REPUBLIKA HRVATSKA
Ministarstvo pravosuđa, uprave i digitalne transformacije

Povezivanje na mobilnu platformu mGrađani – tehnički, funkcionalni i procesni aspekt

Sadržaj

Povezivanje na mobilnu platformu mGrađani – tehnički, funkcionalni i procesni aspekt 1
1. Pregled arhitekture mobilne platforme m-Građani 3
1.1. Mobilna aplikacija mGrađani 3
1.2. Mobilna platfoma mGrađani 4
1.3. API gateway platforma 5
1.4. Vanjski servisi pružatelja usluga 5
1.5. Integracija s NIAS-om 6
2. Integracija m-usluga na mobilnu platformu 7
2.1. Aktivnosti na strani tijela (pružatelja usluge) 7
2.2. Aktivnosti na strani MPUDT 8

1. Pregled arhitekture mobilne platforme m-Građani

Mobilna platforma m-Građani osmišljena je kao višeslojni sustav koji povezuje mobilnu aplikaciju za građane s postojećim državnim e-uslugama putem centralnih komponenti. Arhitektura obuhvaća sljedeće glavne dijelove:

- **Mobilna aplikacija mGrađani:** Mobilna aplikacija na pametnom telefonu korisnika (Android/iOS) koja pruža sučelje za korištenje dostupnih javnih usluga.
- **Mobilna platforma (poslužiteljski dio):** Poslužiteljski sustav smješten u državnom oblaku Centra dijeljenih usluga (CDU) koji poslužuje zahtjeve aplikacije, omogućuje kreiranje novih usluga i formi, upravljanje korisničkim podacima te konfiguraciju usluga od strane administratora.
- **API gateway platforma:** Sloj koji osigurava standardiziranu komunikaciju između mobilne platforme i pozadinskih sustava pružatelja m-usluga. Za sve integracije koristi se državna sabirnica (GSB-Government Service Bus), koja djeluje kao centralni middleware za razmjenu podataka između m-platforme i sustava tijela javne uprave. GSB omogućuje konsolidaciju protokola i sigurnosnih mehanizama za sve povezane servise.
- **Vanjski servisi pružatelja usluga:** Pozadinski sustavi tijela državne uprave koji pružaju konkretnu e-uslugu. Ta tijela svoje usluge izlažu putem GSB-a (kao SOAP ili REST servise), a mobilna platforma im pristupa na standardiziran način.
- **Integracija s NIAS-om**: Integracija s NIAS-om ključna je za autentifikaciju i autorizaciju korisnika unutar m-Građani aplikacije. NIAS je centralizirani sustav koji osigurava identifikaciju korisnika koristeći sigurnosne standarde kao što su SAML (Security Assertion Markup Language) i OpenID Connect (OIDC). Primjenom OIDC-a omogućuje se sigurnija i brža autentifikacija korisnika prilikom pristupa m-Uslugama, jer se osigurava fleksibilnija i laganija implementacija autentifikacijskog toka, a sve kroz API-je koji su prilagođeni mobilnim okruženjima.

Komunikacija unutar sustava odvija se isključivo kroz sigurnosne slojeve. Svi zahtjevi iz mobilne aplikacije prolaze kroz API gateway na GSB-u, gdje se vrši autentikacija i autorizacija prije prosljeđivanja prema ciljnom servisu. Ovakav arhitektonski pristup osigurava da su svi podaci koji putuju između mobilne aplikacije, platforme i državnih sustava zaštićeni i da se primjenjuju jedinstvena pravila razmjene podataka.

1.1. Mobilna aplikacija mGrađani

Mobilna aplikacija omogućuje korisnicima pristup različitim digitalnim javnim uslugama (m-uslugama).

Mobilna aplikacija mGrađani u trenutku uspostave sadrži početnih 20 mobilnih usluga. Nakon integracije početnih 20 usluga, slijedi daljnje uključivanje javnih usluga, a cilj je da s

vremenom mobilna aplikacija m-Građani postane jedinstvena aplikacija koja će građanima trebati za pristup javnim uslugama koje država pruža putem mobilnih uređaja.

Mobilna aplikacija može se preuzeti s App Store-a (iOS) ili Google Play trgovine (Android). Nakon instaliranja aplikacije na mobilni uređaj, vrši se aktivacija aplikacije. Aktivaciju aplikacije moguće je izvršiti na 2 načina - isključivo putem mobilne aplikacije (NIAS prijava) ili putem mobilne aplikacije i računala (QR kod). Aktivacija mobilne aplikacije putem NIAS prijave provodi se prijavom putem vjerodajnica visoke, značajne ili niske razine sigurnosti.

Aktivacija mobilne aplikacije putem QR koda provodi se putem stranice e-Građani gdje korisnik odabere opciju registracije mobilne aplikacije. Korisnik u mobilnoj aplikaciji m-Građani skenira QR kod te započinje proces aktivacije.

Nakon aktivacije mobilne aplikacije, korisnik odabire sigurnosni mehanizam za pristup aplikaciji (PIN ili biometrijske metode dostupne na mobilnom uređaju - otisak prsta, prepoznavanje lica), tako da svaki sljedeći puta ulazi u mGrađani aplikaciju koristeći postavljene sigurnosne mehanizme.

Na početnom ekranu mGrađani aplikacije prikazuje se zaslon s osnovnim informacijama o korisniku, popisom usluga, označenih favorita te nedavno korištenih usluga. Na dnu ekrana nalaze se ikonice za vraćanje na početni ekran, korisnički pretinac, karticu s obavijestima te postavkama profila.

Usluge su dostupne kroz tražilicu usluga, zatim odabirom usluga kroz kategorije usluga (promet i vozila, rad, zdravlje, poslovanje, obitelj i život, pravna država i sigurnost, aktivno građanstvo, odgoj i obrazovanje, financije i porezi) ili odabirom usluga iz abecednog popisa usluga.

1.2. Mobilna platfoma mGrađani

Mobilna platforma predstavlja sustav za izlaganje digitalnih javnih usluga putem mobilnih uređaja. Pristup mobilnoj platformi imaju administratori sustava, a omogućava kreiranje novih usluga za izlaganje putem aplikacije m-Građani, definiranje formi usluga, prilagođavanje korisničkog sučelja svake pojedine usluge, upravljanje korisničkim računima, konfiguraciju postavki i verifikaciju novih usluga.

Glavne dvije komponente koje omogućavaju kreiranje usluga su:

- Konfigurator usluga: Komponenta se koristi za konfiguriranje novih usluga, kao i za ažuriranje i održavanje postojećih usluga. Konfigurator je drag & drop alat unutar kojeg su predefinirane komponente koje se dodatno definiraju za svaku komponentu ekrana mobilne usluge. Gradivni elementi konfiguratora usluga su: layout, header, tab, section, component (info, form, list).

- API postavke: Funkcionalnost API postavki omogućuje administratoru mobilne platforme definiranje API metoda koje se koriste kao izvor podataka usluga. Svaka definicija metode administrativno je vezana za organizaciju (vlasnika/pružatelja usluge). Metodama je potrebno definirati naziv, putanju, vrstu HTTP metode (GET, POST, PUT, DELETE). Administrator ima mogućnost definiranja request bodyja sukladno API specifikacijama. Unutar request bodyja mapiraju se ulazni podaci s layouta koji se šalju kao dio poziva metode. Postoji mogućnost definicije različitih uvjeta na osnovu odgovora metode, a svaki odgovor se mapira na različite akcije.

1.3. API gateway platforma

API gateway predstavlja centralnu točku pristupa svim API zahtjevima, koja osigurava upravljanje prometom i autentifikacijom. Zaprima HTTP zahtjeve od aplikativnih servisa te ih usmjerava ka odgovarajućim servisima pružatelja usluga na osnovu definiranih ruta i pravila.

1.4. Vanjski servisi pružatelja usluga

Mobilna aplikacija sadrži usluge različitih tijela, pri čemu su usluge integrirane s različitim servisima i vanjskim sustavima putem API-ja. Dinamički podaci sadržani unutar pojedinih usluga mobilne aplikacije, pozivaju se putem API servisa koji dohvaćaju te podatke iz backend sustava tijela (pružatelja usluga).

API arhitektura platforme m-Građani definirana je kako bi pružila učinkovit, siguran i skalabilan način za pristup i interakciju s javnim digitalnim uslugama putem mobilnih uređaja. Ova arhitektura temelji se na web standardima i protokolima koji omogućuju jednostavnu integraciju, transparentnost i sigurnost podataka.

API sučelja za m-usluge koriste REST (Representational State Transfer) arhitektonski stil, koji se temelji na standardnim HTTP metodama, kao što su GET, POST, PUT i DELETE. JSON je korišten kao primarni format za razmjenu podataka između klijenata i servera u mGrađani platformi.

Komponente API arhitekture uključuju klijenta (mobilnu aplikaciju mGrađani), koja komunicira sa serverom putem RESTful API-ja. Klijent šalje HTTP zahtjeve prema serveru i prima odgovore u JSON formatu. Server obrađuje sve zahtjeve primljene od klijenata, pristupa odgovarajućim bazama podataka ili sustavima te generira odgovore. Server koristi više slojeva sigurnosti kako bi osigurao zaštitu podataka i spriječio neovlašteni pristup:

- API Gateway (GSB),

- autentifikacijski sloj koji omogućava sigurnu autentifikaciju korisnika koristeći OAuth2 protokol i integraciju s NIAS sustavom,
- Servisi za obradu zahtjeva: Svaki API zahtjev povezan je s odgovarajućim sustavom, tj. bazom podataka pružatelja usluga kako bi se obradili korisnički podaci i generirali odgovori.

1.5. Integracija s NIAS-om

Mobilna platforma koristi OpenID Connect (OIDC) protokol, koji je nadogradnja NIAS sustava za potrebe mobilnih i API integracija. OAuth2 se koristi za autentifikaciju i autorizaciju korisnika unutar platforme m-Građani.

Proces autentikacije (NIAS OIDC): Pri pokretanju aplikacije, korisnik se prijavljuje kroz NIAS modul integriran u m-Građani. Korisniku se prikaže NIAS ekran za prijavu gdje odabire vjerodajnicu s Liste prihvaćenih vjerodajnica. Nakon uspješne autentikacije, NIAS izdaje OIDC ID token i pristupni token koji sadrže informacije o korisniku. Ključna informacija je jedinstveni identifikator korisnika – OIB (Osobni identifikacijski broj), koji NIAS dodjeljuje svakom e-Građani računu. Mobilna platforma preuzima token i dalje ga koristi za autorizaciju pristupa API pozivima.

NIAS omogućuje različite razine autentikacije (tzv. LOA – Level of Assurance). Svaka m-usluga definira minimalnu potrebnu razinu vjerodajnice. NIAS će prilikom prijave osigurati da korisnik odabere odgovarajuću vjerodajnicu; ako korisnik nema dovoljnu vjerodajnicu, neće moći pristupiti toj usluzi i tražiti će ga prijavu s vjerodajnicom zahtijevane razine sigurnosti.

Nakon što NIAS potvrdi identitet, mobilna platforma svaku daljnju komunikaciju s backend servisima autorizira OAuth2 pristupnim tokenom. Token (oblik JSON Web Token – JWT) šalje se kao dio svakog API zahtjeva prema GSB-u, a GSB/API gateway provjerava token prije prosljeđivanja poziva dalje. Time se osigurava da samo autentificirani korisnici mogu izvršavati pozive. Backend servisi ne moraju zasebno autentificirati korisnika – oni vjeruju tokenu kojeg je izdao NIAS, no mogu iz njega pročitati korisnički identifikator (OIB) i druge atribute potrebne za poslovnu logiku.

2. Integracija m-usluga na mobilnu platformu

Prije integracije m-usluge na mobilnu platformu mGrađani, pružatelj usluge i MPUDT će definirati sljedeće elemente:

- spremnost institucije/pružatelja usluge za provedbu aktivnosti potrebnih za integraciju usluge u digitalnu mobilnu platformu

- funkcionalne karakteristike, koje podrazumijevaju analizu prikladnosti korištenja pojedine usluge na mobilnim uređajima

-tehnološke karakteristike koje usključuju analizu podataka o tehnološkoj izvedbi postojećih usluga, primijenjenim tehnologijama, sigurnosnim zahtjevima te mogućnostima integracije na mobilnu platformu

- UX karakteristike usluge koje daju dodatan uvid u prikladnost korištenja na mobilnim uređajima.

Nakon provedene analize po navedenim područjima, donijet će se odluka o daljnjim aktivnostima. Ukoliko se nakon provedene analize utvrdi da su svi preduvjeti zadovoljeni, kreće se u daljnu realizaciju aktivnosti.

2.1. Aktivnosti na strani tijela (pružatelja usluge)

Proces uključuje sljedeće aktivnosti na strani pružatelja usluge kako bi se uspostavila mobilna usluga na mobilnoj platformi/aplikaciji mGrađani:

- **specifikacija API metoda** servisa koji se izlaže. Pružatelj usluge treba dokumentirati svoje API metode u obliku OpenAPI (Swagger) specifikacije. Specifikacija opisuje krajnje točke (endpointe), metode, strukture podataka zahtjeva i odgovora, te potrebne parametre i zaglavlja.

- **Izlaganje REST API-ja na GSB-u**, budući da mobilna platforma komunicira isključivo RESTful protokolom preko HTTPS-a, razmjenjujući JSON podatke. Ako servis koristi SOAP, potrebno je uvesti sloj za transformaciju SOAP poruka u REST/JSON. U okviru projekta m-Građani predviđena je upotreba GSB-a kao integracijskog posrednika koji postojeći SOAP servis “umota” u REST API bez izmjene pozadinskog sustava. Time se klijentima (mobilnoj aplikaciji) prezentira moderno REST sučelje, dok se u pozadini pozivi prevode u postojeće SOAP operacije. Tijelo/pružatelj usluge dostavlja potrebne detalje: URL ili naziv WSDL-a postojećeg servisa, opis željenih metoda, potrebne parametre, te sigurnosne zahtjeve.

- **Prilagodba procesa autentifikacije.** Primjenom OIDC-a omogućuje se sigurnija i brža autentifikacija korisnika prilikom pristupa m-Uslugama, jer se osigurava fleksibilnija i laganija implementacija autentifikacijskog toka, a sve kroz API-je koji su prilagođeni mobilnim okruženjima. Stoga je potrebno osigurati podršku za OAuth2/OIDC autentikaciju, što znači da servis treba očekivati OAuth2 bearer token (JWT) u authorization zaglavlju poziva, kojim mobilna platforma dokazuje identitet korisnika.

- **Testiranje usluge –** pružatelj usluge treba provesti integracijske testove unutar svog sustava, test prema dogovorenoj funkcionalnoj specifikaciji usluge, provjeru poslovnih pravila usluge, ispravnost generiranja podataka, provjeru rubnih slučajeva (validacije ulaznih podataka). Nakon uspješnog testiranja, potrebno je formalno odobrenje da se usluga može javno objaviti u produkcijskoj verziji.

- **Konfiguracija u produkcijskom sustavu –** na strani pružatelja usluga ova aktivnost uključuje objavu produkcijskih verzija API metoda na GSB-u

- **Kontinuirano održavanje** - Pružatelj usluge odgovoran je za održavanje svog pozadinskog servisa (npr. ažuriranje podataka, dostupnost sustava prema dogovorenom SLA).

2.2. Aktivnosti na strani MPUDT

Nakon što je m-usluga razvijena ili prilagođena, slijedi tehnička konfiguracija za spajanje na mobilnu platformu. Ovaj korak uključuje dvije razine konfiguracije: na strani GSB-a (API gatewaya) i unutar same mobilne platforme.

- **Konfiguracija na GSB/API gatewayu.** Usluga mora biti dostupna putem odgovarajućeg endpointa koji m-platforma može pozvati. U praksi, to znači definiranje REST metode unutar GSB sustava. Ako je usluga već dio GSB-a (npr. SOAP servis), potrebno je dodati novi *API mapping*. Primjerice, putem alata WSO2 API Manager ili sličnog, definirat će se REST ruta koja poziva interni servis. Ruta se tipično standardizira prema pravilima platforme.

  GSB konfiguracija obavlja se u suradnji s integracijskim timom. Nakon što pružatelj usluge dostavi potrebne detalje, integracijski stručnjaci zatim postavljaju potrebne *proxy servise* ili *API definicije* na GSB-u. Također se konfiguriraju certifikati – mobilna platforma koristi svoj klijentski certifikat koji GSB prepoznaje (i obratno).

- **Konfiguracija unutar mobilne platforme.** Nakon što je GSB endpoint spreman, uslugu treba dodati u samu platformu m-Građani. Platforma sadrži administratorsko sučelje kroz koje se konfiguriraju API metode i gradi korisničko sučelje usluge. Proces uključuje dodavanje API metode, kreiranje korisničkog

sučelja usluge kroz GUI form builder koji omogućuje dizajniranje ekrana usluge bez potrebe za programiranjem posebne mobilne aplikacije za svaku uslugu, konfiguriranje layouta usluge gdje se svaka komponenta može povezati s ranije definiranim API metodama, definiranje pravila i uvjeta što se događa na temelju rezultata API poziva. Nakon što se API metode i UI komponente iskonfiguriraju, nova usluga postaje vidljiva unutar testne mobilne aplikacije.

- **Testiranje usluge –**testiranje uključuje provjeru usluge prema funkcionalnoj specifikaciji, sigurnosne testove (npr. pokušava se pristupiti usluzi s neodgovarajućim vjerodajnicama, pokušaj poziva API-ja bez tokena ili s manipuliranim tokenom), integracijske testove. Prije produkcije mogu se provesti i eksterni sigurnosni testovi. To podrazumijeva da ovlašteni stručnjaci pokušaju pronaći ranjivosti (npr. SQL injection u parametrima usluge, XSS u prikazu podataka u app, slabosti autentikacijskog toka, itd.). Ako se nađe propust, rješava se prije puštanja uživo.

- **Konfiguracija u produkcijskom sustavu** - konfiguracijske postavke koje su napravljene u testnom okruženju sada se repliciraju u produkciji. To uključuje uvoz konfiguracije API metoda u produkcijski API gateway/GSB. Dodavanje nove usluge uglavnom ne zahtijeva objavu nove verzije same mobilne aplikacije na Apple/Google trgovinama – aplikacija je dizajnirana tako da dinamički povlači konfiguracije i prikazuje nove usluge. U svakom slučaju, tim za mobilnu aplikaciju provjerava uzrokuje li dodavanje usluge neke bugove na klijentskoj strani te po potrebi izdaje update.

- **Kontinuirano održavanje –** sa strane m-platforme, usluga je pod nadzorom korištenjem alata za nadzor te se prati rade li endpointi i koliko brzo odgovaraju. U slučaju problema, incidenti se prijavljuju nadležnim timovima (npr. ako servis tijela nije dostupan, obavještava se IT služba tog tijela). Prilikom budućih izmjena ili poboljšanja usluge (npr. dodavanje nove funkcionalnosti), proces se ponavlja: izmjene se unesu u testno okruženje, testiraju, pa tek onda prenesu u produkciju uz minimalni prekid rada. Modularna arhitektura platforme i dobra praksa verzioniranja omogućava da jedan servis bude nadograđen dok ostali normalno funkcioniraju, a da korisnici to gotovo i ne osjete.