogućnosti obrade podataka, degradacija usluge i sl. Nenamjerne pogreške mogu biti:

- korisničke pogreške,
- operaterske pogreške,
- pogreške administriranja,
- greške pripreme podataka,
- greške izlaza,
- greške računalnih sustava,
- komunikacijske pogreške,
- greške aplikacijskih programa. [3].

Prijetnje ljudi s atribucijom nenamjernosti mogu imati za rezultat gubitak podataka i informacija, uništenje uređaja i mrežnih komponenti, davanje podataka o osobama slučajno (izvan ovlasti) i sl. Do takvih prijetnji dolazi s ljudskom nepažnjom, nemarom i nedisciplinom. Općenito zaposlene osobe nisu dovoljno educirane, koriste neodgovarajuću aplikacijsku opremu i programe, te nisu ni svjesne svojih neodgovarajućih postupaka.

Prijetnje ljudi s atribucijom namjernosti najčešći su uzrok gubitka podataka i oštećenja uređaja te mrežne opreme. U takvoj vrsti prijetnje ljudi namjerno odlučuju o napadaju na sustav s ciljem prikupljanja podataka o osobama i eventualnim ucjenama. Prijetnje se mogu opisati kao uništenje, sabotaža, diverzija, špijunaža, ratno razaranje, krađa, virusi i prisluškivanje. Prijetnje ljudi s atribucijom namjernosti mogu biti:

- građanska neposlušnost,
- neovlašten pristup,
- sabotaža,
- gomilanje prometa,

a mogu se svrstati u dvije skupine: na pasivne i aktivne ljudske napade.

Kod pasivnih ljudskih napada najčešće posljedice su presretanje informacija, a prijetnje mogu biti:

- elektromagnetsko zračenje,
- priključak na liniju,
- otkrivanje osjetljivih informacija.

Kod elektromagnetskog zračenja najčešće stradaju kablovi, zemaljske linije, računala i mrežne komponente. Otkrivanje osjetljivih informacija može se opisati kao gubitak informacija od strane zaposlenog osoblja, nepravilno označavanje informacija, nepravilno rukovanje informacijama te zloupotreba mrežnih resursa. Priključak na liniju pasivnim ljudskim napadom može se ostvariti na kablovima, zemaljskim linijama te mikrovalnim vezama.

Kod aktivnih ljudski napada do izražaja dolazi građanska neposlušnost koja npr. ima za posljedicu onemogućavanje dolaska na posao, oštećenja uređaja i osoblja. Neovlašteni pristup osoba za posljedicu ima gubitak, manipulacija, oštećenje

ili otkrivanje podataka o drugim osobama, dok sabotaža usmjerava na terorizam, bombardiranje, modifikacije programa i vandalizam, gdje dolazi do uništenja ili oštećenja uređaja i/ili osoblja. Gomilanje prometa se opisuje kao povećanje lažnog prometa u mreži, a za posljedicu ima degradaciju ili potpuni gubitak komunikacijske povezanosti, [3].

Najpoznatiji pojam kod ljudi s atribucijom namjernosti je haker (eng. *Hacker*), a označava osobu koja odlično poznaje računala, softver i hardver. Često je predmet aktivnog ljudskog napada jer su osobe koje vole kroz pozitivnu znatiželju istraživati granice onoga što je moguće, to često uključuje prepravljanje postojećih hardverskih i softverski rješenja kako bi se dobila nova funkcija ili otključala neka skrivena, [36].

7.6. Krađa identiteta

Krađa identiteta je oblik kriminalne radnje lažnog predstavljanja radi stjecanja materijalne ili druge koristi. Jedan način krađe identiteta je iz baza podataka informacijskih sustava usluge e-ID i sustava drugih ustanova koje pohranjuju takve informacije, gdje treba pripaziti na transakcije, tj. s kim se posluje. Drugi način je da napadač izravno od osobe ciljanog napada ukrade informacije ili ih dobije na prijevaru. Veliku ulogu u krađi identiteta ima socijalni inženjering koji se oslanja na prirođeno povjerenje u ljude, naročito ljude koji imaju određene društvene uloge, poput osoba u uniformama, odjelima ili sa iskaznicama, koje se predstavljaju kao legitimne osobe. Neki od alata za krađu identiteta opisani su u nastavku.

Spoofing znači kreiranje lažne ili krivotvorene verzije nečega, poput Web lokacije ili adrese e-pošte. Korisnik se prijavljuje sa svojim korisničkim imenom i lozinkom koje tako dolaze u ruke kriminalaca, a oni ih zlorabe za pristup stvarnoj *Web* lokaciji.

Phishing napadi su najštetniji napadi prevaranata, od kojih većina započinje porukom e-pošte. U njima obično piše da je problem s računom vlasnika koji treba riješiti, te se šalje zamolba vlasniku računa za podatke (korisničko ime, broj računa, lozinku i sl.) da bi se riješio problem s računom. Ponekad se umjesto e-pošte formira nova stranica koja izgleda slično kao originalna, te otvaraju mogućnosti za krađu identiteta da osoba unaša svoje podatke, a zapravo se prosljeđuju podaci prevarantima. Oni te podatke koriste većinom u svrhu pribavljanja novaca ili prodaje identiteta.

Key logger je program koji bilježi sve podatke pritiskane na tipke tipkovnice. Program šalje informacije udaljenom napadaču koji skenira podatke radi pronalaska korisnih dijelova koje može iskoristiti u vlastitu korist, poput lozinki, brojeva računa i sl.

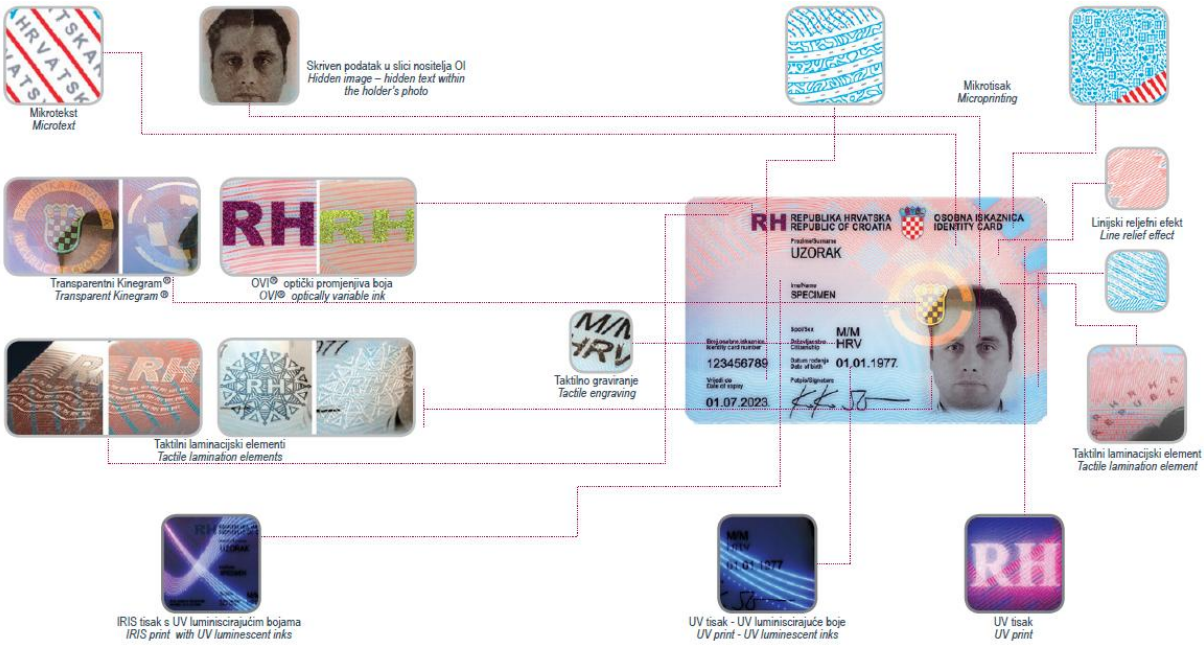
Krađa pošte i „kopanje po smeću“ (eng. *Recycle Bin*) je također prisutno. Napadaču se mogu naći korisne informacije, jer osoba nije dovoljno pažljiva prilikom zbrinjavanja korisničkih podataka. E-poštom se mogu slati i primati lozinke, kodovi, PIN-ovi i slični povjerljivi podaci, koji mogu biti otkriveni prilikom ulaska napadača na elektroničku poštu. Najbolji način sprečavanja kopanja po smeću je uništavanje svih povjerljivih poruka, [35].

7.7. Sigurnost osobne iskaznice

Osobna iskaznica (OI) građana Republike Hrvatske je polikarbonatna kartica, u potpunosti usklađena sa zahtjevima, preporukama i smjernicama ICAO 9303 *Part 3, Volume 1 -2008* međunarodnog standarda koji definira izgled, format i zaštite strojno čitljivih identifikacijskih i putnih dokumenata ID1 formata. Vrsta i količina zaštitnih elemenata osobne iskaznice također su usklađeni i s najboljom europskom praksom.

Zadaća zaštitnih elemenata OI je zaštita dokumenta od potpunog ili djelomičnog krivotvorenja, te zaštita integriteta individualiziranih podataka koji se nalaze na tijelu kartice. Zaštitni elementi dijele se u tri razine:

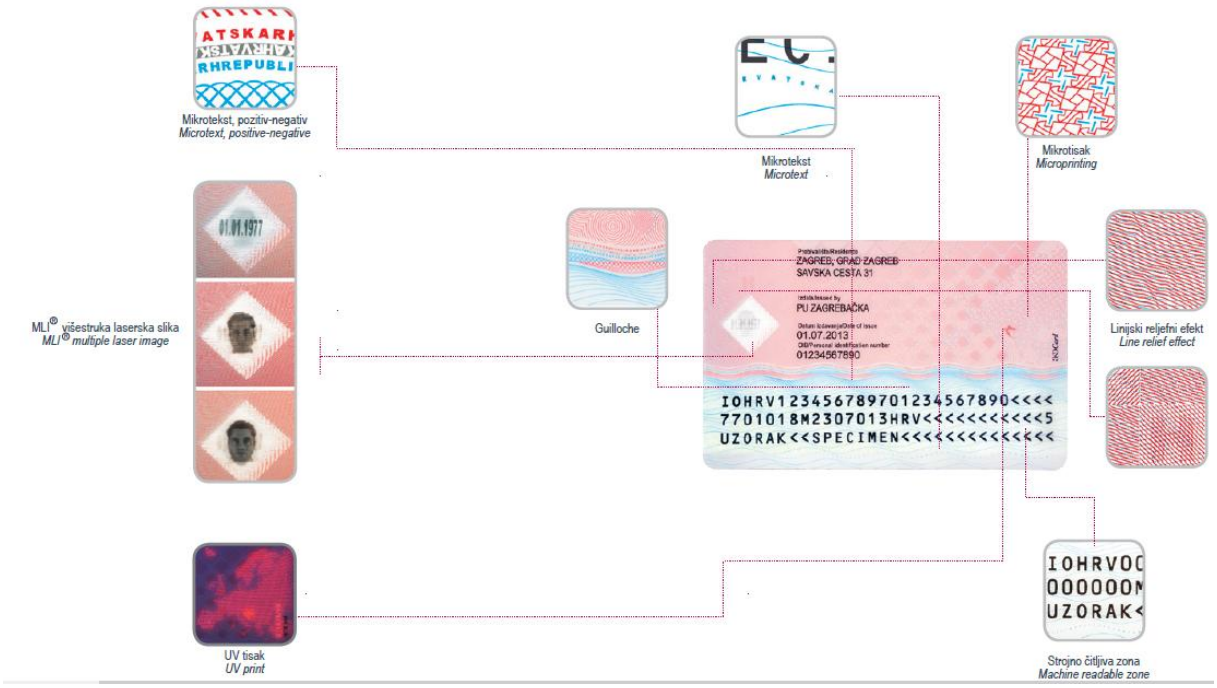
- prva razina: osnovni vizualni zaštitni elementi za čiju provjeru nisu potrebna posebna pomagala
- druga razina: zaštitni elementi poznati ograničenom broju ljudi (policijski službenici, carina i ostale državne službe). Za provjeru ove razine zaštite potrebni su jednostavniji optički ili opto-elektronički uređaji
- treća razina: Forenzička razina zaštite: za utvrđivanje zaštitnih elemenata treće razine zaštite potrebna je forenzička oprema ili laboratorijski uvjeti ispitivanja, [16].



Slika 16. Elementi zaštite na prednjoj strani osobne iskaznice, [16].

Elementi prve razine zaštite:

- obostrani taktilni elementi tijela kartice,
- OVI boja - optički promjenjiva boja,
- transparentni Kinegram (elementi vidljivi bez optičkih uređaja),
- ispupčeno lasersko graviranje državljanstva nositelja OI,
- MLI ® - *Multiple laser image* s podacima sekundarne slike i datuma rođenja nositelja OI,
- anti-kopirajući uzorak; uzorak na prednjoj strani i poleđini OI koji postaje vidljiv pri kopiranju OI,



Slika 17. Elementi zaštite na stražnjoj strani osobne iskaznice, [16].

Elementi druge razine zaštite

- transparentni Kinegram ® (elementi vidljivi upotrebom optičkih uređaja)
- UV luminiscirajuće boje
- IRIS tisak UV luminiscirajućim bojama
- mikrotekst
- *Hidden image* - skriven podatak u slici nositelja OI

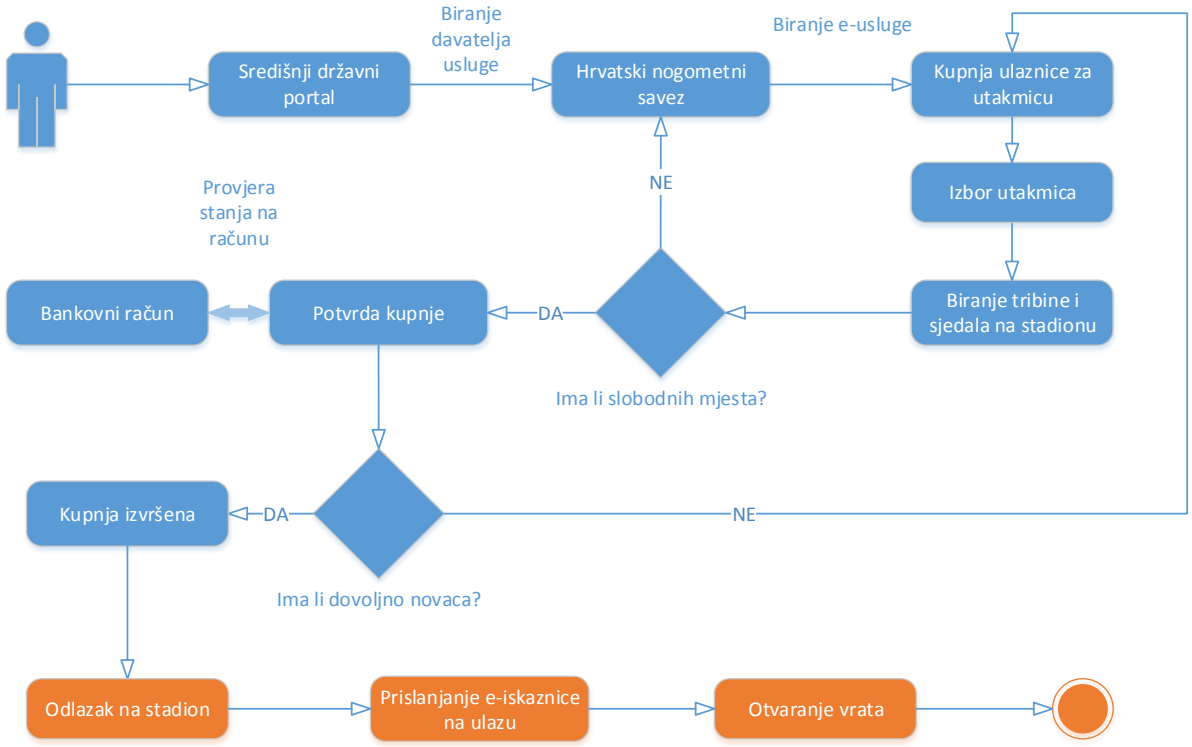
Elementi treće razine zaštite

- *IR Drop Out* boja
- namjerne greške u mikrotekstu
- specijalni rasterski elementi unutar elemenata krune grba RH, [16].

8. Scenarij kupnje ulaznice za nogometne utakmice HNS-a

Scenarij prikazuje kupnju ulaznice za utakmice Hrvatske nogometne reprezentacije putem Hrvatskog nogometnog saveza kao davatelja elektroničkih usluga.

Korisnik se prijavljuje na središnji državni portal gdje bira HNS kao davatelja e-usluga. On kao takav omogućuje kupnju ulaznica online. Uz kupnju ulaznice korisnik bira utakmicu, tribinu i broj sjedala na stadionu. U slučaju da za biranu utakmicu nema slobodnih mjesta, korisnika se upućuje na davatelja usluge, u tom slučaju HNS, te može odlučiti na izbor drugih usluga istog davatelja. Ako ima mjesta na stadionu, korisnik potvrđuje kupnju gdje se istovremeno provjerava stanje na bankovnom računu. Ukoliko korisnik ima dovoljno novaca, ulaznica je kupljena, a u protivnom ga vraća na izbor e-usluga. Na korisniku preostaje odlazak na utakmicu, te na ulazu na stadion korisnik prislanja elektroničku osobnu iskaznicu (e-iskaznicu) prilikom čega se vrši identifikacija korisnika, te na kraju dobiva potvrda o ulazu. Za davatelja usluge smanjeni su troškovi ispisa ulaznica, a za korisnika troškovi odlaska na stadion za kupnju ulaznica i čekanja u redu.



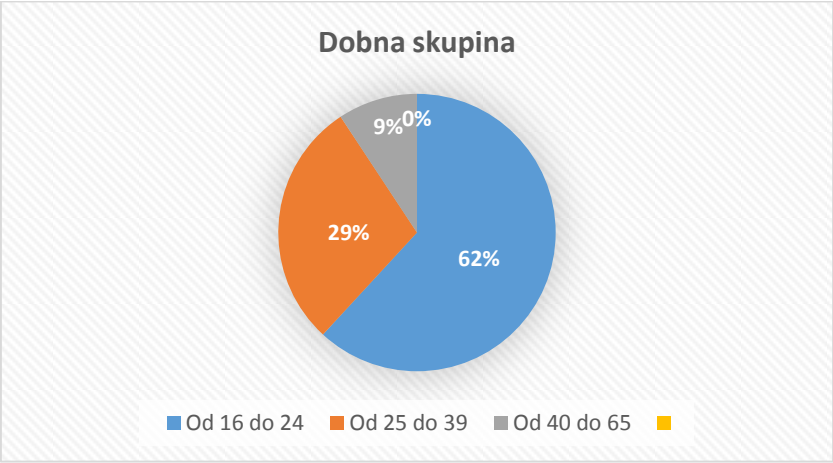
Slika 18. Prikaz kupnje ulaznice online preko središnjeg državnog portala i identifikacija korisnika na ulazu na stadion

9. Analiza ankete ispitanih korisnika

Anketa je naziv za skup postupaka pomoću kojih se pobuđuju, prikupljaju i analiziraju izjave ljudi kako bi se saznali podaci o njihovu ponašanju ili o njihovim stavovima, mišljenjima, preferencijama, interesima i slično, radi statistike, ispitivanja javnog mnijenja, tržišta ili kao temelj za potrebe medicinskog, sociološkog ili nekog drugog istraživanja.

Vrijednost ankete je ograničena, jer spoznaje koje nam ona može dati ovise o iskrenosti ispitanika i o njihovoj sposobnosti da odgovore na postavljena pitanja. Ali, uz primjeren problem istraživanja, dobro konstruiran i provjeren upitnik, reprezentativan uzorak ispitanika i uz konkretno prikupljanje i prikladnu analizu podataka, anketom se može doći do korisnih podataka o ljudskom doživljaju i ponašanju, [37].

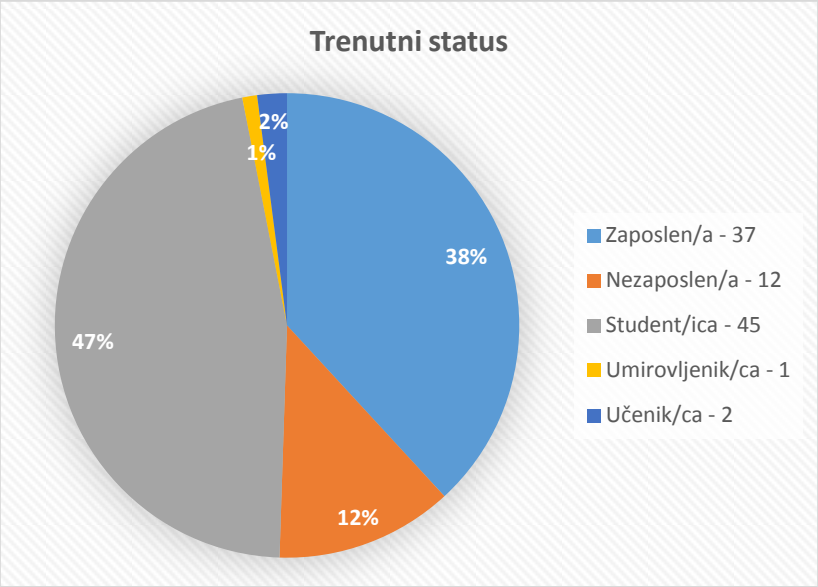
Anketa je provedena u svrhu ispitivanja stavova ljudi prema novoj informacijsko komunikacijskoj usluzi e-ID. Anketom su zabilježeni odgovori 97 ispitanika, među kojima se nalazi 90 fizičkih i 7 poslovnih osoba. Anketa je provedena kroz *Google* obrasce (eng. *Forms*), koji omogućuju sakupljanje odgovora te analizu istih. Korisnici su na anketu odgovarali putem *link-a* objavljenog na društvenoj mreži *Facebook*, te direktnim anketiranjem. Odgovori su prikupljani između 2. i 10. rujna 2015. Anketnim ispitivanjem zabilježeno je 50 ispitanika muškog roda i 47 ispitanika ženskog roda.



Grafikon 1. Prikaz dobne skupine

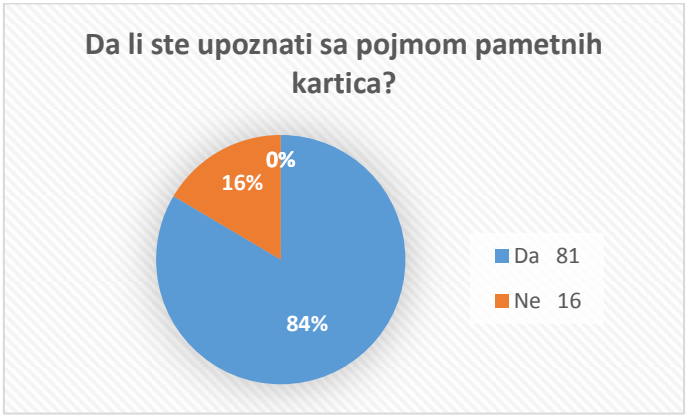
U anketi je sudjelovalo više mlađe populacije pri čemu je prikupljeno 60 odgovora ispitanika između 16 i 24 godine, 28 odgovora ispitanika između 25 i 39 godina, te 9 odgovora ispitanika između 40 i 65 godina.

Prema Grafikonu 2 vidljiv je trenutni status ispitanika, pri čemu je prikupljeno najviše odgovora studenata, ukupno 45, što čini 47% ukupnog broja odgovora.



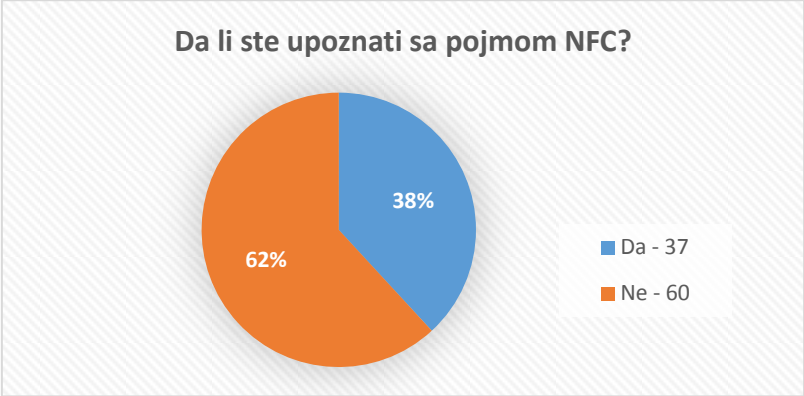
Grafikon 2. Prikaz trenutnog statusa ispitanika

Prema grafikonu 3 većina ispitanika je upoznata sa pojmom pametnih kartica, što znači da je većina njih koristila neku vrstu pametnih kartica do sada. Od ukupnog broja, 81 osoba je čula za pojam pametnih kartica, a 16 nije.



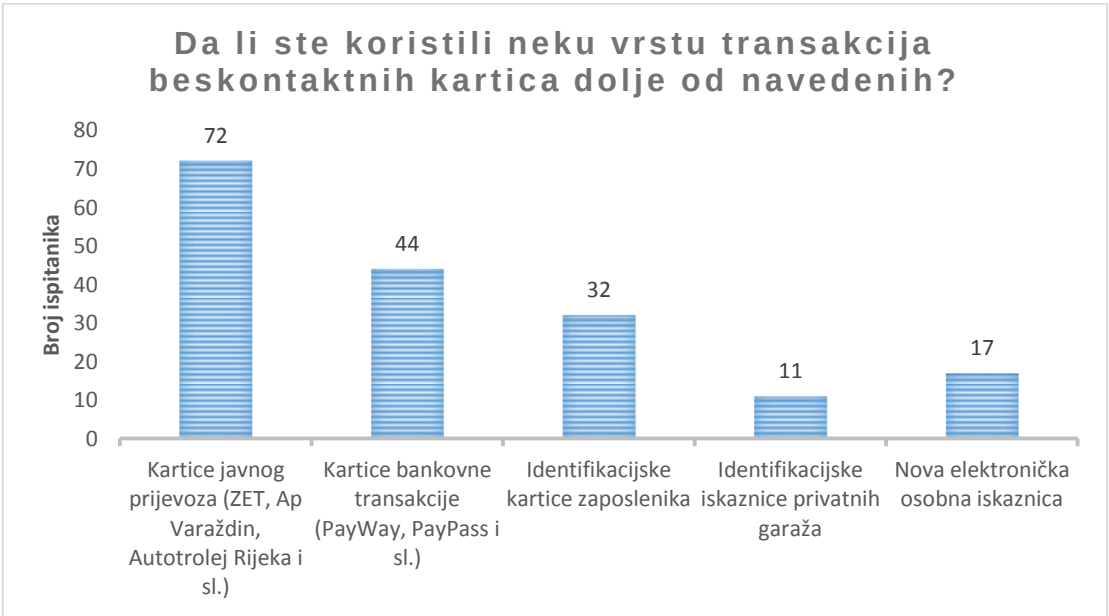
Grafikon 3. Prikaz broja ispitanika koji su upoznati za pojmom pametnih kartica

Od ispitanih osoba, na pitanje da li su upoznati sa pojmom NFC (*Near Field Communication*), njih 60 je odgovorilo da nije, a 37 njih se izjasnilo da su upoznati. Iz viđenog, može se pretpostaviti da ispitanicima nije bitno o kojoj se tehnologiji radi, već da bude pouzdano.



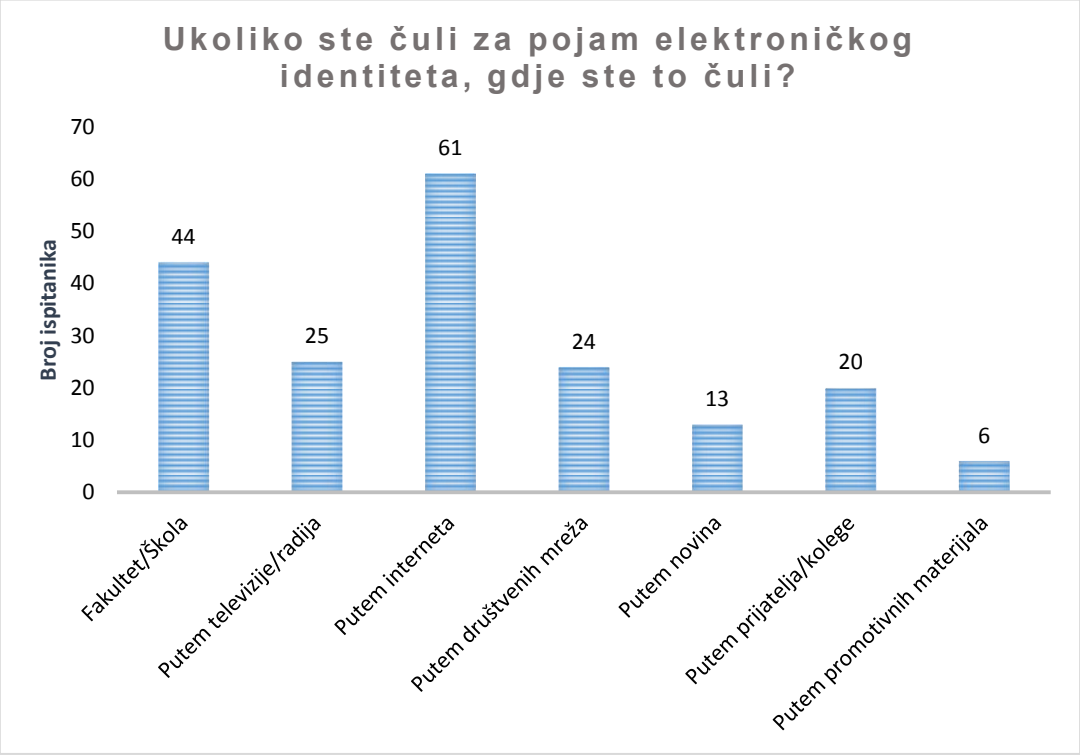
Grafikon 4. Prikaz broja ispitanika koji su upoznati za pojmom NFC

Prema odgovorima ispitanika, u grafikonu 5, prikazan je broj ispitanika koji su koristili neke vrste beskontaktnih pametnih kartica. Najpopularnije su kartice javnog prijevoza, čak 72 osobe su potvrdile korištenje istih. Nove vrste beskontaktnih bankovnih transakcija pomoću kartica od ukupnog broja koristile su 44 osobe. Identifikacijske iskaznice zaposlenika koristile su 32 osobe, 11 osoba kartice za privatne garaže, a 17 osoba novu elektroničku osobnu iskaznicu.



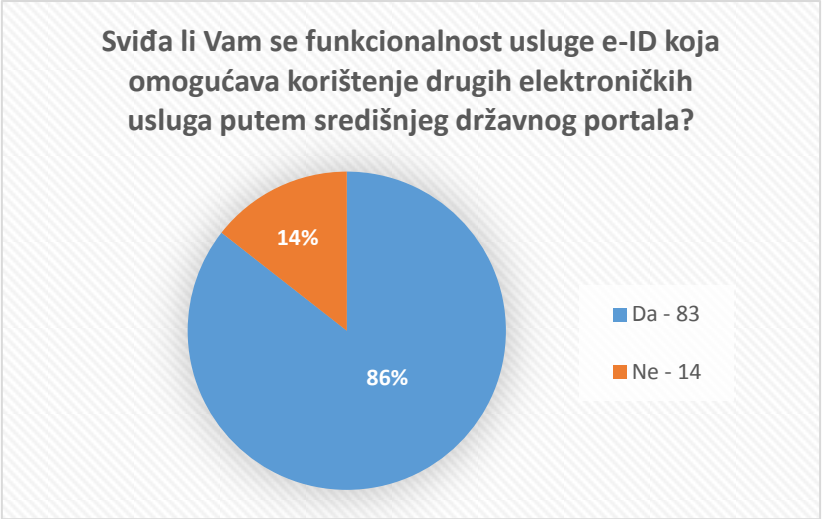
Grafikon 5. Prikaz korištenja beskontaktnih pametnih kartica

Od 97 ispitanika, 16 ih nije upoznato sa pojmom elektroničkog identiteta. Ispitanici koji su čuli za pojam elektroničkog identiteta najviše ih je čulo putem interneta, ukupno 61. Većinu informacija danas ljudi prikupljaju na internetu putem različitih *news* portala koji redovito informiraju o različitim novitetima. Putem fakulteta ili škole za pojam elektroničkog identiteta čulo je 44 ispitanika, što znači da su učenici i studenti informirani u obrazovanju o napretku tehnologije. Na pitanje ispitanicima da li su koristili do sad elektronički identitet u sklopu sustava e-građani, njih 35 je potvrdilo korištenje istog, dok 62 ispitanika nije koristilo elektronički identitet.



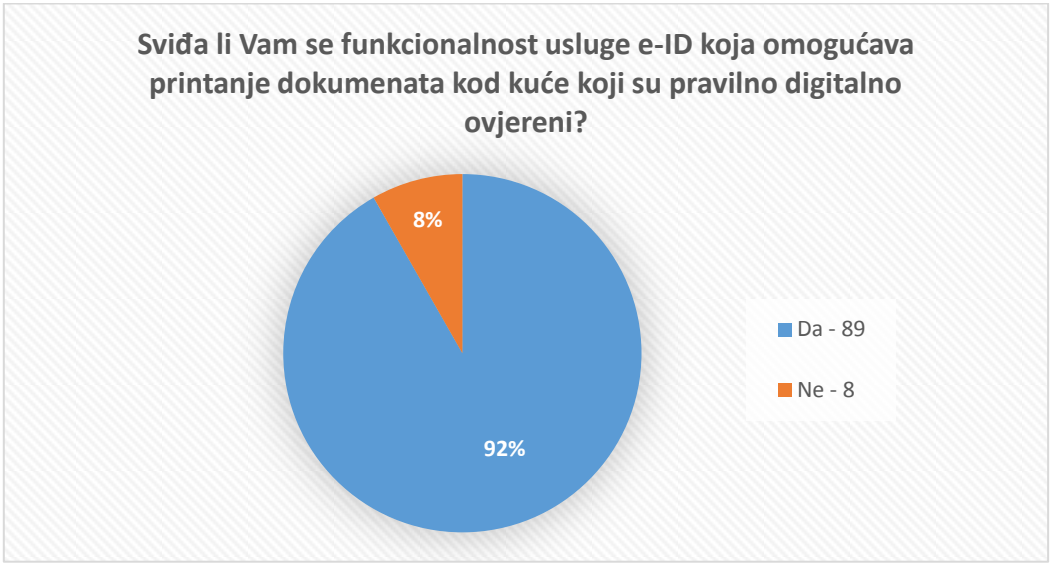
Grafikon 6. Prikaz na koji način su ispitanici čuli za pojam elektroničkog identiteta

Slijedeći grafikon prikazuje broj ispitanika kojima se sviđa funkcionalnost usluge koja omogućava korištenje drugih elektroničkih usluga putem središnjeg državnog portala. Čak 83 ispitanika bi bilo zadovoljno korištenjem ove funkcionalnosti, dok se 14 ispitanika ne bi složilo takvom funkcionalnošću.



Grafikon 7. Prikaz broja osoba kojima se sviđa funkcionalnost korištenja drugih e-usluga putem središnjeg državnog portala

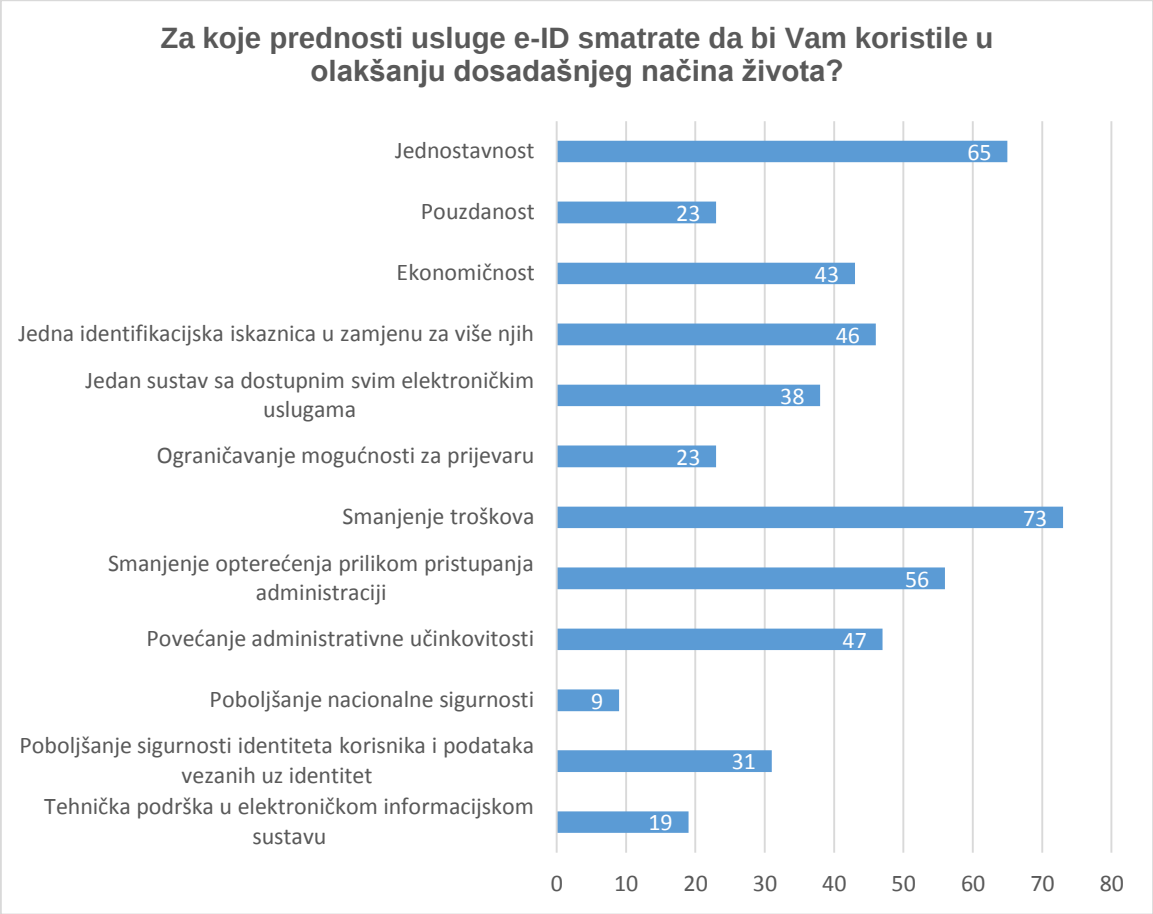
Na pitanje u anketi da li bi korisnici ove usluge bili zadovoljni funkcionalnošću koja omogućuje ispis dokumenata kod kuće koji su pravilno digitalno ovjereni. 89 ispitanika je potvrdilo zadovoljstvo, dok se 8 ispitanika ne slaže sa takvom funkcionalnošću.



Grafikon 8. Prikaz broja osoba kojima se sviđa funkcionalnost ispisivanja dokumenata kod kuće koji su pravilno digitalno ovjereni

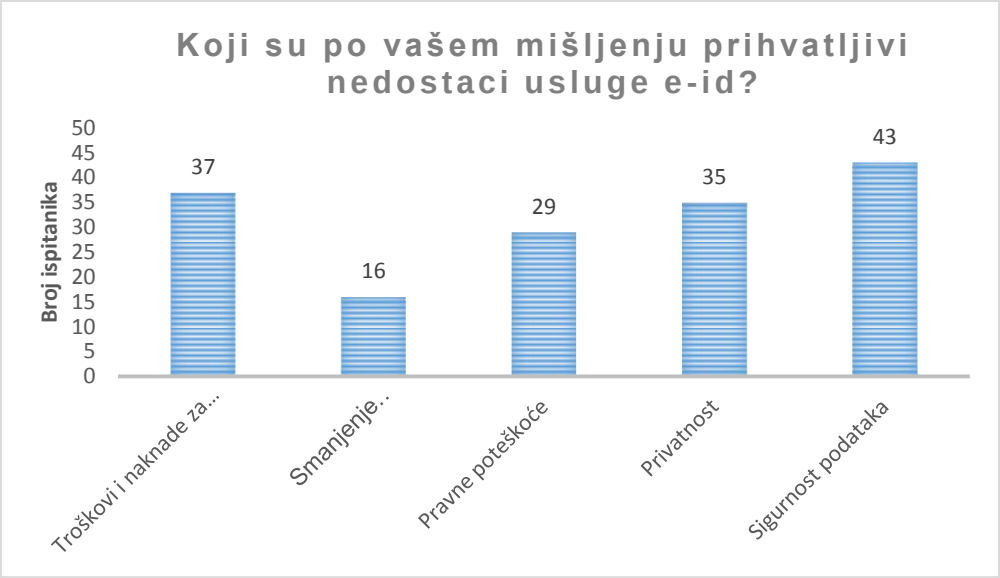
Pitanje o prednostima za koje ispitane osobe smatraju da bi poboljšale njihov dosadašnji način života, 73 ispitanika se izjasnilo za smanjenje troškova, a 65 za

jednostavnost usluge. Smanjenje opterećenja prilikom pristupanja administraciji potvrdilo je 56 osoba, te za povećanje administrativne učinkovitosti odlučilo je 47 osoba. Njih 46 je potvrdilo za prednost jednu identifikacijsku iskaznicu u zamjenu za više njih, te 38 za jedan sustav sa dostupnim svim e-uslugama.



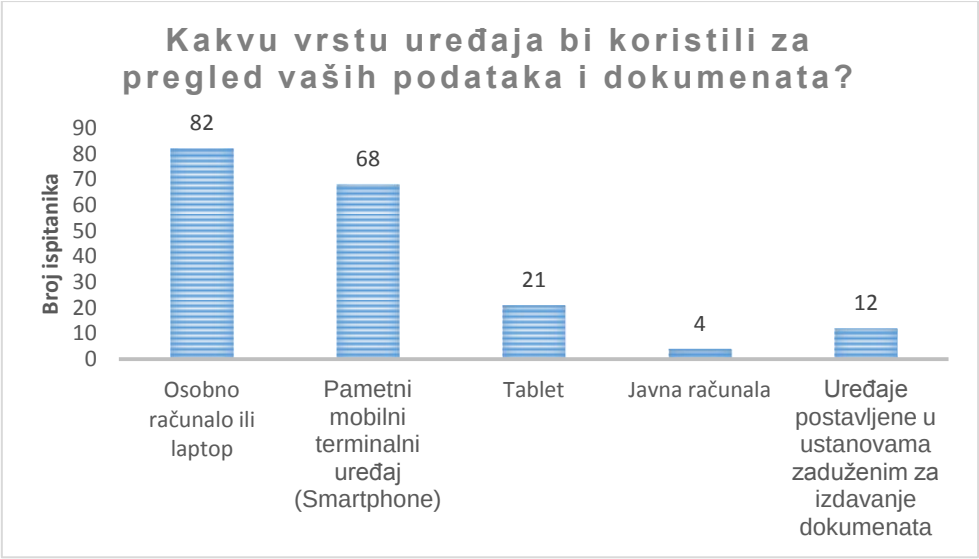
Grafikon 9. Prikaz prednosti za koje ispitanici smatraju da bi poboljšale njihov način života

Na pitanje o prihvatljivim nedostacima usluge, 43 ispitanika se izjasnilo za sigurnost podataka, 37 ispitanika bi prihvatilo troškove implementacije usluge, 35 osoba vidi privatnost kao nedostatak, 29 osoba pravne poteškoće, te 16 osoba smanjenje interoperabilnosti.



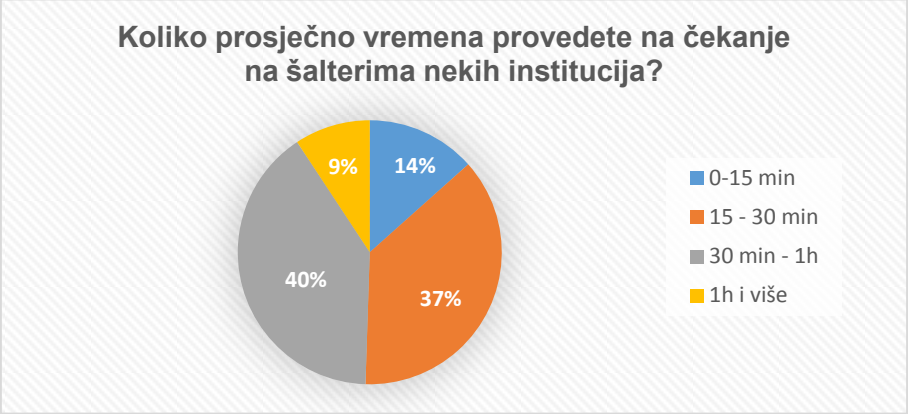
Grafikon 10. Prikaz prihvatljivih nedostataka usluge

Prema grafikonu 11, za pregled svojih podataka i dokumenata, 82 ispitanika se odlučilo za osobno računalo ili laptop, 68 ispitanika bi koristilo Smartphone, 21 ispitanik tablet, dok bi se 12 ispitanika odlučilo za uređaje postavljene u ustanovama zaduženim za izdavanje dokumenata. Samo četvero ispitanika bi se odlučilo za javna računala, što daje dobru sliku o svjesnosti ljudi za sigurnost svojih računa. Općenito su javna računala najviše ranjiva na krađu identiteta.



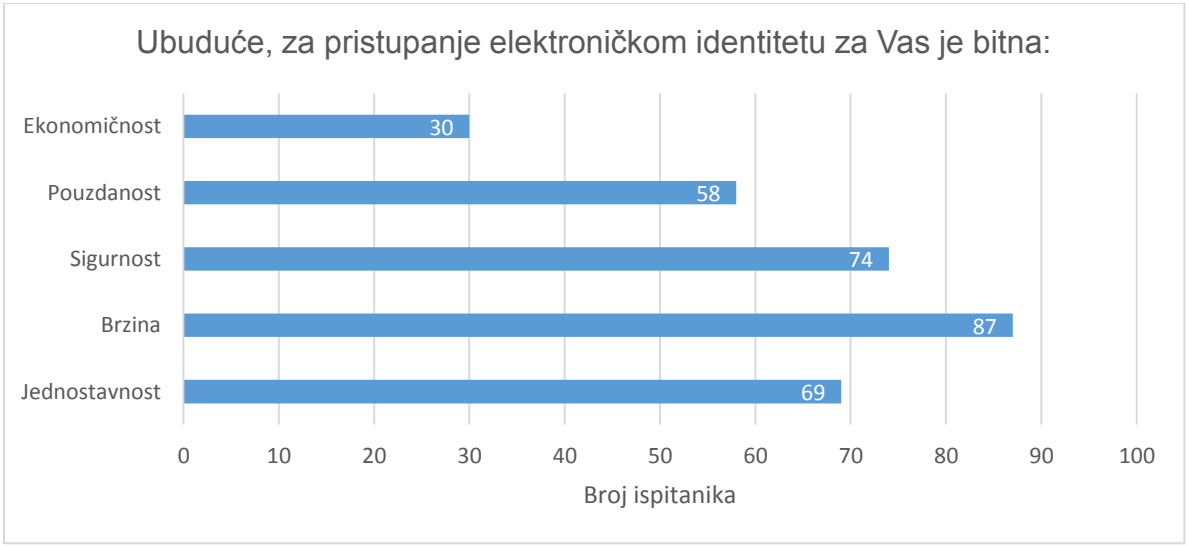
Grafikon 11. Prikaz vrste uređaja koje bi ispitanici koristili za pregled podataka i dokumenata

Iz grafikona 12 vidljivo je čekanje ispitanika na šalterima nekih institucija. Većina ispitanika, njih 39 čeka između 30 minuta i 1 sat, što je dugo vremena na čekanje posluživanja. 36 ispitanika se izjasnilo da čeka između 15 i 30 minuta, njih 13 na čekanje između 0 i 15 minuta, te 9 ispitanika na čekanje između 30 minuta i sat vremena.



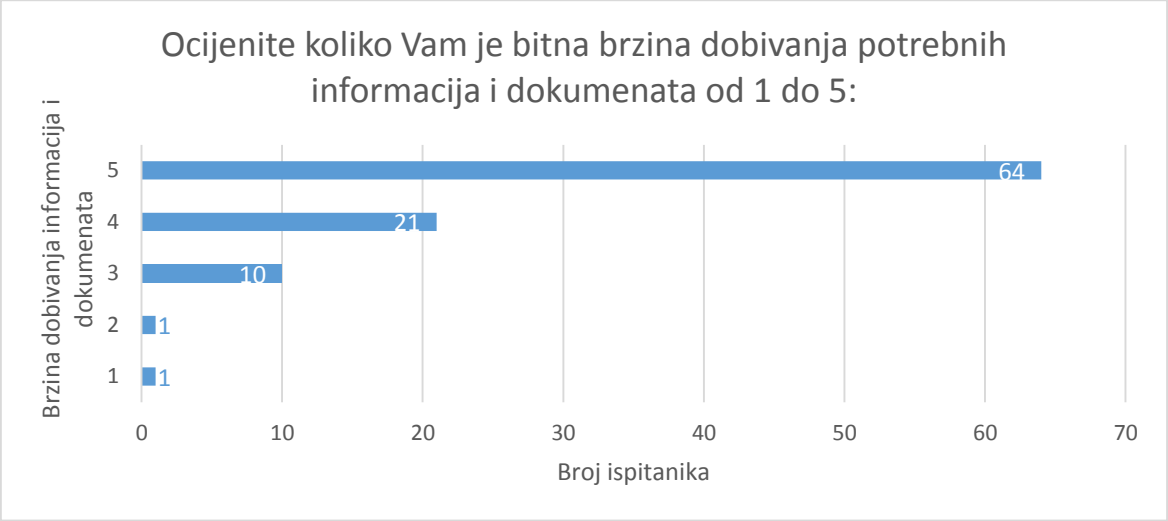
Grafikon 12. Prikaz prosječnog vremena čekanja ispitanika na vrijeme posluživanja u nekim institucijama

U slijedećem grafikonu prikazani su elementi koji su bitni za pristupanje elektroničkom identitetu. Najviše ispitanika, njih 87, potvrdilo je brzinu kao najbitniji element, a njih 74 sigurnost. Jednostavnost je odabralo 69 ispitanika, pouzdanost 58, dok je ekonomičnost odabralo 30 ispitanika.



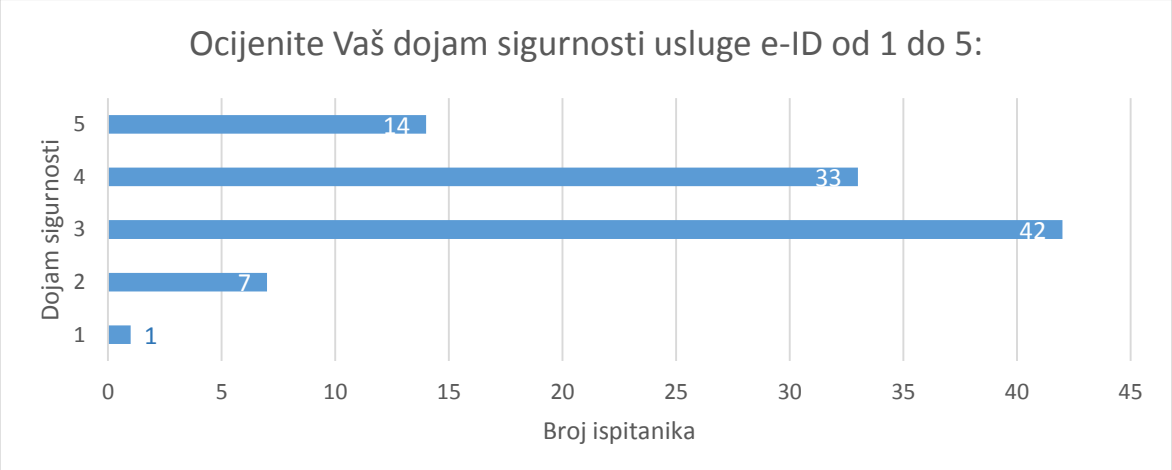
Grafikon 13. Prikaz elemenata koji su bitni ispitanicima za pristupanje elektroničkom identitetu

Ispitanici su ocijenili koliko im je bitna brzina dobivanja potrebnih informacija i dokumenata. Najviše ispitanika se izjasnilo ocjenom 5, njih 64, što upućuje da je korisniku izrazito potrebna brzina dobivanja informacija i dokumenata. Ocjenom 4 izjasnila se 21 osoba, ocjenom 3, 10 osoba, te ocjenama 1 i 2 po jedna osoba.



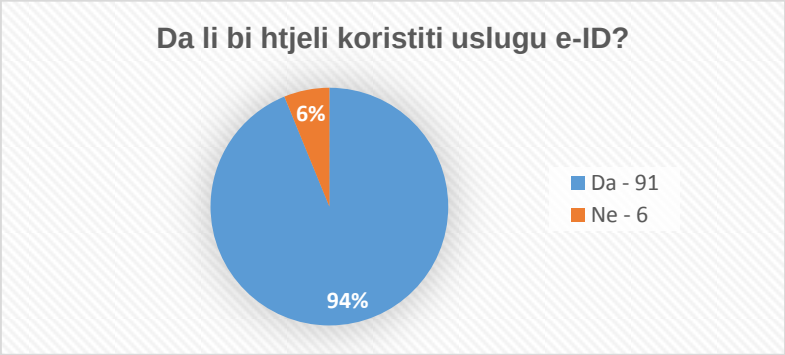
Grafikon 14. Prikaz koliko je ispitaniku bitna brzina dobivanja informacija i dokumenata

Pitanje o sigurnosti usluge e-ID najviše ispitanika ocijenilo je ocjenom 3, njih 42. Dojam sigurnosti ocjenom 4 potvrdile su 33 osobe, ocjenom 5, 14 osoba, te ocjenom 2, 7 osoba. Jedna osoba ocijenila je dojam sigurnosti usluge ocjenom 1. U ovom pitanju ocjena 5 je predstavljala najveću sigurnost, dok je ocjena 1 predstavljala najmanju.



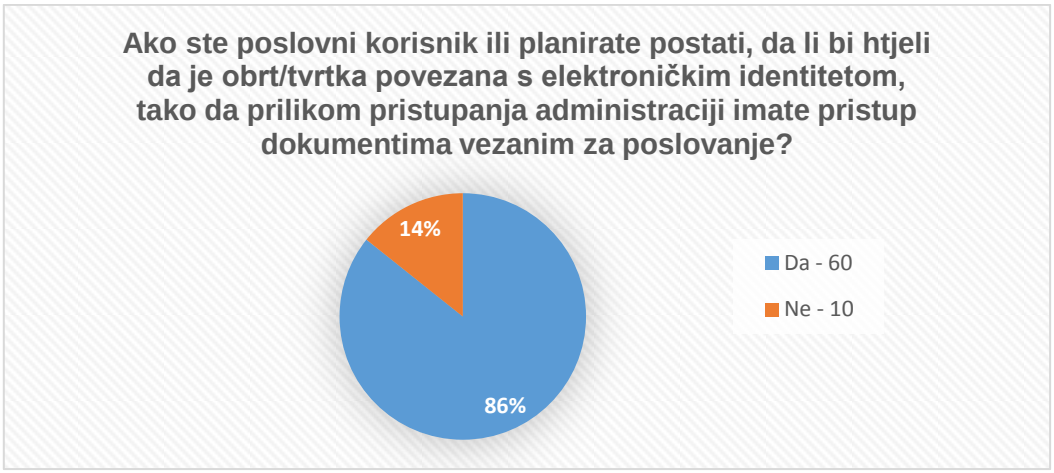
Grafikon 15. Dojam sigurnosti usluge e-ID

U daljnjem anketiranju ispitanici su odgovarali na pitanje da li bi bili zadovoljni sa jednom identifikacijskom ispravom koja bi zamjenila više njih, te je 90 ispitanika potvrdilo korištenje iste, a 7 ispitanika se nije složilo sa time. Nadalje, osobama je ponuđeno pitanje da li bi htjeli koristiti uslugu e-ID, te je očekivanim rezultatima potvrđen pozitivan odgovor. Od 97 ispitanika, 91 osoba bi htjela koristiti takvu uslugu, dok 6 osoba nije zainteresirano.



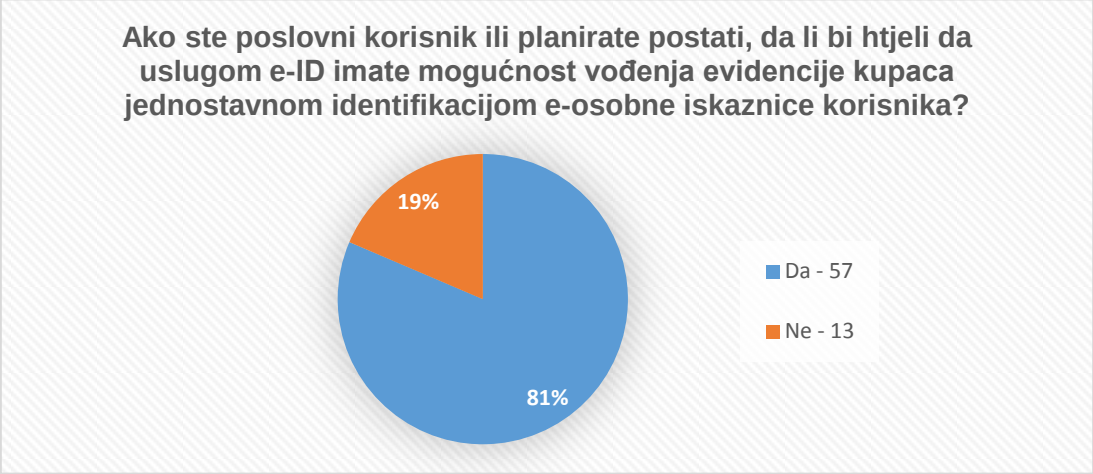
Grafikon 16. Prikaz broja ispitanika koji bi htjeli koristiti uslugu e-ID

Za kraj su postavljena pitanja za poslovne korisnike ili one koji planiraju postati. Na ta pitanja odgovorilo je 70 ispitanika. Osobe su pitane da li bi htjeli da je obrt/tvrtka povezana s elektroničkim identitetom, tako da prilikom pristupanja administraciji imate pristup dokumentima vezanim za poslovanje. 60 ispitanika se složilo sa time, dok je 10 njih potvrdilo da ne bi bili zadovoljni sa takvom funkcionalnošću.



Grafikon 17. Prikaz zainteresiranosti poslovnih korisnika za funkcionalnošću povezivanja obrta/tvrtke sa elektroničkim identitetom

U grafikonu 18, prikazana je zainteresiranost poslovnih korisnika ili onih koji planiraju postati, da li bi htjeli da uslugom e-ID imaju mogućnost vođenja evidencije kupaca jednostavnom identifikacijom elektroničke osobne iskaznice korisnika. Odgovor je dalo 70 ispitanika, gdje je njih 57 potvrdilo takvu funkcionalnost, a 13 ispitanika se ne slaže sa time.



Grafikon 18. Prikaz zainteresiranosti poslovnih korisnika za funkcionalnošću koja omogućuje vođenje evidencije kupaca jednostavnom identifikacijom e-osobne iskaznice korisnika

10. Zaključak

U današnje vrijeme korisnici kreiraju sve više računa za Internet transakcije i poslovanje. Prilikom kreiranja tih računa, korisnik u većini slučajeva kreira svoje korisničko ime i lozinku. Međutim, kreiranjem više računa može doći do zabune korisnika, gdje koristi koje korisničko ime i koju lozinku. Svi ti računi se svode na jednog korisnika, stoga je cilj ovog rada bio stvoriti uslugu koja omogućava stvaranje jednog identifikacijskog profila korisnika na temelju kojeg on pristupa raznim davateljima usluga. Sustav upravljanja identitetom je faktor u rješavanju problema širenja višestrukih identiteta istih korisnika, te pomažu omogućiti dijeljenje podataka između različitih davatelja usluga. Svi građani dužni su nositi osobne iskaznice, stoga bi se elektronička osobna iskaznica (e-iskaznica) uvela kao osnovni identifikator pri identifikaciji korisnika, čime bi se zamijenila uporaba ostalih identifikacijskih iskaznica.

U ovom radu je opisan elektronički identitet, način funkcioniranja istog, napravljen je vrijednosni lanac i demonstrirana arhitektura usluge radi lakšeg razumijevanja ekosustava same usluge. Kroz sigurnosne aspekte opisan je način zaštite podataka, te koji su sigurnosni elementi elektroničke osobne iskaznice. Za sam kraj rada, napravljen je scenarij korištenja usluge e-ID radi lakšeg razumijevanja korisnika.

Znači, usluga e-ID je usluga koja omogućava elektronički identitet za svakog državljanina u Republici Hrvatskoj. Elektronički identitet (e-ID) je način za ljude da se elektronskim putem dokaže da su to oni za koga tvrde da jesu. Njime se omogućuje korištenje elektroničkih usluga raznih davatelja, koji nude svoje usluge putem središnjeg državnog portala. Usluga e-ID nudi rješenja u smislu jednostavnijeg i bržeg dobivanja informacija o osobama, te donosi mnoge pogodnosti za vladu RH, davatelje usluga i samog korisnika. Anketnim ispitivanjem osoba dobiveni su podaci o zainteresiranosti informacijsko komunikacijske usluge e-ID, te je velika većina ispitanika potvrdila kako bi takvu vrstu usluge koristili.

Popis literature

Knjige

[1] Bažat, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I.,Matijašević, M., Mikac, B., Skočir, Z. Telekomunikacije – tehnologija i tržište. Senat Sveučilišta u Zagrebu, Zagreb, 2007.

[2] Konheim, G. A.: Computer Security and Cryptography, Wiley, 2007.

[3] Hadjina, N. Zaštita i sigurnost informacijskih sustava - Skripta za studente; Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zavod za primijenjeno računarstvo, Zagreb, 2009.

Znanstveni radovi i članci

[4] Ahmed, A., Batchelor, D., Bianchin, L., Crestelo, K., Fergusson K., Fernezian A., Gilenson, H., Hansen, M., Hudson, D., Iles, B., Magrath, M., Manes, G., Medich, C., Merkert, B., Pratt, R., Rego, J., Zalnasky, J.: Smart Card Technology in U.S. Healthcare: Frequently Asked Questions; Publication Number: HCC-12002, Smart Card Alliance 191, Clarksville Rd. Princeton Junction, NJ 08550, 2012.

[5] Murrell, S., Einspruch, G. N.: Electronic Identification, Personal Privacy and Security in the Services Sector; 978-1-4244-1672-1/08; IEEE; 2008.

[6] Camenisch, J., Lehmann, A., Neven, G.: Electronic Identities Need Private Credentials; IBM Research, Zurich, 2012.

[7] Roßnagel, H., Camenisch, J., Fritsch, L., Gross, T., Houdeau, D., Hühnlein, D., Lehmann A., Shamah, J. FutureID – Shaping the Future of Electronic Identity - Zurich Research Lab, IBM Research, Zurich, 2012.

[8] Design of NFC based Micro-payment to support MD Authentication and Privacy for Trade Safety in NFC applications – Cha, B. R., Jongwon, K. Schoool of information and communications, GIST, GwangJu, KOREA, 2013.

[9] Poller, A., Waldmann, U., Vowé, S., Türpe, S. Electronic Identity Cards for User Authentication - Promise and Practice; Fraunhofer Institute for Secure Information Technology, Darmstadt, 2012.

[10] Pavić. T., Jelenković, L.: Autentifikacija i autorizacija korisnika na jednom mjestu; Sveučilište u Zagrebu; Fakultet elektrotehnike i računarstva; Zagreb, 2007.

Seminarski, završni i diplomski radovi

[11] Pejić T. Završni rad: Informacijski sustavi temeljeni na cloud computing platformi; Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2013.

[12] Čuljak, D. Diplomski rad: Infrastruktura javnih ključeva u prividnoj mreži računalnih sustava zasnovanih na uslugama; Diplomski rad br. 1658; Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb, 2007.

[13] Gužvinec, D., Mentor: prof. dr.sc. Đurek, M. Seminarski rad iz kolegija: Ergonomija računalne i programske opreme - Elektronički potpis; Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zavod za primijenjenu matematiku, Zagreb, 2005.

[14] Antončić, V., Mentor: prof. dr. sc. Đurek, M., Seminarski rad iz kolegija: Ergonomija računalne i programske opreme - Pametne kartice; Fakultet elektrotehnike i računarstva, Zavod za primjenjenu matematiku, Zagreb, 2005.

Dokumentacija vlade

[15] Hrvatska, Ministarstvo uprave, Vlada Republike Hrvatske: Projekt e-Građani - učestala pitanja i odgovori, Zagreb, 2014.

Prezentacije

[16] PDF prezentacija: AKD d.o.o., Osobna iskaznica, Zagreb 2015.

[17] PDF prezentacija: Peraković, D. Ekosustav tržišta informacijsko komunikacijskih usluga, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2014./2015.

Web izvori na Internetu

[18] http://goo.gl/uUmkOS

[19] http://goo.gl/fOKmVr

[20] https://gov.hr/moja-uprava/drzavljanstvo-i-isprave/isprave/osobna-iskaznica/296

[21] http://www.smartcardbasics.com/smart-card-types.html

[22] https://en.wikipedia.org/wiki/Smart_card

[23] http://goo.gl/g2ttVb

[24] https://hr.wikipedia.org/wiki/Istra%C5%BEivanje

[25] http://www.cs.kau.se/IFIP-summerschool/slides/herbert.pdf

[26] https://hr.wikipedia.org/wiki/Internet

[27] http://www.zakon.hr/z/479/zakon-o-uslugama

[28] https://goo.gl/d7An35

[29] http://web.efzg.hr/dok/OIM/dhruska/SWOT_analiza.pdf

[30] https://hr.wikipedia.org/wiki/Za%C5%A1tita_podataka

[31] http://web.zpr.fer.hr/ergonomija/2004/guzvinec/ElDigDiff.html

[32] http://web.zpr.fer.hr/ergonomija/2004/guzvinec/ElSig.html]

[33] http://web.zpr.fer.hr/ergonomija/2004/guzvinec/DigSig.html

[34] https://goo.gl/SUgIha

[35] https://hr.wikipedia.org/wiki/Kra%C4%91a_identiteta

[36] https://hr.wikipedia.org/wiki/Haker

[37] https://hr.wikipedia.org/wiki/Anketa

[38] https://hr.wikipedia.org/wiki/Informacijski_sustavi

[39] http://limun.hr/main.aspx?id=13851

Popis kratica

API	Application Programming Interface
CA	Certification Authority
EEPROM	Electricaly Erasable Programmable Read-Only Memory
EGP	Europski gospodarski prostor
e-ID	Electronic identity
eOI	Elektronička osobna iskaznica
IAS	Identifikacijski i autentifikacijski sustav
ICAO	International Civil Aviation Organization
ICT	Information and Communication technology
IEC	International Electrotechnical Commission
IP	Internet Protokol
IS	Infromation system
ISO	International Organization for Standardization
IT	Information technology
MHz	Megahertz
MLI	Multiple laser image
NFC	Near Field Communication
OIB	Osobni identifikacijski broj
OKP	Osobni korisnički pretinac
OVI	Optički promjenjiva boja
PKI	Public Key Infrastructure
PVC	Polivinil klorid
RH	Republika Hrvatska

SaaS	Software as a Service
SSO	Single Sign On/Single Sign Out
SWOT	Strenghts, Weakneses, Opportunities, Threats
UHF	Ultra High Frequency
USB	Universal Serial Bus
UV	Ultraviolet
X.509	Standard for Public Key Infrastructure

Popis slika

Slika 1. Dijelovi informacijskog sustava, [18]. 3
Slika 2. Osobna identifikacijska iskaznica RH, [16]. 7
Slika 3. Figurativno prikazana pametna kartica kroz slojeve, [21]. 12
Slika 4. Kontaktni čip pametne kartice, [21]. 14
Slika 5. NFC pametna kartica i čitač, [38]. 17
Slika 6. Atributi elektroničkog identiteta u infrastrukturi, [6]..... 20
Slika 7. Istraživački proces e-ID usluge, [25]. 22
Slika 8. Vrijednosni lanac informacijsko komunikacijske usluge, [17]. 23
Slika 9. Arhitektura informacijsko komunikacijske usluge e-ID 28
Slika 10. NFC oznaka (eng. Tag), [25]. 29
Slika 11. Proces prijave na središnji državni portal..... 33
Slika 12. Simetrična kriptografija, [12]. 42
Slika 13. Asimetrična kriptografija, [12]..... 43
Slika 14. Proces digitalnog potpisa, [33]. 46
Slika 15. Provjera digitalnog potpisa, [33]. 47
Slika 16. Elementi zaštite na prednjoj strani osobne iskaznice, [16]. 53
Slika 17. Elementi zaštite na stražnjoj strani osobne iskaznice, [16]. 54
Slika 18. Prikaz kupnje ulaznice online preko središnjeg državnog portala i identifikacija korisnika na ulazu na stadion 55

Popis tablica

Tablica 1. Prikaz SWOT analize informacijsko komunikacijske usluge e-ID 37

Popis grafikona

Grafikon 1. Prikaz dobne skupine 56
Grafikon 2. Prikaz trenutnog statusa ispitanika 57
Grafikon 3. Prikaz broja ispitanika koji su upoznati za pojmom pametnih kartica 57
Grafikon 4. Prikaz broja ispitanika koji su upoznati za pojmom NFC 58
Grafikon 5. Prikaz korištenja beskontaktnih pametnih kartica 58
Grafikon 6. Prikaz na koji način su ispitanici čuli za pojam elektroničkog identiteta . 59
Grafikon 7. Prikaz broja osoba kojima se sviđa funkcionalnost korištenja drugih e-usluga putem središnjeg državnog portala 60
Grafikon 8. Prikaz broja osoba kojima se sviđa funkcionalnost ispisivanja dokumenata kod kuće koji su pravilno digitalno ovjereni 60
Grafikon 9. Prikaz prednosti za koje ispitanici smatraju da bi poboljšale njihov način života 61
Grafikon 10. Prikaz prihvatljivih nedostataka usluge 62
Grafikon 11. Prikaz vrste uređaja koje bi ispitanici koristili za pregled podataka i dokumenata 62
Grafikon 12. Prikaz prosječnog vremena čekanja ispitanika na vrijeme posluživanja u nekim institucijama 63
Grafikon 13. Prikaz elemenata koji su bitni ispitanicima za pristupanje elektroničkom identitetu 63
Grafikon 14. Prikaz koliko je ispitaniku bitna brzina dobivanja informacija i dokumenata 64
Grafikon 15. Dojam sigurnosti usluge e-ID 64
Grafikon 16. Prikaz broja ispitanika koji bi htjeli koristiti uslugu e-ID 65
Grafikon 17. Prikaz zainteresiranosti poslovnih korisnika za funkcionalnošću povezivanja obrta/tvrtke sa elektroničkim identitetom 65
Grafikon 18. Prikaz zainteresiranosti poslovnih korisnika za funkcionalnošću koja omogućuje vođenje evidencije kupaca jednostavnom identifikacijom e-osobne iskaznice korisnika 66