Digital ID - koncept digitalizacije osobne iskaznice u Republici Hrvatskoj

Bušić, Pavo

Sveučilište u Splitu
Umjetnička akademija

Diplomski rad

Digital ID — koncept digitalizacije osobne iskaznice u Republici Hrvatskoj

Split, 2020.

Sveučilište u Splitu
Umjetnička akademija

Dizajn vizualnih komunikacija
Grafički dizajn

Diplomski rad

Digital ID — koncept digitalizacije osobne iskaznice u Republici Hrvatskoj

Student
Pavo Bušić

Mentor
doc.dr.sc. Ivica Mitrović
asis. Oleg Šuran

Split, lipanj 2020.

Izjava o akademijskoj čestitosti

Ime i prezime studenta/ice:

Pavo Bušić

Izjavljujem i svojim potpisom potvrdujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

U Splitu, 28. lipanj 2020.

Student/ica (potpis)

_____

Sažetak / Temeljna dokumentacijska kartica (TDK)

Sveučilište u Splitu
Umjetnička akademija u Splitu
Odjel: Likovni odjel
Odsjek: DVK; Grafički dizajn

Diplomski rad

Digital ID — koncept digitalizacije osobne iskaznice u Republici Hrvatskoj

Digital ID aplikacija bazira se na digitalizaciji osobne iskaznice u Republici Hrvatskoj, odnosno otkriva se kako bi spomenuti osobni dokument funkcionirao u digitalnom kontekstu. Koncept mobilne osobne iskaznice u potpunosti bi zamijenio postojeće plastične verzije (ako osoba to želi), budući da su pametni telefoni u današnje doba postali standard i koriste se prilikom obavljanja svakodnevnih radnji. Uz to, ova aplikacija zapravo bi bila dodatak sustavu e-Građanin koji postoji u Republici Hrvatskoj, a dodatna prednost je što ne zahtijeva korištenje čitača pametnih kartica jer je glavni cilj prikazati sve informacije na ekranu. Aplikacija bi putem jednostavnog korisničkog sučelja omogućila korisniku obavljanje radnji na jednom mjestu te bi slala obavijesti putem kojih bi državna tijela izravno komunicirala s korisnikom. Cilj ove aplikacije je unaprijediti digitaliziranje osobnog dokumenta i olakšati korištenje ovakvog sustava koji u Republici Hrvatskoj nailazi na mnogo problema.

Ključne riječi: digitalizacija, osobni dokument, aplikacija, dizajn, UX/UI

Rad je pohranjen u knjižnici Umjetničke akademije Sveučilišta u Splitu.

Rad sadrži: 53 stranice, 28 grafičkih prikaza, 46 literaturnih navoda. Izvornik je na hrvatskome jeziku.

Mentori: doc.dr.sc. Ivica Mitrović,
asist. Oleg Šuran

Ocjenjivači: doc.dr.sc. Ivica Mitrović
doc. Mirko Pivčević
izv. prof. Dejan Kršić

Rad je prihvaćen: 27. lipnja 2020.

Sadržaj

1.0 Uvod

Glavni cilj ovog rada je potpuna digitalizacija osobnog dokumenta, odnosno pokazuje kako bi spomenuti dokument izgledao i funkcionirao na ekranu pametnog telefona budući da je isti ključan element u spajanju fizičkog i digitalnog identiteta. Pojava Interneta i njegova široka rasprostranjenost dovode nas do digitalnog doba koje se konstantno mijenja, ali i koje povrh svega uvodi pojam digitalnog identiteta. Upravo digitalni identitet u kombinaciji sa širokom uporabom mobilnih uređaja nudi rješenja za ovaj globalni izazov te pruža subjektima javnog i privatnog sektora efikasnije načine za pružanje usluga građanima.

Zbog svoje popularnosti mobitel postaje osobni višenamjenski uređaj uvijek dostupan pojedincu, a zbog ubrzanog razvoja isti postaje dovoljno siguran za pohranu identifikacijskih podataka. Samim time, mobilni uređaji mogu djelovati kao fizički dokaz (poput pametne kartice) zbog ugrađenog čipa, kao uređaj za provjeru autentičnosti ili kao sigurni nositelj identiteta, npr. za dokumente koji zahtijevaju digitalni potpis.

Ovaj diplomski rad podijeljen je u nekoliko dijelova od kojih je svaki vezan općenito uz pojam identiteta i njegov održivi razvoj. Prvi dio rada opisuje e-vladu, njezine faze razvoja i aktivnosti te modele zemalja koje svojim radom služe kao primjer drugima. Drugi dio rada objašnjava pojam vjerodajnice i navodi vrste istih dok istovremeno definira stupanj sigurnosti svake pojedinačno. Treći dio rada odnosi se na zaštitu privatnosti koja digitalizacijom dobiva na velikom značenju. Ovdje se upoznaje s pravilima i regulativama zaštite osobnih podatka što uključuje i GDPR te ulogom izdavatelja i ulogom korisnika. Četvrti dio kratko objašnjava korisničko iskustvo i korisničko sučelje te njihove međusobne odnose i razlike. Ovdje se još spominju pristupačnost i upotrebljivost kao važni elementi koji utječu na finalni proizvod, kao i utjecaj dobrog korisničkog sučelja na javne online usluge. Peti dio rada detaljno analizira postojeći sustav e-Građani te ukazuje na sve njegove prednosti, ali i mane kojih je mnogo više. Zadnji dio rada upoznaje nas s pojmom mobilnog identiteta, objašnjava aplikaciju i njezin model funkcioniranja, detaljno opisuje sve funkcije unutar aplikacije te daje uvid na korištene dizajnerske elemente, tipografiju, sustav boja i ostalo.

2.0 E-Government

Razvoj i korištenje tehnologije svakim danom sve više utječe na razvoj društva pa samim time i na razvoj državnih tijela te njihov način komunikacije s građanima. Obzirom da su aplikacije i internet postali naši svakodnevni pomagači – od poslovnih procesa gdje svakodnevno koristimo mobilne uređaje i računala do online trgovina na kojima sve češće boravimo, za pretpostaviti je da će internet i nove tehnologije biti glavni čimbenici u budućem razvoju države.

E-Vlada (*eng. E-Government*) skraćenica je nastala od riječi elektronička vlada, iako se ponekad upotrebljavaju izrazi kao digitalna vlada, online vlada ili Internet vlada. E-vlada odnosi se na korištenje informacijskih i komunikacijskih tehnologija (*eng. Information and Communication Technologies*) te ostalih telekomunikacijskih tehnologija na webu radi poboljšanja učinkovitosti pružanja usluga u javnom sektoru.[1] To u širem smislu uključuje olakšani prijenos informacija unutar državnih institucija te istovremeno između državnih institucija, građana i poduzeća. Također, e-vlada može donijeti nove koncepte koji potiču sudjelovanje građana u procesu donošenja odluka.

Pojam e-vlada u općoj je upotrebi od početka 2000-ih, ali sama pojava se javlja se od sredine 1980-ih. Razvoj e-vlade posljedica je interakcije tri razdvojena procesa društveno ekonomskog razvoja; **1.** tehnološka revolucija (širenje računalne opreme, pojava interneta i e-usluga), **2.** promjena u menadžmentu pod sve većim utjecajem informacijskih i komunikacijskih tehnologija (privatni i neprofitni sektori postaju partneri vlasti kao alternativa pružanju javnih usluga) i **3.** odnosi se na utjecaj tehnologije koja donosi uštedu, veću efikasnost te približavanje vlade građanima.[2]

2.1 Četiri Faze razvoja e-vlade

Proces razvoja e-vlade možemo podijeliti u četiri faze. Većina vlada prvo započinje pružanje informacija namijenjenim ciljnim skupinama dok pritisak javnosti i želja za povećanjem efikasnosti ne zahtijevaju distribuciju kompleksnijih usluga. Izbor usluga koje vlada odluči ponuditi elektroničkim putem zavisi od dva faktora: prvi je potražnja javnosti za određenim uslugama, a drugi je smanjenje internih troškova. Razvoj i razina ponuđenih usluga definira se najčešće prema parametrima određenim Bangemannovim izvještajem načina bodovanja:[3]

0 – Nema informacije (informacije i usluge nisu dostupne na internetu, e-uprava ne postoji);

1 – Informacija (na mreži je dostupna samo informacija o usluzi, npr. opis postupka, pravilnici i sl.);

2 – Jednosmjerna interakcija (dostupnost formulara u elektroničkom obliku za pohranjivanje na računalu, prazne formulare moguće je i otisnuti na pisaču);

3 – Dvosmjerna komunikacija (interaktivno ispunjavanje formulara i prijava uz autentikaciju; ispunjavanjem formulara pokreće se pojedina usluga);

4 – Transakcija (cijela usluga je dostupna na mreži, popunjavanje formulara, autentikacija, isporuka potvrda ili drugi oblici potpune usluge putem mreže).

Republika Hrvatska je Središnjim državnim portalom i projektom e-Građani dosegla najviši stupanj faze razvoja jer putem spomenutih usluga nudi brz pristup informacijama i kompletno obavljanje usluga unutar sustava.

2.2 Modeli i aktivnosti e-vlade

U konceptu E-Uprave mogu se izdvojiti tri najvažnije ciljne grupe: vlada, građani i poslovni sektor.[4]

G2C – Government to Citizen
Odnosi se na komunikaciju vlasti i građana. G2C omogućuje građanima pristup uslugama i informacijama odmah, praktično s bilo kojeg mjesta, koristeći više kanala. Ova inicijativa građanima omogućava podnošenje zahtjeva, plaćanje poreza, obnove dozvola itd.

G2B – Government to Business
Sastoji se od e-interakcije između vlade i privatnog sektora. Mogućnost provođenja mrežnih transakcija s vladom smanjuje birokraciju i pojednostavljuje regulatorne procese te tako pomaže tvrtkama da postanu konkurentnije.

G2G – Government to Government
G2G predstavlja ključni faktor e-vlade, uključuje dijeljenje podataka elektronskim putem između zaposlenih u vladi na nacionalnom, regionalnom i lokalnom nivou. G2G olakšava razmjenu baza podataka i resursa, povećavajući učinkovitost i djelotvornost procesa.

2.3 E-government u Hrvatskoj i svijetu

2.3.1 Hrvatska

Središnji državni portal u Republici Hrvatskoj osmišljen je s ciljem lakšeg pristupa informacijama pa tako je na jednom mjestu jednostavno i moderno prezentirana struktura, funkcija i uloga državne uprave. Samim time građani na jednom internetskom mjestu mogu pristupiti svim informacijama iz javne uprave ili pratiti političke aktivnosti, a trenutno je dostupno preko 485 informacija (brojka kontinuirano raste). U Središnji državni portal uveden je i korisnički pretinac za izravnu komunikaciju pod nazivom **e-Građani** — sustav koji omogućava pristup elektroničkim uslugama javne uprave jedinstvenim elektroničkim identitetom te građani mogu uz nekoliko klikova npr. dobiti uvid u ocjene svog djeteta, promijeniti liječnika, dobiti obavijest MUP-a da im ističe osobna iskaznica itd.[5]

Sustav e-Građani osim Središnjeg državnog portala koji predstavlja javni dio sustava, čine i **Osobni korisnički pretinac**

i **Nacionalni identifikacijski i autentifikacijski sustav**. Te komponente omogućavaju sigurnu i naprednu elektroničku komunikaciju s javnim sektorom.

Putem osobnog korisničkog pretinca građani (koji imaju važeći OIB) mogu upravljati i pregledavati poruke koje su poslane od javne uprave. Putem sustava građani su informirani o važnim situacijama i događajima vezanim za osobna zakonska prava i obveze te o korištenju osobnih podataka u javnom sektoru (npr. obavijest o isteku putovnice ili vozačke dozvole, dopunskog osiguranja itd.) te je također dostupan i kao aplikacija na mobilnim uređajima.

Primarni zadatak Nacionalno identifikacijskog i autentifikacijskog sustava (NAIS) je sigurna i pouzdana identifikacija korisnika koji putem određenih vjerodajnica (certifikata) pristupaju javnim elektroničnim uslugama. Prema zakonu, vjerodajnica predstavlja sredstvo dokazivanja/prepoznavanja elektroničkog identiteta, odnosno vjerodajnica je nešto što korisnik zna ili posjeduje, npr. korisničko ime/lozinka, digitalni certifikat token na mobilnom telefonu i slično.[6]

Kako bi korisnik pristupio sustavu e-Građanin, mora posjedovati osobni korisnički pretinac elektroničke vjerodajnice, čiji se popis nalazi na web stranici Središnjeg državnog portala. Svaka vjerodajnica na popisu sadržava četiri određene razine sigurnosti koje su usklađene s preporukama i iskustvima stečenim kroz projekte u EU zemljama.

2.3.2 Estonija

Estonska je vlada u kolovozu 2000. postala prva vlada na svijetu koja je u potpunosti kompjutorizirala svoj rad, a danas se uzima kao model za druge zemlje. Za razliku od mnogih drugih zemalja svaki stanovnik Estonije, bez obzira na svoj položaj, ima državni digitalni identitet. Zahvaljujući tome, Estonija je godinama ispred zemalja koje još uvijek pokušavaju riješiti kako autentificirati ljude bez fizičkog kontakta.[7]

U Zadnjih dvadesetak godina Estonija konstantno razvija svoj pristup e-vladi i integrira je u svakodnevni život svim svojim građanima. Jedan od ključnih elemenata e-Estonije je da su njegove baze podataka decentralizirane što znači da; nema nijednog vlasnika, svaka državna agencija ili poslovni subjekti mogu odabrati proizvod koji im najbolje odgovara i usluge se mogu dodavati pojedinačno (ovisno o tome kad su spremne). Sva estonska e-rješenja koriste bazu podataka **X-Road** koja omogućava maksimalan učinak jer su svi odlazni podaci digitalno potpisani i šifrirani, dok su svi dolazni podaci provjereni i prijavljeni. Od 2015. godine e-Estonija pruža više od 815 usluga koje građani mogu koristiti putem državnog portala. Da bi pristupili svim tim javnim e-uslugama, estonski građani imaju osobnu iskaznicu koja pruža autentičnost i autorizaciju za sve e-usluge.[4]

2.3.3 Danska

Prema Ujedinjenim narodima (UN) Danska je u 2018. godini zemlja s najvećim razvojem u sustavu e-vlada; na prvom je

mjestu po svojoj ponudi online usluga te je zauzela prvo mjesto za sudjelovanje građana u donošenju vladinih odluka i stvaranju politika. Ključna inovacija zaslužna za ovaj uspjeh je *digital first* pristup po kojem je elektronička interakcija sada legalno obvezna. Za interakciju s vladom, bankama i privatnim sektorima građani koriste **NemID** – digitalne identifikacijske brojeve. Pomoću njih mogu obavljati bankovne transakcije, dohvatiti porezne prijave s vladinog portala, pa čak i zakazati sastanke sa svojim frizerom. Danska također koristi personalizirane digitalne usluge pružajući ciljani sadržaj građanima na svojim NemID portalima (npr. kada se prijavljuju na njihove portale građanima na rubu umirovljenja bit će predstavljene opcije planiranja mirovine). Također, pojavio se i telemedicinski model rješenja za osobe s kroničnim poremećajima pa tako pacijenti više ne trebaju ostati u bolnicama, već se mogu oporaviti u svojim domovima dok ih nadgledaju zdravstveni profesionalci putem video konferencija. Još jedan veliki plus je i sustav kojim vlada pomaže građanima koji ne mogu pristupiti digitalnim uslugama, tako da ni oni nisu isključeni prijelazom na digitalne platforme.[8]

3.0 Vjerodajnice

Pojam vjerodajnica predstavlja sredstvo dokazivanja elektroničkog identiteta zaštićenog tehnološkim protokolima. Vjerodajnica je nešto što korisnik zna ili posjeduje npr. korisničko ime i lozinka, digitalni certifikat, token i slično. Također, vjerodajnice se odnose na alate za provjeru autentičnosti te mogu biti dio certifikata koji pomaže u potvrđivanju korisničkog identiteta na drugim ID sustavima.[9]

Autentikacija ili provjera autentičnosti odnosi se na pojam procesa koji osigurava i potvrđuje identitet korisnika. Početak provjere autentičnosti započinje kada korisnik pokuša pristupiti informacijama, npr. prilikom prijave korisnik obično unose podatke kao što su korisničko ime i lozinka kako bi dokazao svoje pravo pristupa. Ova kombinacija prijave mora biti dodjeljena svakom korisniku, no ovaj sistem provjere autentičnosti predstavlja sigurnosno slabu točku za moguće hakerske napade. Postoje i drugi oblici provjere autentičnosti kao što su tokeni i biometrija koja hakerima skoro pa onemogućuje provalu u računalne sustave.[10]

Vjerodajnice i alati za vjerodajnice konstantno se razvijaju i veliki dio sigurnosne industrije uključuje cyberwar tvrtke za nadzor sustava od hakerskih napada. Stručnjaci za sigurnost koriste vjerodajnice i mnoge druge vrste metoda i alata za izgradnju sveobuhvatnije mrežne sigurnosti preko vlasničkih mreža i interneta. Sve navedeno dio je industrije kibernetičke sigurnosti koja dobiva sve više prostora u današnjem svijetu visoke tehnologije.[11]

3.1 Stupanj sigurnosti

Sigurnosne razine predstavljaju stupanj sigurnosti po kojem je korisnik povezan sa svojim elektroničkim identitetom, samim time sigurnosne razine su rezultat zadovoljavanja niza zahtjeva koji osiguravaju dvije komponente: [12]

- prihvatljiv stupanj povjerenja u postupku dokazivanja identiteta, koji je dio faze registracije
- prihvatljiv stupanj povjerenja u postupku dostave elektroničkih vjerodajnica, koji je dio faze elektroničke autentikacije.

Sigurnosna razina koncipirana je načelima EU projekta STORK *(eng. Secure idenTity acrOss boRders linKed)* te se sastoji od sljedećih razina:[13]

- **Sigurnosna razina 1** jamči najnižu razinu sigurnosti ili ne jamči nikakvu sigurnost. Vjerodajnice se prihvaćaju bez bilo kakve provjere jer su posljedice od lažnog predstavljanja vrlo male ili nikakve. Najčešći mehanizam dokazivanja identiteta na ovoj razini je korištenje korisničkog imena i lozinke.

· **Sigurnosna razina 2** predstavlja srednju razinu zaštite, koristi se kada su posljedice od lažnog predstavljanja male i ne zahtijeva fizičku prisutnost prilikom podnošenja zahtjeva za izdavanje vjerodajnice. Prilikom korištenja vjerodajnice uz korisničko ime i lozinku, u postupku autentikacije mora se koristiti barem jedan dokaz posjedovanja određenog objekta od strane korisnika koji pristupa usluzi, kao što je npr. token koji generira jednokratne lozinke.

· **Sigurnosna razina 3** namijenjena je uslugama koje traže visoku razinu zaštite te kod kojih su štetne posljedice od lažnog predstavljanja znatne. Provjera i potvrđivanje identiteta obavlja se metodama koje nedvosmisleno identificiraju podnositelja zahtjeva za izdavanje vjerodajnice. Registracija identiteta zasnovana je na infrastrukturi javnog ključa (PKI) koji s visokom sigurnošću identificira tražitelja vjerodajnice.

· **Sigurnosna razina 4** predstavlja najvišu razinu osiguranja kod kojih štetne posljedice od lažnog predstavljanja imaju težak utjecaj. Postupak registracije zahtjeva barem jednu provjeru i potvrđivanje identiteta uz fizičku prisutnost podnositelja zahtjeva. U slučaju on-line zahtjeva, identitet podnositelja zahtjeva se može ustanoviti korištenjem kvalificiranog e-potpisa. Pored infrastrukture javnog ključa, na ovoj razini koriste se i biometrijske metode autentikacije.

3.2 Token

U današnje vrijeme postoji mnogo vrsta tokena čiji je zadatak kroz jednostavan postupak prikazati unikatni broj koji se zatim koristi za logiranje na određeni servis. Međutim kako znamo da je dobiveni broj dobar? Ukratko, brojevi se generiraju prema određenom kriptoalgoritmu koji uzima spomenuti broj, spaja ga najčešće s trenutačnim vremenom te provuče taj isti broj kroz kriptoalgoritam (svaki korisnik ima jedinstveni broj koji je povezan s njegovim računom a token na osnovu tih brojeva generira brojeve koji se poslije prikažu na ekranu).

Najmoderniji sistem uporabe tokena je putem pametnih telefona ili tableta. Potrebno je jedino instalirati aplikaciju na svoj pametni telefon ili tablet te aplikacija automatski izgenerira broj koji je potrebno upisati na željeni web servis. Iako funkcionira isto kao i fizički token, prednost aplikacije u odnosu na token je dodatna zaštita koja uklanja mogućnost „čovjek u sredini“ *(eng. man in the middle)*. Ovaj pojam predstavlja vrstu hakerskog napada koji funkcionira tako da haker presretne poruku koju šaljemo serveru i blokira je te se umjesto vas spaja na server ili samo pokupi podatke koje kasnije koristi za spajanje na isti.

Prednost tokena definitivno je dodatni sloj zaštite koji pruža korisniku jer čak i ako druga osoba zna lozinku, ne može se direktno spojiti na korisnički račun. S druge strane, ako se korisnik želi logirati uvijek mora imati token uz sebe, mora paziti da se ne izgubi i slično. Sve u svemu, pozitivne strane korištenja

tokena puno su veće od negativnih, osobito ako je isti ugrađen u aplikaciju.[14]

3.3 Digitalni certifikat

Pojam digitalni certifikat odnosi se na elektroničku potvrdu identiteta korisnika koja omogućava sigurnu i povjerljivu komunikaciju internetom. Certifikat označava potvrdu u elektroničkom obliku koja povezuje podatke za ovjeru elektroničkog potpisa (javni ključ) s nekom osobom i potvrđuje identitet te osobe pa se samim time smatra i digitalnom osobnom iskaznicom. Digitalne certifikate izdaje CA *(eng. Certificate Authority)*, a sistem funkcionira tako da korisnik šalje svoj javni ključ i dokaz identiteta CA i ako su zadovoljeni svi uvjeti identifikacije, CA izdaje digitalni certifikat koji sadrži javni ključ korisnika.[15]

Pojava PKI tehnologije (kriptografije javnog ključa) koja se temelji na pametnim karticama s digitalnim certifikatima te korištenje elektroničkog potpisa značajno je unaprjeđena poslovna komunikacija i potpuno je eliminirano korištenje papira, što dovodi do znatne uštede vremena u mnogo poslovnih segmenata. **Elektronički potpis**, kao bitan segment certifikacije, zamjenjuje tradicionalni potpis ako se koristi po zakonsko propisanim uvjetima, ali s istim se može potpisati isključivo elektronički dokument, odnosno tradicionalni/papirnati dokumenti ne mogu se kombinirati s e-potpisom. Korištenjem elektroničkog potpisa osigurava se autentičnost (potvrda da je pošiljatelj stvarno onaj koji tvrdi da on jest) i integritet (jamstvo za cjelovitost i nepromijenjenost poruke).[16]

3.4 Ime/lozinka

Vjerodajnica tipa - ime/lozinka dokazano je najranjiviji tip vjerodajnice, no ako je mi kao vlasnici znamo čuvati, dugo će nam poslužiti. Ovaj tip vjerodajnice spada pod tip čiji su podaci tajni, odnosno sadržaj stvara isključivo korisnik. Prednosti ovakvog tipa su cijena, laka zamjenjivost (u slučaju gubitka) i jednostavnost postavljanja, što je veliki plus za slabije obrazovane korisnike. Kod ovakvog tipa vjerodajnice prijave u sustav se često koriste u kombinaciji s nečim što imamo, kao npr. kreditna kartica. Kao što je već ranije spomenuto, ime/lozinka je najranjiviji tip te samim time ne nudi visoku razinu zaštite. Veliki dio krivice ipak pripada korisnicima jer odabiru jednostavne lozinke kao što su datumi rođenja, imena, a to je relativno lako pogoditi. Rješenje za ovakve slučajeve su kompliciranije lozinke koje ne sadrže tzv. osnovne podatke, tehničke stvari kao npr. sustav koji provjerava da takva lozinka nije prije bila korištena kod drugog korisnika. U slučaju zaboravljanja lozinke, što je čest slučaj, službe u velikom broju slučajeva koriste unaprijed dogovoreno tajno pitanje (ime kućnog ljubimca, ime najdražeg filma itd.) kako bi korisnik potvrdio svoj identitet. Još jedan rizik kod lozinki je njihova loša zbrinutost tj., korisnici svoje lozinke pohranjuju na nesiguran način zapisujući ih ili spremajući na lako vidljiva mjesta.[17]

3.5 Biometrija

Pojam biometrije koja od svih trenutno nudi najviši stupanj sigurnosti jer se ne može dijeliti s drugom osobom. U užem smislu predstavlja tehniku kojom se identificira korisnik pomoću njegove jedinstvene ljudske osobine, kao što su skeniranje mrežnice ili šarenice oka, prepoznavanje lica, prepoznavanje glasa, otisak prsta – koji je ujedno i najpopularniji oblik, itd. Velika prednost biometrije u odnosu u ostale je nemogućnost zaboravljanja ili gubitka s obzirom na to da se nalaze uz korisnika cijelo vrijeme pa je samim time i lako prenosiv. Međutim najveći nedostatak iste je kompliciranost njegova izvođenja jer zahtijeva specijalizirane uređaje koji još uvijek nisu široko rasprostranjeni i svima dostupni osim na primjeru mobilnih uređaja koji sadrže senzor za otisak prsta. Također, ovakva provjera autentičnosti postavlja pitanja kulturne prihvatljivosti i zadiranja u privatnost korisnika jer se neke od tehnika, npr. otisak prsta, koriste i u kriminalističkim aktivnostima.[12]

Svaka biometrijska metoda ima svoje prednosti i mane te treba imati na umu da ovo nije jedino sredstvo kojim se može utvrditi identitet korisnika i da ne postoji savršena metoda koja sa stopostotnom sigurnošću čuva korisnikove podatke. Posebno je važno spomenuti i pozadinu iza koje stoji tehnička infrastruktura kojom se vrši analiza, pohrana podataka u bazu, uspoređivanje, daljnja distribucija i da pristup takvim sustavima zahtijeva postavljanje posebnih sigurnosnih protokola. Pitanja vezana uz čuvanje podataka i distribuciju istih su pitanja na koja odgovor trebaju dati čelnici država unije s obzirom na postojeći zakonsku regulativu koja predstavlja dobar temelj za uređivanje ovakvih pitanja.[18]

4.0 Zaštita privatnosti

Zaštita privatnosti bitan je element u današnjem informacijskom društvu koji koristi podatke kao temelj za svoj razvitak te je gotovo nemoguće dobiti određenu uslugu bez davanja osobnih podataka. Sve šira dostupnost podataka dovodi do sve češćih prevara na internetu, a korisnici svojim (ne)znanjem dozvoljavaju prikupljanje podataka, bez razmišljanja o posljedicama koje to donosi. Možemo reći da se mnogo puta osobni podaci na Internetu prikupljaju uz pristanak korisnika, no često se prikupljaju i bez njegova znanja što nam dokazuju sve češći medijski primjeri u kojima korisnici tuže tvrtke za prodaju ili davanje osobnih podataka trećim stranama.

4.1 Pravila i regulativa zaštite osobnih podataka

Pravila o zaštiti osobnih podataka primjenjuju se svaki put kada se isti prikupljaju. Obrada podataka dopuštena je u svim situacijama koje su propisane pravilima EU-a o zaštiti podataka, dok u svim ostalim situacijama druga strana mora tražiti korisnikov pristanak odnosno **privolu** kako bi mogli upotrebljavati korisnikove osobne podatke. Korisnik svoju privolu mora dati jasno afirmativnom radnjom odnosno, mora potvrditi da se njegovi podaci koriste u znanu svrhu. S druge strane, određeno poduzeće/organizacija dužna je razumljivo i jasno objaviti informacije koje uključuju podatke za kontakt, razlog i vremenski period upotrebe korisnikovih osobnih podataka, podatke o bilo kojem drugom poduzeću/organizaciji koja će primati korisnikove osobne podatke te mora sadržavati opće informacije o korisničkim pravima na zaštitu podataka kao što su ispravak, brisanje, pristup, pritužba i povlačenje privole.

Korisnik ima zakonsko **pravo pristupa** koji mu omogućava pristup osobnim podacima i načinu njihove obrade.
Ovim pravom korisnik dobiva kopiju vlastitih podataka u pristupačnom formatu bez naknade, kroz vremenski period do mjesec dana od predaje zahtjeva. Isti sadrži pregled kategorija podataka koje se obrađuju kao i informacije o tome kako se isti podaci upotrebljavaju.

Pravo na prenosivost podataka odnosi se na izravno vraćanje ili prenošenje podataka drugom poduzeću na zahtjev korisnika bez da ih u tome sputava voditelj obrade. Ovo pravo može se iskoristiti u slučaju prelaska s jedne na drugu sličnu uslugu (npr. prelazak s Microsoftovog na Google račun) kroz brz postupak i značajnu uštedu vremena.

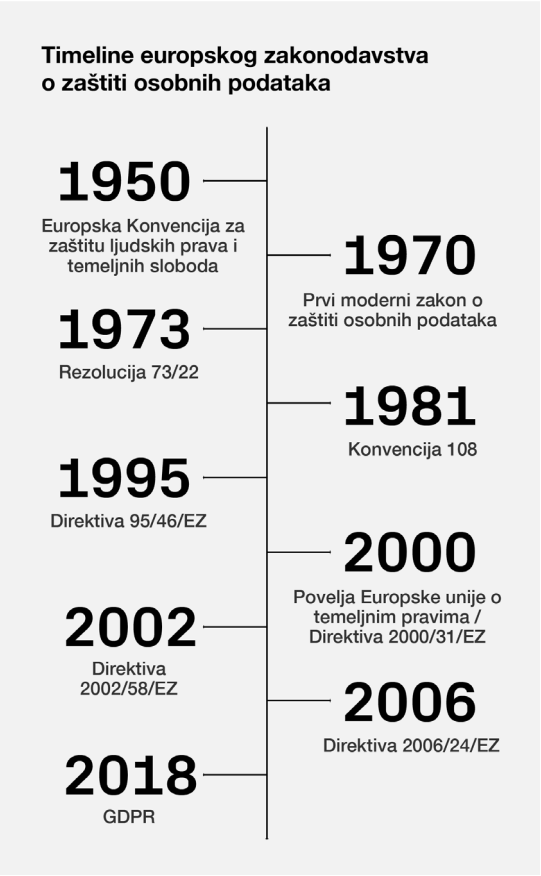
Korisnik također ima pravo i na brisanje osobnih podataka, odnosno **pravo na zaborav** putem kojeg osobni podaci mogu biti trajno izbrisani ako ih korisnik smatra nepotrebnima ili ako se nezakonito upotrebljavaju. Ova pravila primjenjuju se i na tražilice jer se one smatraju glavnim izvorom obrade podataka pa se tako na zahtjev korisnika mogu ukloniti svi podaci iz rezultata

pretrage koje uključuju korisnikovo ime. Također, poduzeće mora obavijestiti sve druge internetske stranice s kojima su podaci podijeljeni kako bi zatražili brisanje poveznica. Međutim, neki podaci možda neće biti automatski izbrisani radi zaštite drugih prava kao što je sloboda izražavanja, pa tako primjerice kontroverzne izjave ljudi u središtu pozornosti možda neće biti izbrisane ako je u interesu javnosti da ostanu na internetu.

U slučaju povrede podataka koja uključuje gubitak, krađu ili nezakonitost upotrebe podataka, voditelj obrade podataka mora to prijaviti nacionalnom nadležnom tijelu za zaštitu podataka, zatim ako postoje rizici, dužan je izravno obavijestiti korisnika o negativnim utjecajima koje donosi takva povreda. Uz sve navedeno, ako korisnik smatra da prava na zaštitu podataka nisu poštovana, može izravno podnijeti pritužbu nacionalnom nadležnom tijelu za zaštitu podataka koje će istražiti pritužbu i odgovoriti u roku od tri mjeseca. Također, korisnik može započeti sudski postupak protiv predmetnog poduzeća/organizacije ako smatra da mu je nanesena materijalna ili nematerijalna šteta i u slučaju dobitka ima pravo na naknadu.[19]

4.2. GDPR

Osobne podatke dajemo tijekom cijelog života (privatnog i poslovnog) jer je gotovo nemoguće izvršiti bilo kakvu obvezu ili ostvariti ikakvo pravo bez upotrebe osobnih podataka. Svaki pojedinac ima pravo na privatnost i zaštitu istog ukoliko to nema lošeg utjecaja na javnost. Pojava novih tehnologija, novih načina komuniciranja i razvoj informatičkog društva utječu i nadopunjuju pravila zakonske regulacije za zaštitu osobnih podataka. U ovom dijelu rada detaljan razvoj zaštite osobnih podataka bit će prikazan kroz *timeline* na *Prikazu 1*, dok će se poseban naglasak staviti na **Opću uredbu o zaštiti osobnih podataka** koja je donijela brojne promjene, kako za korisnike, tako i za pružatelje usluga.



Prikaz 1 Timeline europskog zakonodavstva o zaštiti osobnih podataka

Novi načini obrade osobnih podataka i ubrzani tehnološki razvoj doveli su do potrebe za mijenjanjem zakona o zaštiti osobnih podataka te je zastarjela *Direktiva 95/46/EZ* zamijenjena novom nadopunjenom verzijom pod nazivom Opća uredba o zaštiti osobnih podataka (*eng. General Data Protection Regulation*). Ova uredba predstavlja bitan napredak u području zaštite osobnih podataka jer se njenim donošenjem kontroliraju novi načini poslovanja na internetu i osigurava ujednačeno postupanje nadzornih tijela za zaštitu osobnih podataka, što dovodi do jednostavnije i ravnomjernije zaštite prava svih korisnika. Osim navedenog, uvode se nove i pojednostavljuju postojeće definicije, jačaju prava korisnika, određuju se biometrijski i genetski podaci te se uvodi mogućnost izricanja kazni od strane tijela za zaštitu osobnih podataka. Najveća novost ipak je uvođenje obveze procjene učinka prema kojoj se procjenjuje zaštita osobnih podataka i razina rizika (osobitu putem novih tehnologija) pa tako isti po prvi put imaju e videntan učinka provođenja u području zakonodavstva.[20]

Opća uredba o zaštiti osobnih podataka počela se razvijati 2012. godine, a prvobitni cilj bio je unaprijediti digitalno gospodarstvo i ojačati pravo na zaštitu osobnih podataka te kao što je već ranije u tekstu navedeno, nadopuniti zastarjelu Direktivu 95/46/EZ, jer kako navodi (Boban, 2018) *"velike i brze tehničko-tehnološke promjene u posljednjih 150 godina nisu rješavale stare probleme; već se postojeći problemi uvijek odgađaju ili zamjenjuju novima – stari postaju irelevantni, a novi sudbonosni."*[20] Donešena je 27. travnja 2016. godine u Bruxellesu od strane Europskog parlamenta i Vijeća Europske unije, a stupila je na snagu dvadesetog dana od objave u Službenom listu Europske unije te se zakonski počinje primjenjivati 25. svibnja 2018. i obvezna je svim članicama Europske unije.

Prema Općoj uredbi o zaštiti osobnih podataka donesena je nova definicija po kojoj se osobni podaci definiraju kao "svi podaci koji se donose na pojedinca čiji je identitet utvrđen ili se može utvrditi; pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca" te se putem ove definicije po prvi puta biometrijski podaci zakonski definiraju kao osobni. Po prvi puta spominje se i pojam **pseudonimizacija** koja onemogućuje pripisivanje osobnih podataka korisniku bez uporabe dodatnih informacija, pod uvjetom da se iste dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama putem kojih isti osobni podaci ne mogu biti pripisani korisniku čiji je identitet utvrđen ili se može utvrditi.[21]

Opća uredba o zaštiti osobnih podataka uvodi i obavezno postavljanje nadzornih tijela u svim državama članicama kako bi osigurali primjenu odredbi o zaštiti osobnih podataka. U Republici Hrvatskoj ova uloga pripada **Agenciji za zaštitu osobnih podataka** (AZOP) koja, osim provođenja uredbe, promiče

svijest o rizicima i mjerama zaštite podataka te rješava pritužbe o kršenju istih. Također, AZOP je razvila dvije edukativne mobilne aplikacije koje se mogu besplatno preuzeti na mobilne telefone. Prva aplikacija AZOP namijenjena je djeci i sadrži korisne savjete o zaštiti i načinu ponašanja na internetu, kratki internetski pojmovnik, ali i savjete za odrasle (roditelje, učitelje itd.) te cjeline koje upozoravaju na važnost privatnosti djece i mladih u svijetu modernih tehnologija. Druga aplikacija GDPR na dlanu služi kao informativni alat, namijenjena je široj javnosti te pruža detaljan prikaz teksta Opće uredbe o zaštiti podataka s poveznicama na relevantne tekstove.[22]

4.3 Uloga izdavatelja i uloga korisnika

4.3.1 Uloga izdavatelja

Glavni element koji štiti i informira korisnika o radu određene mrežne stranice neke tvrtke/organizacije je **Izjava o privatnosti** ili kako se još često naziva – **Politika privatnosti**. Ovaj dokument jednostavnim jezikom detaljno opisuje načine rukovanja korisničkih podataka te objašnjava pravila upotrebe, prikupljanja, dijeljenja i zaštite osobnih podataka. Izjava o privatnosti treba sadržavati tipove i razloge zbog kojih se navedeni podaci prikupljaju, kako i tko će sve koristiti prikupljene podatke, vremenski period zadržavanja podataka kao i informaciju o kontaktu osobe koja je zadužena za pojašnjavanje ovakvog tipa dokumenta. Izjava o privatnosti bitan je dokument za svakog korisnika jer mu pruža uvid u njegova zakonska prava te je sukladno time prije ostavljanja osobnih podataka vrlo bitno pročitati isti tip dokumenta.[23]

4.3.2 Uloga korisnika

Zaštita privatnosti postaje sve teži zadatak jer automatizirani načini obrade podataka omogućavaju sve veću količinu prikupljanja istih. S druge strane, korisnici su glavni krivci jer oni sami odlučuju koliko i koje informacije ostavljaju iza sebe što dovodi (poznajući današnje društvo), do zaključka da potpune privatnosti na internetu gotovo da i nema. Privatnost ovisi o pažljivosti korisnika pa se tako, ovisno o stupnju iste, mogu djelomično ublažiti posljedice te sačuvati barem dio osobnih podataka ako je korisnik svjestan da ona proizlazi iz samoedukacije i korištenja tehničkih sustava zaštite.

Kako bi u što većoj mjeri zaštitili privatnost na internetu, korisnici se trebaju držati osnovnih pravila ponašanja koji se mogu podijeliti u dvije kategorije: one koje govore o pravima, odnosno zašto treba štititi te podatke i one koje govore kako to najbolje učiniti.

Načini zaštite osobnih podatka u kratkim crtama prema AZOP-u su:[23]

- nikada ne koristiti poznate riječi i osobne podatke (poput imena i prezimena) u zaporkama jer predstavljaju niski stupanj sigurnosti
- prilikom kreiranja zaporki uvijek upotrebljavati barem jedan verzal, jednu brojku te barem jedan kontrolni znak.

· nikada ne upotrebljavati zaporke kraće od šest znakova (iako je osam znakova standardna duljina lozinke)

· ne koristiti se istim zaporkama na različitim internetskim stranicama i servisima

· prilikom online plaćanja treba koristiti usluge provjerenih partnera a osobne podatke putem maila treba slati isključivo provjerenim adresama

· pri postupku registracije na neku mrežnu stranicu potrebno je ispuniti samo polja koja su nužna; ako se postupak registracije ne može nastaviti bez podataka koje korisnik smatramo nužnima, potrebno je procijeniti opravdanost takve radnje kao i sigurnost i vjerodostojnost te stranice

· važno je pročitati opće uvjete te ako isti nije razumljiv potrebno je obratiti se stručnim osobama

· nužno je koristiti antivirusne programe kao i najnovije verzije web preglednika

· kolačići se mogu obrisati putem internetskog preglednika pa ih je potrebno redovito brisati

· povremeno pitati veće tvrtke koje podatke o nama posjeduju te napraviti modifikaciju podataka ukoliko su netočni ili tražiti njihovo brisanje ako za to postoji opravdani razlog.

5.0 Korisničko sučelje i javne online usluge

5.1 UX (User Experience)

Korisničko iskustvo (*eng. user experience*) kao relativno mlad pojam, dobiva na važnosti razvojem tehnologije i porastom potrebe čovjeka za osobnijim i kvalitetnijim načinom korištenja određenih usluga ili proizvoda. Sukladno time, UX u centar pažnje postavlja upravo korisnika i njegove želje, odnosno uključuje stavove, ponašanja i emocije koje korisnik doživljava prilikom korištenja određene usluge ili proizvoda. Osim navedenog, korisničko iskustvo u odnosu interakcije čovjeka i računala (*eng. human computer interaction; HCI*) proučava praktične aspekte te uključuje i percepciju aspekata sustava kao što su korisnost, učinkovitost i jednostavnost uporabe.[24]

Danas je korisničko iskustvo interdisciplinarno i dinamično područje rada obzirom da se stalno mijenjaju načini pojedinih rješenja i usluga. Ubrzani razvoj tehnologije dovodi do transformacije interneta, odnosno mobilne aplikacije i web stranice imaju sve više sadržaja što dovodi do potrebe za dobrim korisničkim doživljajem te razvijanje istog u svrhu bolje efikasnosti. Također, korisnici pristupaju uslugama i informacijama putem različitih uređaja (pametnih telefona, tableta, osobnih računala) pa se samim time te iste usluge moraju istaknuti kako bi omogućile pozitivno korisničko iskustvo korisniku koji ih upotrebljava.[25]

5.2 UI (User interface)

Dizajn **korisničkog sučelja** (*eng. User Interface*) odnosi se na pojam izrade sučelja u računalnim uređajima ili softverima s naglaskom na izgled i stil, odnosno posao dizajnera je stvoriti dizajn kojeg će korisnici smatrati ugodnim i jednostavnim za korištenje.[26]

Iako se UI dizajn odnosi na različite vrste sučelja, danas se taj pojam u najvećoj mjeri odnosi na dizajn weba i aplikacija, odnosno na IT tehnologiju. Dizajn korisničkog sučelja odnosi se na vizualni izgled elemenata s kojima korisnik može stupiti u interakciju i učiniti iskustvo estetski ugodnim. Bitno je da korisnici bez poteškoća i prethodnog iskustva mogu jednostavno naučiti koristiti proizvod/uslugu a dobar dizajn korisničkog sučelja potiče prirodnu interakciju te pomaže korisniku u savladavanju sustava, dok loše dizajnirano korisničko sučelje otežava korištenje istog.

5.3. Razlike i odnosi između UX/UI

Nije neuobičajeno da se pojmovi UX i UI miješaju ili povezuju čak i u dizajnerskim krugovima, međutim, ovi pojmovi su po svojim karakteristikama različiti te su oba ključne komponente

za dobar dizajn. Npr., dobar dizajn korisničkog sučelja u kombinaciji s lošim korisničkim iskustvom još uvijek čini dizajn lošim. Najjednostavnije rečeno – korisničko sučelje odnosi se na to kako stvari **izgledaju** dok korisničko iskustvo označava kako stvari **funkcioniraju**. Tek kada se UI i UX neprimjetno stapaju i nadopunjuju, tek tada mogu proizvod ili uslugu učiniti kvalitetnom. Glavna zadaća UX dizajnera je ciljanoj publici osigurati učinkovito i ugodno korisničko iskustvo pa su tako prilagodljivost, funkcionalnost i upotrebljivost vrlo važni kriteriji pri postizanju krajnjeg cilja.

Procesi i teorije koje koriste UX dizajneri mogu se primijeniti na gotovo sve, iako su uglavnom usmjereni na razvoj digitalnih proizvoda pa tako ti procesi uključuju **strategiju** i **kontekst** (analiza korisnika i konkurenata, strategija, struktura proizvoda, razvoj sadržaja), **wireframing i prototyping** (izrada skica odnosno wireframe, izrada prototipa, planiranje razvoja, testiranje) te **analitiku i završnu obradu** (koordinacija s razvojnim programerima i UI dizajnerima, praćenje ciljeva, integracija, analiza). Uloga dizajnera korisničkog iskustva je višestruka, složena i izazovna jer uključuje i marketinški i dizajnerski dio kod kojih je ponavljanje vrlo bitna stavka koja dovodi do provjereno dobrih rezultata. Krajnji rezultat dobrog korisničkog iskustva povezuje potrebe korisnika i poslovne ciljeve pružatelja usluga kroz proces testiranja i usavršavanja do postizanja zadovoljstva s obje strane. Posao UI dizajnera zahtijeva intuitivnost te uključuje mnoštvo izazova čiji je cilj učiniti proizvod i tehnologiju jednostavnom za korištenje jer dizajneri korisničkog sučelja rade na područjima gdje korisnici izravno komuniciraju s proizvodom. Samim time, posao dizajnera korisničkog sučelja uključuje **izgled i dojam** (analiza korisnika, istraživanje dizajna, grafički razvoj, branding, storyline) te **interaktivnost i odaziv** (prototipiranje korisničkog sučelja, animacija i interaktivnost, responzivnost, implementacija s razvojnim programerima).[27]

Stvaranje dobrog korisničkog iskustva od krucijalne je važnosti jer olakšava birokraciju te dugoročno donosi uštedu kroz poboljšanja temeljenima na analizama i povratnim informacijama. PEW-ovo vladino izvješće provedeno 2010., utvrdilo je da je 61% odraslih osoba tražilo informacije ili izvršilo transakcije na vladinoj web stranici u posljednjih godinu dana. Napomenuli su da je to posebno važno jer dokazuje da se ljudi ne uključuju samo u rad vlade na zanimljive načine, nego koriste ove alate kako bi podijelili svoje mišljenje s drugima i doprinijeli široj raspravi o vladinim politikama.[28]

5.4. Upotrebljivost

Prema definiciji, upotrebljivost je definirana kao osnovni koncept interakcije čovjeka i računala koji pokazuje koliko se lako i jednostavno koristi funkcionalnost proizvoda ili usluge, njihove djelotvornosti, sigurnosti, učinkovitosti te subjektivan stav korisnika prema određenom sustavu.[29]

Na proces upotrebljivosti uvelike utječe razvoj tehnologije

jer proizvodi i usluge razvojem iste postaju sve kompleksniji za korisnikovu uporabu, stoga je zadatak dizajna smanjiti kompleksnost interakcija i time povećati upotrebljivost. Sam proces ponavlja se nekoliko puta (završava kada se postigne zadovoljavajuće rješenje po mjeri korisnika) te obuhvaća evaluacijski dio i proces razvoja u potpunom dizajnerskom ciklusu (*eng. full design circle*) koji uključuje korake razumijevanja stvarnog okruženja, izradu prototipa, postavljanja koncepta dizajna i evaluaciju sa stvarnim korisnicima u stvarnom kontekstu. Same metode po kojima se vrednuje upotrebljivost podijeljene su u dva pristupa, od kojih svaki mora biti zadovoljen kako bi se dobila sveobuhvatna slika. Prvi pristup **metode testiranja** (*eng. usability testing*) odnosi na laboratorijsko ili terensko testiranje koje uključuje fokusne grupe, testiranje zadataka i intervjue te u svom procesu moraju uključivati korisnika. Drugi pristup **metode pregledavanja** (eng. usability inspection) ne uključuje korisnika, odnosno provode ih stručnjaci iz područja upotrebljivosti te uključuju heurističko vrednovanje, spoznajno prošetavanje (*eng. cognitive walkthrough*) i smjernice upotrebljivosti (*eng. guideline reviews*).[29]

5.5 Pristupačnost i njezina zakonska odredba

Pojam **pristupačnosti** (*eng. accessibility*) dobio je posebnu važnost u posljednje vrijeme te je postao zakonski obavezan od 23. rujna 2019. (za aplikacije od 23. lipnja 2021.). Jednostavno rečeno, digitalna pristupačnost odnosi se na prilagodbu web stranica i mobilnih aplikacija osobama s invaliditetom te uključuje skup pravila koji u konačnici olakšavaju pristup sadržaju u digitalnom okruženju.

Osim osobama s poteškoćama, digitalna pristupačnost pomaže i starijim osobama koje s godinama gube vizualne i motoričke sposobnosti. Ovim postupkom osigurava se aktivnija uloga u društvu te ravnopravnost kroz primjenu četiri glavna standarda:[30]

1. **Mogućnost opažanja** – korisnici moraju moći vidjeti podatke koji se prikazuju (ne mogu biti nevidljivi svim njihovim osjetilima)
2. **Operativnost** – korisnici moraju moći upravljati sučeljem (sučelje ne može zahtijevati interakciju koju korisnik ne može izvršiti)
3. **Razumljivost** – korisnici moraju moći razumjeti informacije i rad korisničkog sučelja (sadržaj ili operacija ne smiju biti izvan njihova razumijevanja)
4. **Stabilnost** – korisnici moraju moći pristupiti sadržaju uz razvoj tehnologije (bez obzira na razvoj tehnologija, sadržaj bi trebao ostati jednako dostupan).

Promatrajući gore navedene informacije, logično je zaključiti kako će digitalna pristupačnost utjecati i na korisničko iskustvo. Nejasne i duge rečenice zamijenjene su kratkim i jednostavnim rječnikom (ovo ne uključuje kratice), obavezno je korištenje hijerarhije u tekstu (naslovi, odlomci, popisi) te je zabranjeno ponavljanje informacija. Osobe s vizualnim poteškoćama

imaju mogućnost uvećanja veličine teksta direktno kroz web preglednik ili pomoću alata i tehnika koje dizajneri i programeri mogu upotrebljavati. Kontrast boja je također važan jer povećava kvalitetu pregleda sadržaja, ne samo slabovidnim osobama već i zdravim, npr. na otvorenom prostoru prilikom sunčanog dana odgovarajući kontrast boja poboljšava čitljivost. Pružanje jasnih povratnih informacija korisniku dižu povjerenje prilikom obavljanja interakcija i dobre povratne informacije jasno ukazuju na probleme ili uspješnost korisničkog unosa, npr. „Unesite valjanu adresu e-pošte“, „Postupak je uspješno proveden“ itd.[31] Ovo su samo neke od navedenih smjernica koje se mogu implementirati ovisno o potrebama i uređaju na kojem korisnik obavlja digitalne radnje.

6.0 Referentni primjeri

6.1 Primjeri iz popularne kulture i umj. radova

6.1.1 Minority Report

Prepoznavanje lica, skeniranje mrežnice oka ili glasa nekad su bili znanstvena fantastika koju smo mogli vidjeti samo u filmovima, a danas ti sigurnosni sustavi pomažu pri održavanju sigurnosti. Korištenje biometrije u filmovima česta je pojava koja svjedoči o ljudskoj fascinaciji ovim fenomenom. Jedan od mnogih takvih primjera je futuristički film **Minority Report** iz 2002. godine. U ovom filmu društvo intenzivno koristi biometrijske sustave poput skeniranja lica koji im pomažu u identifikacijama, praćenjima i marketingu pa tako, npr. dok ljudi hodaju, personalizirane reklame ih pozdravljaju vlastitim imenom dok ulaze u zgradu. Glavni protagonist John Anderton (Tom Cruise) pokušava izbjeći zakon pa zamjenjuje svoje oči s onima drugog čovjeka kako bi zavarao skeniranje šarenice. Zapanjujuća je činjenica da bi putem stvarne medicinske transplantacije oka, ovaj postupak zapravo funkcionirao. Ovom spoznajom možemo zaključiti da kriminalac ima mogućnosti postati netko drugi (ako su voljni proći nevjerojatno skup i bolan postupak), ali još i važnije – ukazuje na činjenicu da čak i biometrija kao najsigurniji sustav zaštite može biti probijena ako drugi čimbenik ima dovoljno lukavosti i znanja.[32]

6.1.2 Snowden

Ovaj film temelji se na stvarnim događajima koji su potresli svijet 2013. godine te čija agonija još uvijek traje i predstavlja jednu od najvećih afera prisluškivanja i zadiranja u ljudsku privatnost od strane vlada. Riječ je o biografskom uratku redatelja Olivera Stonea koji donosi priču o Edwardu Snowdenu, bivšem zaposleniku CIA-e, koji je neovlašteno kopirao informacije iz Nacionalne sigurnosne agencije (*eng. National Security Agency, NSA*) te ih pustio u javnost putem novinara. Dokumenti koje je Snowden predao novinarima sadržavali su dokaze o NSA-ovom nezakonitom praćenju mobilnih telefona i društvenih mreža, sve pod krinkom osiguravanja državne sigurnosti. Film odlično opisuje aferu koja je razdrmala svijet i Snowdenovu odluku zbog koje je riskirao sve s ciljem da otkrije istinu i promjeni stvari. Upravo iz ovog razloga film nije samo biografska priča, nego i podsjetnik da su informacije najveće blago vremena u kojem živimo. O Edwardu Snowdenu snimljen je i dokumentarac **Citizenfour (2014)** koji iz prve ruke prepričava istu tematiku.[33]

6.1.3 Džepni priručnik za zaštitu podataka i skrivanje od nadzora

Ovaj priručnik nastao je u sklopu manifestacije **Moje, tvoje, naše 2016**, koja se bavila temom sveukupnog nadzora. Publikacija je zamišljena kao džepni priručnik koji upozorava na svakodnevnu prisutnost tehnologije nadzora, a referira se na "post-Snowden" pojam koji označava saznanje da je u današnjem svijetu tehnologija nadzora sveprisutna a njihov razvoj nezaustavljiv.

Priručnik sadrži tekst “Svi bismo trebali imati nešto za sakriti” analitičara računalne sigurnosti Moxiea Marlinspikea, koji je objavljen uz dopuštenje autora, a radi se o primjerima suvremenih oblika nadzora i zlouporabe osobnih podataka putem nadzornih kamera, pametnih telefona i interneta, uz savjete kako se od navedenih prijetnji zaštititi i tekst o zakonskoj dimenziji zaštite podataka u Republici Hrvatskoj.[34]

6.1.4 USB killer

Sve više građana uključeno je u digitalne interakcije s tijelima državnih uprava, međutim većina njih je slabo ili nikako upoznata sa zaštitom vlastitih podataka, njihovih računala i posljedica koje to donosi. Jedan od spekulativnih dizajnerskih radova koji koristi USB stick kao primjer hakerstva je rad Damira Prizmića i Nikola Bojića pod nazivom USB killer. Ovaj rad referira se na priču o ruskom hakeru koji je dizajnirao na prvi pogled standardni flash drive čija je uloga prženje USB kontrolera i matične ploče računala prilikom spajanja. USB killer nadovezuje se na ovu tematiku i spekulira o bliskoj budućnosti u kojoj *open source* i autorstvo ostaju zaključani unutar rigidnih pravnih regulativa, a umrežena kolektivna fikcija postaje jedini slobodni oblik dizajnerskog stvaranja, bez obzira na opasnosti i moguće ishode.[35]

6.2 Referentni primjeri i aplikacije

6.2.1 HYPR-3

HYPR-3 je bežični token koji putem najsigurnije trostruke provjere autentičnosti omogućava praktično mobilno plaćanje povezujući se putem Bluetooth veze. Uz uređaj dolazi i aplikacija koja ima ulogu novčanika za sigurno pohranjivanje kreditnih i debitnih kartica. Glavna prednost ovog tokena je korištenje trostruke umjesto dvostruke autentifikacije, što uvelike povećava razinu sigurnosti i očuvanje korisnikovih podataka. Vrlo jednostavno, koncept je baziran na spoznaji da korisnik mora znati sva tri faktora kako bi napravio transakciju koja se odvija u oblaku (*eng. cloud*) čime se zaobilazi zlonamjerni softver i napad hackera koji bi mogao oštetiti korisnikov račun. Spomenuta aplikacija, koja služi kao novčanik, nudi i podršku za Bitcoin transakcije. Ako trgovac podržava Bitcoins, ali ne posjeduje Hypr-3, aplikacija će se spojiti na internet, izračunati dolar vrijednost Bitcoina i naplatiti taj iznos na korisnikovu kreditnu ili debitnu karticu što predstavlja novu eru digitalne trgovine gdje su prijevare i krađe identiteta dodatno otežani.[36]

6.2.2 Estonski smartID

Estonija danas ima jedan od najrazvijenijih nacionalnih sustava ID-kartica na svijetu, uz to razvili su i smartID – aplikaciju koja služi kao identifikacijsko rješenje bez uporabe SIM kartice. Ova aplikacija služi kao alternativa bankovnim karticama pa se može koristiti za online bankarstvo, digitalno potpisivanje dokumenata te za pristup e-uslugama. SmartID je od 2018. godine prepoznat

kao QSCD (*eng. Qualified Signature Creation Device*), što znači da svi dokumenti digitalno potpisani ovom aplikacijom moraju biti priznati u svim članicama EU. Aplikacija koristi PIN kodove za sigurnost i prijavu: prvi kod mora imati najmanje 4 znamenke i koristi se za pristup e-uslugama, dok drugi kod ima najmanje 5 znamenki i potreban je za digitalno potpisivanje transakcija. SmartID ne sprema korisnikove identitetske ili PIN podatke već stvara privatne ključeve prilikom registracije te kasnije posreduje zahtjeve za autorizacijom i potpisom.[37]

6.2.3 Apple pay

Apple Pay je beskontaktna tehnologija plaćanja koja zamjenjuje fizičke novčanike i sprema kartice na uređaje koji imaju ugrađen NFC (*eng. Near Field Communication*) čip. Apple pay usluga omogućava plaćanja unutar aplikacija, u trgovinama ili putem interneta a za korištenje usluge potrebna je aplikacija **Wallet** putem koje se upravlja računima i dodaju ili uklanjaju željene kartice. U usporedbi s drugim platnim sustavima, Apple pay jedan je od najsigurnijih sustava plaćanja jer koristi više razina provjera sigurnosti za razliku od standardnog beskontaktnog plaćanja koje koristi samo PIN za provjeru. Uz sigurnosne brojeve uređaja (koji zamjenjuje broj kartice) i dinamičke sigurnosne kodove (koji zamjenjuje CVV kod na pozadini kartice), Apple provjerava autentičnost svake transakcije putem biometrijskih metoda, odnosno *Touch ID-a* ili *Face ID-a*. Cijeli sistem provjere vrlo je jednostavan. Kad god se određena transakcija provodi korisnik mora postaviti prst na senzor otiska prsta ili započeti skeniranje lica kako bi plaćanje bilo uspješno provedeno. Osim što se korisnikova kartica nikad ne dijeli s trgovcima niti se prenosi plaćanjem, službenici u trgovini nemaju pristup osobnim podacima kao što su ime ili adresa jer ID nije potreban u svrhu provjere. Osim toga, banke su toliko sigurne u sigurnost Apple Pay-a, da su odlučile preuzeti odgovornost za bilo kakve lažne kupnje unutar prodajnih objekata i na mreži putem sustava. [38]

7.0 Analiza gov.hr

7.1 Općenita analiza novog vladinog sustava

Vlada Republike Hrvatske započela je projekt kojim se od 2014. godine želi olakšati komunikacija između građana i javnih ustanova. Predstavljen je **središnji državni portal gov.hr**, na koji odlazi cijela Vlada kao i usluga e-Građani, sve s ciljem ulaganja u buduće planove digitalne vlade.

Na prvi problem nailazimo već prilikom otvaranja početne stranice koja više izgleda poput bloga, nego internetske stranice najvažnije državne institucije, obzirom da se na početku ne dobiva niti jedna važna informacija, već sadržaj koji je fokusiran na (samo)promociji vlade. Drugo, pomalo subjektivno mišljenje, odnosi se na pretjerano korištenje crvene boje koja se mogla kvalitetnije iskoristiti, npr. za isticanje bitnih elemenata ili linkova koji nisu ništa posebno istaknuti osim što lagano promijene boju kada se prijeđe mišem preko njih, što zasigurno rezultira nepotpunom isporučenom informacijom slabovidnim osobama. Nedovoljno jasno je napravljena i hijerarhija te sustav traženja informacija jer je npr., malo teže pronaći kontakte te informacije o ministrima i njihovim pomoćnicima. Umjesto toga, sve kontakt informacije nalaze se na dnu stranice pa tako, ako želimo određeni kontakt broj, moramo kliknuti na link *Adresar* > *Popis tijela državne uprave* koji se zatim uvijek otvara u novom prozoru, što cijeli postupak čini kompliciranim te nikako osmišljenim s korisnikom na umu.

Središnji državni portal kao jedna od sastavnica hrvatske e-vlade sadrži mnogo pitanja i odgovora te potrebne informacije kao što su upisi u škole, registracija vozila, potrebni dokumenti za izradu putovnica itd. Ovdje također pronalazimo problem već na početku jer nam uvodna stranica odmah prikazuje Moju upravu (kao prostor u kojem se nalaze sve navedene informacije), koja nije na nikakav način istaknuta već se stapa s ostatkom sadržaja. Također, samo korištenje naziva *Moja uprava* umjesto nekog zvučnijeg poput *Teme koje bi vas mogle zanimati*, govore o nedostatku kvalitetne sadržajne strategije.

Možda najvažniji projekt **e-Građanin**, za kojeg na samom početku možemo reći da nije dovoljno istaknut na naslovnici, odnosi se na bolju komunikaciju građana i javne uprave tj., nije više potrebno po dokumente ići na šaltere, već se isti mogu nakon prijave u sustav preuzeti kroz osobni korisnički pretinac, što je bila dobra ideja, ali loše realizirana. Za pristup e-Građanin potrebno je imati ePass ili mToken koji se preuzima u FINI za kasniju prijavu u sustav. Međutim, nakon toga nastaje problem jer korisničke upute ne postoje (barem ne uredno, pregledno i na jednom mjestu), već su iste zamijenjene nejasnim porukama koje možemo pronaći po cijelom webu. Jedan od primjera je kod odabira načina prijave u sustav, gdje se uz ostale informacije pojavljuje i pojam sigurnosna razina koji nije prethodno

objašnjen te prosječnom posjetitelju ne znači ništa. Upravo zbog loših korisničkih uputa i nepoznatih termina poput vjerodajnica ili osobni certifikat, koji prosječnom korisniku ne znače ništa, projekt e-građanin pada na testu jer je osnovni zadatak dizajna osmisli kvalitetno sučelje i kvalitetne poruke koje će korisnici razumjeti.

Uporabljivost (*eng. usability*) kompletne stranice Vlade lošija je u odnosu na prošlu verziju jer nudi manje informacija koje su skrivene unutar nepovezanih linkova. Isti se linkovi, bez obzira na kojoj se stranici nalaze, otvaraju u novim prozorima, poveznice vode na vanjske stranice bez nekog vizualnog objašnjenja, što ih čini nepovezanima i zbunjujućima. Poruke koje se prikazuju građanima su neusklađene; poput onih koje se dobivaju prilikom prijave u Korisnički pretinac, nisu usklađene s porukama koje se pojavljuju na ostalim stranicama što ih čini zbunjujućima te izgledaju kao da su napisane prisilno.

Pristupačnost (*eng. accessibility*) također nailazi na probleme jer stranica treba biti prilagođena osobama s poteškoćama kako bi lakše pronalazile informacije koje ih zanimaju. Ovo uključuje i izgled stranice koji je bitan svima i semantiku, koja je osobito bitna osobama s motoričkim poteškoćama zbog pristupa internetu na drugačiji način. S druge strane, postoje i dobro odrađene komponente kao što su povećana slova koja su dobro pozicionirana te kontrastni prikaz čije postavke pamte kada se kreće po stranicama.

Možemo reći kako projekt ima potencijal za razvitak, no sam portal mora biti dostupniji većem broju građana jer je servis e-Građani namijenjen samo onima s visokim informatičkim znanjem (uzmemo li u obzir da zbog kompleksnosti sustava osobe treće dobi neće znati/moći koristiti ove usluge).

7.2. Detaljna analiza sustava e-građani na primjeru podnošenja zahtijeva

korak_1

· ulazak na web stranicu e-građanin (prikaz 2)

· na samom početku obasipanost informacijama pa pogled bježi na sve strane

· više je istaknut naziv «osobni korisnički pretinac» i nazivi članaka/usluga nego samo ime stranice

· nema nikakvih korisničkih uputa na samom početku niti na jednom mjestu

· kombinacija boja i njihova uloga zbunjuje te ne razdvaja informacije

· za primarni cilj odnosno pronalazak usluga, korisnik mora scrollati dolje umjesto da ovakvi podaci budu na samom početku ili barem istaknuti na neki način

korak_2

· pronalazak e-usluga u sustavu e-građani (prikaz 3)

· pozitivna stvar je mogućnost filtriranja po temi, institucijama i abecedno

· sučelje je pregledno i su svi podaci kategorizirani

korak_3

· odabir kategorije “uvjerenje da se ne vodi kazneni postupak” (prikaz 4)

· otvara se nova kartica koja sadrži tekst o uvjetima i mogućnostima ovog uvjerenja

· stranica izgleda uredno te je u skladu s prethodnom

korak_4

· predaja zahtjeva za izdavanje uvjerenja da se ne vodi kazneni postupak (prikaz 5)

· na staroj kartici se učitava potvrda autentifikacije

· u prvi plan upada obavijest koja je istaknuta sivom bojom ista obavijest loše je napisana (pomalo zbunjujuća)

korak_5

· ulazak u način autentifikacije (prikaz 6)

· ovaj (kao i prošli korak) nisu vizualno dovoljno istaknuti već se samo uz brojeve nalaze u gornjem dijelu stranice

· nailazi se na nepoznate pojmove kao što su vjerodajnica, sigurnosna razina itd.

korak_6

· odabir vjerodajnice (prikaz 7)

· učitava se nova stranica bez ikakvog upozorenja

· na njoj se nalazi tekst “ako Vam se ekran za prijavu na AAI@EduHr nije automatski otvorio, kliknite ovdje kako biste ručno otvorili navedeni ekran”

korak_7

· podnošenje zahtjeva (prikaz 8)

· u gornjem izborniku ponuđene su kategorije te su istaknute crvenom bojom te korisnički podaci koji se nalaze na plavoj traci

· ispod navedenog pojavljuju se podaci koje treba ispunit za dobitak zahtijeva – loš odabir veličine tekstova (nije usklađeno)

· na kraju se nalazi tekst koji opisuje daljnji postupak i još neke informacije

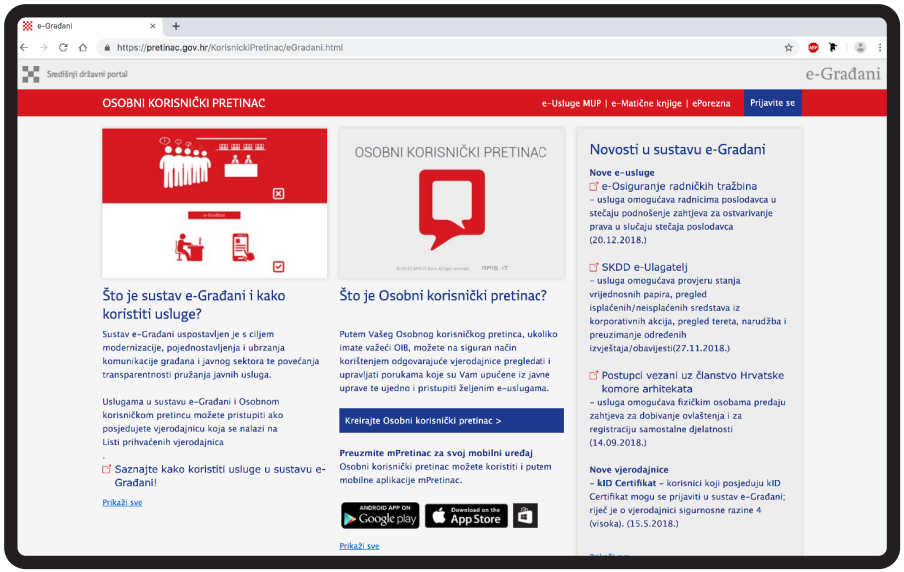
korak_8

· zadnji korak je potvrda o uspješno zaprimljenom zahtjevu o uvjerenju (prikaz 9)

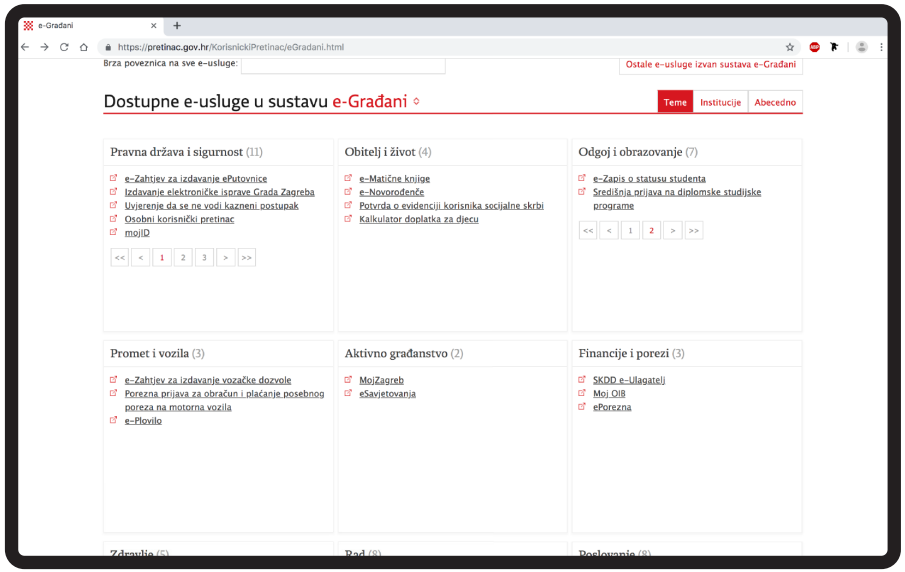
· stranica je dizajnom ista kao i prethodna

· najistaknutija je zelena poruka na ekranu koja obavještava o zaprimljenom zahtjevu i sve vezano uz isti

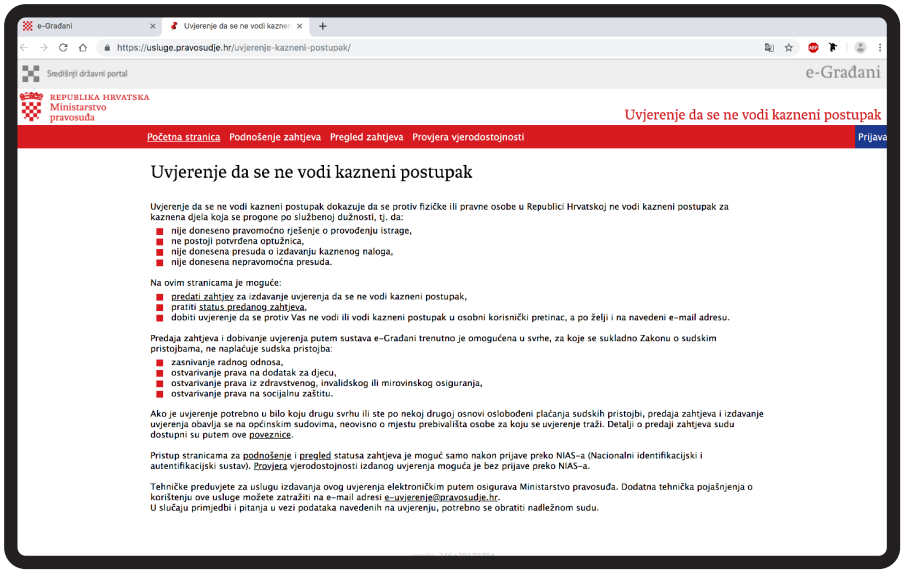
· na kraju se nalaze svi podignuti zahtjevi koji se mogu downloadati ako nisu stariji od šest mjeseci



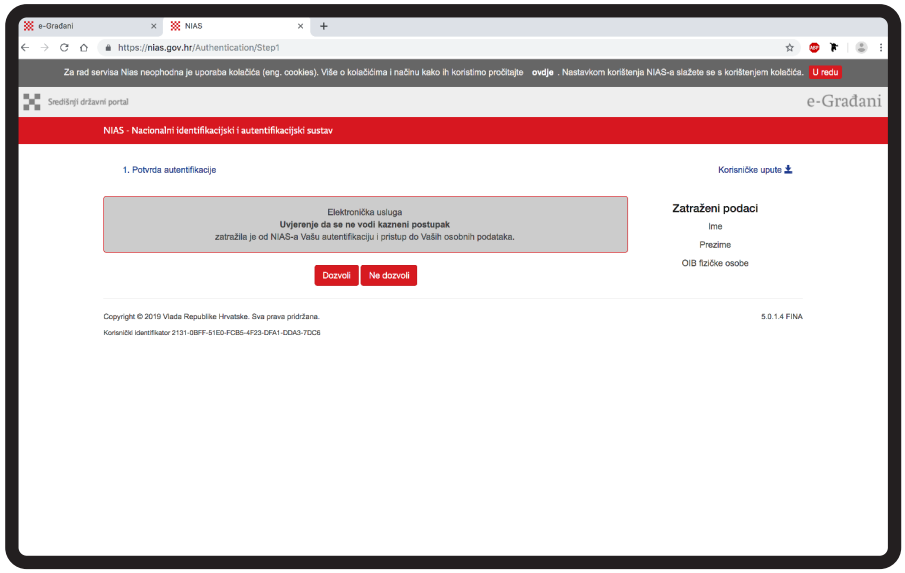
Prikaz 2 korak_1



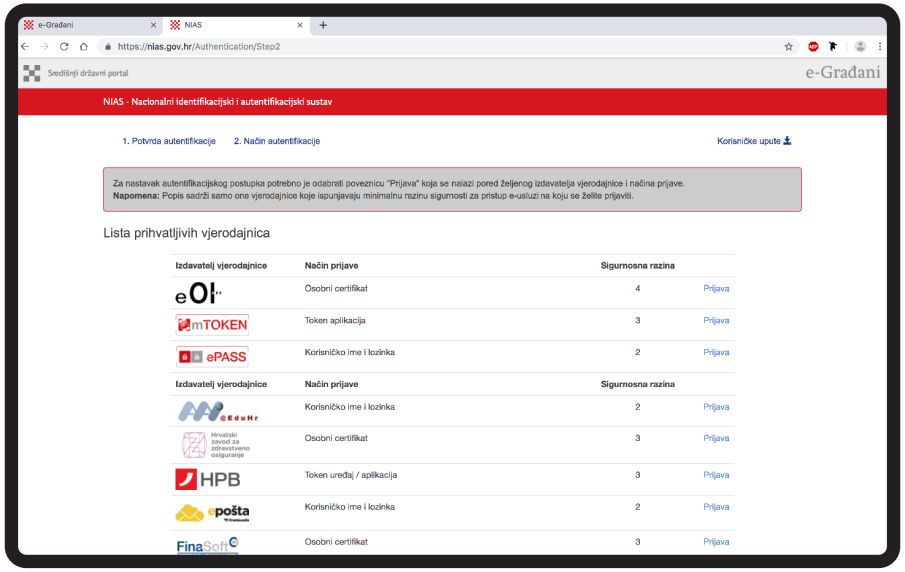
Prikaz 3 korak_2



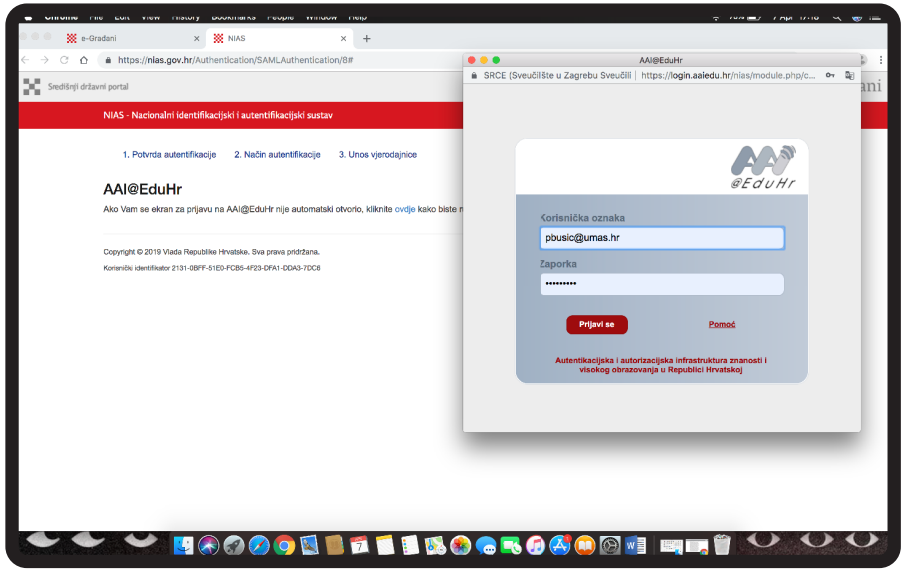
Prikaz 4 korak_3



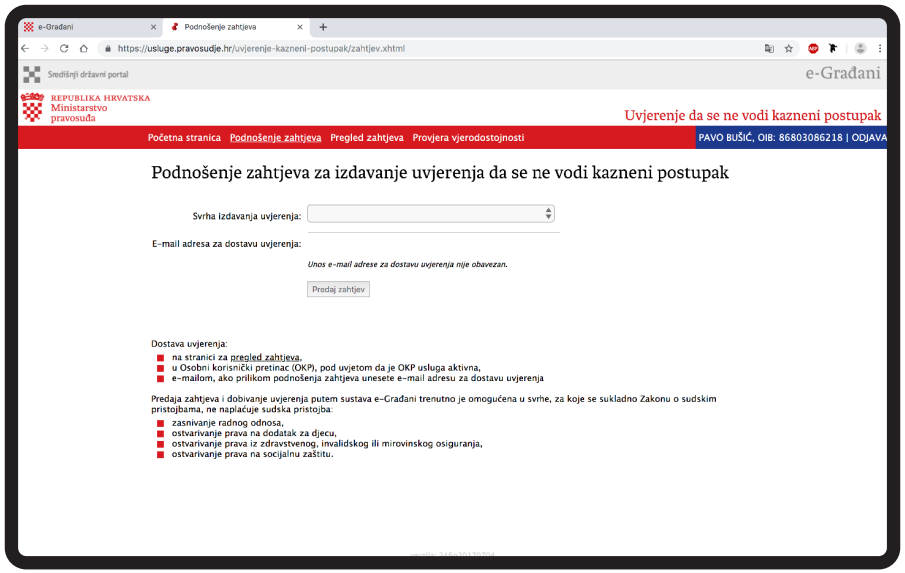
Prikaz 5 korak_4



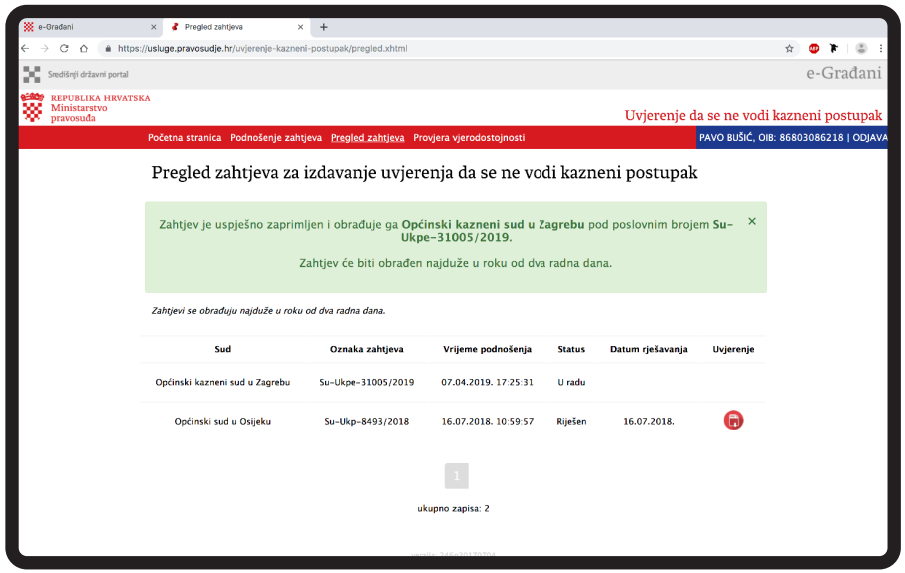
Prikaz 6 korak_5



Prikaz 7 korak_6



Prikaz 7 korak_8



Prikaz 9 korak_8

8.0 Aplikacija Digital ID

8.1 Digitalni identitet

Zapisi o identitetima osoba postoje već stotinama godina iako se u danas poznatim oblicima počinju upotrebljavati tek u 20. stoljeću, kada vlade prihvaćaju identifikacijske dokumente te započinju određivati njihove veličine i informacije. Pojam osobnog identiteta definira se kao skup svojstava povezanih s entitetom na kojeg ne utječu promjenjivi uvjeti (poput vremena), što svaku osobu čini jedinstvenom i razlikuje je ostalih.[39]

Pojava interneta i društvenih mreža te razvoj tehnologija utjecali su na daljnje oblikovanje identiteta osoba pa se sukladno tomu razvija pojam **digitalni identitet.** Ovaj termin definira identitet kao zbirku elektroničko pohranjenih podataka koji identificiraju, jedinstveno opisuju osobu u određenom kontekstu i koriste se za elektroničke transakcije.

Osim što služi kao dokaz za potvrdu identiteta, digitalni identitet nudi javnom i privatnom sektoru efikasnije upravljanje državnim mehanizmima i optimizaciji uprave. Konkretno, dobro implementirani digitalni identifikacijski sustavi mogu imati značajan pozitivan utjecaj na financijsku uključenost, rodnu ravnopravnost, pristup zdravstvenim uslugama itd. Osim navedenog sustavi digitalnog identiteta poboljšavaju državnu efikasnost, odgovornost i transparentnost što smanjuje operativne troškove i korupciju, npr. u Argentini je vladin sustav digitalnog identiteta povezao 13 javnih baza podataka i različite registre ID-a te tako uštedio 104 milijuna USD na propuštanju i utaji poreza. Za primjenjivanje digitalnog sustava identiteta ključno je imati snažne pravne i tehničke okvire za zaštitu privatnosti jer su podaci glavna komponenta digitalnog identiteta koje treba zaštititi.[40]

Faktori koji se danas koriste za potvrdu digitalnog identiteta mogu varirati od konteksta pa sve do zemlje, ovisno o vrsti sustava identiteta koji se koristi. Samim time digitalni identitet može sadržavati biometrijske podatke, npr. otisak prsta, biografske podatke kao što su ime, starost, mjesto rođenja, ali i sve ostale priznate atribute vezane za ono što osoba čini ili što netko drugi zna o njoj. Kada su prije navedeni podaci ovjereni, osoba može zajedno s vjerodajnicama koje je izdao pružatelj usluga (npr. e-osobna, e-dokument, mobile ID) potvrditi svoj identitet i odgovoriti na pitanje "Jesi li ti onaj koji tvrdiš da jesi?". U svijetu međusobne povezanosti poput onoga u kojem danas živimo, digitalni identitet postaje temeljni pojam koji mora jamčiti istinitost svih vrsta informacija.[40]

Da bi se identifikacijski dokument smatrao digitalnim, mora sve svoje vjerodajnice/potvrde pohranjivati i dijeliti elektroničkim putem. Primjeri dostupnih digitalnih vjerodajnica su pametne

kartice (kao najčešća pojava danas), 2D kartice s bar kodom, ID u oblaku i mobilni identitet. Rastuće korištenje pametnih uređaja i njihova uloga povezivanja pojedinaca putem interneta briše granice između fizičkog i virtualnog, pa se zahvaljujući tome uvodi pojam **mobilnog identiteta** kao novi izazov koji treba prevladati.

Mobilni identitet definira se kao sigurna integracija podataka koji nepogrešivo identificiraju osobu u fizičkom i mrežnom svijetu, ali na mobilnom telefonu. Opće je poznato kako mobitel više nije samo sredstvo za komunikaciju, već i alat kojim korisnici mjere prostore, fotografiraju, obavljaju bankovne transakcije itd. Upravo zbog razvoja, funkcionalnosti unutar mobilnih uređaja mogu poslužiti kao fizička vjerodajnica. Dobar primjer su aplikacije s virtualnim karticama koje sadrže podatke o pojedincu i njegovim bankovnim detaljima, uz napomenu da je ovaj sistem još sigurniji jer prikazuje manje informacija nego fizička kartica (npr. ne vidimo CVC kod, broj kartice i slično.). Također, većina današnjih pametnih telefona ima ugrađenu NFC tehnologiju pomoću koje korisnici mogu pohranjivati podatke i iste slati kroz terminal. Osim uloge fizičke vjerodajnice, pametni telefon može postati uređaj za provjeru autentičnosti jer sadrži biometrijske podatke, ali i siguran nositelj faktora provjere autentičnosti jer omogućuje, npr., digitalno potpisivanje dokumenata. Zbog ovih razloga, pametni telefoni zasigurno imaju budućnost u kojoj će pristupačnost i sigurnost dobiti na snazi.[41]

Mnoge su razvijene zemlje uočile prednost korištenja mobitela kao uređaja za potvrdu identiteta i tako postavile zadovoljavajuće sustave koji mogu poslužiti kao dobra referenca ostalim državama. Prva je definitivno Estonija koja je prepoznata kao jedna od najnaprednijih digitalnih zemalja na svijetu, zahvaljujući širokom spektru krajnjih usluga kojih koristi mobilni identitet, kao i suradnji između javne uprave, pružatelja usluga i operatera. Ostale zemlje su također uvidjele prednosti digitalnog svijeta pa tako Finska bilježi najveću integraciju mobilnih telefona, dok je Turska je nositelj standarda mobilnog potpisa.[41]

8.2 Opis i model aplikacije

Digital ID aplikacija bazira se na digitalizaciji osobne iskaznice u Republici Hrvatskoj, odnosno otkriva se kako bi spomenuti osobni dokument funkcionirao u digitalnom kontekstu. Koncept mobilne osobne iskaznice u potpunosti bi zamijenio postojeće plastične verzije (ako osoba to želi), budući da su pametni telefoni u današnje doba postali standard i koriste se prilikom obavljanja svakodnevnih radnji. Uz to, ova aplikacija zapravo bi bila dodatak sustavu e-Građanin koji postoji u Republici Hrvatskoj, a dodatna prednost je što ne zahtijeva korištenje čitača pametnih kartica jer je glavni cilj prikazati sve informacije na ekranu. Aplikacija bi putem jednostavnog korisničkog sučelja omogućila korisniku obavljanje radnji na jednom mjestu, kao što je podizanje potvrda ili slanje uvjerenja putem e-usluga, digitalno potpisivanje dokumenata itd. te bi slala obavijesti (dolazak dokumenata,

potvrda liječničkog pregleda i sl.) putem kojeg bi državna tijela izravno komunicirala s korisnikom. Cilj ove aplikacije je unaprijediti digitaliziranje osobnog dokumenta i olakšati korištenje ovakvog sustava koji u Republici Hrvatskoj nailazi na mnogo problema.

8.2.1 Detaljan opis modela

1. Odlaskom u Ministarstvo unutarnjih poslova Republike Hrvatske korisnik dobiva digital ID certifikate koji mu služe za dokazivanje identiteta te pristup ponuđenim funkcijama (Prikaz 10). Certifikati se sastoje od dva koda. Prvi je aktivacijski kod prikazan u QR obliku koji sadrži sve informacije o korisniku, nešto slično poput čipa ugrađenima u pametne kartice. Drugi, odnosno identifikacijski kod, dolazi putem SMS poruke, provjerava točnost informacija i omogućuje korištenje uređaja kao fizičke vjerodajnice za potvrdu identiteta (Prikaz 12). Aktivacija digital ID-a vrši se isključivo u obližnjoj policijskoj stanici, a dobiveni podaci iz sigurnosnih razloga vrijede 48 sati od preuzimanja.

2. Nakon aktivacije u obližnjoj policijskoj stanici, korisnik kroz dobivene korisničke upute instalira aplikaciju i postavlja željeni sustav zaštite za svoj digitalni identitet. Svi korisnički podaci poput imena i prezimena, dobi i ostaloga, automatski se unose kroz bazu podataka. Dostupni tipovi sigurnosti unutar aplikacije su PIN s nasumičnom tipkovnicom koja zamjenjuje standardu verziju iste i nudi viši stupanj zaštite ovakvog primjera jer pomicanje brojeva po tipkovnici onemogućava pamćenje redoslijeda odabranih brojeva. Uz PIN kao uvijek dostupnu opciju, korisnik može izabrati biometrijske metode poput prepoznavanja lica i otiska prsta koji su prema današnjim standardima najsigurniji odabir.

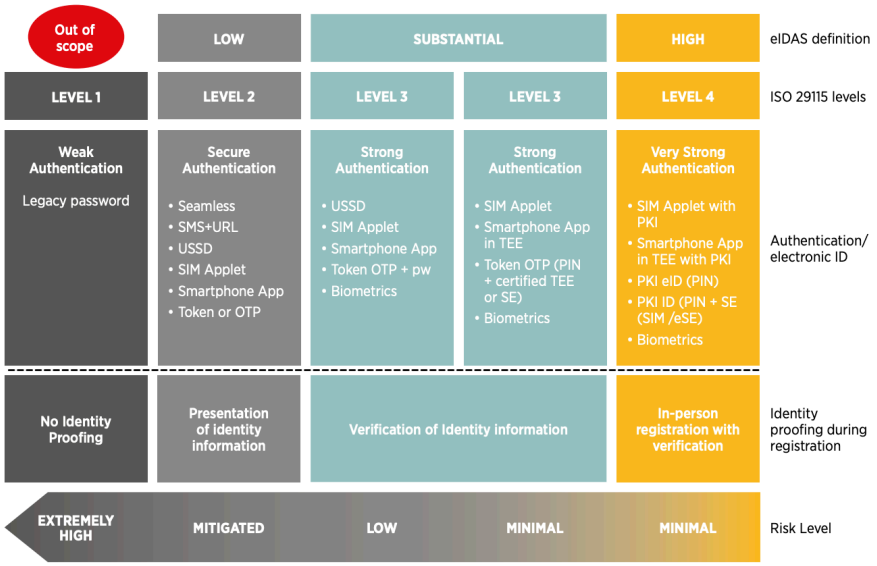
3. Nakon instalacije, korisnik odabire dostupnu uslugu koju želi obaviti, slijedi korake, potvrđuje autentifikaciju te na kraju podnosi zahtjev za odabranom radnjom. Svi podaci izravno se razmjenjuju između korisnika i pružatelja usluga na mreži putem sustava te niti jedna treća strana nema pristup podacima. Sve osobne podatke kontrolira isključivo korisnik, koji u bilo kojem trenutku može pitati tko, kada i zašto je zatražio ili zaprimio informacije o njemu, jer se sigurnost nad podacima rješava potpisivanjem svake podatkovne transakcije digitalnim potpisom i vremenskom oznakom (eng. timestamp), što jamči vjerodostojnost podataka koji se nalaze u decentraliziranom sustavu. Svaka obavljena transakcija je zabilježena i potpisana digitalnim identitetom koji podupire vlada.

4. Svi podaci, zahtjevi, dokumenti prolaze kroz Croroam – konceptualno strukturirani sustav za sigurnosno razmjenu podataka između korisnika, javnih ustanova i privatnih tvrtki. Croroam je izgrađen na decentraliziran način, što znači da sadrži različite tehnološke stupove izgrađene u različitim vremenskim okvirima gdje su osobni podaci raspršeni i čuvani u različitim bazama podataka.[42] Uz bolju sigurnost, decentralizirani sistem omogućava vidljivost upotrebe podataka pa tako korisnik ima

osjećaj nad vlasništvom i kontrolom.

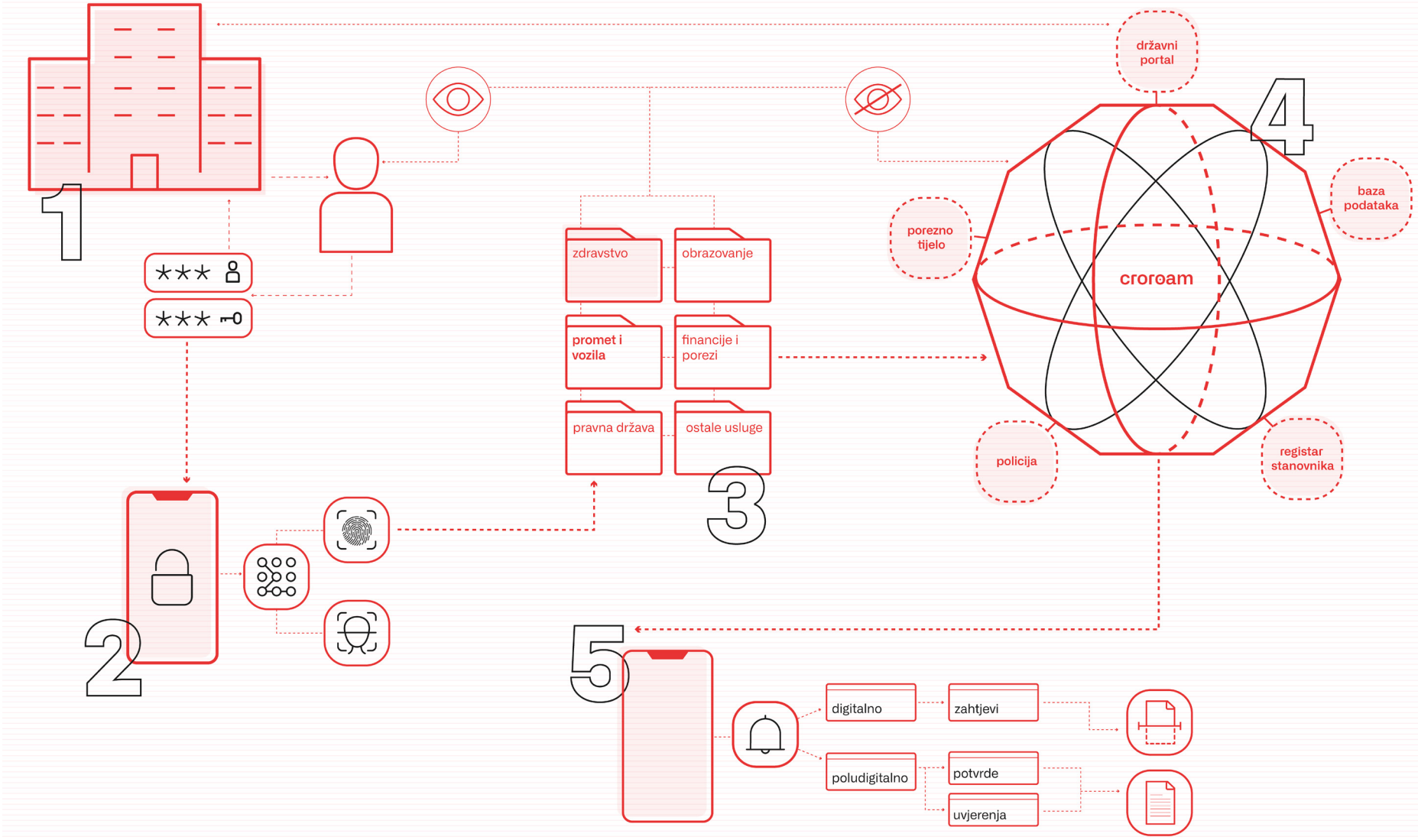
5. Nakon odrađene provjere zatražene usluge, javna ustanova šalje ovjerene podatke korisniku na aplikaciju. Korisnik dobiva notifikaciju na kojoj se nalazi obavijest o dobivenoj usluzi. Ovisno o mogućnostima, svaka usluga može se koristiti poludigitalno ili digitalno. Poludigitalni sistem koristi se kad treća strana zahtjeva printani dokument, npr. korisnik sakuplja dokumentaciju za koju je potreban elektronički zapis o boravištu, kojeg on dobiva putem aplikacije, i kasnije ga printa. Digitalni sistem ne zahtjeva printanje dokumenata i slične radnje već se svi podaci prenose direktno putem mreže, npr. različiti zahtjevi koji se šalju javnim ustanovama. Još jedan digitalni primjer je NFC tehnologija za bežičnu razmjenu podataka. Ovakav sustav koristi se kada pružatelj usluga podržava ovakav tip tehnologije, npr. prilikom prelaska granice korisnik samo treba obaviti biometrisjku potvrdu te prisloniti svoj mobitel na uređaj koji zatim automatski učitava/šalje potrebne podatke.

Gledajući opisani model možemo zaključiti kako su faktori razine pouzdanosti (Prikaz 11) zadovoljili sve standarde te smanjili razinu rizika na minimum. Osobni odlazak do zadane ustanove po odgovarajuće certifikate, snažna provjera autentičnosti kroz biometriju te posjedovanje virtualnog tokena ugrađenog u aplikaciju omogućuju još sigurniju provjeru identiteta te na jednostavan način dovode korisnika do traženog cilja ili usluge.

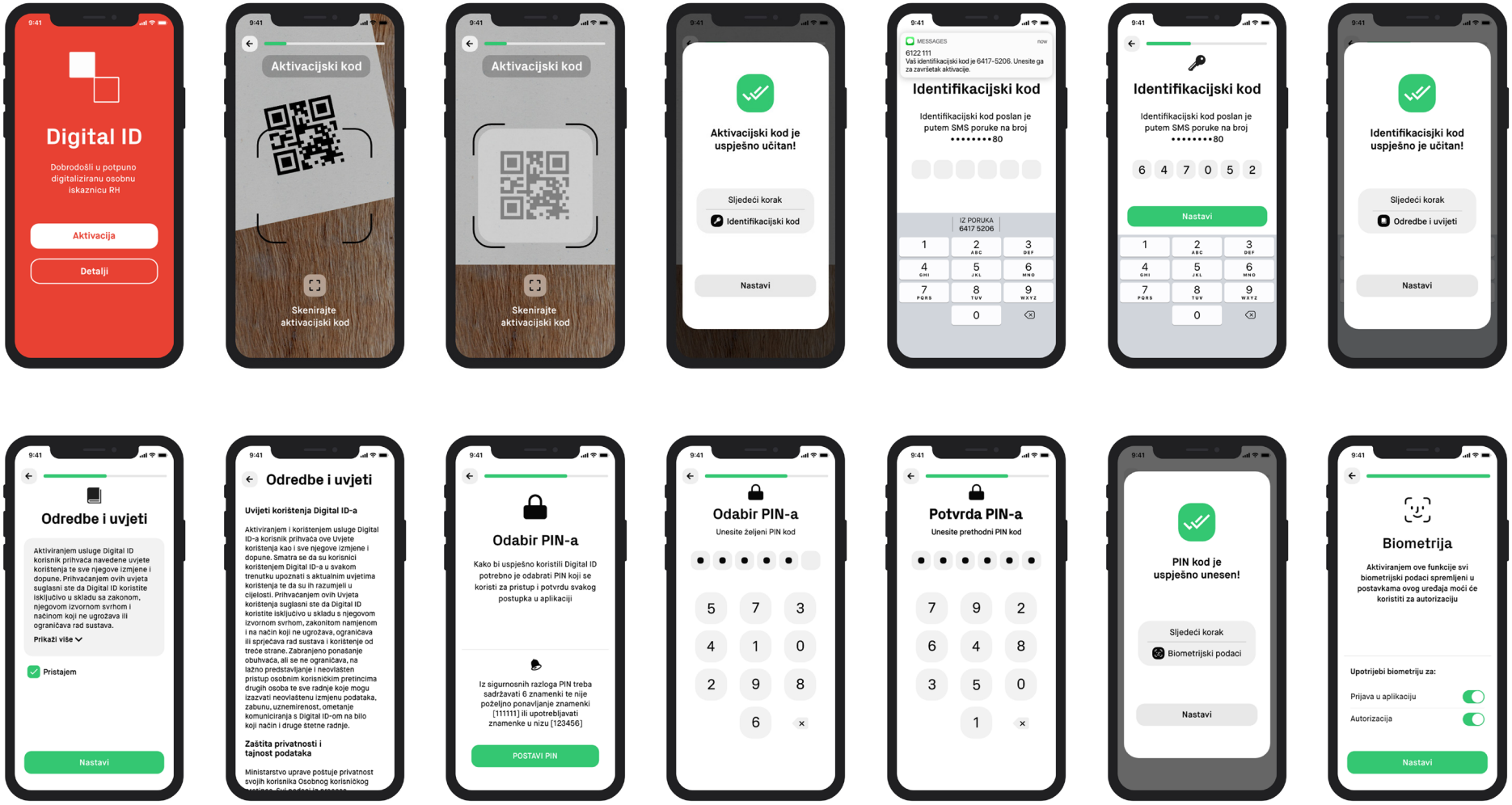


Key: OTP = one-time password; PKI = public key infrastructure; (e)SE = secure element or embedded secure element (a tamper-resistant hardware platform); TEE = trusted execution environment (a secure area of the smartphone); USSD = unstructured supplementary service data ("quick codes"). *Note:* NISTIC 800-63A draft standard guidelines on identity proofing also allow for virtual-in person proofing and enrollment transactions[25]

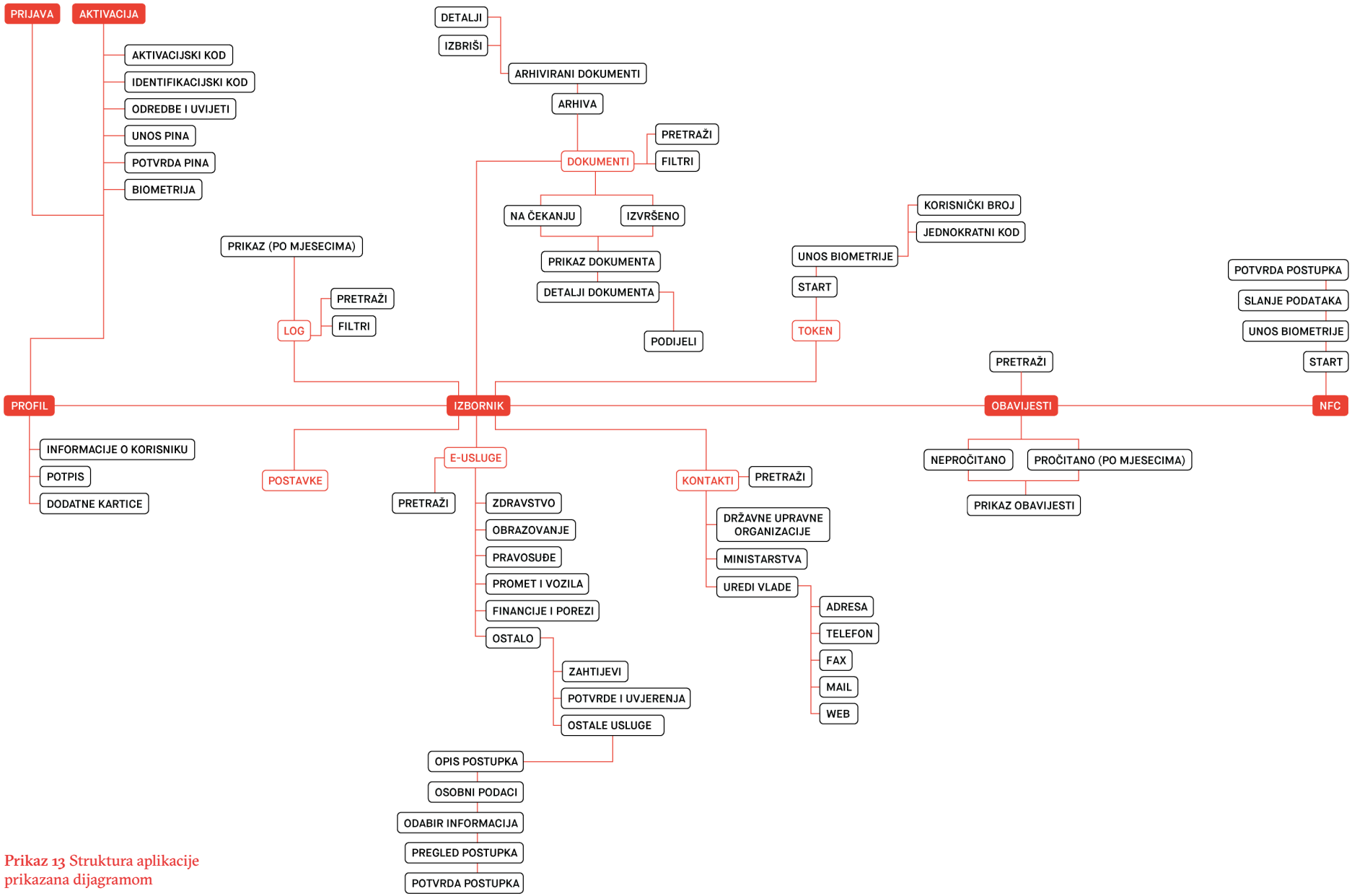
Prikaz 11 Razine pouzdanosti



Prikaz 10 Model aplikacije



Prikaz 12 Proces aktivacije



Prikaz 13 Struktura aplikacije prikazana dijagramom

8.3 Dizajn korisničkog sučelja

8.3.1 Vizualni identitet

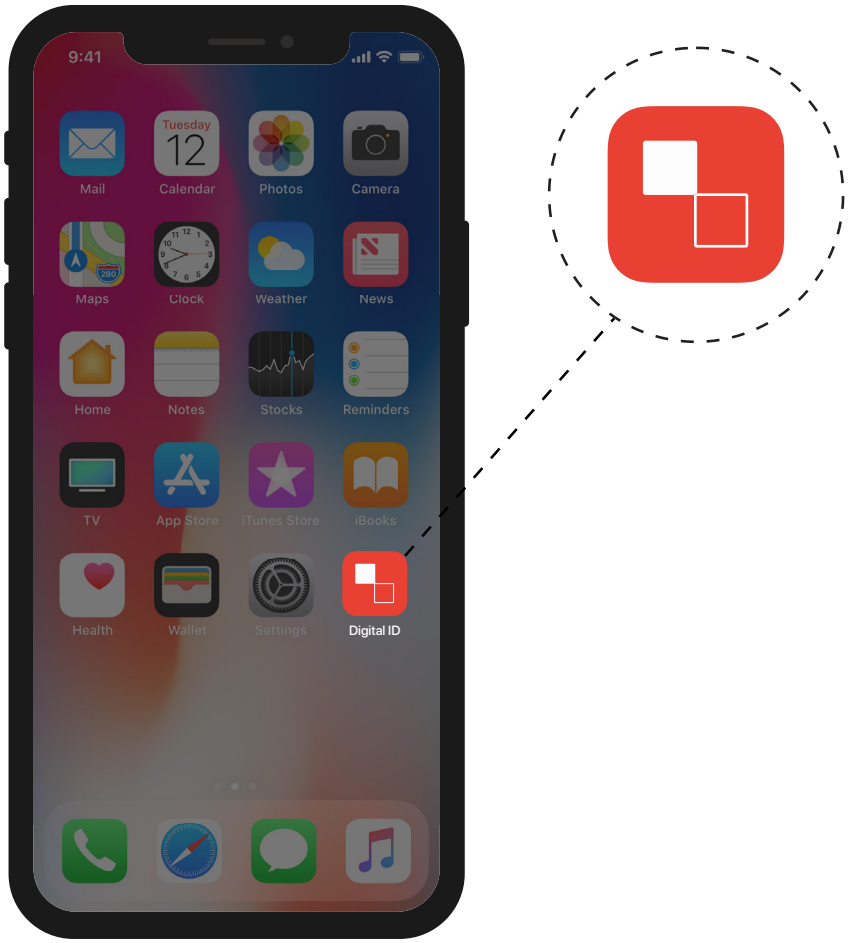
Vizualni identitet aplikacije simbolizira pojednostavljenu hrvatsku šahovnicu, odnosno dva izmjenična kvadrata – puni i prazni, koji predstavljaju nacionalni identitet (prikaz 14). Identitet se još nadovezuje na Ljubičićeve popularne "hrvatske kockice" koje dizajnerska struka prihvaća i koristi kao osnovu za većinu identiteta u novonastaloj državi.[43]

8.3.2 Tipografija

Zbog svog geometrijskog pojednostavljenja koje nudi spektakularnu čitljivost i oštrinu, **Px Grotesk** je tipografija korištena za naslove (prikaz 15). Ovaj sans-serifni font inspiriran je načinom kojim se tipografske krivulje pikseliraju na ekranima.[44] Upravo se zbog spomenutih piksela (sitnih kvadrata) ova tipografija odlično veže uz kompletan vizualni identitet. Za tekst u aplikaciji korišten je **Maison Neue** font; cjelovita obrada izvornog Maison-a, s ažuriranjima koja su napravljena kako bi se iskoristile prednosti novih tehnologija prikazivanja i reprodukcije.[45]

8.3.3 Boje

Primarna boja unutar aplikacije je crvena koja se inače koristi kao glavna boja hrvatskog identiteta (prikaz 16). Uz crvenu, u aplikaciji se nalaze crveno-ružičasta, ružičasta, ljubičasta te svijetlo i tamno plava kao druga boja nacionalnog identiteta. Sve navedene boje nalaze se blizu spektra crvene i plave te se tako razlikuju, ali vizualno ne odskaču jedna od druge.



Prikaz 14 Primjer apliciranja vizaulnog identiteta

Px Grotesk 54pt

Px Grotesk 35pt

Px Grotesk 30pt

Px Grotesk 28pt

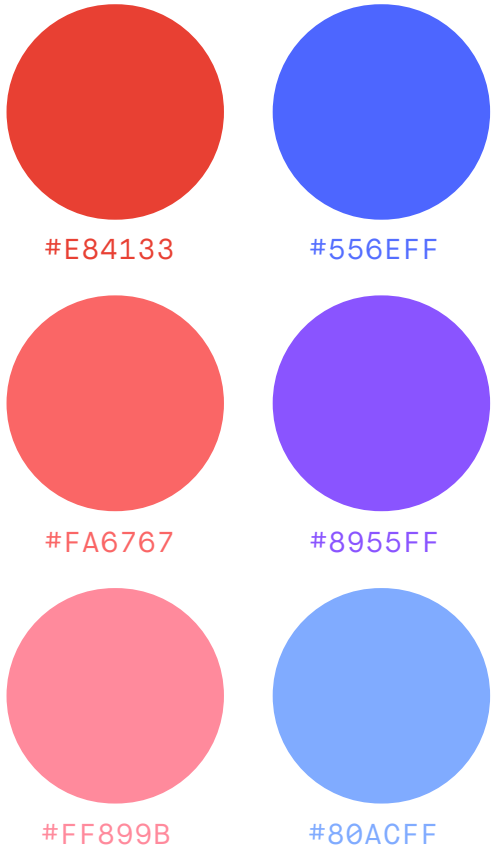
Maison Neue 25pt

Maison Neue 20pt

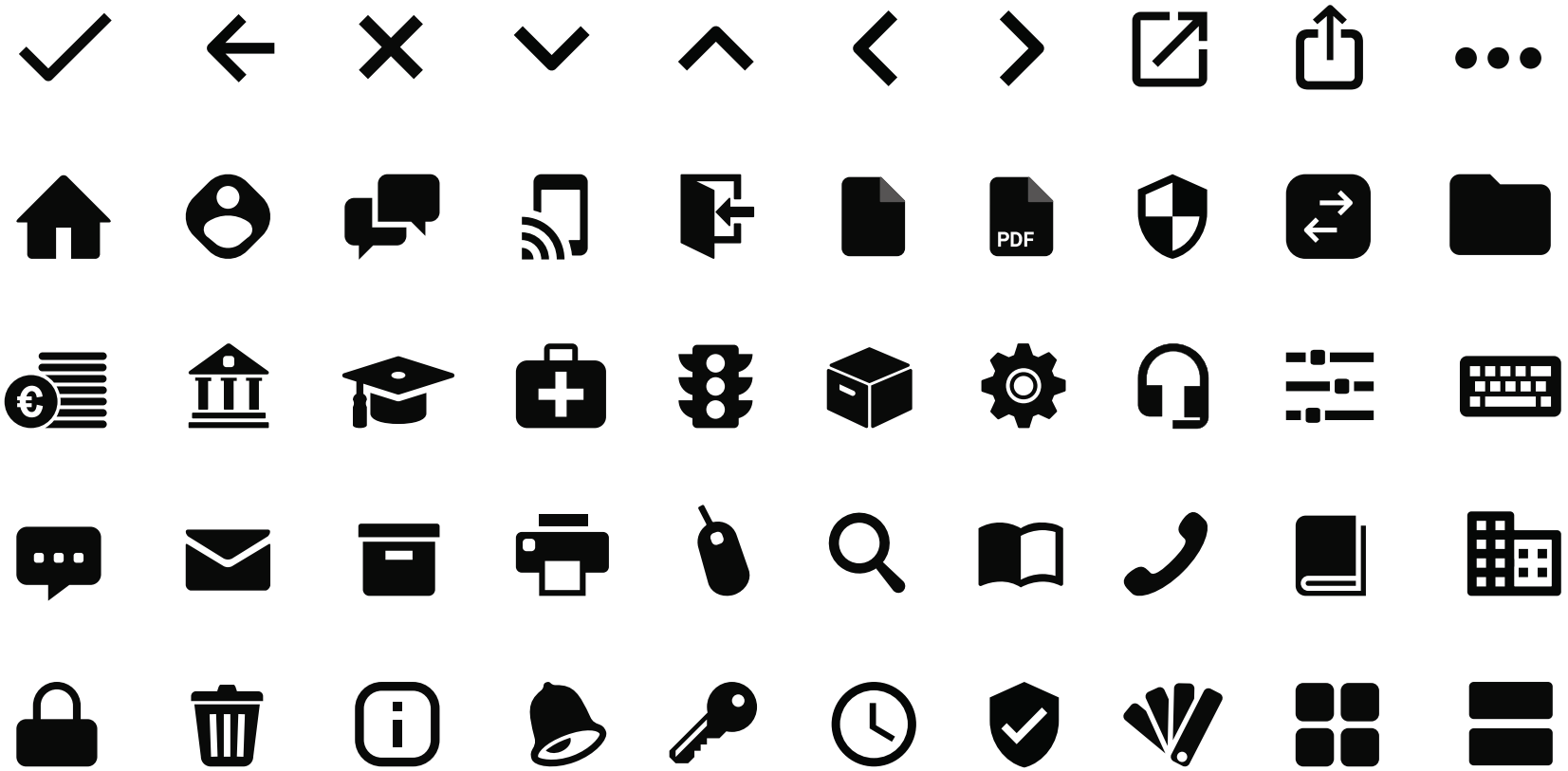
Maison Neue 18pt

Maison Neue 16pt

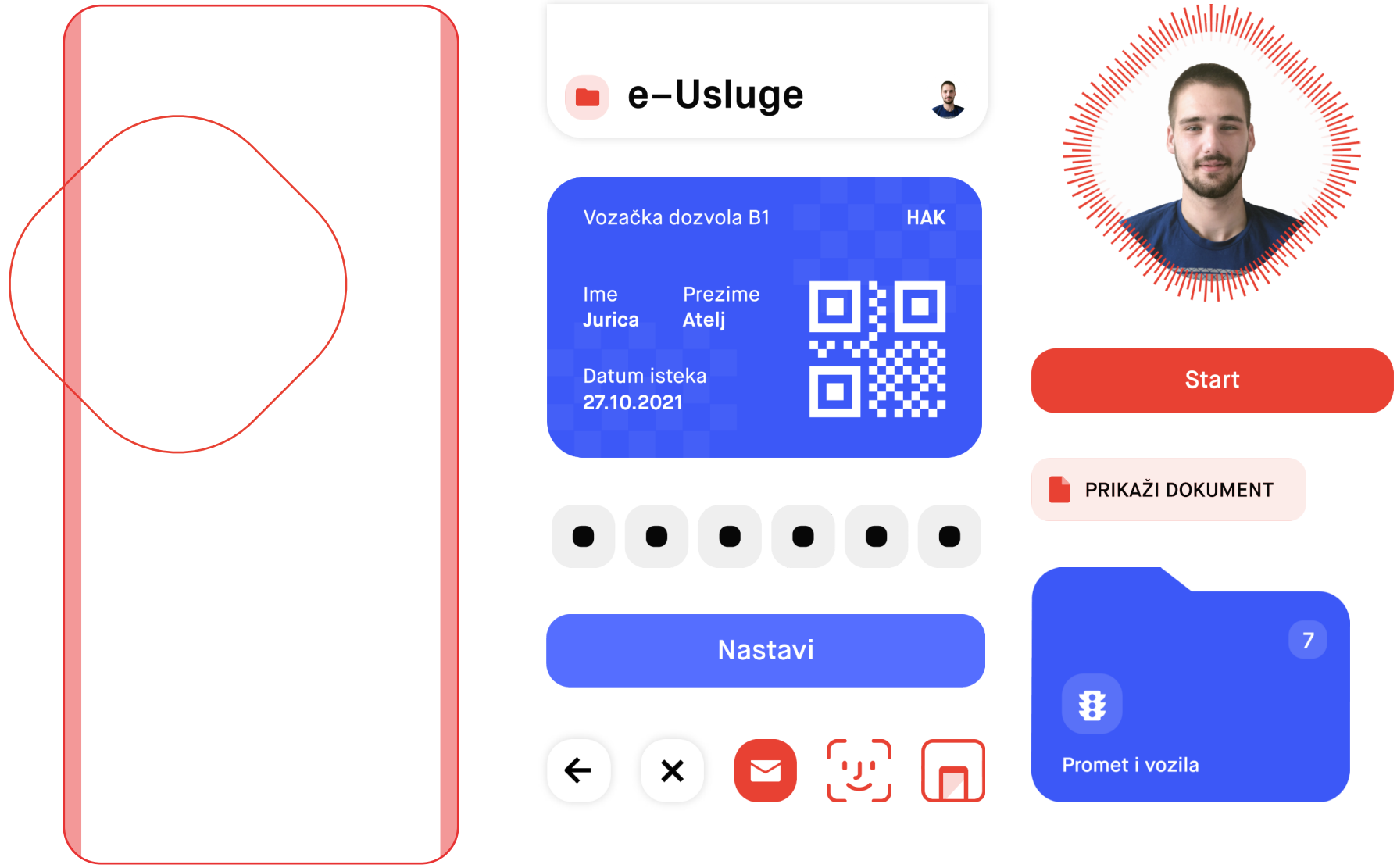
Prikaz 15 Hijerarhija tipografije



Prikaz 16 Boje



Prikaz 17 Sustav ikona



Prikaz 18 Komponente aplikacije

8.4 Funkcije unutar Digital ID aplikacije

8.4.1 Profil

Nakon obavljene aktivacije korisnik ulazi na karticu profila gdje se prikazuju sve njegove osobne informacije. Na profilu se nalazi većina podataka kao na plastičnoj osobnoj iskaznici poput imena i prezimena, spola, datuma rođenja, potpisa itd. Novost je ukidanje brojeva kartica koje zamjenjuje osobni identifikacijski broj (OIB) što znači da su svi podaci unutar sustava povezani i prepoznati pomoću jednog univerzalnog broja kojeg ima svaki korisnik. Sukladno navedenom, na dnu profila nalaze se sve dodatne kartice koje korisnik posjeduje kao što su vozačka dozvola, studentska iskaznica itd., a iste sadrže samo osnovne podatke (ime i prezime, datum isteka), dok se svi ostali potrebi podaci nalaze u QR kodu kojeg službena osoba može učitati.

8.4.2 NFC

Pomoću komunikacije bliskog polja (*eng. Near Field Communication*) korisnik može potvrđivati svoj identitet temeljem bežične tehnologije. Cijeli proces sastoji se od nekoliko jednostavnih koraka; pritiskom na Start korisnik započinje proces koji prvobitno traži biometrijske podatke za potvrdu identiteta, zatim informira da se uređaj približi drugom uređaju za slanje podataka te na kraju šalje potvrdnu informaciju o uspješnom postupku. Korištenje ove funkcije moguće je kod npr., prelaska granica, a cijeli proces nedvojbeno je vjerodostojan jer se odvija u realnom vremenu i zahtjeva biometrijske podatke koji su jedinstveni kod svakog čovjeka.

8.4.3 Token

Pomoću virtualnog tokena ugrađenog u aplikaciju korisnik može pristupiti izradi sigurnosnih podataka koji služe za prijavu i potvrde postupka u sustav e-Građani. Tako ova funkcija zamjenjuje sve postojeće dostupne vjerodajnice u sustavu e-Građani i nudi najvišu razinu sigurnosti. Proces započinje pritiskom na Start, nakon čega korisnik potvrđuje postupak biometrijom kako bi dobio korisnički broj za prijavu te jednokratni kod kao zamjenu za lozinku. Iz sigurnosnih razloga navedeni podaci aktivni su jednu minutu nakon čega je potrebno ponovno zatražiti podatke.

8.4.4 Obavijesti

Kroz obavijesti na aplikaciji korisnik prima informacije usko vezane uz digitalni identitet. To uključuje poruke o dolaznim zatraženim dokumentima i njihov pregled ulaskom u istu, kao i informacije o važnim situacijama i događajima vezane za osobna zakonska prava i obveze, kao npr. istek vozačke dozvole. Možemo reći da obavijesti unutar aplikacije zamjenjuju osobni korisnički pretinac koji trenutno postoji u Republici Hrvatskoj.

8.4.5 E-Usluge

Putem e-Usluga korisnik pristupa svim dostupnim javnim uslugama koje se nalaze na Središnjem državnom portalu, a

osnovna svrha je povezivanje svih podataka na jednom mjestu kako bi korisnik na što lakši način došao do traženih informacija. Svaka e-Usluga označena je vlastitom bojom i ikonicom, a su podijeljene u šest kategorija: zdravstvo, obrazovanje, promet i vozila, financije i porezi, pravosuđe i ostalo. Svaka kategorija unutar sebe sadrži još nekoliko podkategorija (zahtjevi, potvrde i uvjerenje, ostale usluge) koje sugeriraju na vrstu usluge te tako poboljšavaju preglednost i olakšavaju pretragu.

Obavljanje odabranog postupka podijeljeno je u sljedećih nekoliko faza:

· Opis postupka – ovdje se nalaze sve opće informacije vezane za odabranu uslugu uz prikaz dodatnih upozorenja ako isti postoje

· Osobni podaci – obavještavaju korisnika koje podatke određena institucija treba za izradu zatražene usluge. Ovaj korak je važan jer korisniku ukazuje na sve podatke koje u tom trenutku pruža institucijama

· Odabir informacija – ovdje korisnik odabire sve vrste podatka koji služe za ispunu traženog dokumenta

· Pregled postupka – u ovom dijelu korisnik može još jednom pregledati odabrane podatke prije same potvrde te odabrati vrstu autentikacije.

· Potvrda postupka – ovdje korisnik unosi PIN ili biometrijske podatke te na kraju dobiva obavijest o uspješno provedenom postupku.

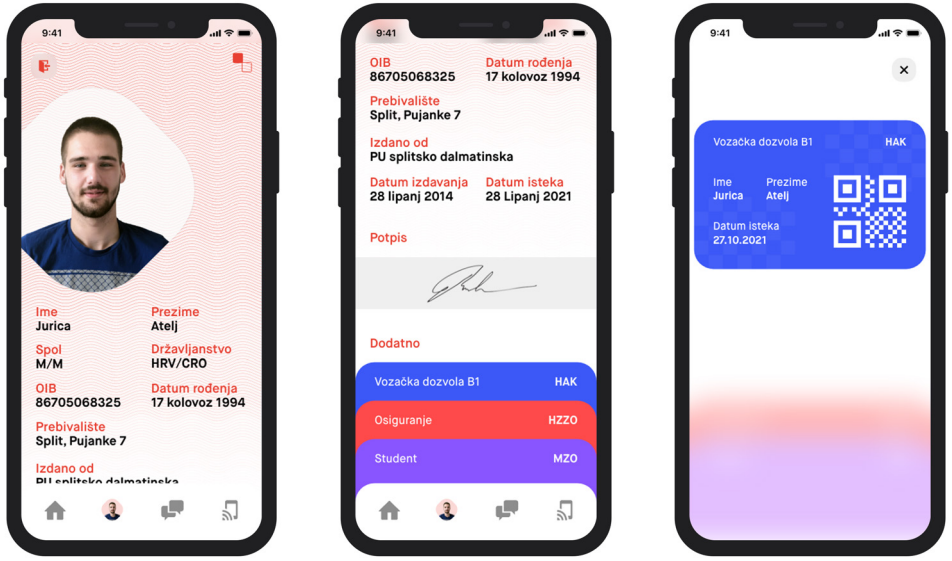
8.4.6 Dokumenti

Svi podaci zatraženi putem e-Usluga nalaze se u dokumentima. Ovdje korisnik može pronaći sva uvjerenja, potvrde i zapise koje je zatražio od tijela državne uprave. Zbog bolje preglednosti dokumenti su filtrirani po mjesecima, dok su dokumenti koji još nisu poslani ili ovjereni prikazani zasebno kako bi korisnik uvijek znao status dokumenta, ali i imao brži pristup istom. Svaki dokument može se podijeliti raznim metodama te je vidljiv u digitalno potpisanom PDF formatu koji ne može biti promijenjen. Osim navedenog, u ovom dijelu aplikacije nalazi se i **arhiva** gdje se automatski spremaju svi digitalni postupci informacijske prirode, kao npr. određeni izračuni.

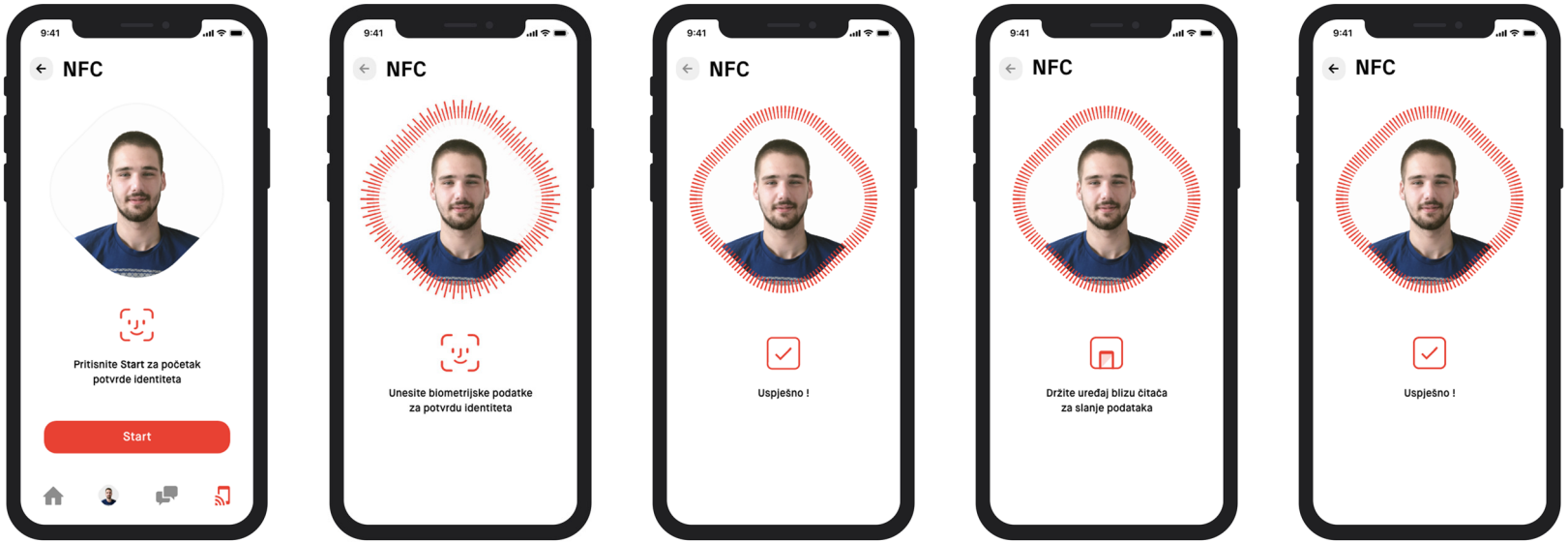
8.4.7 Log

Uloga log-a je evidentiranje svih aktivnosti koje se odvijaju unutar Croroam sustava. Ova funkcija zapravo je svojevrsni dnevnik aktivnost putem kojeg korisnik može pratiti što se događa s njegovim informacijama i postupcima.

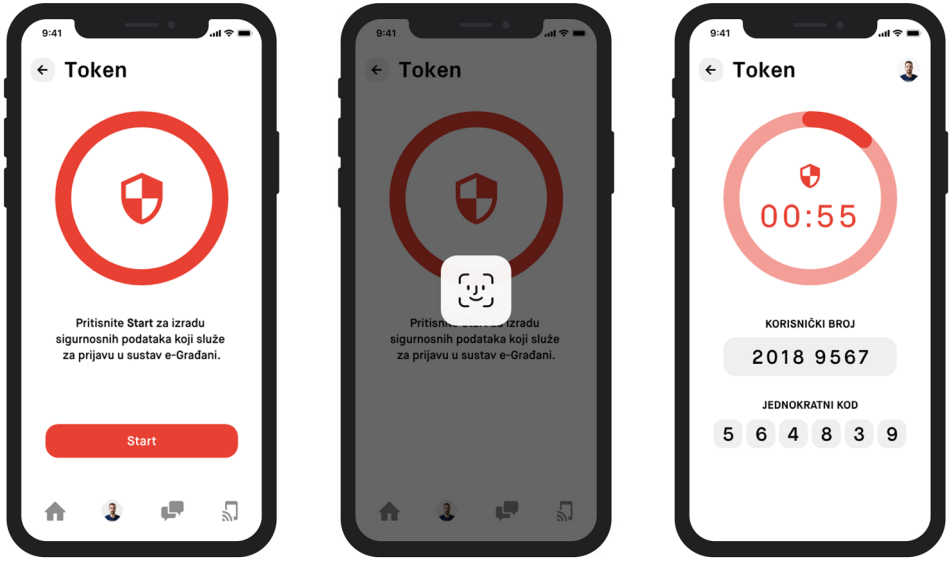
Unutar aplikacije se nalaze i **kontakti** koji sadrže sve informacije o tijelima državnih uprava te **postavke** pomoću kojih korisnik personalizira korisnički račun.



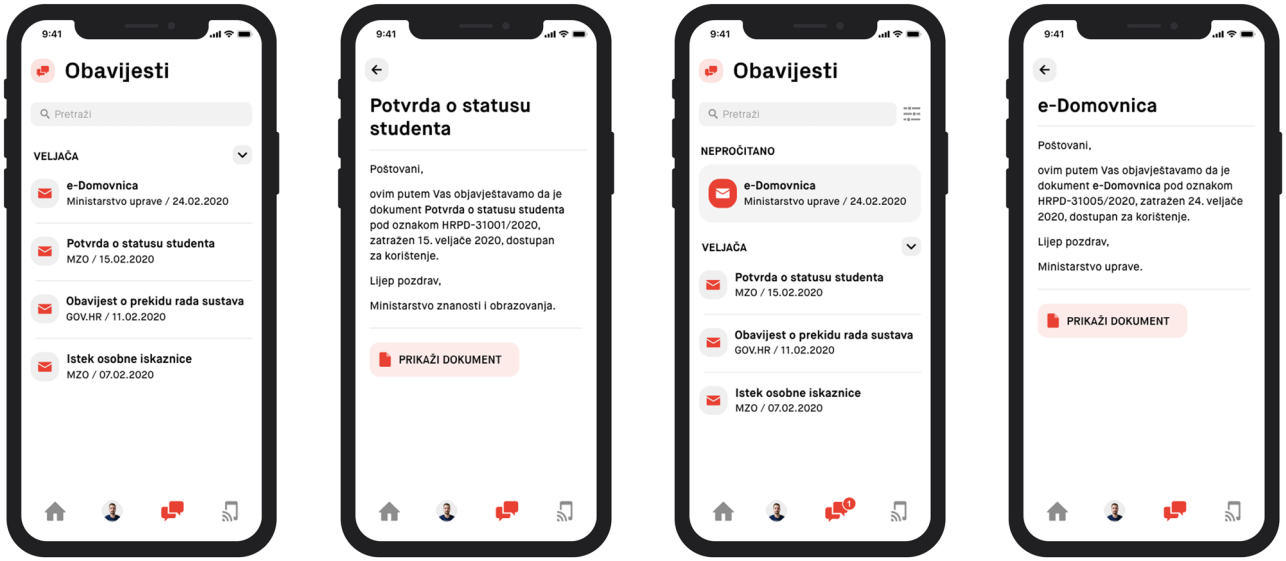
Prikaz 19 Profil



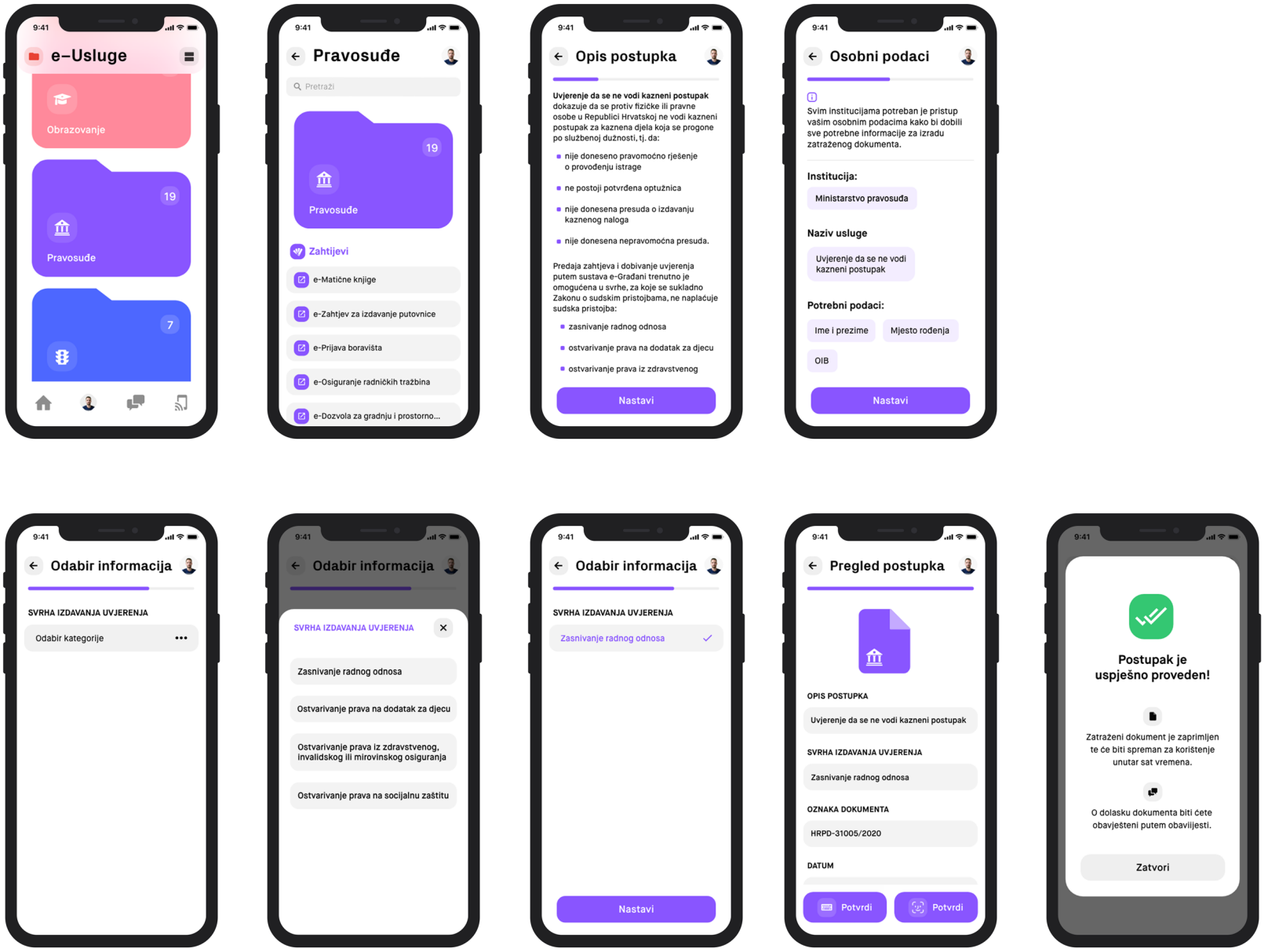
Prikaz 20 NFC



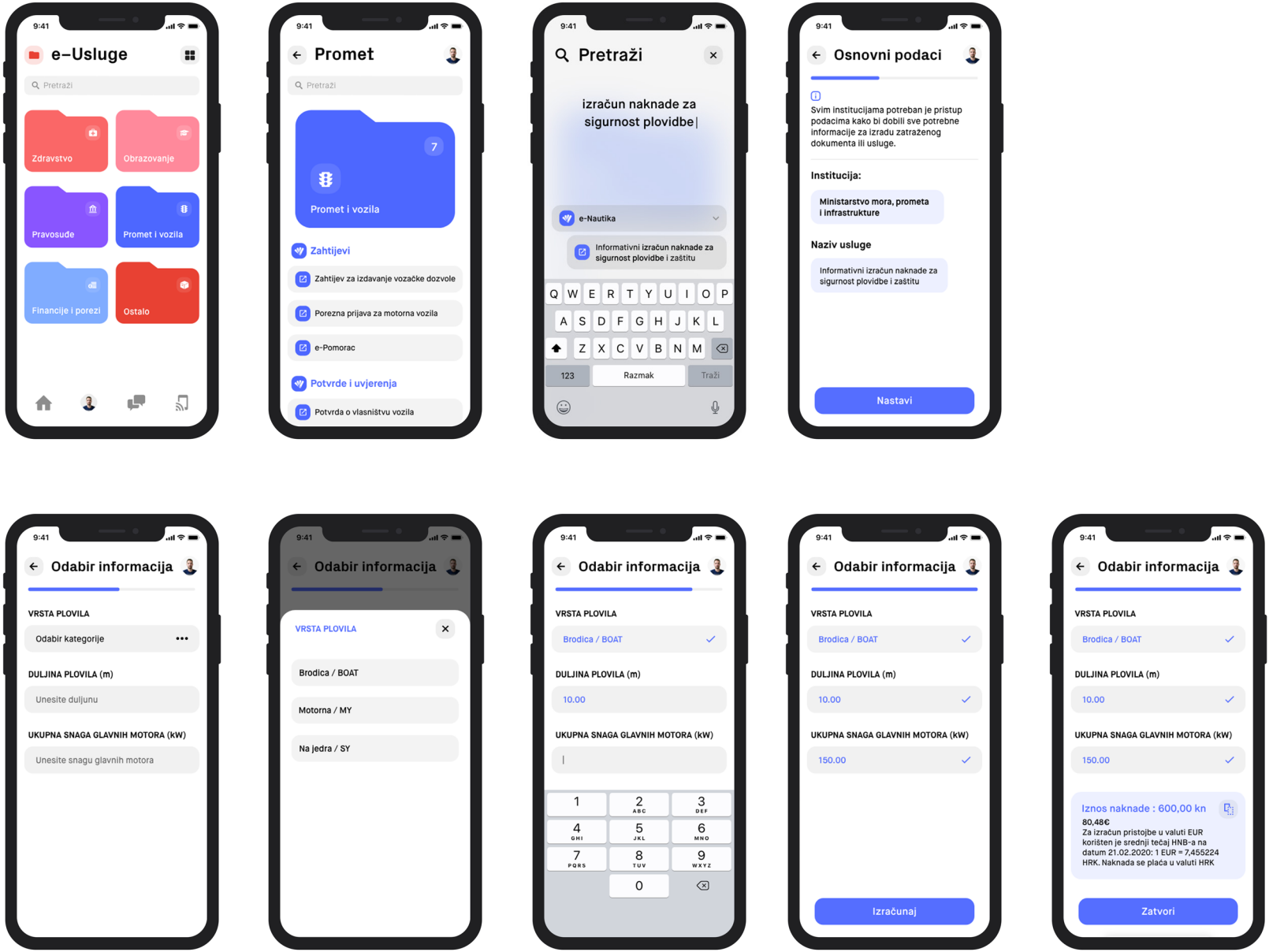
Prikaz 21 Token



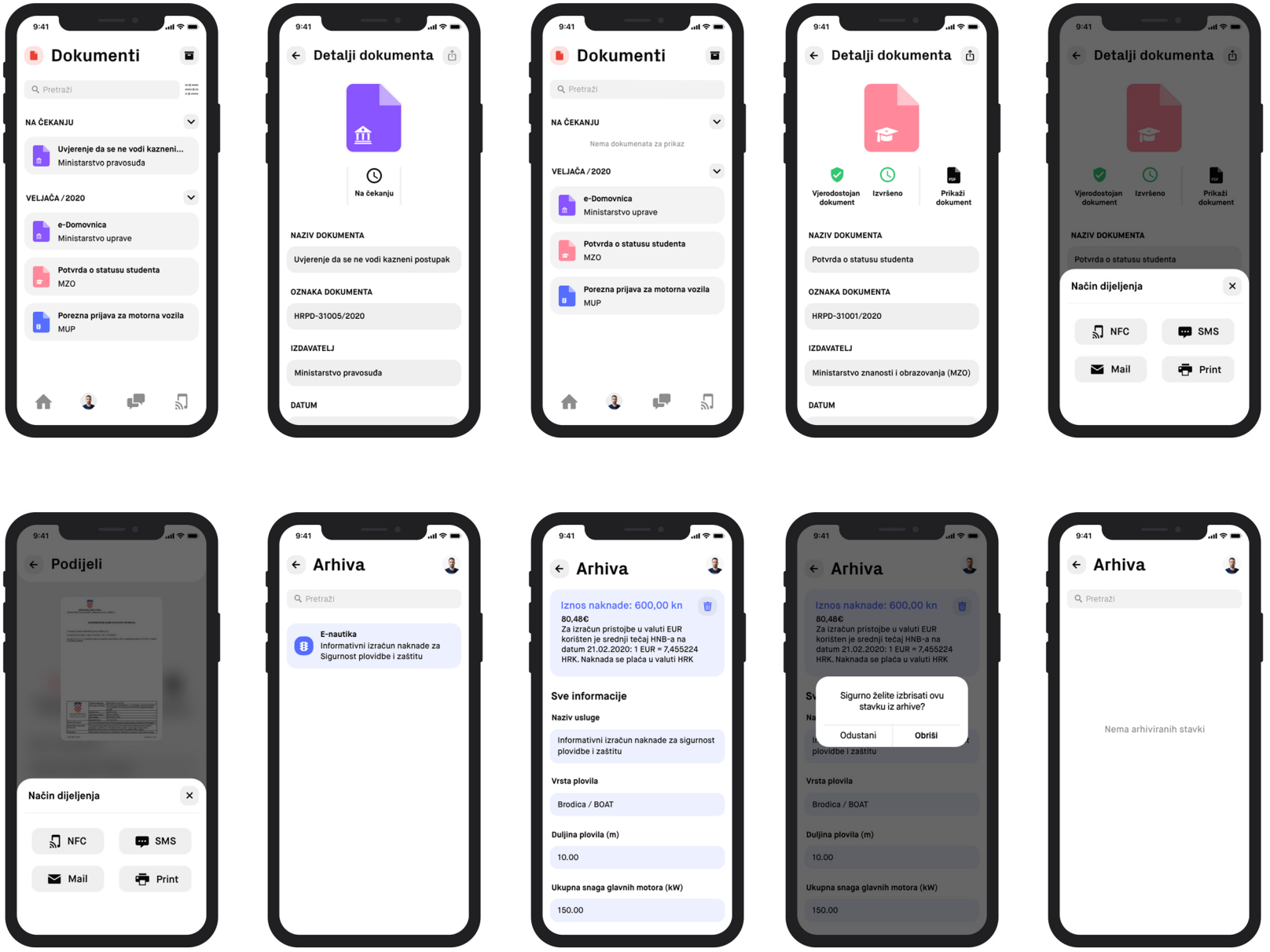
Prikaz 22 Obavijesti



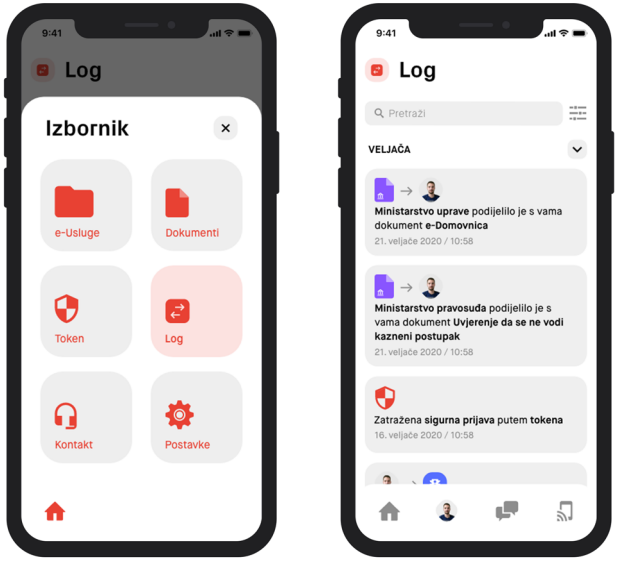
Prikaz 23 e-Usluge, poludigitalni sistem



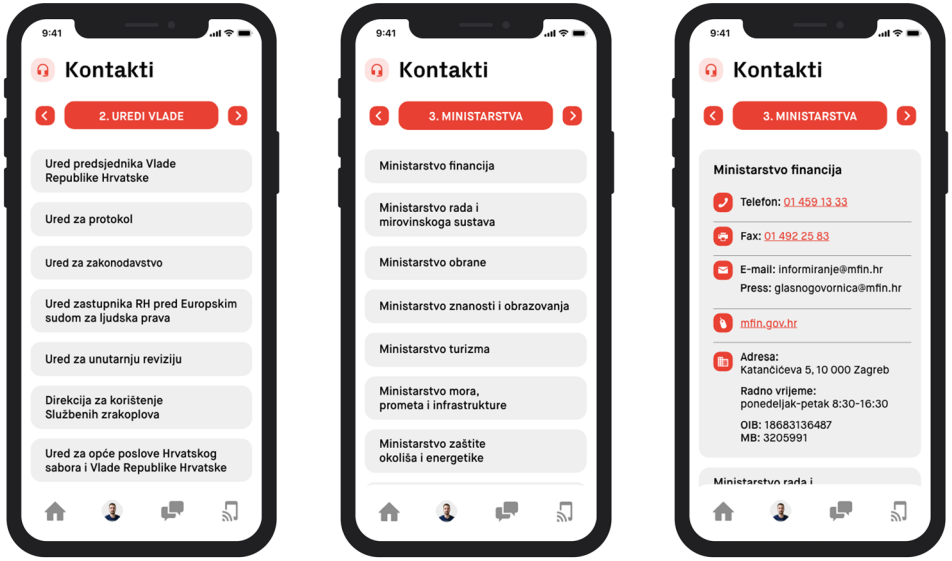
Prikaz 24 e-Usluge, digitalni sistem



Prikaz 25 Dokumenti i arhiva



Prikaz 26 Log



Prikaz 27 Kontakti

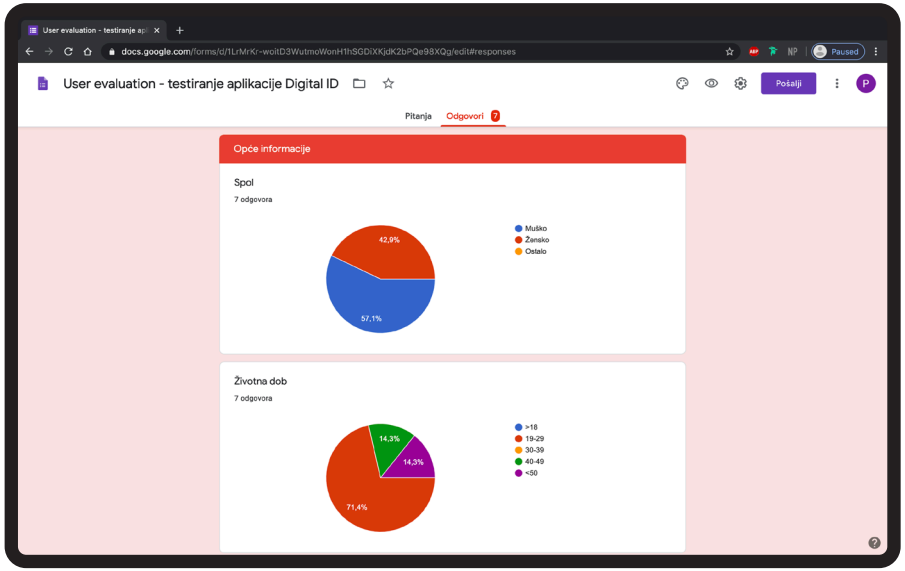
9.0 User evaluation — testiranje aplikacije

Nakon izrade prototipa slijedi testiranje korisnikove interakcije s istim kako bi uvidjeli probleme, prikupili kvalitativne i kvantitativne podatke te utvrditi zadovoljstvo sudionika.[46] Cijeli proces podijeljen je u tri glavna dijela. Prvi dio odnosi se na osnovne podatke o korisniku, kao što su spol, dob, razina obrazovanja te na odabir ponuđenih pojmova od prije poznatih korisniku. Drugi dio sadrži šest zadataka koje korisnik rješava te kasnije upisuje kroz upitnik kako bi dobili povratnu informaciju za poboljšanje prototipa. Treći dio ispituje opći dojam korisnika putem ponuđenih tvrdnji usko vezanih za prototip, ali i implementaciju istog u stvarnom svijetu.

Testiranje je uključivalo 7 osoba, od toga 57,1% ispitanika čine muškarci dok žene čine 42,9%. Najveći postotak ispitanika životne je dobi od 19-29 godina te imaju srednji ili visoki stupanj obrazovanja. Kod odabira poznatih pojmova, većina ispitanika upoznata je s terminima token i QR kod, dok je najmanje njih čulo za pojmove sigurnosni zapisnik i NFC.

Rezultati testiranja ukazali su na dobru funkcionalnost aplikacije jer veliki broj korisnika u globalu aplikaciju opisuje kao jednostavnu. Svaki korisnik obavio je zadatke bez značajnih problema; tekstualni sadržaj razumljivo je napisan, a vizualni dio jasno definira vrstu sadržaja, što dokazuje lakoću pristupa informacijama koje čine glavni segment dizajna. Kritike su uključivale modifikaciju pojedinih ikonica te arhivu koju bi jedan korisnik postavio u otvarajući izbornik, umjesto u dokumente.

Završetak testiranja navedenog prototipa rezultirao je više nego pozitivnim ishodom, putem kojeg možemo zaključiti da isti pokazuje potencijal za zadovoljavanje očekivanja pojedinaca. Zbog preglednosti i razumljivosti sadržaja većina osoba želi i preporučiti i koristiti ovakav sistem provjere identiteta te smatraju da će isti u budućnosti zamijeniti plastične osobne iskaznice.



User evaluation - testiranje aplikacije Digital ID

Pošalji

Pitanja | Odgovori 7

Zadatak 6

Da li je cijeli postupak bio dovoljno vizualno popraćen? Ako imaš nekih komentara napiši pod ostalo.

7 odgovora

Da li je tekstualni dio jasno opisivao potrebne korake? Ako nije, opiši što te zbunjivalo.

7 odgovora

- da
- zanimljivo ,znatizeljno pomalo i plasljivo misleci da ce bit tesko ali vrlo jednostavno
- sve je bilo jasno
- Tekstualni dio je bio kratak i jasan s svim potrebnim informacijama
- samo bi postavio praceni tekst prilikom biometrije prije ikone telefona

User evaluation - testiranje aplikacije Digital ID

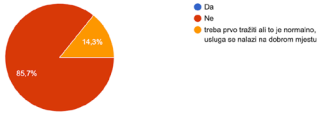
Pošalji

Pitanja | Odgovori 7

Zadatak 2

Jesi li imao/la problema s pronalaskom potrebnog uvjerenja? Ako je odgovor da, pod ostalo opiši problem.

7 odgovora



Je li sav tekstualni sadržaj dovoljno razumljiv? Jesu li upozorenja i informacije dovoljno vizualno odvojene od ostatka sadržaja?

7 odgovora

- cjeli postupak mi je bio jasan i jednostavan
- da
- Tekstualni sadržaj bio je jasno definiran, a važnije informacije bile su vizualno odvojene i lake za primjetiti
- Sve je bilo razumljivo osim ikone "home" koja otvara overlay, a nije zapravo zasebni ekran. Možda bi to trebalo prebaciti u zasebni ekran ili promijeniti ikonu

User evaluation - testiranje aplikacije Digital ID

Pošalji

Pitanja | Odgovori 7

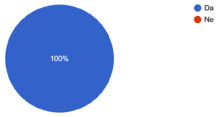
Je li povratna potvrda kod odabira informacija (npr. vrsta plovila) bila dovoljno jasna? Ako nije, što je nedostajalo?

7 odgovora

- da
- je kvacica mi je potvrdila da je odabir prihvacen
- Povratna potvrda je bila jasna
- prilagodjeno u par jednostavnih koraka doci do onog sto vas interesira
- Sve je jasno jer slova promejne boju ali dobiju i oznaku kvačice

Da li je veličina svakog teksta dovoljno vidljiva?

7 odgovora



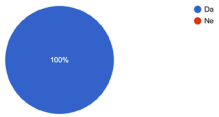
User evaluation - testiranje aplikacije Digital ID

Pošalji

Pitanja | Odgovori 7

Jesu li sve informacije (npr. tekst, vizualni prikaz) bile razumljivijive?

7 odgovora



Kakav je po težini/kompleksnosti postupak aktivacije? Ako ima nekih nejasnoća napiši ovdje.

7 odgovora

- jasno sve
- vrlo lako
- poprilično jednostavan, uredan te jasan postupak
- Veoma jednostavan i intuitivan
- Nisam imao nikakih poteškoća prilokom aktivacije aplikacije
- razumljiv i jednostavan nacin za uporabu

10.0 Zaključak

Pojavom digitalnog doba, masovni razvoj tehnologije duboko ulazi u sve sfere života te uvodi milijarde ljudi u internetski svijet koji kao rezultat nudi brzi pristup informacijama, neovisno o vremenu ili mjestu. Sve to utječe na nove načine komuniciranja koji stvaraju potrebu za digitalnim identitetom. Mogućnost da osoba dokaže vlastiti identitet i potvrdi isti čine prvu stavku koja osigurava osnovnu kvalitetu života i neometano sudjelovanje u svim društvenim aktivnostima. U brzo promjenjivom digitalnom dobu koncept identiteta postaje sve kompleksniji; osoba može imati jedan osobni identitet na temelju stvarne fizičke cjeline, a opet imati više digitalnih ili virtualnih identiteta na temelju različitih osobnih profila.

Osim što digitalni identitet utječe na način komunikacije vlade s građanima i razvoj državnih tijela, isti može potencijalno stvoriti velike uštede za vladu, poduzeća i građane te tako povećati transparentnost i poticati na inovacije u pružanju usluga. Za izradu kvalitetnog identifikacijskog sustava svaka vlada mora potrošiti dovoljno vremena i resursa kako bi finalni rezultat imao pozitivan učinak koji može dostići visoki stupanj učinkovitosti i doprinijeti poboljšanju životnog standarda. Međutim, još uvijek postoje problemi koji uključuju pitanja vezana za privatnost i zaštitu podataka te nedostatak dobro postavljenog pravnog okvira, što otežava održivost ovakvog sustava. Da bi stvorili učinkovite sustave koji su prije svega pouzdani, glavni akteri moraju raditi na ublažavanju navedenih problema.

Dolazak pametnog telefona zauvijek mijenja načine pristupanja traženim uslugama pa nije ni čudno što su tehnološki razvijene zemlje poput Finske i Estonije postavile mobitel kao novog nositelja identiteta korisnika. Upravo zbog svoje dostupnosti, ali i zbog brojnih funkcionalnosti, mobitel pruža raznovrsne mogućnosti za rješavanje prepreka vezanih uz identitet korisnika. Sukladno tomu, mobilni telefon može poslužiti kao uređaj za provjeru autentičnosti, ali može djelovati i kao nositelj fizičkih vjerodajnica. Pitanje identiteta postaje važnije nego ikad, a pametni telefoni kao sigurne i fleksibilne platforme za upravljanje osobnim identitetom mogu pružiti učinkovite opcije za rješavanje problema.

Projekt Digital ID bazira se na digitalizaciji osobne iskaznice u Republici Hrvatskoj, odnosno otkriva kako bi spomenuti dokument funkcionirao u digitalnom kontekstu. Osobni odlazak po certifikate i jednostavna registracija u kombinaciji s visokom razinom pouzdanosti, zadovoljavaju sve standarde te pružaju najvišu sigurnost. Decentralizacija sustava donosi bolji nadzor nad osobnim podacima te pojednostavljuje komunikaciju i razmjenu informacija između građana, vlade i javnog sektora. Jednostavno korisničko sučelje popraćeno razumljivim tekstualnim i vizualnim sadržajem olakšava korištenje aplikacije te cijeli proces čini prirodnim. Digital first pristup bitan je

za razvitak svake zemlje, a potpuna digitalizacija osobnog dokumenta definitivno postaje budućnost u kojoj funkcionalnost, točnost i sigurnost dobivaju na snazi i olakšavaju svakodnevno potvrđivanje identiteta korisnika, kako u stvarnom tako i u digitalnom svijetu.

11.0 Literatura

1. E-Government, Wikipedia, https://en.wikipedia.org/wiki/Egovernment#Definition, [pristupljeno: 17. Listopad 2018]

2. Kos, I., E-uprava, Hrčak, https://webcache.googleusercontent.com/search?q=cache:gdserK6aiYMJ:https://hrcak.srce.hr/file/284170+&cd=1&hl=hr&ct=clnk&gl=hr, [pristupljeno 15. Listipad 2018]

3. Musa, A (2006), Digitalna podjela: E-uprava i pitanje pristupa, CROSBI Hrvatska znanstvena bibliografija, 953-6071-28-2 https://www.pravo.unizg.hr/_download/repository/Anamarija_Musa_E-uprava_i_problem_digitalne_podjele_2006%5B1%5D.pdf, [pristupljeno 17. Listopad 2018]

4. E-Government, Basel insitute of governance, < https://www.baselgovernance.org/e-government#footnotes)> [pristupljeno 17. listopad 2018]

5. O središnjem državnom portalu, Vlada Republike Hrvatske < https://vlada.gov.hr/sredisnji-drzavni-portal/203> [pristupljeno 18 listopada 2018]

6. O sustavu e-građanin, Središnji državni portal, < https://gov.hr/e-gradjani/o-sustavu-e-gradjani/1584 [pristupljeno 18. listopada 2018]

7. E-Estonia, < https://e-estonia.com/>, [pristupljeno 18. listopada 2018]

8. Denmark leads the world in digital government, GovInsider, <https://govinsider.asia/innovation/denmark-online-services-digital-government-australia-korea/>, [pristupljeno 18. Listopad 2018]

9. Credentials, Techopedia, <https://www.techopedia.com/definition/10259/credentials> [pristupljeno 16. Siječanj 2019]

10. Authentication, Techopedia, <https://www.techopedia.com/definition/342/authentication> [pristupljeno 16. Siječanj 2019]

11. Credentials, Technopedia, <https://www.techopedia.com/definition/10259/credentials> [pristupljeno 16. Siječanj 2019]

12. Prijedlog koncepta integriranog središnjeg sustava autentikacije i autorizacije, Scribd, <https://www.scribd.com/doc/40313895/Prijedlog-koncepta-integriranog-sredio161njeg-sustava-autentikacije-i-autorizacije-Verzija-1-1>, [pristupljeno 16. Siječnja 2019]

13. Kriteriji za određivanje razine osiguranja kvalitete autentifikacije, Vlada Republike hrvatske <https://www.gov.hr/UserDocsImages/e-Gradjani_dok/NIAS%20-%20Kriteriji%20za%20odredjivanje%20razine%20osiguranja%20kvalitete%20autentifikacije%20u%20sustavu%20NIAS%20(Ver.%201.2).pdf>, [pristupljeno 16. siječnja 2019]

14. Dvostruka ili višestruka autorizacija, Pcchip, <https://pcchip.hr/softver/sigurnost/dvostruka-ili-visestruka-autorizacija/>, [pristupljeno 17. siječanj 2019]

15. Što je digitalni certifikat, Fina, <https://www.fina.hr/sto-je-to-digitalni-certifikati>, [pristupljeno 17 siječnja 2019]

16. E-potpis, Ministarstvo zdravstva, poduzetništva i obrta, <https://www.mingo.hr/page/kategorija/e-potpis>, [pristupljeno 17 siječnja 2019]

17. Što treba znati o vjerodajnici tipa ime/lozinka, Sys portal Carnet <https://sysportal.carnet.hr/node/1413>, [pristupljeno 17. siječnja 2019]

18. Boban M., Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava, Hrčak, < https://hrcak.srce.hr/142285>, [pristupljeno 18. siječnja 2018]

19. Zaštita podataka i privatnost na internetu, Službena internetska stranica Europske unije, < https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_hr.htm>, [pristupljeno 12. veljače 2019]

20. Boban, M., Zaštita osobnih podataka i nova EU uredba o zaštiti podataka, Hrčak, <https://hrcak.srce.hr/193680>, [pristupljeno 12. veljače 2019]

21. EU Opća uredba o zaštiti podataka "Definicije", Privazy plan, < https://www.privacy-regulation.eu/hr/4.htm>, [pristupljeno 12. veljače 2019]

22. Mobilne aplikacije #AZOP i #GDPR na dlanu, Agencija za zaštitu osobnih podataka <https://azop.hr/info-servis/detaljnije/mobilne-aplikacije-azop-i-gdpr-na-dlanu>, [pristupljeno 13. veljače 2019]

23. Zaštita digitalnog-sadržaja i pojedinca u digitalnom okruženju, E-škole, <https://pilot.e-skole.hr/wp-content/uploads/2018/08/Prirucnik_Zastita-digitalnog-sadrzaja-i-pojedinca-u-digitalnom-okruzenju.pdf>, [pristupljeno 13. veljače 2019]

24. Korisničko iskustvo, Wikipedia, <https://hr.wikipedia.org/wiki/Korisni%C4%8Dko_iskustvo#cite_note-3>, [pristupljeno 04. ožujka 2019]

25. What Is User Experience Design? Overview, Tools And Resources, Smashing magazine, < https://www.smashingmagazine.com/2010/10/what-is-user-experience-design-overview-tools-and-resources/#top>, [pristupljeno 04. ožujka 2019]

26. User Interface (UI) Design, Interaction design foundation, < https://www.interaction-design.org/literature/topics/ui-design>, [pristupljeno 04. ožujka 2019]

27. What is UI & UX Design, Hackernoon, <https://hackernoon.com/what-is-ui-ux-design-1f01e9dbbf02> [pristupljeno 04. užujka 2019]

28. Creating a User-Centered Approach in Government, Usability.gov, <https://www.usability.gov/what-and-why/user-centered-government.html> [pristupljeno 04. užujka 2019]

29. Upotrebljivost, Dizajn.hr, < http://dizajn.hr/blog/upotrebljivost/>, [pristupljeno 04 ožujka 2019]

30. Digitalna pristupačnost, Središnji državni ured za razvoj digitalnog društva, <https://rdd.gov.hr/digitalna-pristupacnost/254>, [pristupljeno 16. svibnja 2020]

31. Accessibility for everyone - making public service websites inclusive has become a legal requirement, Valtech, < https://www.valtech.com/en-gb/insights/accessibility-for-everyone/>, [pristupljeno 16. svibnja 2020]

32. Biometric in film true or false, Veridiumid Trusted digital identity <https://veridiumid.com/blog/biometrics-in-film-true-or-false/>, [pristupljeno 13. veljače 2019]

33. Terrorism is just an excuse ("Snowden", O. Stone), Zicer.hr, <https://www.ziher.hr/recenzija-terrorism-is-just-an-excuse-snowden-o-stone/>, [pristupljeno 13. veljače 2019]

34. Džepni priručnik za zaštitu podataka i skrivanje od nadzora, Drugo more, <http://drugo-more.hr/skrivanje-od-nadzora/>, [pristupljeno 13. veljače 2019]

35. USB Killer, Spekulativno, < http://speculative.hr/hr/usb-killer-hr/>, [pristupljeno 18. siječanj 2019]

36. The Hypr-3 lets you make secure payments with your finger, Cnet, <https://www.cnet.com/reviews/hypr-3-preview/>, [pristupljeno 17. siječnja 2019]

37. Smart ID, Smart ID, <https://www.smart-id.com/>, [pristupljeno, 12. svibanj 2019]

38. Apple pay, Apple, <https://www.apple.com/apple-pay/>, [pristupljeno 12. svibnja 2019]

39. Digital identity, Wikipedia, < https://en.wikipedia.org/wiki/Digital_identity> [pristupljeno 16. lipnja 2020]

40. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, World Bank Group / GSMA / Secure Identity Alliance Discussion Paper, <https://secureidentityalliance.org/publications-docman/public/4-july-2016-report-digital-identity/file> [pristupljeno 16. lipnja 2020]

41. Mobile Identity – Delivering secure, accessible and trusted services to the public, World Bank Group / GSMA / Secure Identity Alliance Discussion Paper, <https://mobileworldcapital.com/ID_M/mIDENG/MWCapital_mID_vENG.pdf> [pristupljeno 16. lipnja 2020]

42. What exporting a country and its digital infrastructure looks like, Rubiks Digital, <https://blog.rubiksdigital.com/what-exporting-a-country-and-its-digital-infrastructure-looks-like-c809f2c87228> [pristupljeno 16. lipnja 2020]

43. Pitanje (kulturno-umjetničkog) identiteta, Vizkultura, https://vizkultura.hr/pitanje-kulturno-umjetnickog-identiteta/?fbclid=IwAR2v-7Y2flSuPB3Ag6DP39phhXOR0a31OfeQshW8eQD85jpgWs_mX0wOq54 [pristupljeno, 16. lipanj 2020]

44. Px Grotesk, Optimo <https://www.optimo.ch/typefaces_Px-Grotesk_all_FontInformation.html> [pristupljeno 16. lipnja 2020]

45. Maison Neue, Typewolf, < https://www.typewolf.com/site-of-the-day/fonts/maison-neue> [pristupljeno 16. lipnja 2020]

46. Usability testing, Usability.gov, <https://www.usability.gov/how-to-and-tools/methods/usability-testing.html> [pristupljeno 16. lipnja 2020]