



Univerzitet u Sarajevu
Elektrotehnički fakultet Sarajevo
Odsjek za računarstvo i informatiku

Specifikacija softverskih zahtjeva

Secure remote control

Projektna dokumentacija

Softver inženjering-

Predmetni profesor:
Red. prof. Dr. Novica Nosović

Predmetni asistenti:
Kenan Halilović
Tarik Hrnjić

Akadska 2024/2025 godina

Sadržaj

SRS za web aplikaciju (web side & communication layer)	4
Uvod	4
Svrha	4
Konvencija dokumenta	4
Kome je namijenjen sistem	5
Obim projekta	5
Opis sistema	6
Perspektiva proizvoda i Entity Relationship Dijagram	6
Korisničke klase i njihove karakteristike uz Activity i Use Case dijagrame	7
Karakteristike sistema	12
Opis i prioritet	12
Funkcionalni zahtjevi i dijagram komponenti	13
Vanjski zahtjevi interfejsa	14
Korisnički interfejs	14
Hardverski interfejs	15
Softverski interfejs	16
Komunikacijski interfejs i dijagram raspoređivanja	17
Nefunkcionalni zahtjevi	18
End to end enkripcija (E2EE) za prenos podataka	18
Podrška za najmanje 1.000 istovremenih sesija	18
Vremenski odziv za komande treba biti manji od 100ms u optimalnim mrežnim uslovima...	18
Efikasnost potrošnje baterije – maksimalno 5% CPU pri mirovanju	18
Usklađenost sa GDPR i ISO 27001 sigurnosnim standardima	18
FURPS+	19
Funkcionalnosti	19
Upotrebljivost	21
Pouzdanost	21
Performanse	21
Podržanost	21
Implementacijski zahtjevi	22
Ograničenja interfejsa	22
Fizički zahtjevi	22
Ograničenja dizajna	22
SRS za android aplikaciju	23
Uvod	23
Svrha	23
Kome je namijenjen	23
Obim projekta	23
Opis sistema	24
Perspektiva proizvoda	24

Korisničke klase i njihove karakteristike uz Activity i Use Case dijagrame.....	24
Operativno okruženje.....	31
Ograničenja dizajna i implementacije.....	31
Dijagram komponenti.....	32
1. Client-Side App (Android).....	32
2. Communication Layer (Remote Control Gateway).....	32
3. Controller (Web Admin Panel).....	33
4. Baza podataka (Database).....	33
Nefunkcionalni zahtjevi.....	34
FURPS+.....	35
Vanjski zahtjevi interfejsa.....	36
WebSocket API (Glavni komunikacioni kanal).....	37
WebRTC signaling kanal.....	37
Push Notification servis.....	37
OAuth 2.0 / SSO autentifikacija.....	37
Pristup bazi podataka.....	37

SRS za web aplikaciju (web side & communication layer)

Uvod

Ovaj dokument predstavlja specifikaciju softverskih zahtjeva (Software Requirement Specification - SRS) za Secure remote control sistem. Za opis sistema biće korišten FURPS model.

Svrha

Svrha ovog SRS dokumenta jeste predstavljanje detaljnog opisa Secure remote control sistema, njegove karakteristike, interfejse, funkcionalnosti, namjene, i način na koji će se upravljati sistemom. Ovaj dokument služi kao referenca svim korisnicima sistema i svima koji su radili ili će tek raditi na razvoju ovog sistema.

Konvencija dokumenta

Termin	Objašnjenje
FURPS	FURPS je akronim za skup kriterija kvalitete softvera – Functionality, Usability, Reliability, Performance i Supportability – koji se koristi za ocjenu i specifikaciju zahtjeva softverskog sistema.
UI	User interface - korisnički interfejs
UX	User experience - korisničko iskustvo
JWT	Java web token - čuva sesiju web browser-a
dodajte	Šta vam bude trebalo

Kome je namijenjen sistem

Ovaj sistem je namijenjen IT podršci i administratorima u kompanijama kako bi mogli sigurno upravljati Android uređajima na daljinu putem web-based panela. Također, namijenjen je krajnjim korisnicima Android uređaja, kojima omogućava da primaju pomoć i nadgledaju daljinske sesije. Sistem je dizajniran za okruženja gdje su sigurnost, privatnost i brz odziv ključni, kao što su korporativni, obrazovni ili ? sektori.

Obim projekta

Obim projekta obuhvata tri glavne komponente sistema:

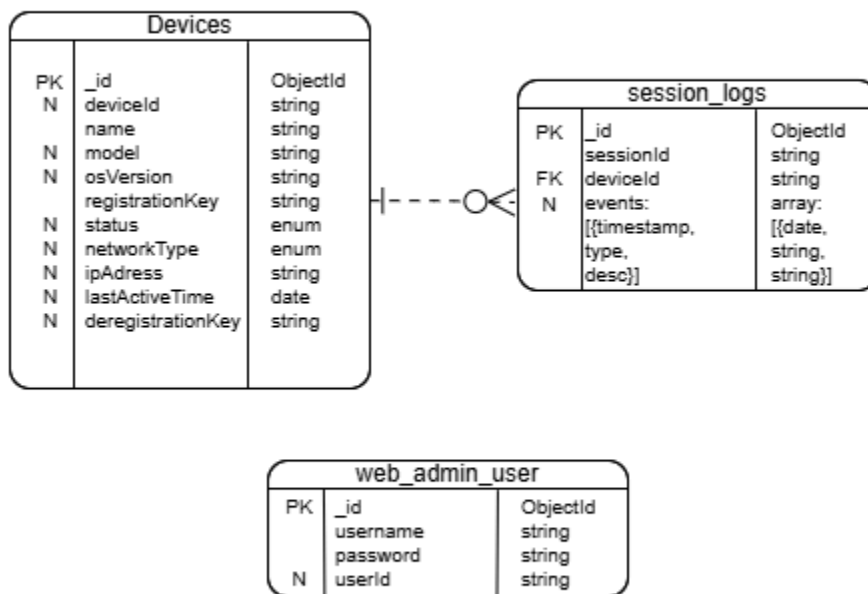
1. **Client-Side App (Android)** – aplikacija koja radi u pozadini, omogućava daljinsku kontrolu i ekran sharing, omogućava registraciju uređaja, prikaz trenutne aktivnosti i prekid sesije, uz sigurnu komunikaciju (TLS 1.2).
2. **Controller (Web-Based Admin Panel)** – web aplikacija za IT podršku i administratore koja omogućava autentifikaciju (SSO/OAuth2), prikaz statusa uređaja, upravljanje sesijama, bidirekcijsku komunikaciju, slanje komandi, i vođenje sigurnosnih logova.
3. **Communication Layer (Remote Control Gateway)** – sloj koji osigurava trajnu, šifrovanu vezu između uređaja i servera, omogućava niskolatenatnu dvosmjernu komunikaciju i automatsko prekidanje sesije u slučaju neaktivnosti ili prekida veze.

Projekat obuhvata razvoj sigurnog sistema za daljinsko upravljanje Android uređajima koji uključuje klijentsku aplikaciju, web-bazirani kontrolni panel i komunikacioni sloj. Sistem omogućava IT podršci i administratorima da upravljaju uređajima na daljinu putem enkriptovane veze, uz funkcije poput ekranskog prikaza, slanja komandi i vođenja sigurnosnih logova. Uređaji se moraju registrovati i autentifikovati prije kontrole, a sve sesije se bilježe i mogu se prekinuti s obje strane. Projekat takođe podrazumijeva visoku dostupnost, nisku latenciju, skalabilnost za veliki broj istovremenih sesija te usklađenost sa sigurnosnim standardima poput GDPR-a i ISO 27001. Ukratko, obim projekta uključuje sigurnu, pouzdanu i efikasnu platformu za daljinsko upravljanje Android uređajima, sa svim potrebnim funkcionalnostima i sigurnosnim zahtjevima.

Opis sistema

Perspektiva proizvoda i Entity Relationship Dijagram

U današnje vrijeme, kada je rad na daljinu sve češći i popularniji, ovakav sistem se lako uklapa u savremene IT infrastrukture jer omogućava sigurnu i efikasnu podršku bez fizičke prisutnosti, čime dodatno povećava svoju primjenjivost i tržišni potencijal. Sa sve većim brojem mobilnih uređaja u upotrebi i povećanim zahtjevima za sigurnost, ovaj sistem se pozicionira kao pouzdano i skalabilno rješenje koje omogućava efikasno upravljanje Android uređajima na daljinu. Integracija sa savremenim sigurnosnim standardima i podrška za veliki broj sesija čine ga idealnim za velike organizacije koje zahtijevaju centralizovanu i sigurnu kontrolu nad mobilnim uređajima.



Slika 1. Entity Relationship Diagram

Korisničke klase i njihove karakteristike uz Activity i Use Case dijagrame

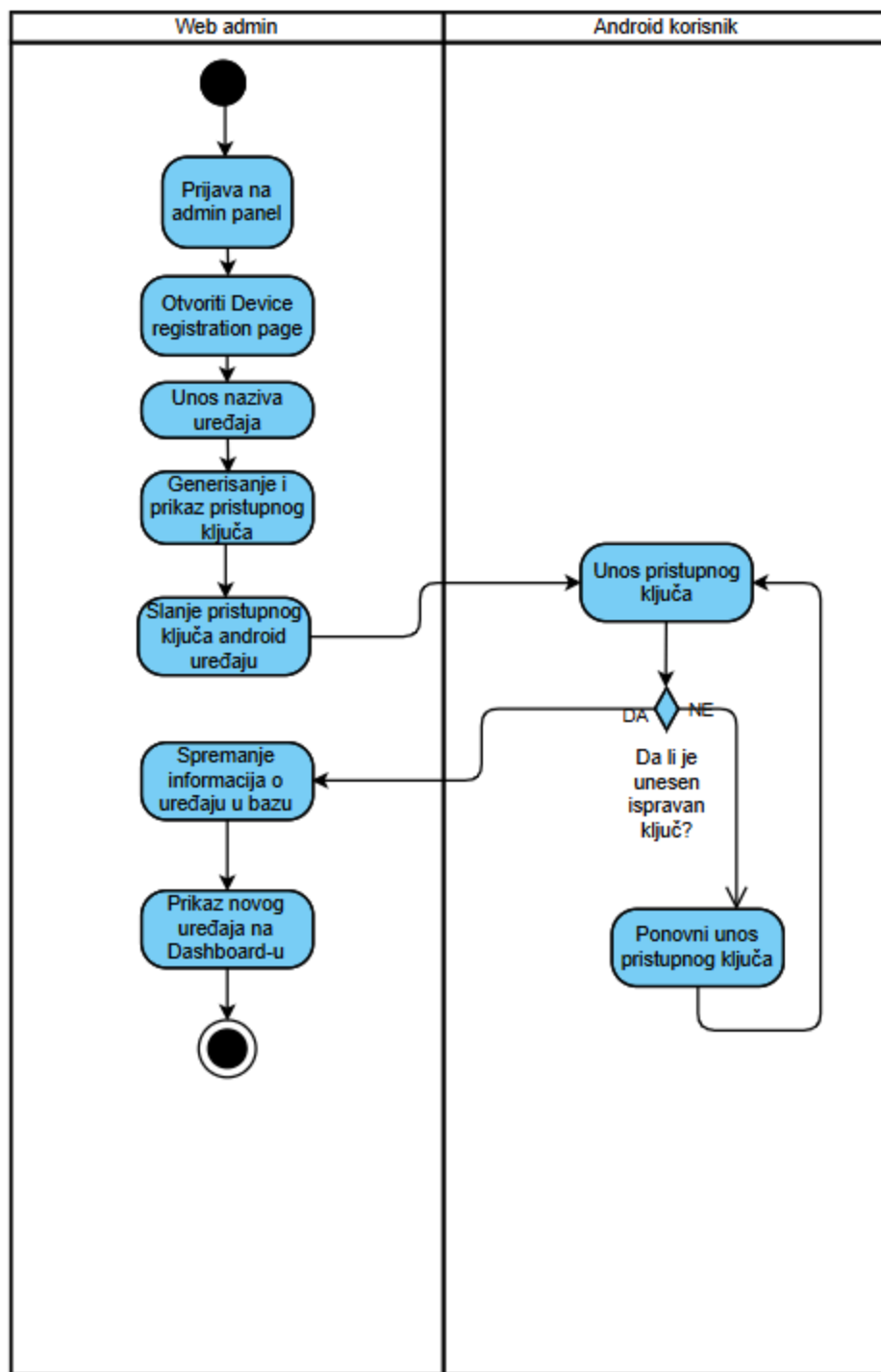
Korisnici Secure remote control sistema mogu imati jednu od dvije uloge, i to: Android korisnik i Web admin.

Android korisnik ima mogućnost korištenja sljedećih funkcionalnosti:

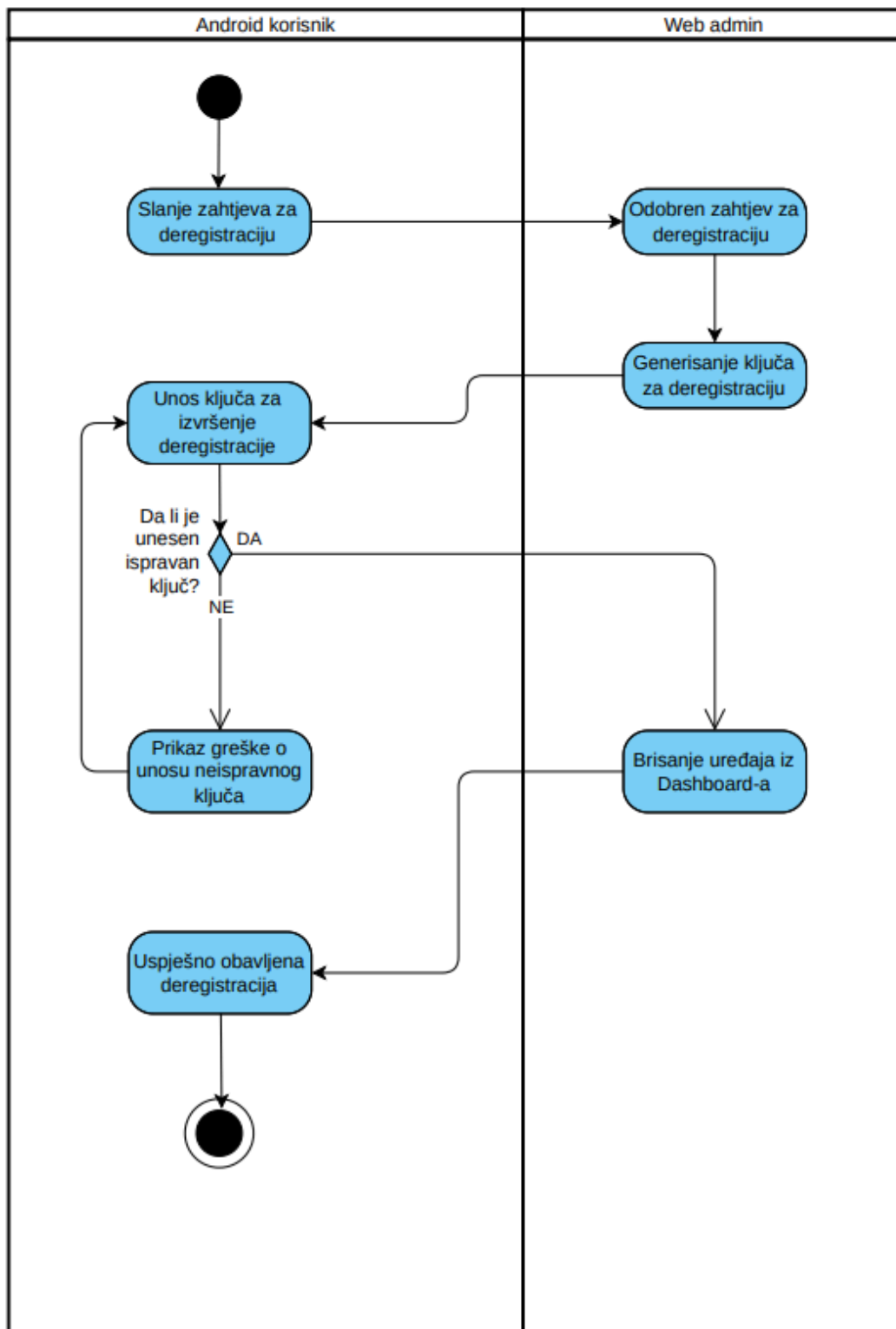
- Registracija uređaja
- Deregistracija uređaja
- Zahtijevanje sesije
- Pregled i brisanje logova aktivnosti
- Upravljanje file-ovima (browse, upload, download)

Web admin ima mogućnost korištenja sljedećih funkcionalnosti:

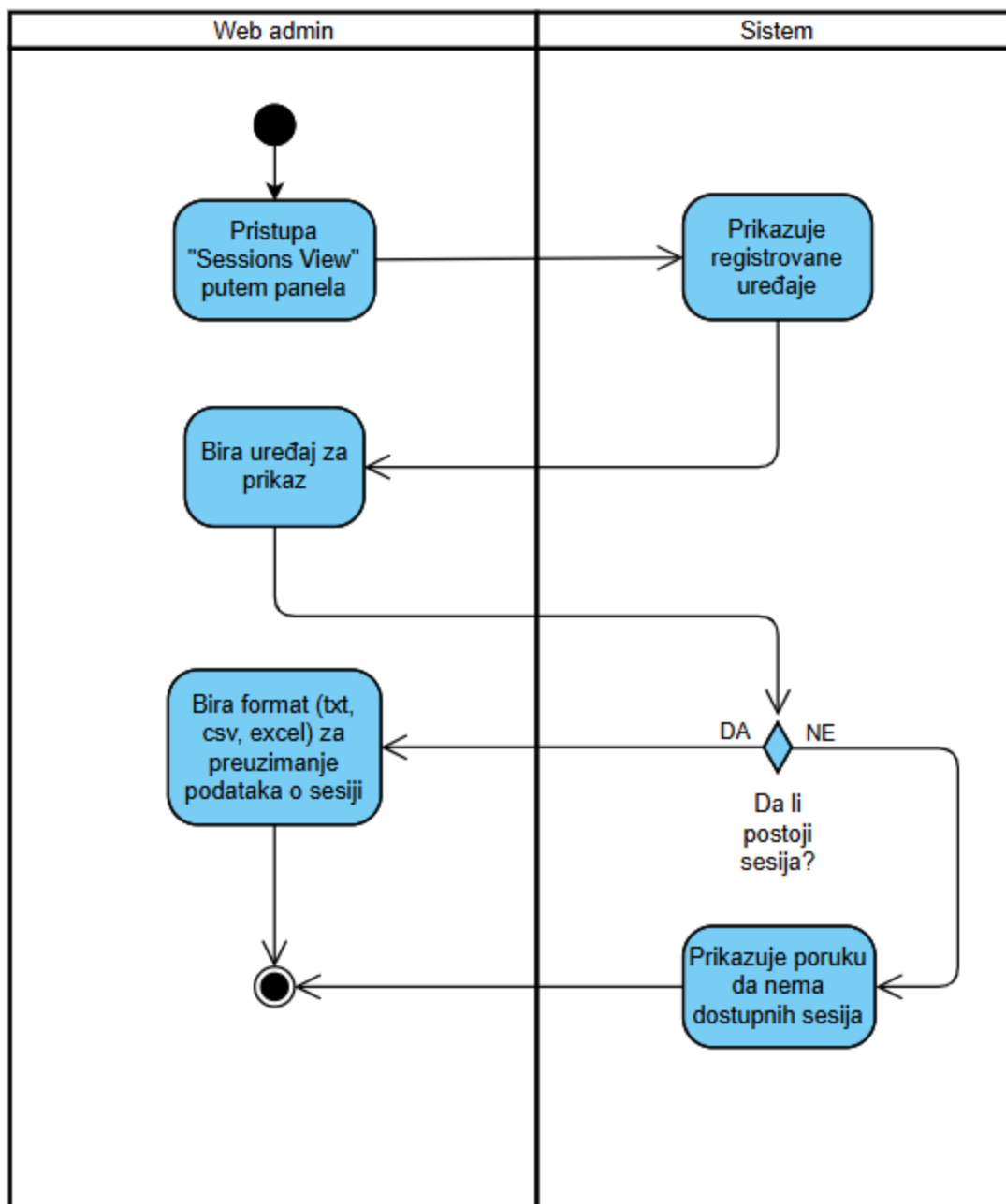
- Prijava
- Registracija novog admina
- Odobravanje i odbijanje zahtjeva za sesiju
- Registracija uređaja
- Snimanje sesije
- Pregled sesija svakog uređaja
- Upravljanje file-ovima na uređaju (browse, upload, download)
- Export sesija u fajl (.txt, .csv, .exe)
- Konfiguracije sesija



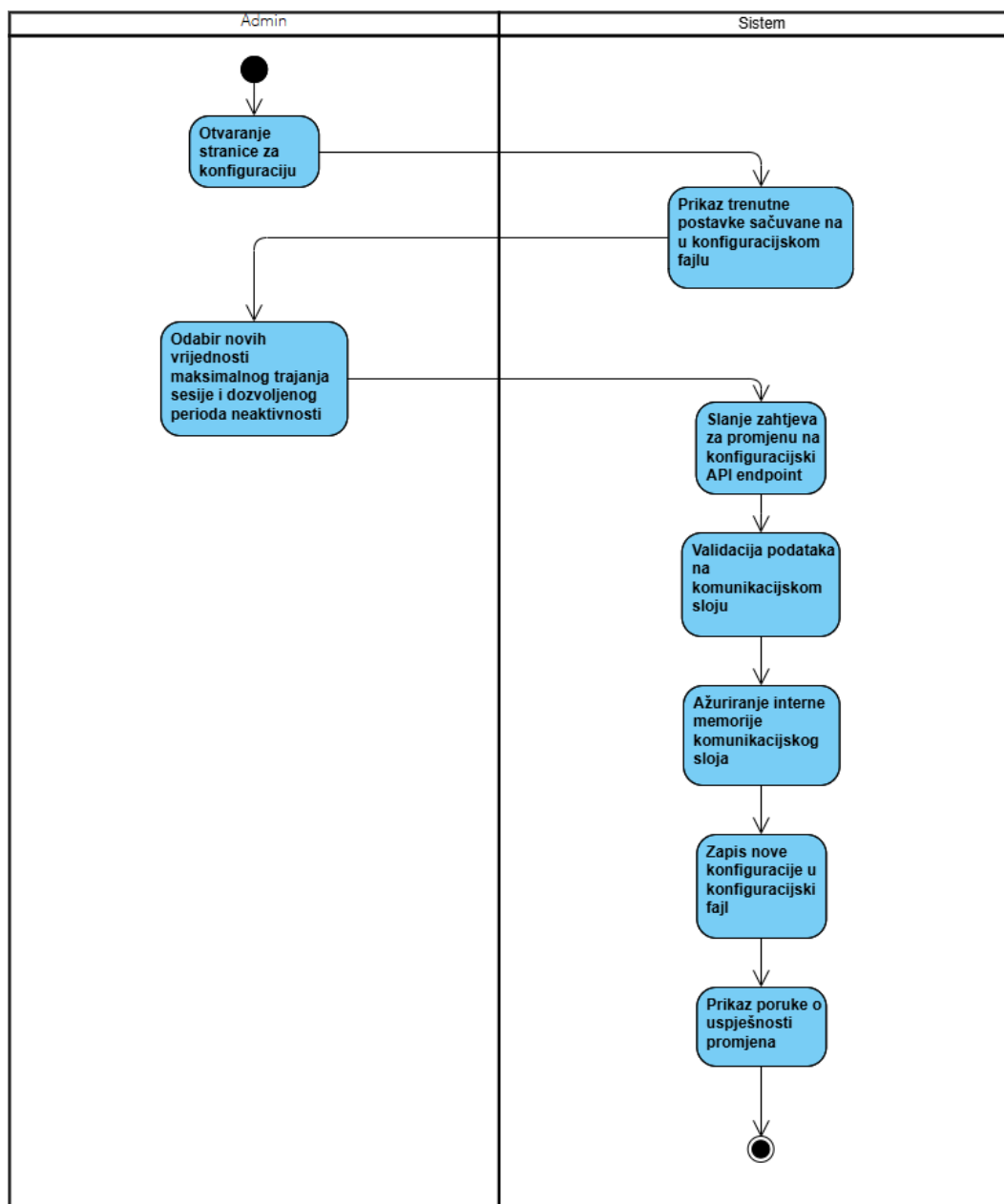
Slika 2. Dijagram aktivnosti za registraciju uređaja



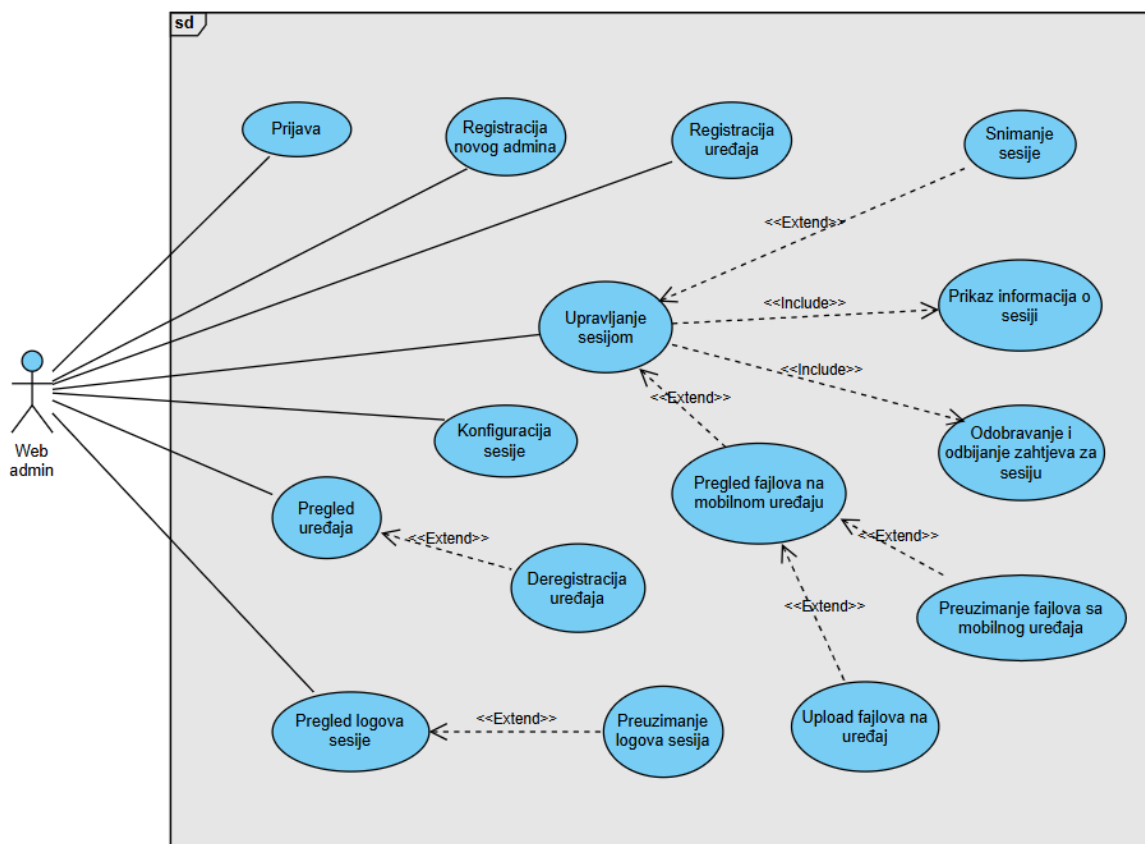
Slika 3. Dijagram aktivnosti za deregistraciju uređaja



Slika 4. Dijagram aktivnosti za pregled i export sesijskih logova



Slika 5. Dijagram aktivnosti za postavke sesija



Slika 6. Dijagram slučajeva upotrebe za Web admina

Karakteristike sistema

Opis i prioritet

Secure Remote Control sistem predstavlja integrisano rešenje za sigurnu daljinsku kontrolu Android uređaja namenjeno IT podršci i administratorima u korporativnom okruženju. Sistem omogućava efikasnu podršku mobilnim korisnicima bez potrebe za fizičkom prisutnošću, što značajno poboljšava operativnu efikasnost i smanjuje troškove podrške.

Prioritet sistema se ogleda u sledećim ključnim aspektima:

Visoki prioritet:

- Registracija i autentifikacija uređaja pre bilo kakve kontrole
- Mogućnost prekidanja sesije sa obe strane (korisnik i admin)
- Real-time screen sharing i daljinsko upravljanje
- Vođenje detaljnih logova svih sesija za sigurnosne potrebe

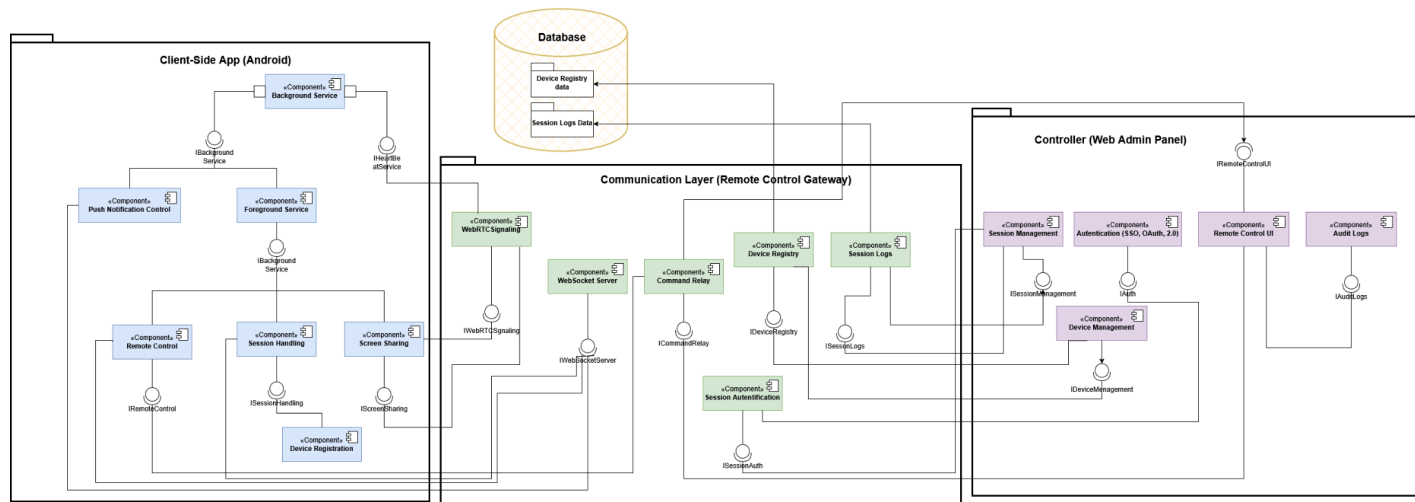
Srednji prioritet:

- Niska latencija (<100ms u optimalnim uslovima)
- Efikasna potrošnja baterije
- File management funkcionalnosti
- Automatska sesijska konfiguracija i timeout mehanizmi

Sistem je posebno dizajniran za okruženja gde su sigurnost, privatnost i brz odziv ključni faktori uspeha, kao što su korporativni, obrazovni i javni sektori.

Funkcionalni zahtjevi i dijagram komponenti

- Admin ima mogućnost registracije novog admina
- Admin ima mogućnost registracije uređaja
- Admin ima mogućnost deregistracije uređaja
- Admin ima mogućnost upravljanja sesijom
- Admin ima mogućnost odobravanja i odbijanja zahtjeva za sesiju
- Admin ima mogućnost snimanja sesije
- Admin ima mogućnost pregleda fajlova na mobilnom uređaju
- Admin ima mogućnost preuzimanja fajlova sa mobilnog uređaja
- Admin ima mogućnost upload fajlova na mobilni uređaj
- Admin ima mogućnost da konfiguriše sesiju (postavi vrijeme trajanja sesije i vrijeme isteka uslijed neaktivnosti)
- Admin ima mogućnost pregleda logova sesije
- Admin ima mogućnost preuzimanja informacija o logovima sesije
- Korisnik ima mogućnost registracije pomoću pristupnih podataka
- Korisnik ima mogućnost da zahtijeva sesiju za remote control
- Korisnik ima mogućnost upravljanja fajlovima
- Korisnik ima mogućnost pregleda i brisanja logova
- Korisnik ima mogućnost slanja zahtjeva za deregistraciju uređaja



Slika 7. Dijagram komponenti sistema

Vanjski zahtjevi interfejsa

Korisnički interfejs

Korisnički interfejs se sastoji od sljedećih interfejsa:

- Login stranica za admina - za prikaz svih informacija na web-based admin panelu potrebno je ulogovati se kao admin koristeći Username i Password
- Dashboard - stranica za prikaz svih registrovanih uređaja
- Device registration - stranica za registrovanje novog korisnika i prikaz generisanog pristupnog ključa
- Sessions View - stranica za prikaz uređaja, klik na bilo koji od uređaja vodi na stranicu za prikaz svih sesija i logova sesije za odabrani uređaj, na toj stranici je omogućeno i preuzimanje informacija o sesiji
- Register Admin - stranica za registraciju novog admina u sistem
- Session Settings - stranica za postavljanje preferenci za svaku sesiju, kada odabrani kriteriji budu ispunjeni, communication layer prekida sesiju

Hardverski interfejs

Serverska strana:

- **Minimalni zahtevi:** 4-core CPU, 8GB RAM, 100GB SSD storage
- **Preporučeni zahtevi:** 8-core CPU (Intel Xeon ili AMD EPYC), 16GB RAM, 500GB SSD
- **Mrežni zahtevi:** Stabilna internet konekcija sa bandwidth-om min. 100 Mbps
- **Port zahtevi:** Otvoreni portovi za HTTPS (443), WebSocket komunikaciju (8080), i WebRTC (dinamički port range)

Klijentska strana (Android uređaji):

- **OS zahtevi:** Android 8.0 (API level 26) ili noviji
- **RAM:** Minimum 2GB, preporučeno 4GB ili više
- **Procesor:** Minimum 1.5 GHz quad-core
- **Storage:** Minimum 200MB slobodnog prostora za aplikaciju
- **Mreža:** WiFi ili mobilni internet sa stabilnom konekcijom

Admin Panel (Web Client):

- **Uređaji:** Desktop računari, laptop računari, tablet uređaji
- **RAM:** Minimum 4GB za smooth rad
- **Procesor:** Minimum dual-core 2.0 GHz
- **Internet:** Stabilna konekcija min. 10 Mbps za pojedinačnu sesiju

Dodatni hardverski zahtevi:

- Dedicated GPU preporučeno za server pri velikom broju istovremenih video stream-ova
- UPS sistem za server infrastrukturu zbog kritičnosti servisa

Softverski interfejs

Server komponente:

- **Operativni sistem:** Linux (Ubuntu 20.04+/CentOS 8+) ili Windows Server 2019+
- **Runtime environment:** Node.js 16+ za Communication Layer
- **Baza podataka:** MySQL 8.0+ ili PostgreSQL 13+ za čuvanje sesijskih logova i korisničkih podataka
- **Web server:** Nginx ili Apache za load balancing i SSL terminaciju
- **WebRTC biblioteke:** aiortc ili node-webrtc za real-time komunikaciju

Android aplikacija:

- **Target SDK:** Android API 33 (Android 13)
- **Minimum SDK:** Android API 26 (Android 8.0)
- **Frameworks:** Jetpack Compose za UI, Kotlin kao glavni jezik
- **Komunikacija:** OkHttp za HTTP klijent, WebSocket client biblioteke
- **Media handling:** MediaProjection API za screen capture, Camera2 API

Web Admin Panel:

- **Frontend framework:** React.js 18+ sa TypeScript
- **UI biblioteke:** Tailwind CSS ili Material-UI za responsive design
- **State management:** Redux Toolkit ili Context API
- **Real-time komunikacija:** Socket.io client za WebSocket konekcije
- **Video rendering:** WebRTC APIs, HTML5 Canvas za screen display

Komunikacijski sloj:

- **WebSocket server:** Socket.io ili native WebSocket implementation
- **API framework:** Express.js za REST endpoints
- **Authentication:** JWT (JSON Web Tokens) za session management
- **Encryption:** OpenSSL biblioteke za TLS/SSL, crypto biblioteke za E2EE

Browser podrška (Admin Panel):

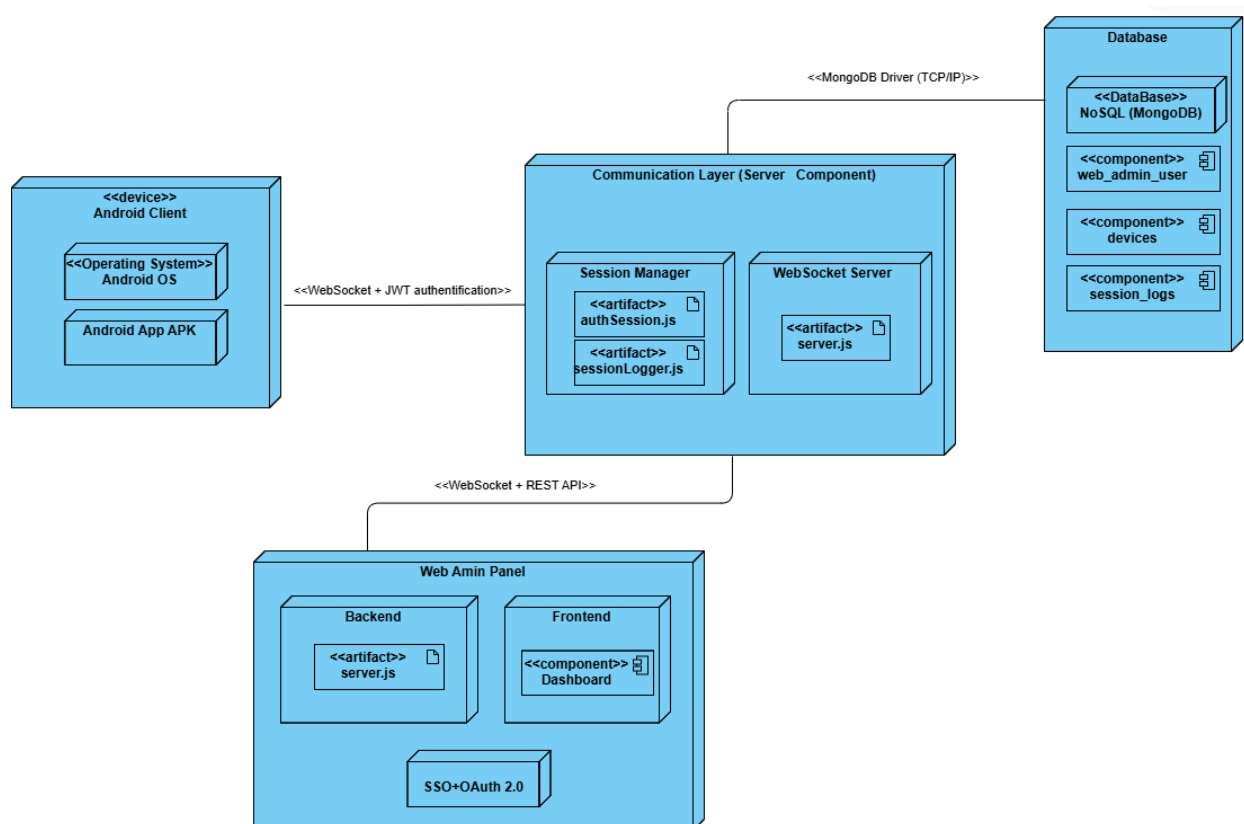
- Chrome 90+, Firefox 88+, Safari 14+, Edge 90+
- WebRTC podrška obavezna
- JavaScript ES2020+ podrška

Sigurnosni zahtevi:

- Firewall konfiguracija za ograničavanje pristupa
- Anti-virus softver na serverskim komponentama
- Regular security updates i patch management sistem

Ovaj softverski interfejs obezbeđuje pouzdanu, sigurnu i skalabilnu arhitekturu koja podržava sve planirane funkcionalnosti sistema.

Komunikacijski interfejs i dijagram raspoređivanja



Slika 8. Dijagram raspoređivanja sistema

Nefunkcionalni zahtjevi

End to end enkripcija (E2EE) za prenos podataka

Svi podaci koji se prenose između klijenta i servera moraju biti šifrovani od izvora do odredišta, bez mogućnosti presretanja ili pristupa od strane trećih strana.

Podrška za najmanje 1.000 istovremenih sesija

Sistem mora skalirati i održavati stabilnost pri rukovanju s najmanje 1.000 paralelnih korisničkih veza bez značajnog pada performansi.

Vremenski odziv za komande treba biti manji od 100ms u optimalnim mrežnim uslovima

Kada su mrežni uslovi optimalni (npr. niska latencija, stabilna konekcija), sistem mora izvršavati korisničke komande unutar 100 milisekundi.

Efikasnost potrošnje baterije – maksimalno 5% CPU pri mirovanju

Aplikacija mora biti optimizovana tako da troši $\leq 5\%$ procesorskih resursa (CPU) kada se ne koristi aktivno, kako bi se očuvala baterija uređaja.

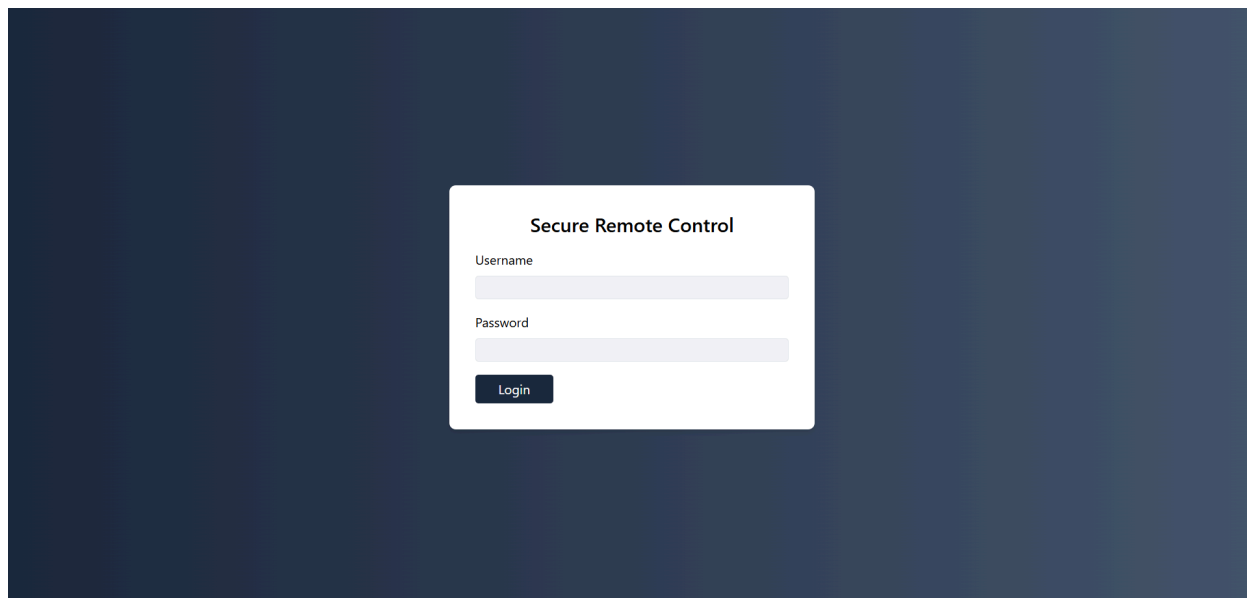
Usklađenost sa GDPR i ISO 27001 sigurnosnim standardima

Sistem mora obezbijediti zaštitu podataka u skladu sa regulativom Opšte uredbe o zaštiti podataka (GDPR) i standardima informaciono-bezbjednog menadžmenta (ISO/IEC 27001).

FURPS+

Funkcionalnosti

Sistem omogućava daljinsku kontrolu Android uređaja uključujući ekran sharing, slanje komandi, sesijsko logovanje i registraciju uređaja. Podržava autentifikaciju korisnika (SSO, OAuth2), sigurnu komunikaciju i prekidanje sesije sa obje strane.



Slika 9: Prikaz login forme

Dashboard

Device Registration

Sessions View

Register Admin

Session Settings

Logged in as administrator

Connected

Q

Search by name or model...

All Status

All Network Types

DEVICE	STATUS	NETWORK	IP ADDRESS	LAST ACTIVE	ACTIONS
<div><div></div><div>test</div><div>SM-A137F</div></div>	active	-	-	8. 6. 2025. 08:55:09	<div>Unregister</div>
<div><div></div><div>Xiaomi 12</div><div>2201123G</div></div>	active	-	-	8. 6. 2025. 08:51:10	<div>Unregister</div>
<div><div></div><div>abc</div><div>sdk_gphone64_x86_64</div></div>	active	-	-	27. 5. 2025. 21:26:50	<div>Unregister</div>
<div><div></div><div>Musa's Device</div><div>M2101K7AG</div></div>	inactive	-	-	8. 6. 2025. 11:19:41	<div>Unregister</div>
<div><div></div><div>OldVerTest</div><div>2201123G</div></div>	inactive	-	-	8. 6. 2025. 09:10:46	<div>Unregister</div>
<div><div></div><div>Adna-gr1</div><div>SM-S901B</div></div>	inactive	-	-	6. 6. 2025. 23:59:28	<div>Unregister</div>
<div><div></div><div>ImadA52s</div><div>SM-A528B</div></div>	inactive	-	-	6. 6. 2025. 23:59:28	<div>Unregister</div>

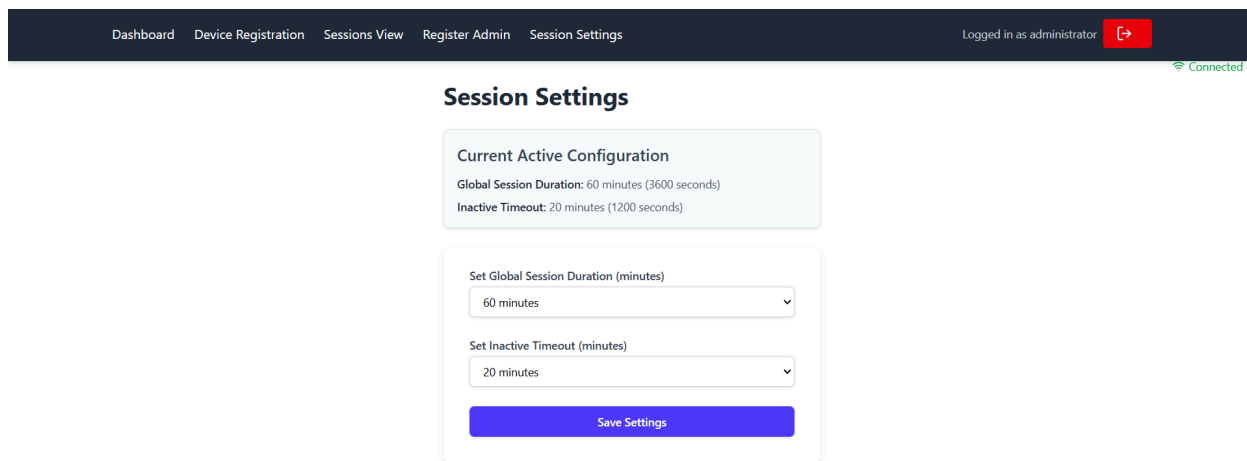
Slika 10: Prikaz registrovanih uređaja

The screenshot shows a web application interface with a dark blue header. The header contains navigation links: Dashboard, Device Registration, Sessions View, Register Admin, and Session Settings. On the right side of the header, it says "Logged in as administrator" with a red button containing a right arrow icon. A green "Connected" status indicator is visible in the top right corner. The main content area is light blue and features a white card titled "Device Registration" with a blue mobile phone icon. Inside the card, there is a "Device Name" label, a text input field with the placeholder "Enter device name", and a descriptive text "Enter a descriptive name for the Android device". At the bottom of the card is a blue button labeled "Register Device".

Slika 11: Prikaz forme za registraciju uređaja

The screenshot shows a web application interface with a dark blue header. The header contains navigation links: Dashboard, Device Registration, Sessions View, Register Admin, and Session Settings. On the right side of the header, it says "Logged in as administrator" with a red button containing a right arrow icon. A green "Connected" status indicator is visible in the top right corner. The main content area is light blue and features a white card titled "Session Logs for test123". Inside the card, there is a section for "Session 1" with the following details: Device: test123, Session ID: eyJhbGciOiJIUzI1NiIs..., Date of Session: 27. 5. 2025, Start Time: 18:10:08, End Time: 18:10:43, and Duration: 0m 35s. Below these details is a list of log entries with timestamps and descriptions of session events. At the bottom of the card, there are three buttons: "Export as TXT", "Export as CSV", and "Export as Excel". Below the card, there are three buttons: "Previous", "Page 1 of 2", and "Next".

Slika 12: Prikaz sesijskih logova



Slika 13: Konfiguracija sesije

Upotrebljivost

Web-based kontrolni panel je dizajniran za IT osoblje s intuitivnim interfejsom i jasnim prikazom statusa uređaja. Krajnji korisnici imaju transparentan uvid u sesiju, a interakcije su svedene na minimum radi jednostavnosti korištenja.

Pouzdanost

Sistem koristi TLS 1.2 i E2EE za sigurnost i pouzdanost komunikacije. Mehanizmi za automatsko zatvaranje sesije u slučaju prekida veze i logovanje svih aktivnosti povećavaju stabilnost i sigurnost sistema.

Performanse

Sistem podržava 1,000+ istovremenih sesija uz kašnjenje ispod 100ms u optimalnim uslovima. Android aplikacija je optimizovana za nisku potrošnju resursa ($\leq 5\%$ CPU pri mirovanju), što omogućava dugotrajnu upotrebu bez uticaja na performanse uređaja.

Podržanost

Sistem je modularno dizajniran (klijent, admin, komunikacioni sloj), što omogućava lako održavanje i nadogradnju. Dokumentacija, standardi poput GDPR-a i ISO 27001, te skalabilnost ka većem broju uređaja i korisnika doprinose dugoročnoj podržanosti i proširivosti sistema.

Implementacijski zahtjevi

Sistem mora biti razvijen koristeći moderne tehnologije: **Android (Jetpack Compose)** za klijentsku aplikaciju, **React.js** za web kontrolni panel i **Node.js/Express** za komunikacijski sloj. Komunikacija između klijenta i servera mora koristiti **TLS 1.2** i **WebSocket** za dvosmjernu, real-time interakciju, a baza podataka treba da podržava visoku dostupnost i skalabilnost

Ograničenja interfejsa

Web interfejs mora biti kompatibilan s modernim browserima (Chrome, Firefox, Edge). Klijentska aplikacija mora podržavati Android uređaje sa verzijom **Android 8.0 (API 26)** i novije. UI mora biti responsivan i prilagođen za desktop uređaje, dok mobilna aplikacija mora biti intuitivna za sve vrste korisnika (raznog iskustva i različite životne dobi).

Fizički zahtjevi

Serveri na kojima se pokreće komunikacijski sloj moraju imati stabilnu internet konekciju i podržavati minimalno 1,000 simultanih WebSocket konekcija. Klijentski Android uređaji moraju imati pristup internetu i minimalne hardverske resurse (1 GB RAM, 1 GHz CPU). Sistem se može hostovati u cloud okruženju (npr. Render, Railway) ili na lokalnim virtualnim mašinama.

Ograničenja dizajna

Sistem mora omogućiti šifrovanu komunikaciju od početka do kraja bez mogućnosti presretanja podataka. Aplikacija ne smije narušavati privatnost korisnika — mora prikazivati aktivnu sesiju i omogućiti prekid u svakom trenutku. Arhitektura mora biti modularna, s jasno odvojenim slojevima (klijent, admin, komunikacija), radi lakšeg održavanja i nadogradnje.

SRS za android aplikaciju

Uvod

Ovaj dokument predstavlja specifikaciju softverskih zahtjeva (Software Requirement Specification - SRS) SecureRemoteControl sistema. Za opis sistema biće korišten FURPS model.

Svrha

Svrha ovog dokumenta je da definiše softverske zahtjeve za aplikaciju Secure Remote Control. Ovaj dokument precizno opisuje funkcionalnosti, nefunkcionalne zahtjeve, interfejse i ograničenja sistema, kako bi se obezbijedilo zajedničko razumijevanje između svih uključenih strana — uključujući klijente, članove razvojnog tima, testere i buduće korisnike sistema.

Kome je namijenjen

Sistem je specijalno kreiran za kompanije i organizacije koje zahtijevaju pouzdano i sigurno daljinsko upravljanje svojim uređajima i infrastrukturom. Namijenjen je IT administratorima, tehničkom osoblju, kao i ovlaštenim korisnicima koji nadgledaju ili upravljaju uređajima sa udaljenih lokacija. Može poslužiti i kao konkretan primjer primjene sigurnih komunikacionih protokola u upravljanju distribuiranim sistemima.

Obim projekta

Secure Remote Control aplikacija je razvijena s ciljem da omogući sigurno i pouzdano daljinsko upravljanje uređajima putem Android platforme. Sistem je dizajniran tako da korisnicima pruži jednostavan i efikasan način nadzora i kontrole udaljenih uređaja u realnom vremenu, uz visok nivo sigurnosti i zaštite podataka. Komunikacija između mobilne aplikacije i uređaja odvija se putem sigurnih kanala, čime se osigurava zaštita od neovlaštenog pristupa i gubitka informacija.

Aplikacija je prilagođena korisnicima kojima je neophodan siguran pristup distribuiranim sistemima bez potrebe za direktnim fizičkim kontaktom s uređajima, olakšavajući im rad i ubrzavajući procese upravljanja. Pored osnovnih funkcionalnosti upravljanja, sistem je osmišljen da bude fleksibilan i spreman za buduće nadogradnje i integracije.

Razvoj aplikacije uzima u obzir kako sigurnosne, tako i upotrebljivosti aspekte, nastojeći da pruži intuitivno korisničko iskustvo bez kompromisa u pogledu funkcionalnosti i zaštite.

Opis sistema

Perspektiva proizvoda

Secure Remote Control Android aplikacija predstavlja jednu od ključnih komponenti šireg sistema koji se sastoji od tri međusobno povezana podsistema: mobilne aplikacije, web platforme i komunikacionog sloja. Cjelokupan sistem razvija se u sklopu timskog projekta, gdje svaka grupa ima jasno definisanu odgovornost nad određenim dijelom sistema.

Mobilna aplikacija, koju razvija naša grupa, zadužena je za omogućavanje sigurnog i intuitivnog pristupa krajnjim korisnicima koji putem svojih mobilnih uređaja komuniciraju sa udaljenim sistemima. Ova aplikacija funkcioniše kao klijentska komponenta i oslanja se na server koji obezbjeđuje komunikaciju i obradu zahtjeva, kao i na web interfejs koji koriste administratori za nadzor i konfiguraciju.

Aplikacija je razvijena tako da se besprijekorno integriše u širu arhitekturu sistema, uz korištenje standardizovanih komunikacionih protokola i mehanizama autentifikacije. Ima ulogu povezivanja korisnika sa udaljenim uređajima, omogućavajući im izvršavanje osnovnih operacija, pregled statusa sistema i pravovremeno reagovanje u slučaju promjena ili problema.

U kontekstu cjelokupnog sistema, Android aplikacija predstavlja alat za svakodnevnu upotrebu u pokretu, osiguravajući dostupnost ključnih funkcionalnosti korisnicima bez obzira na njihovu fizičku lokaciju, čime se značajno doprinosi fleksibilnosti i efikasnosti upravljanja udaljenim uređajima.

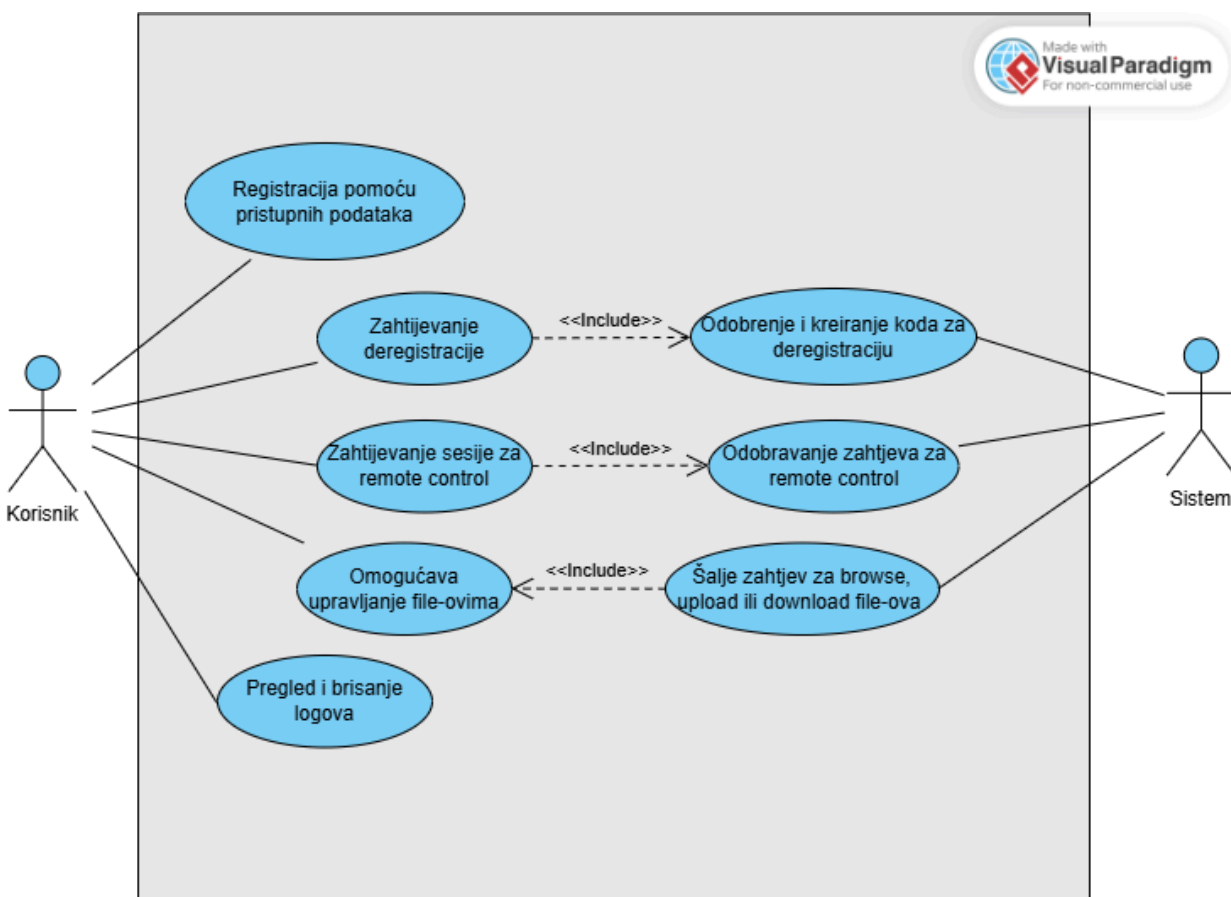
Korisničke klase i njihove karakteristike uz Activity i Use Case dijagrame

Korisnici Secure Remote Controle android aplikacije mogu imati ulogu Korisnika.

Use Case dijagram prikazuje osnovne interakcije između korisnika i Android aplikacije za sigurnu daljinsku kontrolu uređaja.

Korisnik putem aplikacije ima mogućnost registracije i deregistracije uređaja, upravljanja sesijama daljinske kontrole, pregledanja i brisanja logova aktivnosti, kao i upravljanja fajlovima na udaljenom uređaju (pregled, prenos i preuzimanje).

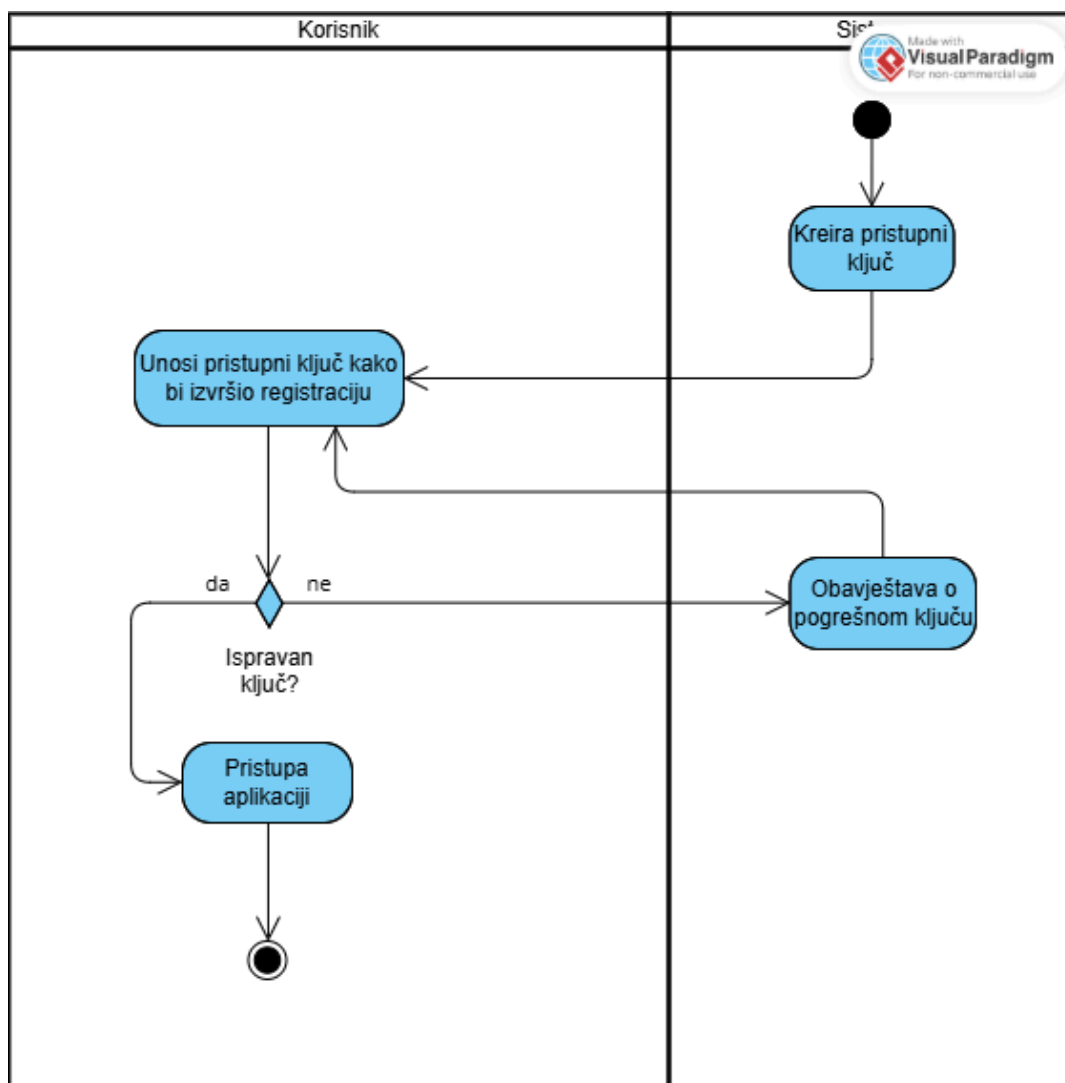
Ove funkcionalnosti su grupisane oko centralnog aktera – korisnika, koji komunicira s aplikacijom kako bi ostvario željene operacije u sigurnom i kontrolisanom okruženju. Dijagram služi za vizualizaciju osnovnih tokova upotrebe sistema i identifikaciju glavnih funkcionalnosti iz korisničke perspektive.



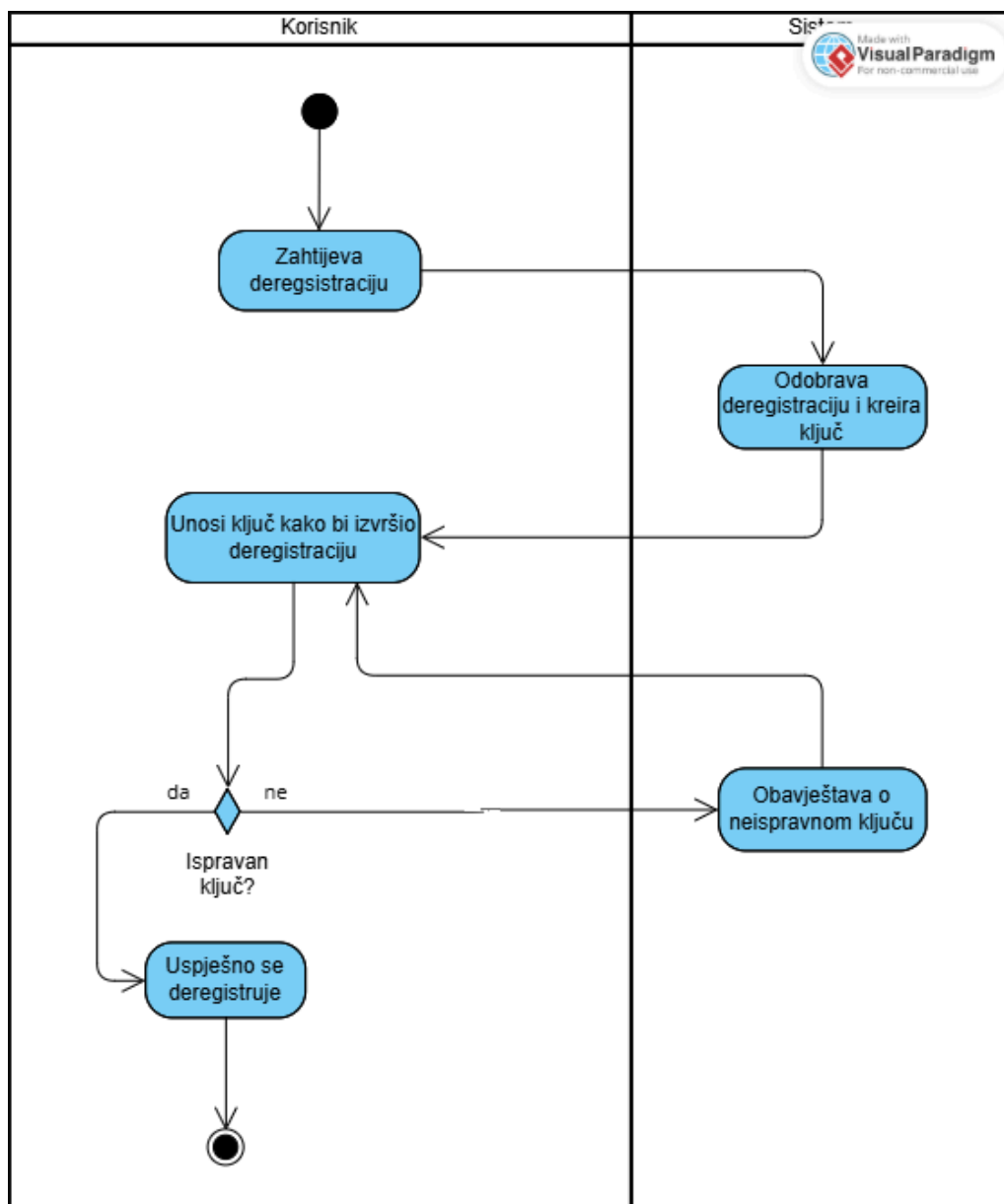
Slika 1: Dijagram slučajeva upotrebe za Korisnika

Korisnik ima mogućnost korištenja sljedećih funkcionalnosti:

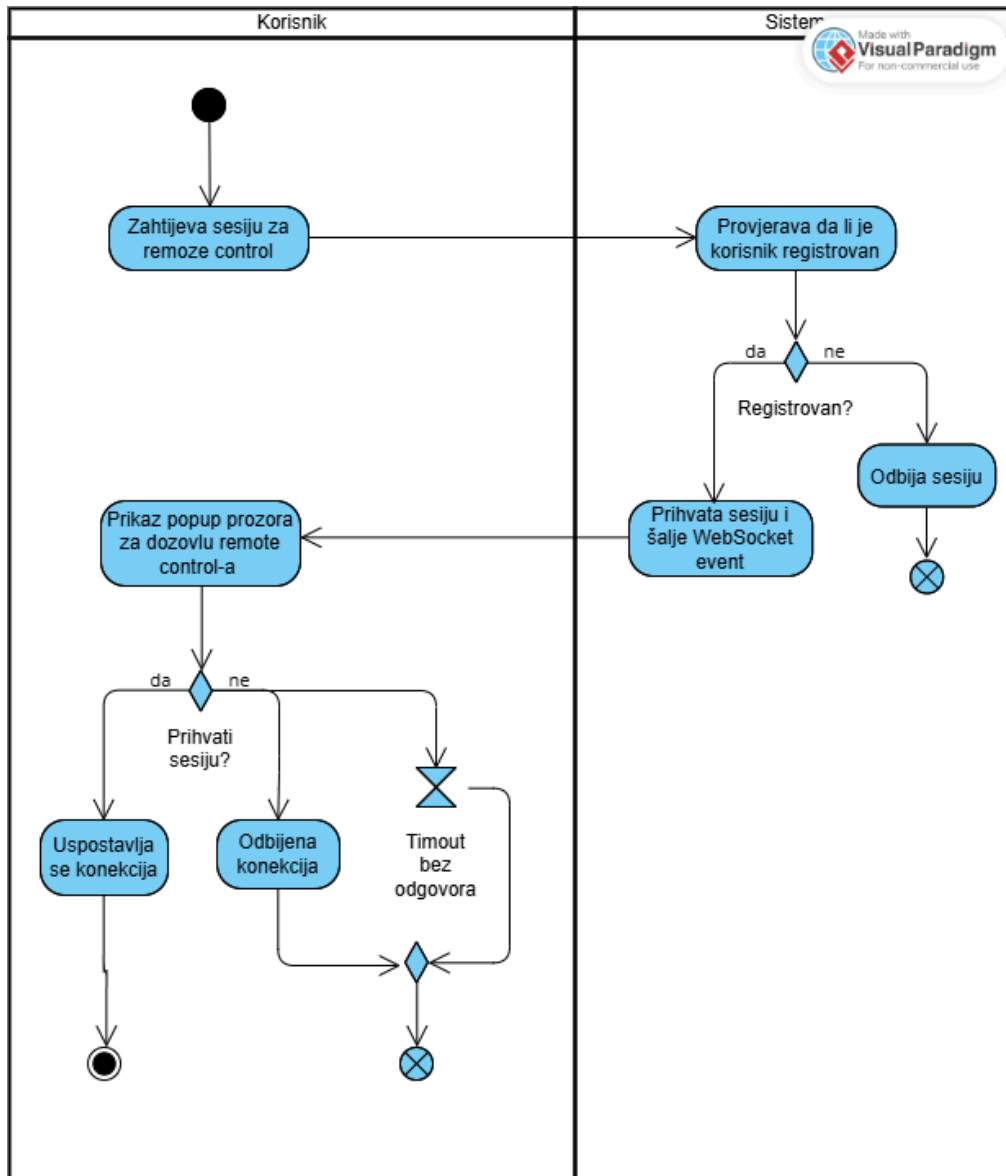
- Mogućnost registracije
- Mogućnost deregistracije
- Zahtijevanje sesije za remote control
- Pregled i brisanje logova aktivnosti
- Upravljanje file-ovima(browse, upload, download)



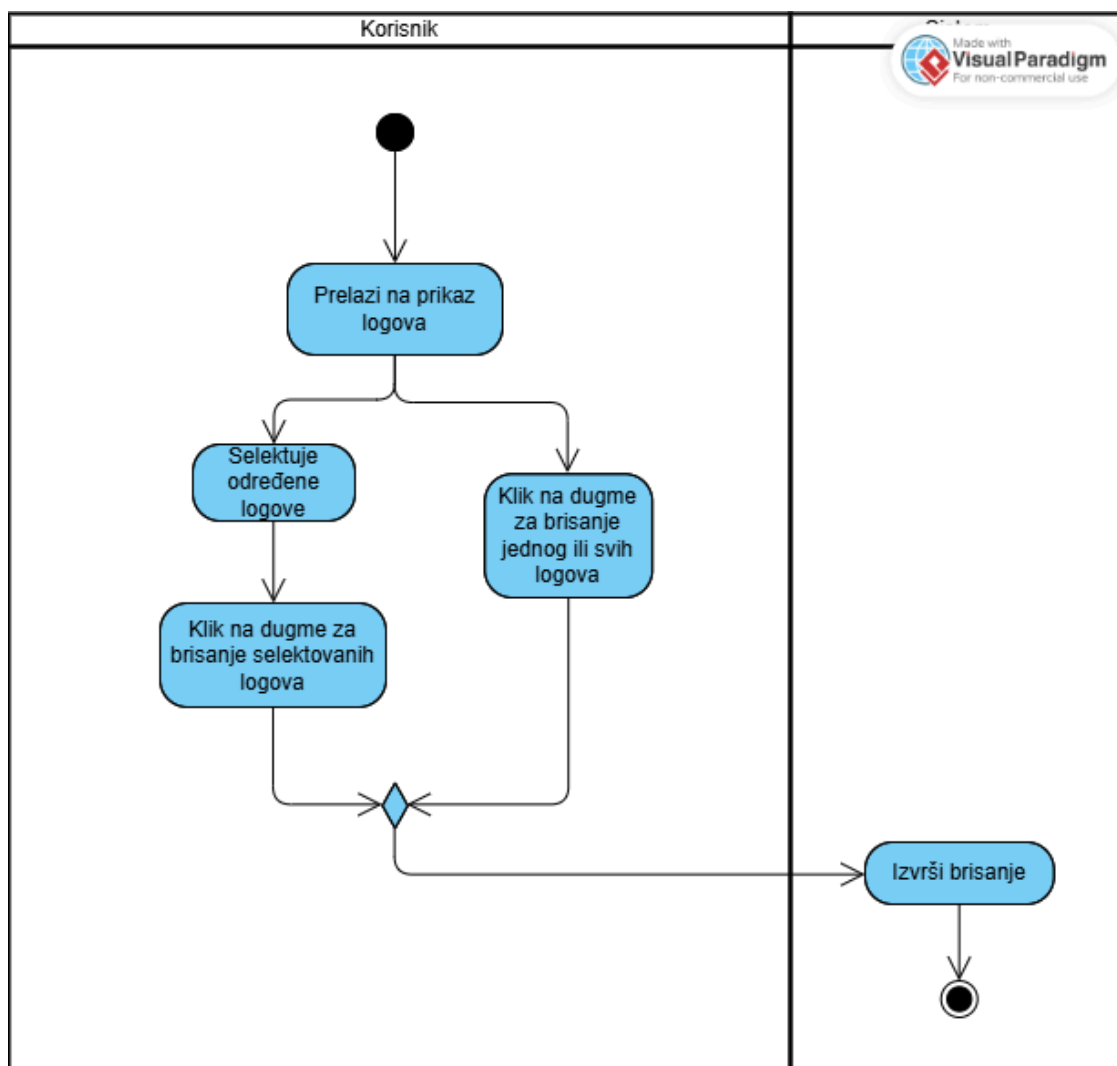
Slika 2: Dijagram aktivnosti za registraciju korisnika



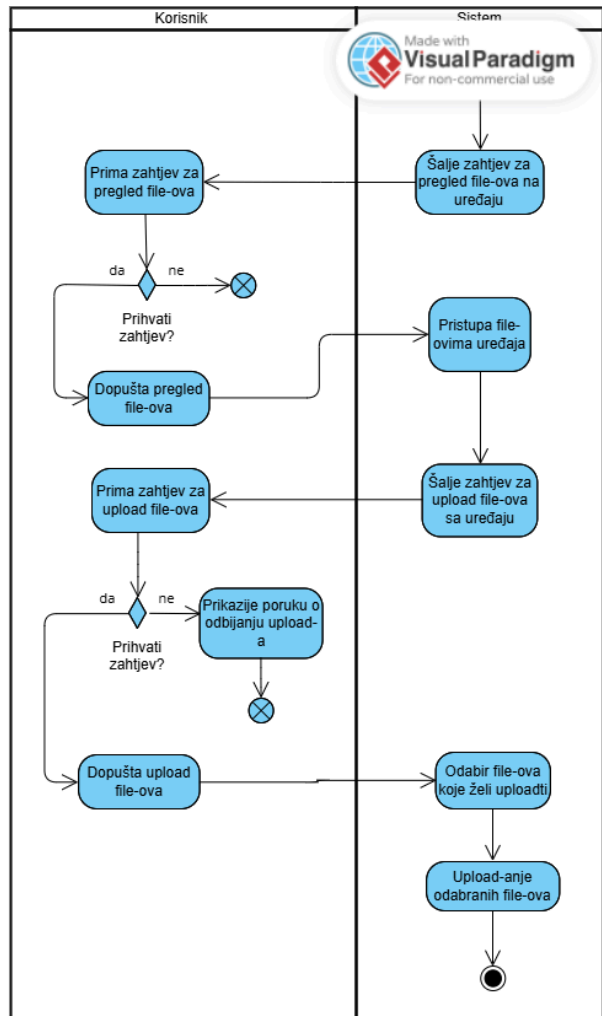
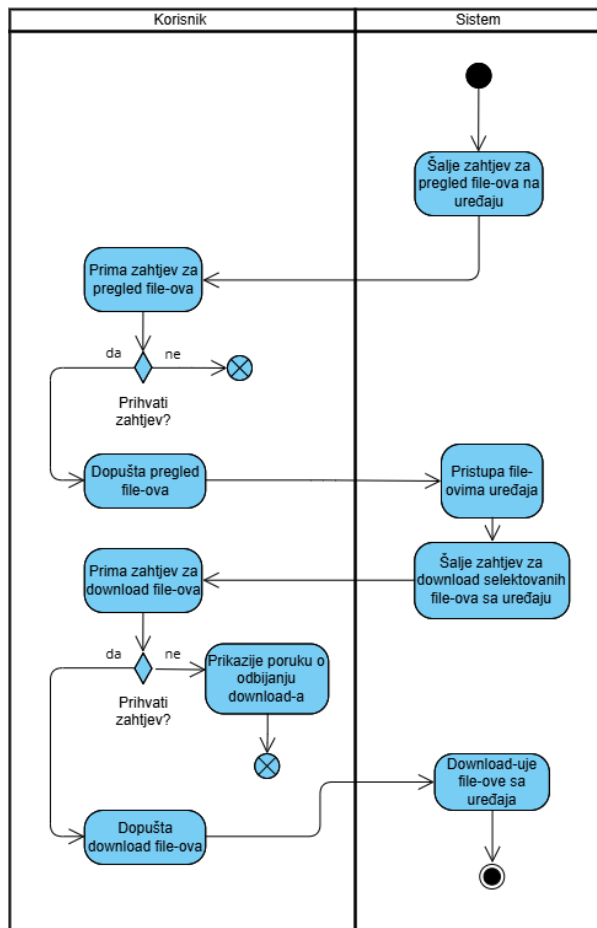
Slika 3: Dijagram aktivnosti za deregistraciju Korisnika



Slika 4: Dijagram aktivnosti za zahtjev sesije



Slika 5: Dijagram aktivnosti za upravljanje logovima



Slika 6: Dijagrami aktivnosti za browse, download i upload file-ova

Operativno okruženje

Secure Remote Control sistem implementiran je na principu klijent-server arhitekture, s centralizovanom cloud komunikacionom tačkom koja omogućava sigurnu razmjenu podataka i upravljanje udaljenim uređajima. Sistem se sastoji iz tri glavne komponente: web administratorski panel, Android klijentska aplikacija i serverski komunikacioni sloj.

Admin panel (web aplikacija) :

- Operativni sistemi: Linux (preporučeno: Ubuntu Server 20.04 LTS ili noviji). Lokalni razvoj je moguć i na Windows i macOS platformama.

Klijent (Android aplikacija) :

- Operativni sistem: Android 8 (API 26) kao minimum, preporučeno Android 12+ zbog stabilnosti funkcionalnosti kao što su WebRTC i screen-capture.
- Podržani uređaji: Svi moderni Android telefoni i tableti sa najmanje 4 GB RAM-a i podrškom za Accessibility Services.

Server-side komunikacioni sloj :

- Operativni sistem: Linux (preporučeno: Ubuntu Server 20.04 LTS ili noviji)
- Mrežni zahtjevi: Minimum 10 Mbps za upload i download, zbog real-time prenosa podataka
- Deployment: Cloud platforme kao što su Railway i Render sa ugrađenom CI/CD podrškom

Ograničenja dizajna i implementacije

- Frontend aplikacija razvijena je korištenjem React biblioteke u kombinaciji sa TailwindCSS za stilizaciju i Vite kao alatom za razvoj i optimizaciju.
- Backend sistem razvijen je u [Node.js](#) okruženju koristeći Express framework, WebSocket komunikaciju i MongoDB kao bazu podataka.
- U implementaciji se koristi JWT autentikacija i bcrypt za sigurno čuvanje lozinki.
- Android aplikacija koristi Jetpack Compose za UI, dok su Retrofit i OkHttp zaduženi za mrežnu komunikaciju.
- WebRTC funkcionalnost implementirana je lokalno na Android uređaju i koristi native biblioteke

- Docker je korišten isključivo za lokalni razvoj i testiranje, dok se produkcijski deployment vrši direktno iz repozitorija na cloud platformu.
- Komunikacija između web panela, Android aplikacije i servera mora se odvijati isključivo putem sigurnih WebSocket (WSS) veza.
- Aplikacija na Android uređaju zahtjeva određene sistemske dozvole, uključujući pristup Accessibility Service-u i Media Projection servisu, koji mogu biti blokirani na nekim uređajima od strane proizvođača.
- Backend server mora biti sposoban da simultano podrži preko 1000 aktivnih sesija, što zahtjeva minimalno 8 GB RAM-a i SSD skladište.

Dijagram komponenti

Na slici ispod prikazan je **dijagram komponenti SecureRemoteControl sistema**, koji ilustruje ključne softverske module i njihovu međusobnu povezanost unutar tri glavne cjeline:

1. Client-Side App (Android)

Ova komponenta predstavlja korisničku stranu aplikacije koja omogućava direktnu interakciju s udaljenim uređajem. Sadrži module kao što su:

- **Push Notification Control** – prima obavijesti o novim sesijama ili događajima.
- **Foreground Service i Background Service** – omogućavaju kontinuiran rad aplikacije, čak i kada nije u fokusu.
- **Remote Control, Screen Sharing, Session Handling, Device Registration** – ključne funkcionalnosti za upravljanje sesijama i uređajem.

2. Communication Layer (Remote Control Gateway)

Ovaj sloj služi kao posrednik između klijenta i web panela:

- **WebRTC Signaling** – omogućava uspostavljanje P2P konekcije za screen sharing.
- **WebSocket Server i Command Relay** – omogućavaju dvosmjernu komunikaciju u realnom vremenu.

- **Device Registry, Session Logs, Session Authentication** – komponente za upravljanje uređajima, zapisima aktivnosti i autentifikaciju sesija.

3. Controller (Web Admin Panel)

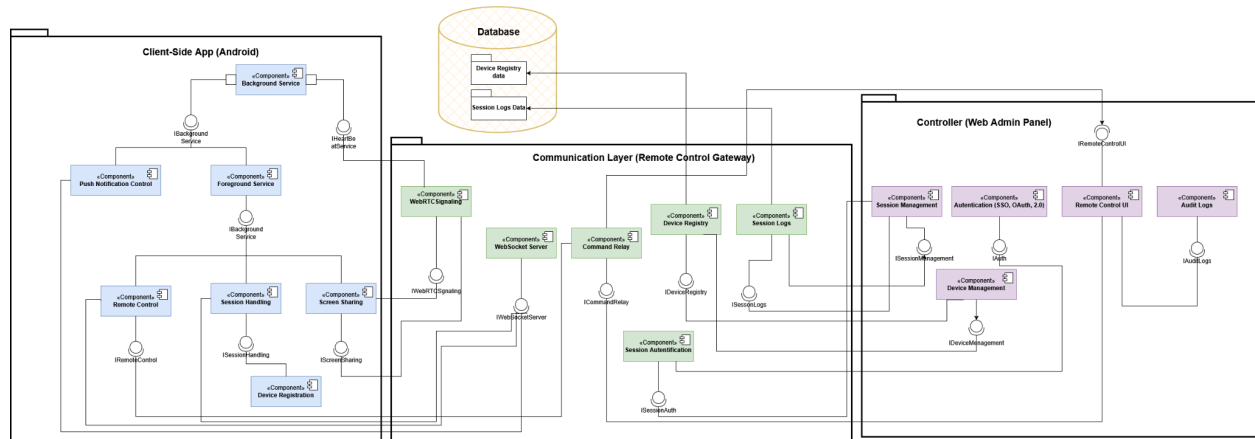
Web panel omogućava administratorima nadzor i upravljanje uređajima i korisnicima:

- **Session Management, Device Management, Authentication (SSO, OAuth 2.0)** – omogućavaju kontrolu nad korisnicima i uređajima.
- **Remote Control UI** – korisnički interfejs za daljinsko upravljanje iz pretraživača.
- **Audit Logs** – komponenta za evidenciju i reviziju aktivnosti korisnika.

4. Baza podataka (Database)

Centralizovana baza podataka sadrži:

- **Device Registry Data** – informacije o registrovanim uređajima.
- **Session Logs Data** – detalji o svim sesijama kontrole.



Nefunkcionalni zahtjevi

Upotrebljivost sistema

Korisnički interfejs sistema Secure Remote Control osmišljen je tako da omogućiti administratorima i korisnicima jednostavno, intuitivno i efikasno upravljanje uređajima na daljinu. Web administratorski panel koristi jasan i responzivan dizajn koji omogućava brzo snalaženje bez potrebe za dugim obukama. Korišteni su čitki fontovi, logično strukturirani meniji i jasno označene funkcionalnosti. Mobilna Android aplikacija koristi moderne UI komponente preko Jetpack Compose-a, uz podršku za razne veličine ekrana i jednostavno korisničko iskustvo prilagođeno touch uređajima.

Sigurnost sistema

Sigurnost je ključna komponenta sistema. Komunikacija između klijenta i servera vrši se isključivo putem šifrovanih WebSocket (WSS) konekcija. Pristup sistemu je zaštićen token-baziranom autentikacijom (JWT), a korisničke lozinke se pohranjuju u heširanom obliku pomoću bcrypt algoritma. Pristup osjetljivim funkcijama kao što su daljinsko upravljanje, snimanje ekrana i slanje komandi omogućen je samo nakon eksplicitne autorizacije korisnika uređaja.

Dostupnost sistema

Sistem je dizajniran da bude visoko dostupan, sa ciljem dostupnosti od najmanje 99.7% vremena tokom godine. Server-side komponenta je hostovana na cloud platformama (npr. Railway, Render) koje nude automatski failover, horizontalno skaliranje i dnevni backup podataka. Web panel je dostupan iz svih modernih web pretraživača i operativnih sistema, dok se Android aplikaciji može pristupiti sa bilo kojeg Android 8+ uređaja.

Održavanje sistema

Održavanje sistema podrazumijeva dvije odvojene cjeline:

- Tim za infrastrukturu (zadužen za servere, CI/CD i cloud deployment)
- Tim za aplikacioni sloj (zadužen za održavanje frontend i backend koda)

CI/CD pipeline automatski pokreće testove i deployment na svaku promjenu koda. Sistem je dizajniran tako da podržava proširenje funkcionalnosti bez potrebe za velikih refaktoringom - koriste se modularna arhitektura i Docker za lokalni razvoj i testiranje.

Skalabilnost sistema

Sistem mora podržavati rad sa velikim brojem povezanih korisnika i uređaja, s planiranim kapacitetom od 1000+ aktivnih sesija istovremeno. Komunikacioni sloj (WebSocket server) je optimizovan za horizontalno skaliranje i može biti postavljen na više instanci kako bi se obradilo veće opterećenje. Baza podataka (MongoDB) koristi indekse za brzi pristup sesijama i logovima.

Performanse sistema

Sistem je optimizovan za brz odziv i rad u realnom vremenu. Administratorski panel prosječno odgovara na korisničke zahtjeve unutar 300ms, dok komunikacija između servera i Android klijenta putem WebSocket-a ostvaruje kašnjenje ispod 100ms. Android aplikacija koristi moderne i lagane tehnologije, omogućavajući brzo učitavanje i glatko korisničko iskustvo. Performanse mogu biti privremeno pogođene slabijim hardverom ili lošom internet konekcijom, ali je sistem dizajniran da funkcioniše stabilno i pod opterećenjem.

FURPS+

Funkcionalnosti

Sistem SecureRemoteControl omogućava korisnicima sigurno daljinsko upravljanje Android uređajima putem mobilne aplikacije, kao i administratorski nadzor putem web panela. Ključne funkcionalnosti uključuju prijavu i registraciju korisnika, registraciju i deregistraciju uređaja, uspostavljanje i upravljanje sesijama daljinske kontrole, kao i pregled, prijenos i preuzimanje fajlova sa udaljenog uređaja. Korisnici također imaju mogućnost pregleda i brisanja logova aktivnosti. Administratori putem web panela upravljaju korisnicima, uređajima i sesijama, te imaju pristup audit logovima. Komunikacija unutar sistema odvija se u realnom vremenu putem sigurnih WebSocket konekcija, uz autentifikaciju i autorizaciju baziranu na JWT tokenima.

Upotrebljivost

Prema ISO standardu, upotrebljivost predstavlja mjeru u kojoj korisnici mogu efikasno i sa zadovoljstvom koristiti aplikaciju za ostvarenje svojih ciljeva. Interfejs aplikacije je dizajniran intuitivno, uz jasan raspored elemenata i bez suvišnih informacija, kako bi korisnici brzo savladali osnovne funkcije, čak i bez prethodnog iskustva.

Pouzdanost

Pouzdanost sistema ogleda se u sposobnosti aplikacije da radi stabilno i bez grešaka tokom dužeg vremenskog perioda. Sistem je dizajniran tako da se kvarovi svedu na minimum zahvaljujući upotrebi sigurnih tehnologija kao što su JWT autentifikacija, enkripcija lozinki putem bcrypt-a, kao i jasno definisanim greškama i validacijama na backendu. U slučaju nepredviđenih problema ili prekida rada, podaci se čuvaju u pouzdanoj MongoDB bazi koja omogućava redovan backup i brzu restauraciju sistema.

Performanse

Aplikacija koristi Node.js i Express za brz i skalabilan rad servera, uz podršku real-time komunikacije putem WebSocket-a. Podaci se efikasno upravljaju u MongoDB bazi, čime se omogućava brzo izvršavanje upita i responzivno korisničko iskustvo. Frontend koristi React i Vite, koji omogućavaju brzo pokretanje i renderovanje aplikacije. Vremena odziva aplikacije su minimalna čak i prilikom istovremenog korištenja više korisnika.

Podržanost

Sistem se može lako održavati zahvaljujući modularnoj strukturi koda i korištenju modernih alata. Svi API-jevi su dokumentovani i testirani putem Swaggera, čime je olakšano testiranje i budući razvoj. Docker je korišten za lokalni razvoj, dok se produkcijsko okruženje postavlja direktno na cloud, čime se olakšava deployment i održavanje.

Implementacijski zahtjevi

- **Frontend:** React.js, Vite, TailwindCSS, Axios
- **Backend:** Node.js, Express, JWT, bcrypt, dotenv, ws
- **Baza podataka:** MongoDB
- **Android aplikacija:** Kotlin, Jetpack Compose, Retrofit, WebRTC, Dagger Hilt
- **Autentifikacija:** JWT tokeni

Fizički zahtjevi

Server treba imati instaliran Node.js, otvorene portove 5000 i 5001 za backend komunikaciju, te podršku za MongoDB. Za Android klijent potrebne su određene dozvole sistema.

Ograničenja dizajna

- **Vremensko ograničenje:** Sprintovi su morali biti završeni unutar unaprijed definisanih rokova.
- **Tehnološki stack:** Odabrani stack (Node.js + React + MongoDB) je definisan unaprijed i nije bilo moguće koristiti alternativne tehnologije.

Vanjski zahtjevi interfejsa

Sistem **SecureRemoteControl** koristi jasno definisane interfejse za sigurnu i efikasnu komunikaciju između svojih podsistema. Komunikacija između Android aplikacije, servera i web administratorskog panela odvija se primarno putem **sigurnih WebSocket (WSS)** konekcija, uz podršku za WebRTC i push notifikacije.

WebSocket API (Glavni komunikacioni kanal)

WebSocket veza predstavlja osnovu za kompletnu razmjenu podataka unutar sistema. Sve ključne funkcionalnosti, uključujući:

- registraciju i autentifikaciju korisnika i uređaja,
 - upravljanje sesijama daljinske kontrole,
 - slanje i prijem komandi,
 - sinkronizaciju statusa uređaja,
- realizovane su kroz **šifrovane WSS konekcije**.

Korisnici se autentifikuju slanjem svojih pristupnih podataka kroz WebSocket poruku, nakon čega server validira podatke i vraća JWT token. Na isti način funkcioniše i registracija novog uređaja. Ova arhitektura eliminiše potrebu za REST API komunikacijom, omogućavajući potpunu real-time obradu zahtjeva i odziva sistema.

WebRTC signaling kanal

Za screen sharing funkcionalnost koristi se WebRTC tehnologija. Android aplikacija koristi lokalne servise za snimanje ekrana, dok se signaling protokol (SDP, ICE) prenosi putem posebnog WebSocket kanala ka serverskom sloju. Ova komunikacija omogućava uspostavljanje peer-to-peer veze sa web administratorskim panelom radi daljinskog pregleda ekrana.

Push Notification servis

Aplikacija uključuje komponentu za primanje push notifikacija, kojom se korisnici obavještavaju o važnim događajima (npr. novi zahtjev za sesiju, greške, sigurnosna upozorenja). Iako nije eksplicitno navedeno, vjerovatno se koristi Firebase Cloud Messaging (FCM) kao standardni servis za Android push obavještenja.

OAuth 2.0 / SSO autentifikacija

Web administratorski panel podržava autentifikaciju putem sistema jedinstvene prijave (SSO) i vanjskih identitet provajdera koristeći OAuth 2.0 protokol. Korisnici se mogu prijaviti putem trećih servisa (npr. Google, GitHub), nakon čega server izdaje JWT token za autentifikaciju unutar sistema.

Pristup bazi podataka

Nijedna klijentska komponenta nema direktan pristup bazi podataka. Svi upiti prema bazi (registracija uređaja, pregled logova sesija itd.) vrše se putem backend komponenti “Device Registry”, “Session Logs” i sličnih. Baza podataka koristi MongoDB sa indeksiranjem za brzi pristup i sigurnosnim backup-om na serverskoj strani.