**PetMe**

În contextul dezvoltării aplicațiilor mobile, securitatea și eficiența procesului de autentificare sunt esențiale pentru a asigura o experiență de utilizator optimă și pentru protejarea datelor personale ale utilizatorilor. În prima faza, voi aborda arhitectura și logica din spatele implementării metodelor de autentificare într-o aplicație Android care utilizează Firebase, concentrându-mă pe două metode populare de autentificare: autentificarea prin email și parolă și autentificarea prin Google Auth. Integrarea Firebase în aplicațiile Android oferă un cadru robust și scalabil pentru gestionarea autentificării și a altor servicii backend. Firebase Authentication simplifică procesul de implementare a diverselor metode de autentificare, oferind în același timp un nivel ridicat de securitate și conformitate.

Autentificarea prin email și parolă este o metodă tradițională și larg răspândită. Aceasta implică crearea unui cont de utilizator unde emailul servește ca identificator unic, iar parola asigură securitatea contului. Procesul de autentificare prin email și parolă în Firebase presupune configurarea inițială a Firebase Authentication și crearea unei interfețe utilizator în aplicația Android pentru înregistrarea și logarea utilizatorilor. Implementarea acestei metode necesită o gestionare atentă a securității, inclusiv stocarea sigură a parolelor și protecția împotriva atacurilor comune, cum ar fi brute-force sau phishing.

In urma configurarii intiale, este necesara apelarea functiilor din SDK-ul de autentificare oferit de Firebase. Aceasta ofera verificarea datelor la nivel rudimentar, totusi se poate adauga si o verificare locala. In urma autentificarii, un obiect pentru utilizator este stocat local si poate sa fie apelat oricand folosind functiile din librarie.

Autentificarea prin Google este similara, adaugat totusi un nivel de complexitate. Intre autentificarea finala prin Firebase si aplicatie se afla un nivel de autentificare prin sistemul Google. Aceasta o sa-i afiseze utilizatorului posibilitatea de a alege un cont Google deja existent.

In urma autentificari cu oricare dintre cele doua metode, in baza de date RTDB FIREBASE sunt generate "Documente" , acestea fiind similare cu entitatile dintr-o baza de date tranditionala. Documentele sunt identificate si accesate prin UUID-ul utilizatorilor ce este de asemenea generat la inregistrearea initiala.

Astfel, autentificarea este folosita ca microserviciu si este COMPLET decuplata de baza de date sau de serviciile locale oferite de aplicatie. Redundata sistemului creste prin aceasta strategie.

|  |  |  |
| --- | --- | --- |
|  |  |  |