A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

Autentikacijski sustavi i baze podataka
WEB APLIKACIJA „ASIBP Projekt“

Kristijan Rosandić
Visoko učilište Algebra

A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

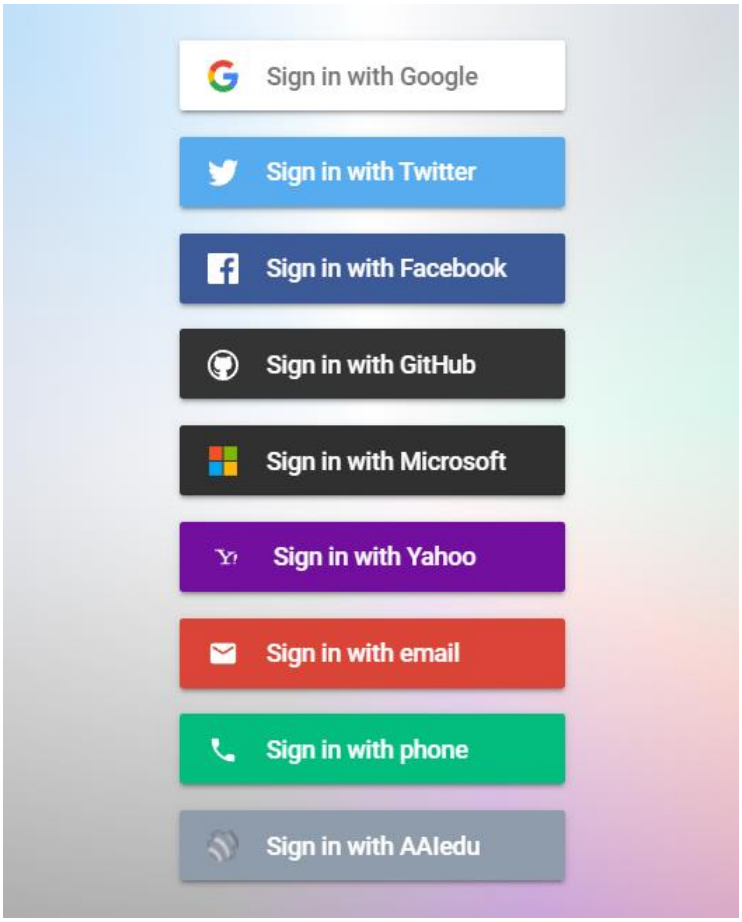
ALGEBRA

Sadržaj

1. Sažetak

Web Aplikacija „ASIBP Projekt“ osmišljena je na način da pruži korisnicima što veći odabir autentikacijskih metoda. Ukupno ih je devet, a to su: autentikacija putem Google-a, Twitter-a, Facebook-a, GitHub-a, Microsoft-a, Yahoo-a, Email/Password-a, mobitela i AAIedu sustava. Nakon autentikacije, korisnik vidi pod kojim imenom/mail-om je prijavljen te može unositi poruku koja se automatski sprema i kojoj može pristupiti samo on. Aplikacija je implementirana koristeći Google Firebase i Identity Platform za autentikaciju, bazu podataka i hosting. Za kontrolu verzija te automatski deployment na Firebase koristim Github i Github Actions/Workflows. Za registar domene koristim Namecheap s custom DNS nameserverom – Cloudflare-om. Frontend aplikacije sastoji se od jedne HTML i CSS datoteke.

Aplikacija je javno dostupna na adresi https://asibp.k1k1.dev



Slika 1: Početno sučelje aplikacije

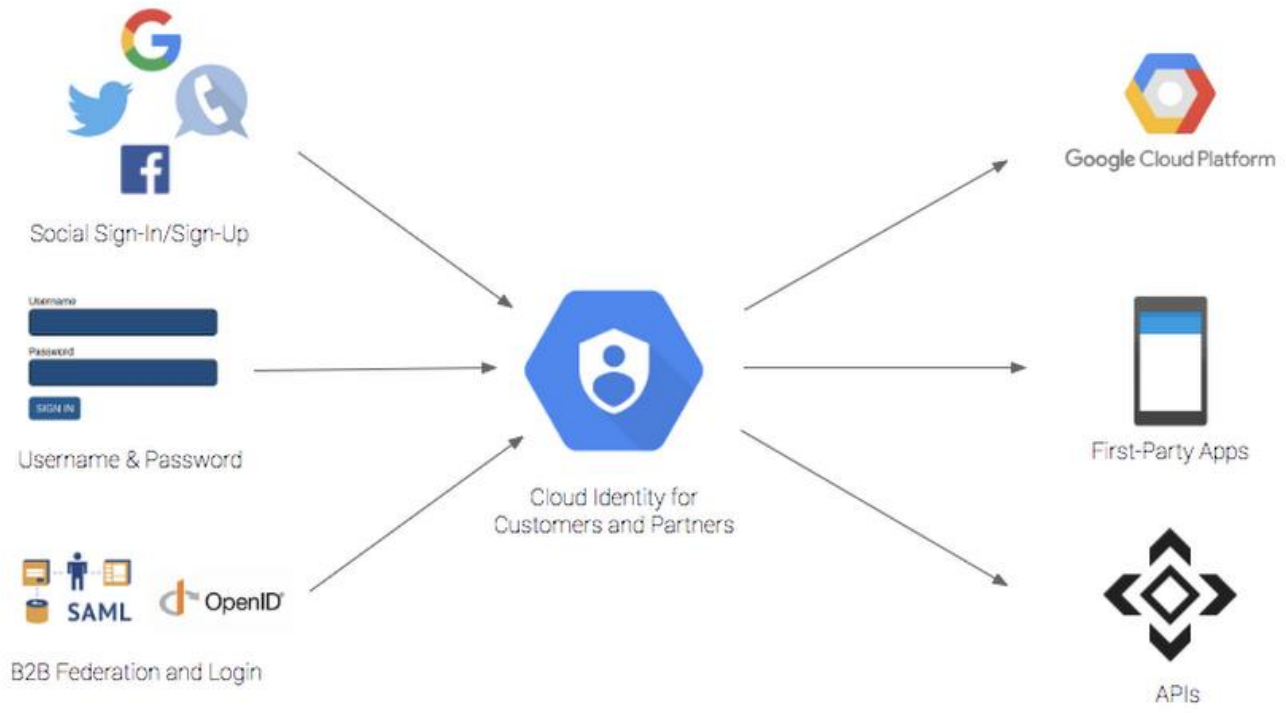
2. Uvod

Aplikacija rješava problem autentikacije koristeći besplatno Cloud rješenje. Od popularnih rješenja koje danas nude Amazon (AWS), Google (GCP) i Microsoft (Azure), odabrao sam Google Cloud Platform (GCP) zbog prethodne upoznatosti, preglednosti i popularnosti servisa koje nudi.

Odličan prikaz svih servisa nalazi se na Google Developer Cheat Sheet-u [1], na kojem se vidi Google-ova predanost tehnologijama „Identity Platform“ i „Firebase“. To su dvije ključne platforme koje su aktivirane u ASIBP Projektu, koji je pokrenut na Google Cloud Console središtu.

Identity Platform omogućuje razne načine autentikacija i kontrolu nad registriranim korisnicima [2].

Firebase je Backend-as-a-Service (BAAS) rješenje za integraciju Identity Platforme, bazu podataka i hosting aplikacije [3].



Slika 2: Cloud Identity Flow

3. Razrada projekta

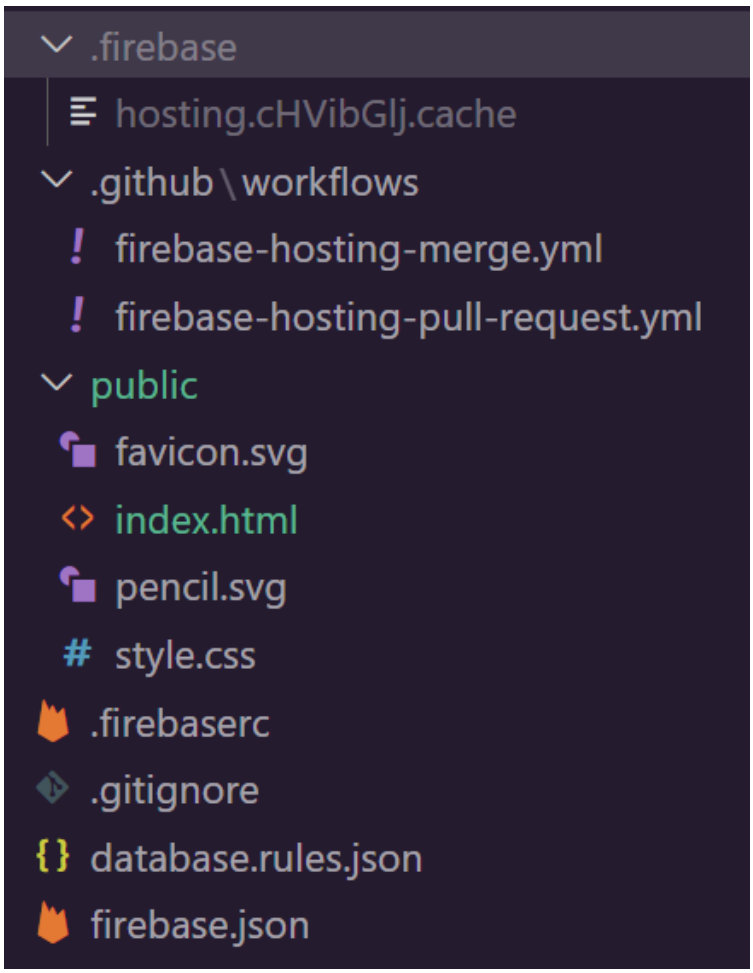
Razrada projekta sastoji se od pripreme razvojnog okruženja, back-enda i, na kraju, front-enda.

3.1. Priprema razvojnog okruženja

Direktorij u kojem stvaram aplikaciju inicijaliziram naredbom „firebase init“, koristeći Firebase CLI, nakon čega pratim sve upute i konfiguracije koje mi Firebase nudi preko konzole [4].

Zatim inicijaliziram git i istovremeno otvaram javni projekt na GitHub-u.

Konačno, u novostvorenom „public“ direktoriju stvaram sve datoteke koje će biti hostane na Firebase-u.



Slika 3: Direktorij aplikacije

3.2. Konfiguracija Firebase projekta

Na **Authentication** sekciji potrebno je omogućiti povezivanje Identity Platforme s Firebase-om. Nakon povezivanja dostupne su napredne postavke poput aktivacije SAML i OpenID Connet providera, što je nužno za posljednji tip autentikacije – AAIedu.

Zbog velikog broja autentikacijskih metoda, u postavkama sam omogućio povezivanje računa s istim email-om. To znači da se korisnik može prijaviti na isti račun na više načina. Na primjer, korisnik stvori račun s gmail-om i lozinkom, a sljedeći put se prijavi preko Google-a.

Zbog sigurnosnih razloga, u postavkama je nužno unijeti niz domena kojima Firebase-u dopuštam OAuth redirect zahtjeve. Za razvoj, domene su localhost ili IP adresa, a za produkciju to je asibp.k1k1.dev.

Na **Realtime Database** sekciji jedino je potrebno stvoriti pravila kojima definiram uvjete čitanja i pisanja u bazu podataka. To je JSON datoteka koja se može uređivati na web-u ili u razvojnom direktoriju „database.rules.json“.

Slika 4: Realtime Database pravila

Pravila sa slike dopuštaju korisniku da čita i piše podatke jedino na svoju lokaciju u bazi, s putanjom users.[uid], gdje je uid identifikator korisnika koji se generira prilikom otvaranja računa.

Na **Hosting** sekciji mogao sam ostaviti zadanu Firebase domenu s nazivom [asibp].web.app ili [asibp].firebaseapp.com, ali već imam kupljenu domenu sa svojim portfoliom k1k1.dev pa sam je odlučio iskoristiti na način da stvorim poddomenu. Na Cloudflare-ovom DNS kontroleru je potrebno dodati samo jedan novi „A rekord“ koji upućuje „asibp.k1k1.dev“ na IP adresu od Firebase-a.

3.3. Konfiguracija provider-a za autentikaciju

Postoje tri tipa provider-a za autentikaciju: nativni (oni koje nudi Firebase), dodatni (oni koje nude popularne aplikacije), i custom provideri (oni koji koriste OpenID Connect ili SAML) [5].

Nativni su Email/Password i Phone, koje nije potrebno konfigurirati.

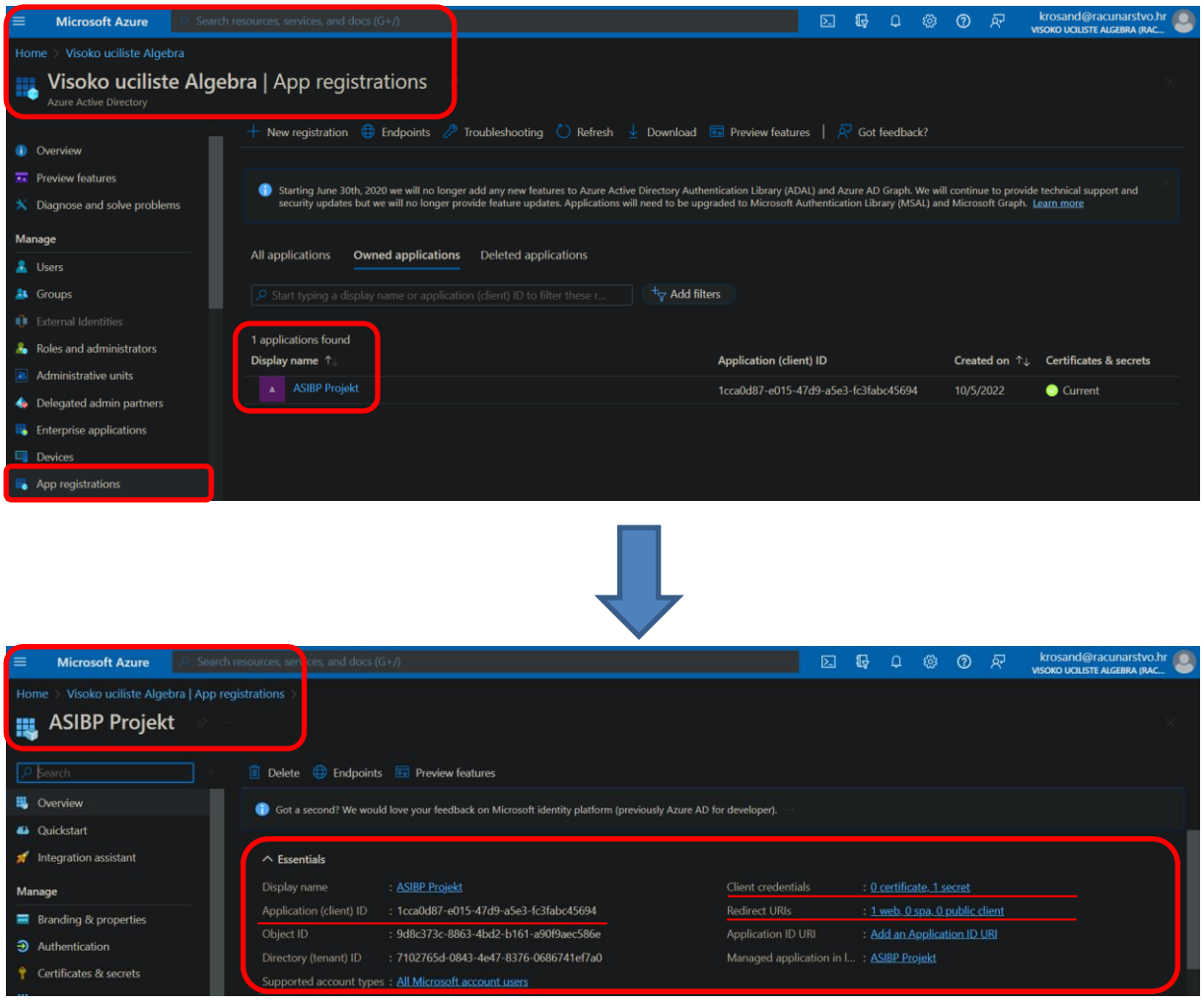
Dodatni su: Google, Twitter, Facebook, GitHub, Microsoft i Yahoo. Za svaki od navedenih potrebno je stvoriti developerski račun i na njemu definirati novu aplikaciju (registrirati), nakon čega se dobiva Application ID i Application Secret. Dvije vrijednosti se unose u Firebase, a Firebase-ov Redirect URL (koji je uvijek isti) unosim za svaku novodefiniranu aplikaciju. Dakle, Firebase je Service Provider (SP), a aplikacije koje nude svoje korisnike su Identity Provider-i (IdP).

Slijedi niz linkova na kojima je registrirana aplikacija:

- https://developer.google.com
- https://developer.twitter.com
- https://developers.facebook.com
- https://github.com
- https://portal.azure.com
- https://developer.yahoo.com
- *(Apple traži 100$ da bi uopće otvorio developerski račun, na godišnju pretplatu)*

Na svim autentikacijskim sustavima mogu definirati koje sve informacije želim od korisnika. Na primjer, korisnik se autenticira putem Twitter-a i meni daje dopuštenje da čitam sve njegove tweet-ove, pišem tweet-ove umjesto njega ili čak njegove osobne poruke. Ako korisnik nije oprezan i ne gleda na što pristaje, Twitter API meni može omogućiti da radim gotovo sve umjesto njega, bez da znam njegovu lozinku. Zbog tog razloga, kad se netko prijavljuje na ASIBP Projekt, tražim minimalnu količinu podataka koje mi svaki autentikacijski sustav nudi.

Kao primjer registracije aplikacije, uzeo sam Azure Active Directory od Microsoft-a.



Slika 5: Azure Active Directory registracija aplikacije

Za autentikaciju putem custom provider-a, AAIedu sustava, odabrao sam OpenID Connect (OIDC) tehnologiju zbog jednostavnosti povezivanja. Za registraciju aplikacije na AAIedu sustav potrebno je stvoriti račun na stranici https://registar.aaiedu.hr/ i registrirati novi resurs, nakon čega definiram koje autentikacijske protokole želim dodijeliti tome resursu, što je samo OIDC.

Slično ostalim provider-ima, OIDC sa strane SP-a traži Client ID i Client Secret, a IdP-u nudi isti callback URL kao i prije. Jedina je razlika u tome što SP traži Issuer URL od IdP-a, kojeg sam pronašao na stranici https://wiki.srce.hr/pages/viewpage.action?pageId=59867172, a to je:

„https://login.aaiedu.hr/.well-known/openid-configuration“.

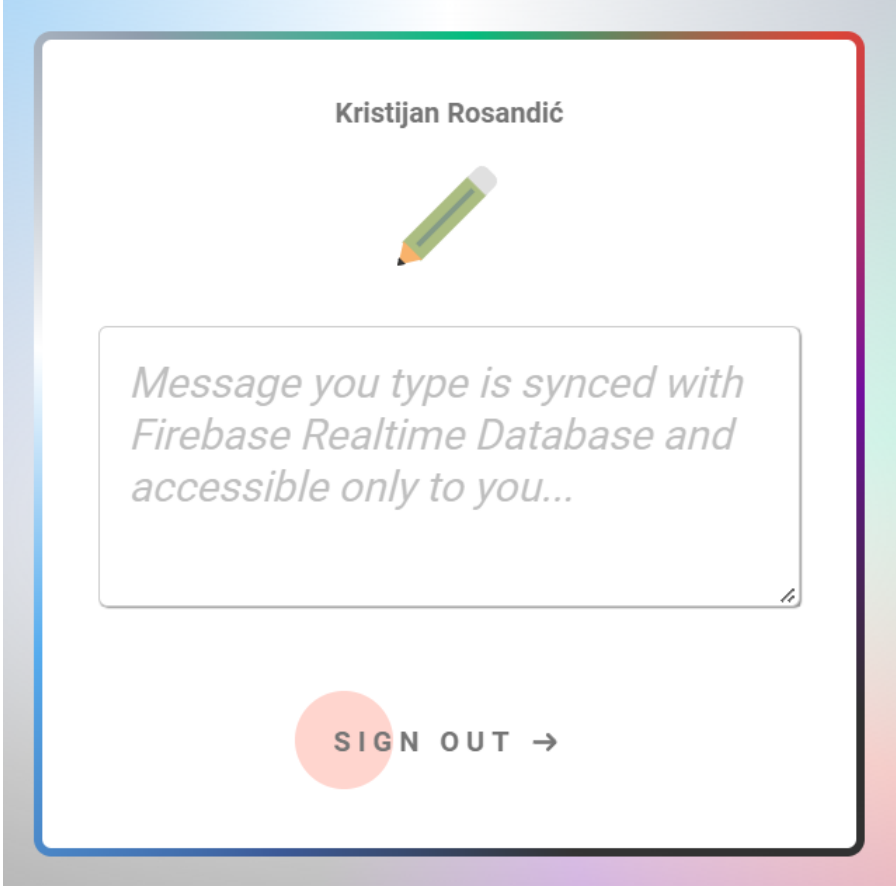
3.4. Razvoj frontend-a

Za prijavu koristim gotovo rješenje koje mi nudi Firebase – FirebaseUI [6].

Kako bi aplikacija imala barem nekakvu svrhu, nakon prijave pojavljuje se prostor za upis poruke. Korisnik unosi poruku koja se automatski sprema na Realtime Database. Da biste vidjeli brzinu WebSocket-a (komunikacijskog protokola kojeg koristi Firebase) otvorite novu karticu u pregledniku ili se prijavite na mobitel s istim korisničkim računom i započnite pisati poruku. Izgleda impresivno, a implementacija je vrlo jednostavna.

Iznad prostora za upis piše ime korisnika, ako ga je odabrani provider pokupio, a u suprotnom email. Ispod prostora za upis je gumb za odjavu. CSS se nalazi u zasebnoj datoteci i aplikacija je prilagođena za uređaje svih rezolucija.

Izvorni kod je dostupan na GitHubu: https://github.com/ChrisRoss5/firebase-auth



Slika 6: Sučelje aplikacije nakon prijave

4. Zaključak

Google Cloud Platform (GCP) je odlična platforma za razvoj raznih IT rješenja i pomoću Google Identity Platforme (koja je dio GCP-a) nudi sjajnu podršku za autentikaciju i kontrolu korisnika. Firebase je također velik dio GCP-a, koji implementira Identity Platformu i spaja je sa svojim servisima kao što je Realtime Database. Osim što je u potpunosti besplatno koristiti sve servise, Google ima visoke kvote nakon kojih kreće naplaćivanje. Svaki identity provider, kao što je Microsoft, Twitter ili Facebook, ima svoj developerski portal s kojim povezujem aplikaciju. Na taj način, uz nativne i custom providere koje nudi Firebase, korisnici imaju velik odabir ulaza u aplikaciju.

5. Reference

[1] [Mrežno]. Available: https://googlecloudcheatsheet.withgoogle.com/.

[2] [Mrežno]. Available: https://cloud.google.com/identity-platform.

[3] [Mrežno]. Available: https://firebase.google.com/.

[4] [Mrežno]. Available: https://firebase.google.com/docs/cli.

[5] [Mrežno]. Available: https://firebase.google.com/docs/auth.

[6] [Mrežno]. Available: https://github.com/firebase/firebaseui-web.