DIMS

Decentralized Identity Management System – DIMS Using Blockchain

Date: November 12, 2025

Supervisor:	Group Members:
Dr. Rashad M. Jillani	Ayesha Kashif 2022132
Co-Supervisor:	Mohammad Abdur Rehman 2022299
Muhammad Qasim Riaz	Noor ul Ain Islam 2022485

Faculty of Computer Sciences & Engineering

Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Pakistan

Decentralized Identity Management System Using Blockchain Technology

Revision History:

Revision History	*Date*	*Comments*
1.00		
2.00		

Document Approval:
The following document has been accepted and approved by the following:

Signature	*Date*	*Name*
		Dr. Rashad M. Jillani
		Muhammad Qasim Riaz

List of Contents

List of Figures

List of Tables

1. INTRODUCTION

1.1. PURPOSE

The primary purpose of this document is to specify the software requirements for the Decentralized Identity Management System for SIM Registration (DIMS-SR). This system is a critical infrastructure project designed to create a secure, tamper-proof, and auditable SIM registration process by leveraging the immutability of a blockchain (Distributed Ledger) for record-keeping and linking it with a national biometric verification system.

1.2. PRODUCT SCOPE

DIMS-SR's scope includes the development of a hybrid registration platform comprising:

1. **Mobile Client (Mobile App):** For customer self-registration, identity initiation, and secure access using MFA.
2. **Application Server:** The central component for business logic, communication with external APIs (NADRA/MNO), and logging.
3. **Blockchain Integration:** Deployment of Smart Contracts and transaction submission to the Distributed Ledger for immutable record storage.

Table 1: Terms used in this document and their description

Name	Description
BVS	Biometric Verification System
MFA	Multi-factor authentication
DIMS-SR	Decentralized Identity Management System for SIM Registration
API	Application Programmable Interface
UI	User Interface
UC	Use Case
FR	Functional Requirement
MNO	Mobile Network Operator
SSI	Self Sovereign Identity
VC	Verifiable Credentials
ZKP	Zero Knowledge Proof
DID	Decentralized Identity
TOTP	Time based one time password
IPFS	Interplanetary File System
SDK	Software Development Kit
SMTP	Simple Mail Transfer Protocol
HTTP	Hypertext transfer protocol

HTTPS	Secure Hypertext transfer protocol
TLS	Transport Layer security
DLT	Distributed Ledger Technology
PII	Personally Identifiable Information

1.3. OVERVIEW

The Decentralized Identity Management System for SIM Registration (DIMS-SR) addresses critical vulnerabilities inherent in traditional centralized SIM registration processes, primarily focusing on fraud mitigation and regulatory compliance via immutable record-keeping.

The system's core innovation lies in its hybrid design, which leverages the security and speed of existing centralized identity services (NADRA) for verification, while utilizing a Distributed Ledger Technology (DLT), specifically Smart Contracts, to enforce regulatory logic (SIM limits) and guarantee the non-repudiation of the final registration record (Write Block). This two-pronged approach ensures compliance is transparently and automatically enforced across the entire Mobile Network Operator (MNO) ecosystem.

Architecturally, DIMS-SR adopts a Three-Tier Distributed Model, with the Application Tier acting as the secure, auditable orchestrator. This design is critical for supporting dual access channels: the highly controlled Retailer BVS Client and the modern, secure Mobile Application Client. The Mobile Application, enforced by Mandatory Multi-Factor Authentication (MFA), broadens accessibility while upholding stringent security protocols, transitioning identity initiation towards a self-service, user-controlled model. The subsequent sections of this document detail the architectural rationale, the modular decomposition, and the dynamic behavior of the system using the 4+1 Architectural View Model.

2. THE OVERALL DESCRIPTION

DIMS-SR is a hybrid identity management system that mandates successful biometric verification against a central national database (e.g., NADRA) and a trustless limit check via a smart contract before any SIM registration can be finalized and recorded on an immutable ledger.

2.1. PRODUCT PERSPECTIVE

DIMS-SR is a **new, self-contained system** that functions as an intermediary layer. It replaces traditional centralized MNO registration databases with a distributed ledger for the immutable record. It integrates with three key external systems: the NADRA API, the MNO's core SIM activation system, and the Blockchain Network.

3. WORK BREAKDOWN STRUCTURE

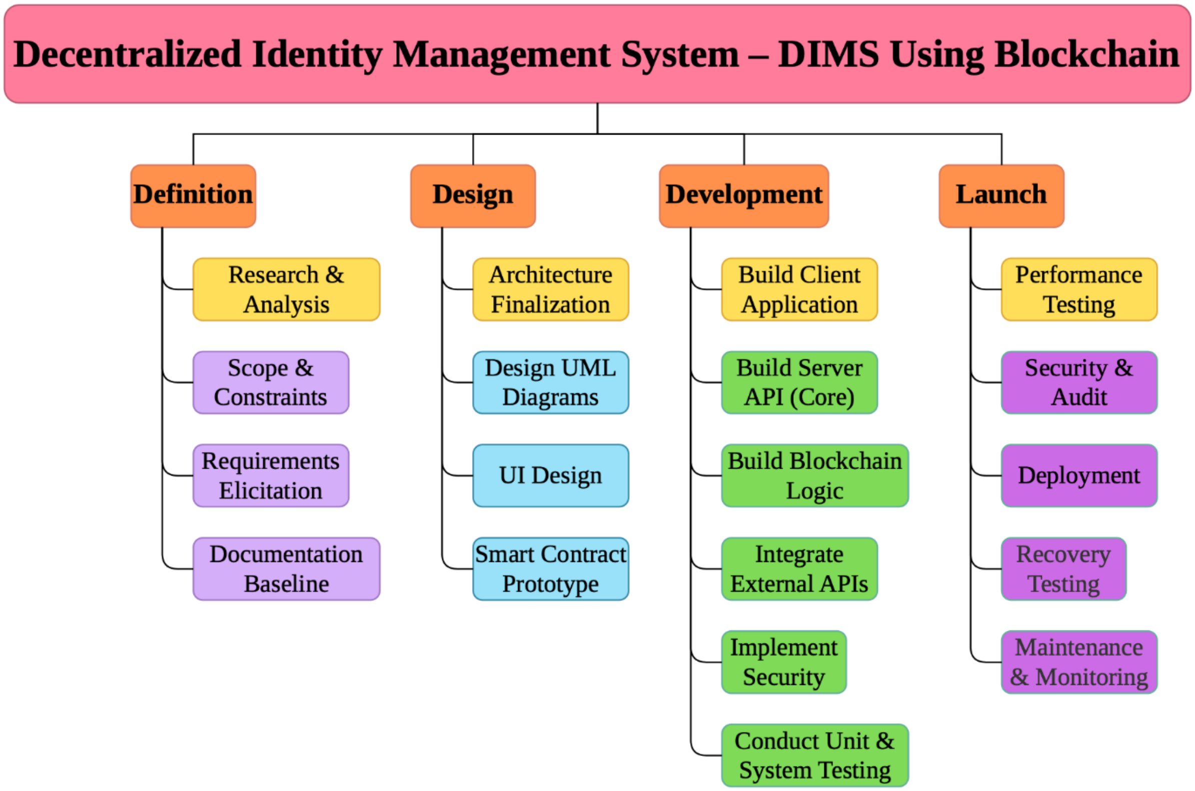


Figure 1 Work Breakdown Structure

4. Design

4.1 ARCHITECTURAL DESIGN

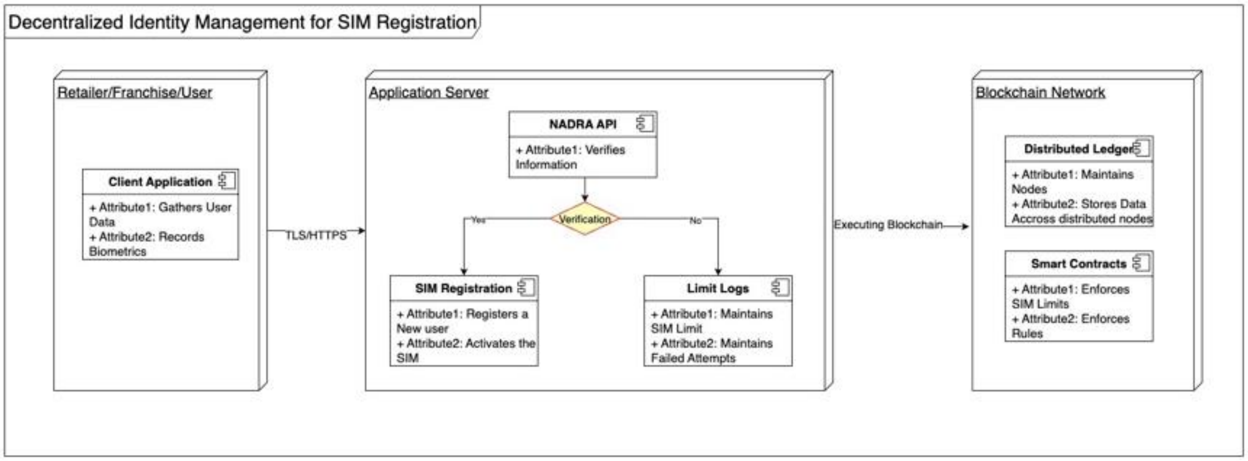

Decentralized Identity Management for SIM Registration
Retailer/Franchise/User
Client Application
+ Attribute1: Gathers User Data
+ Attribute2: Records Biometrics
TLS/HTTPS
Application Server
NADRA API
+ Attribute1: Verifies Information
Verification
Yes
No
SIM Registration
+ Attribute1: Registers a New user
+ Attribute2: Activates the SIM
Limit Logs
+ Attribute1: Maintains SIM Limit
+ Attribute2: Maintains Failed Attempts
Executing Blockchain
Blockchain Network
Distributed Ledger
+ Attribute1: Maintains Nodes
+ Attribute2: Stores Data Accross distributed nodes
Smart Contracts
+ Attribute1: Enforces SIM Limits
+ Attribute2: Enforces Rules

Figure 2. Architecture Design

4.2. Why we choose Three-Tier (N-tier) Distributed Architecture Design?

The N-Tier model was selected for the following critical reasons, specifically related to mobile client support:

- **Security Isolation (Mobile Client Protection):** The architecture rigorously isolates the highly distributed **Presentation Tier (Mobile App)** from the sensitive core logic and data tier. This containment ensures that even if a mobile client device is compromised, the integrity of the **Identity Verification Module** and the **Blockchain Client Module** remains protected. The mobile application never handles sensitive API keys or credentials for the external NADRA or the Blockchain network.
- **Separation of Concerns and Robust Communication:** The Application Tier acts as the sole secure mediator, ensuring all mobile traffic is processed via secure, stateless RESTful APIs. This decoupling facilitates the implementation of the **MFA/Auth Service Module** within the Application Tier, making authentication policy centralized and easily auditable.
- **Service Independence and Scalability:** The mobile application enables a massive potential user base. The N-Tier structure allows the Application Tier to be horizontally scaled (load balanced) to accommodate high concurrency from both the Mobile App and BVS

devices, ensuring the performance requirement is met under peak load.

4.3. MODULE IDENTIFICATION

The primary software modules in the DIMS-SR Application Tier are:

1. **Client Gateway Module:** Handles requests from both BVS and Mobile Clients, authenticates Mobile users via MFA, and manages session state.
2. **Identity Verification Module:** Manages all communication with the external NADRA API for biometric and identity verification.
3. **Blockchain Client Module:** Responsible for encoding registration data, interacting with the Limit Smart Contract, and submitting the final Write Block transaction.
4. **Logging and Alert Module:** Captures all transaction attempts, errors, and fraudulent activity (Limit Logs) and triggers administrative alerts.
5. **MFA/Auth Service Module (New Component):** This module is integral to the security model of the Mobile Application. It manages the cryptographic generation, storage, and validation of user-configured Multi-Factor Authentication tokens. Access to core system features is strictly gated by a successful challenge-response validation from this service.

5. 4+1 ARCHITECTURE VIEW MODEL

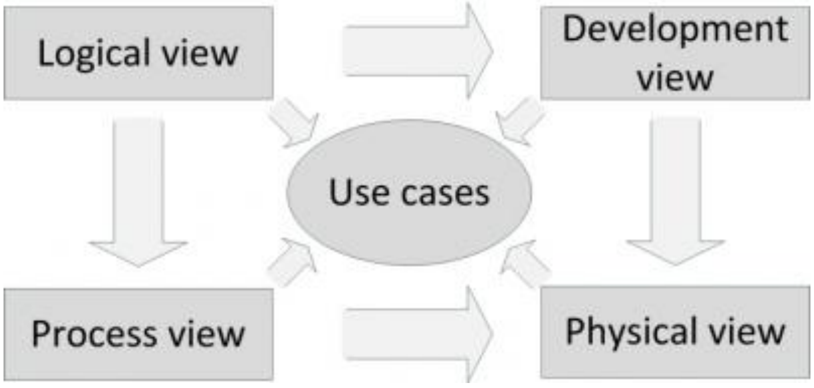


Figure 3. 4+1 Architecture View

5.1. Use Case View

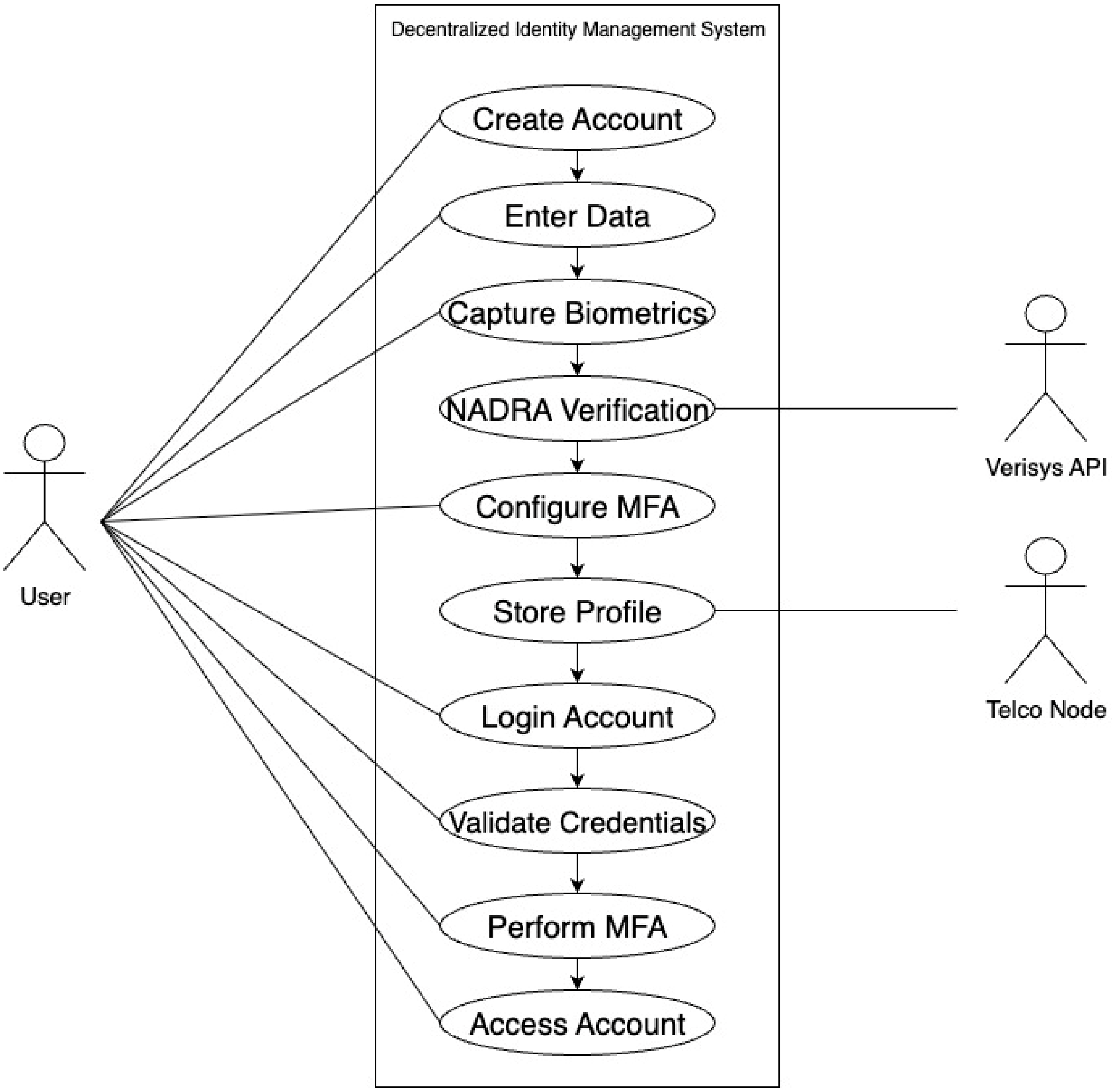


Figure 4. Create and Login Account Use Case Diagram

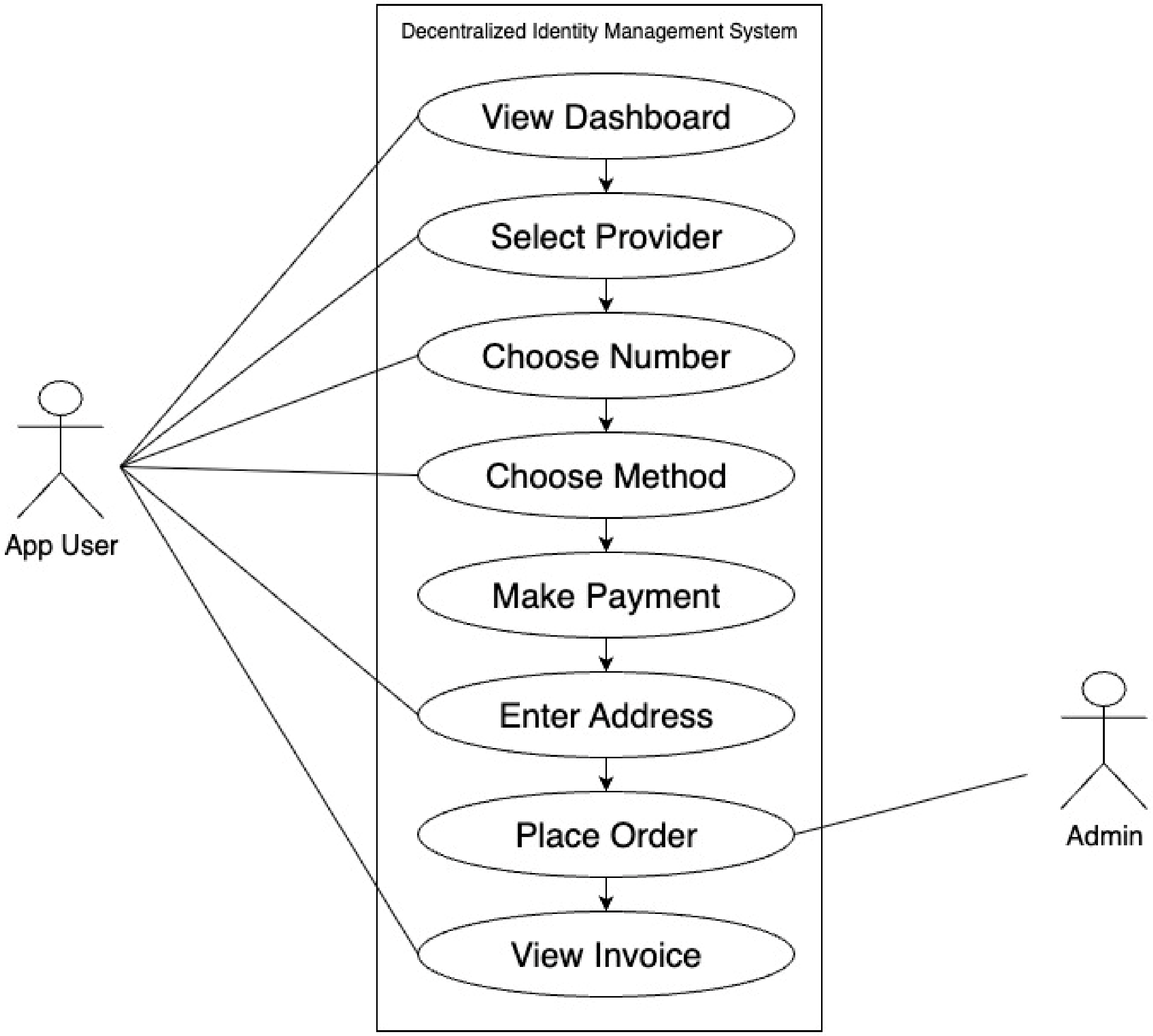


Figure 5 Registration Flow

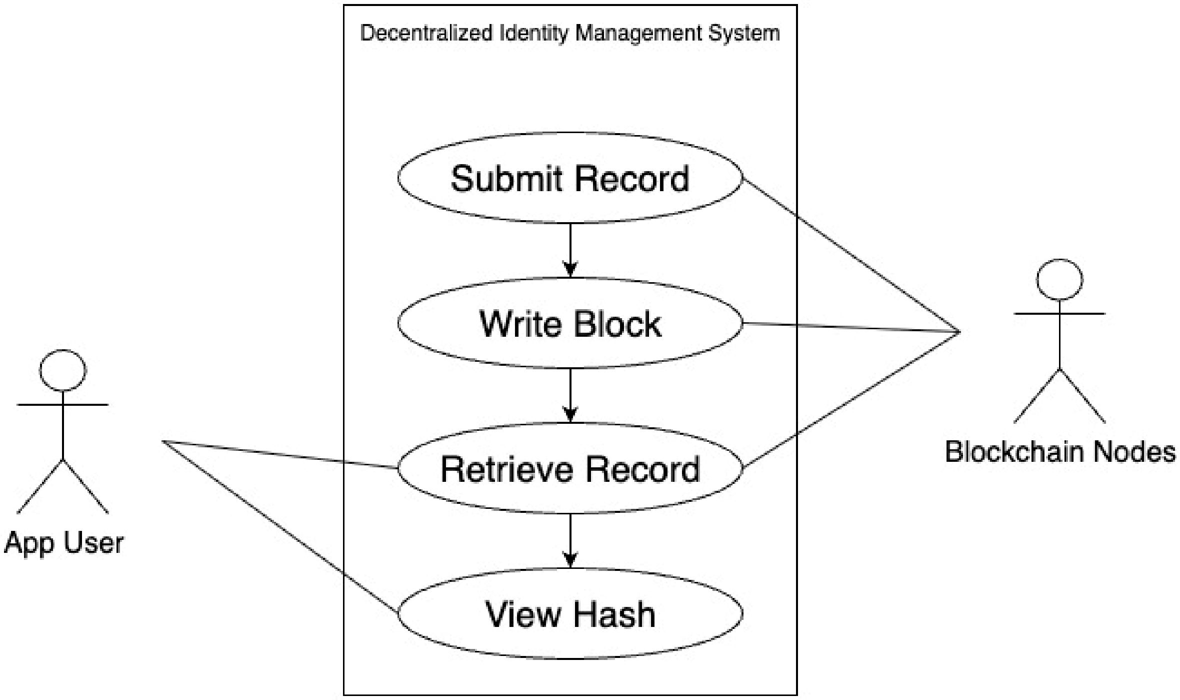


Figure 6 View Record

5.2. Logical View

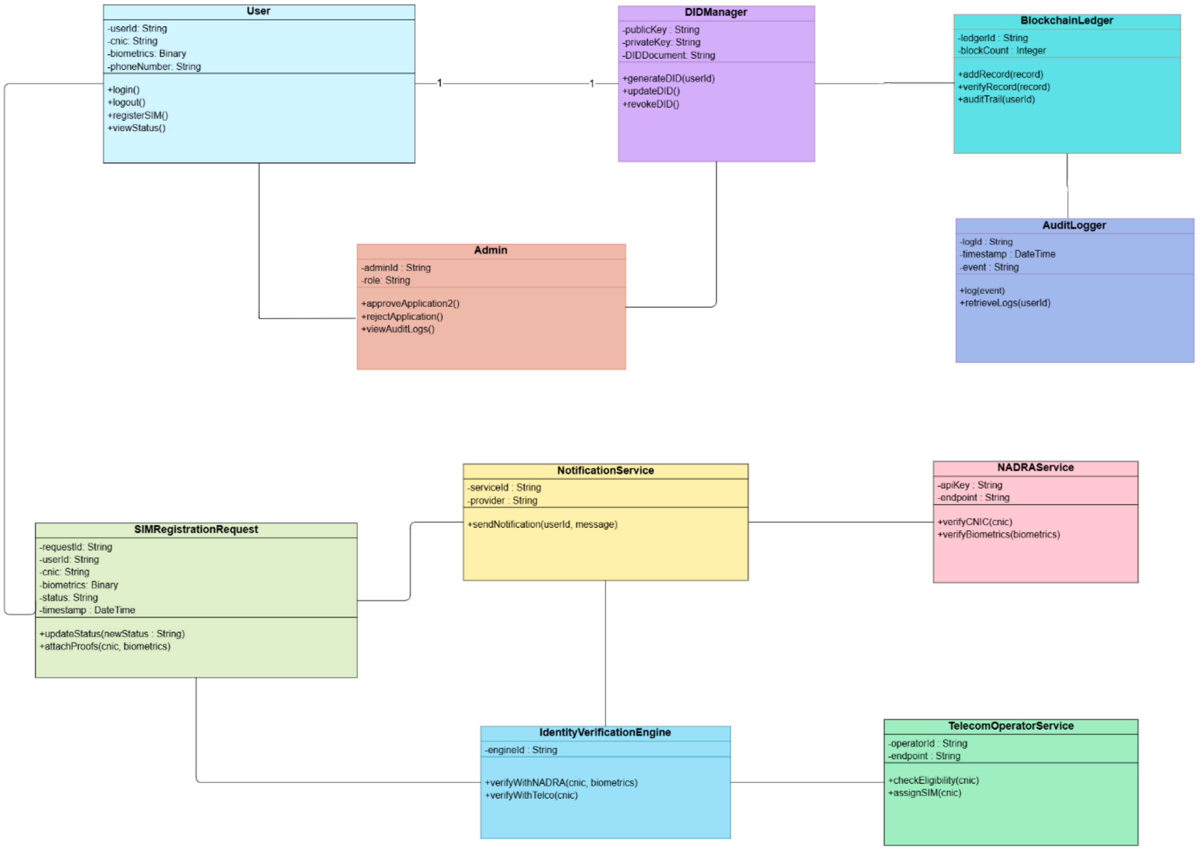


Figure 7. Logical View

5.3. Development View

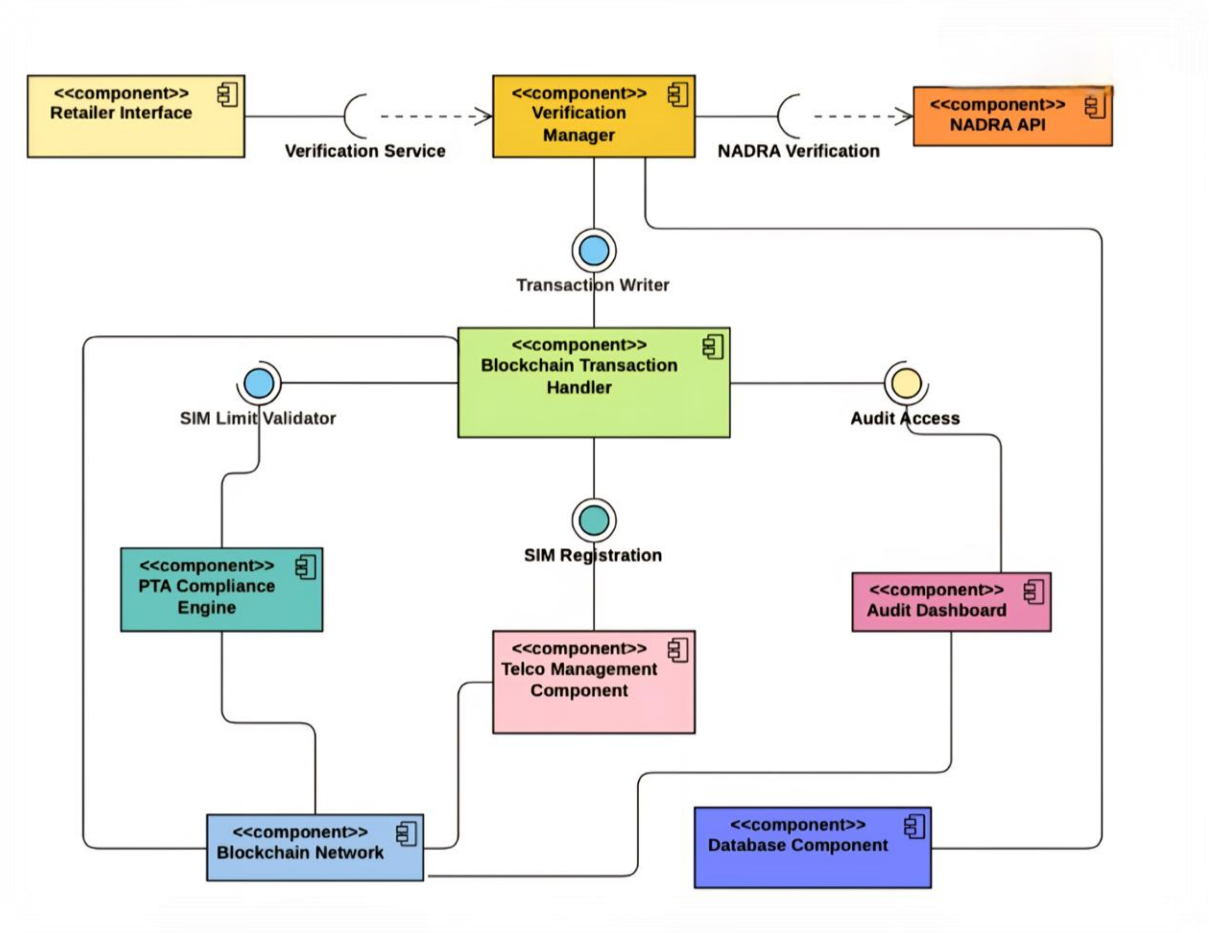


Figure 8. Development View

5.4. Process View:

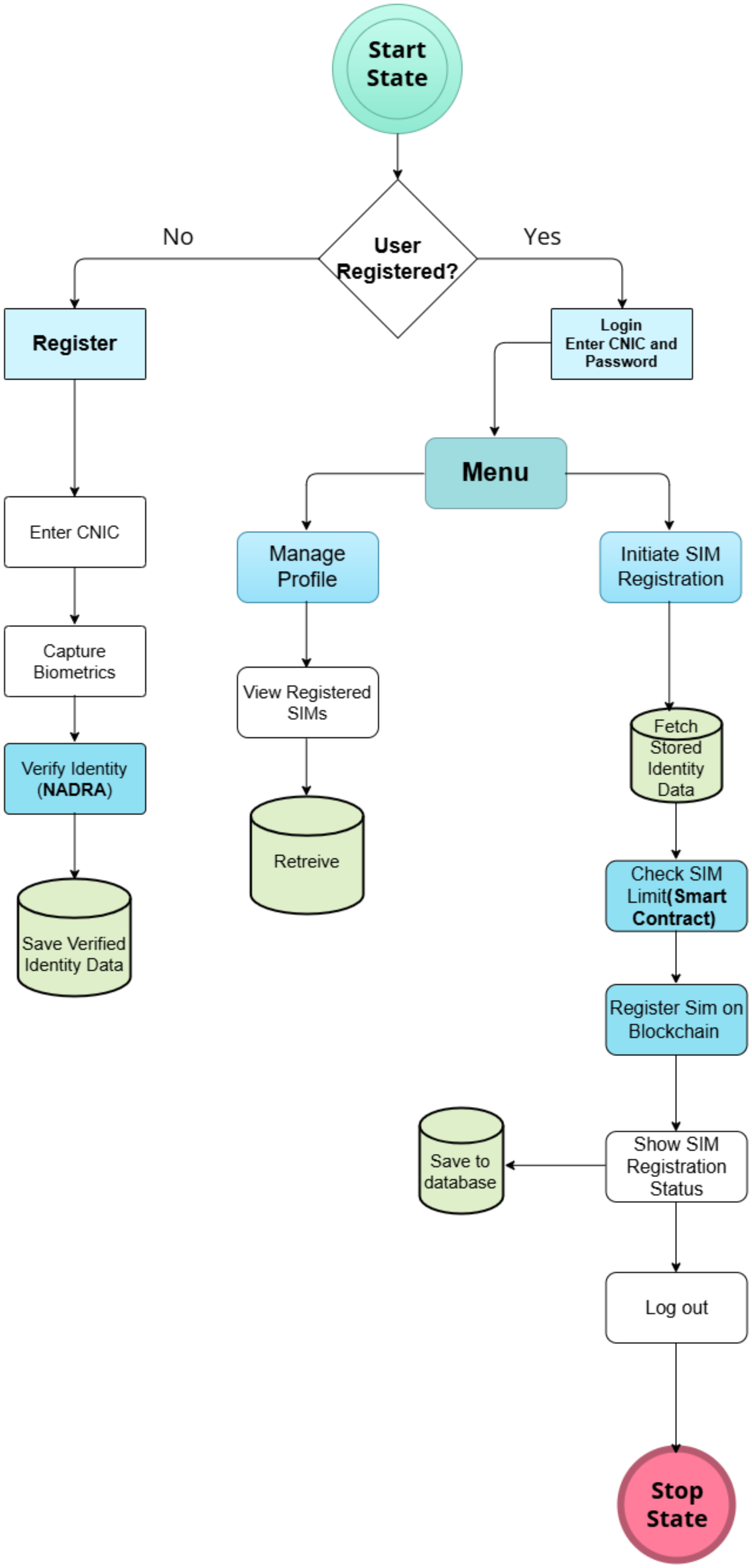


Figure 9. Process View

5.5. Physical View

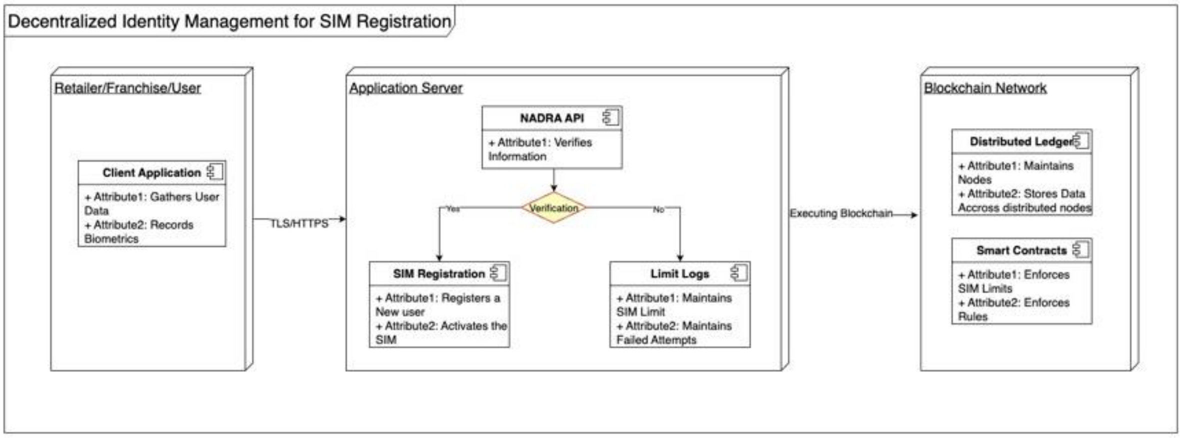
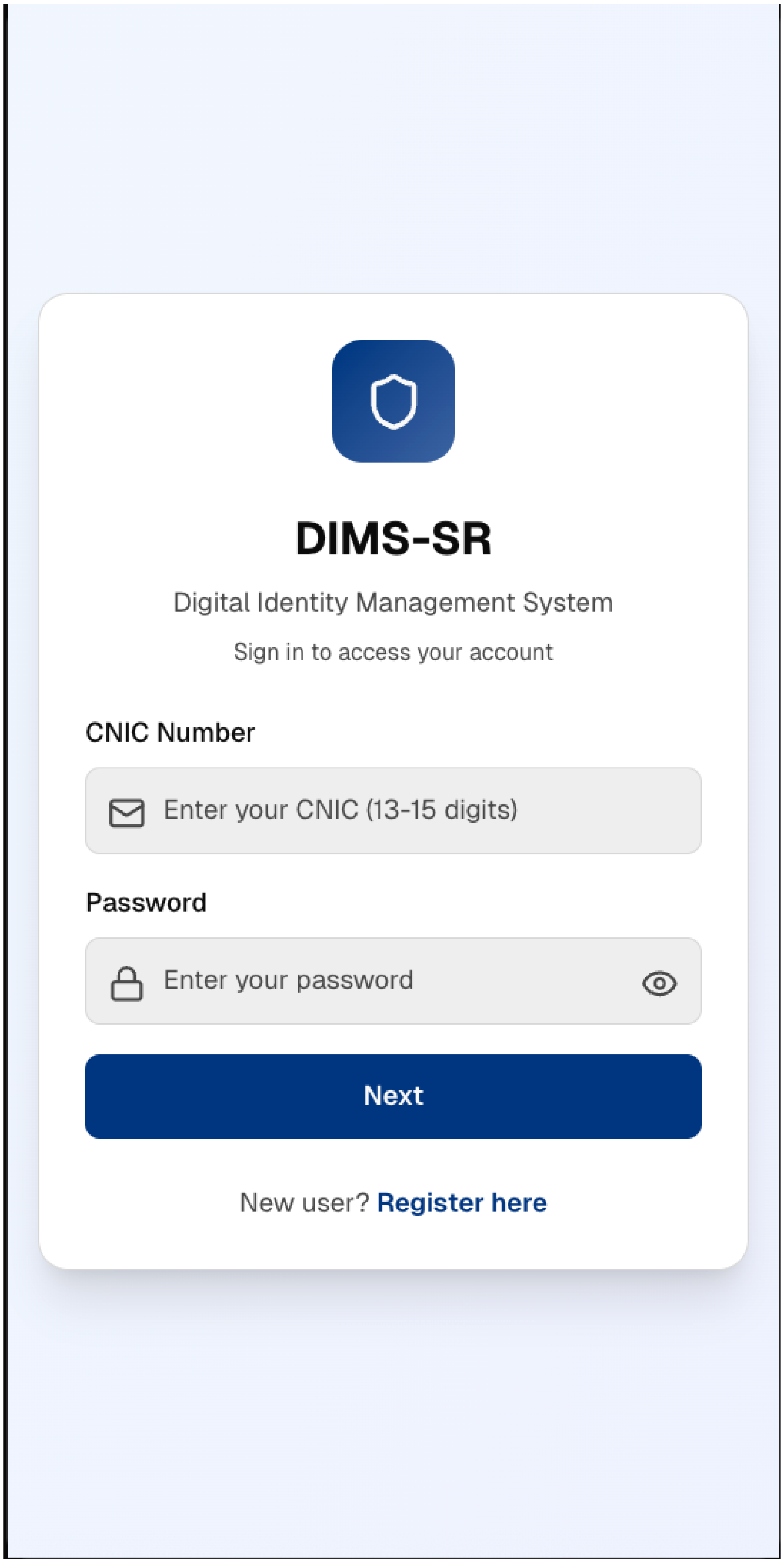

Decentralized Identity Management for SIM Registration
Retailer/Franchise/User
Client Application
+ Attribute1: Gathers User Data
+ Attribute2: Records Biometrics
TLS/HTTPS
Application Server
NADRA API
+ Attribute1: Verifies Information
Verification
Yes
No
SIM Registration
+ Attribute1: Registers a New user
+ Attribute2: Activates the SIM
Limit Logs
+ Attribute1: Maintains SIM Limit
+ Attribute2: Maintains Failed Attempts
Executing Blockchain
Blockchain Network
Distributed Ledger
+ Attribute1: Maintains Nodes
+ Attribute2: Stores Data Accross distributed nodes
Smart Contracts
+ Attribute1: Enforces SIM Limits
+ Attribute2: Enforces Rules

Figure 10. Physical View

5.6. User Interface Design:



DIMS-SR

Digital Identity Management System

Sign in to access your account

CNIC Number

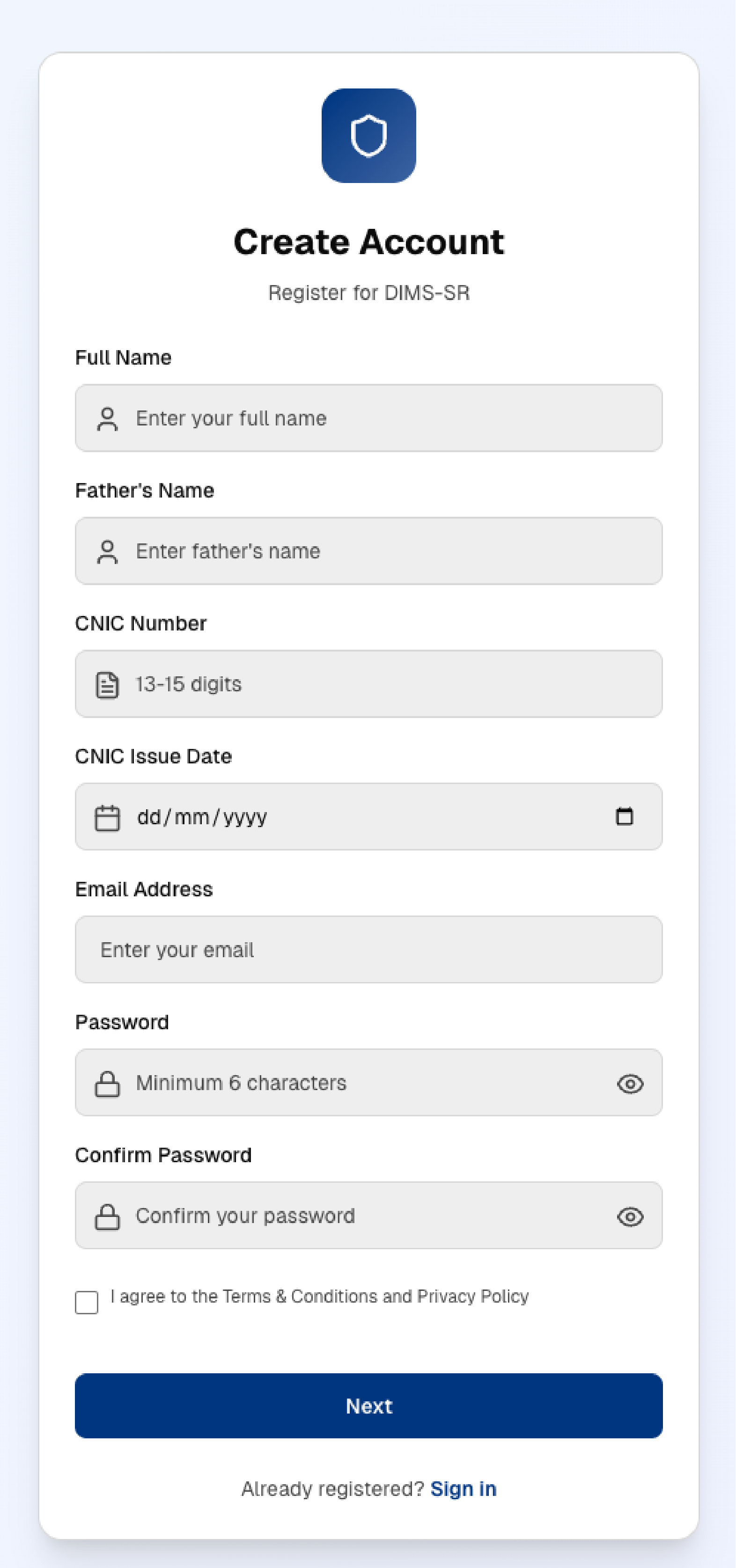
Enter your CNIC (13-15 digits)

Password

Enter your password

New user? Register here

Figure 11 Login Page



Create Account

Register for DIMS-SR

Full Name

Enter your full name

Father's Name

Enter father's name

CNIC Number

13-15 digits

CNIC Issue Date

dd/mm/yyyy

Email Address

Enter your email

Password

Minimum 6 characters

Confirm Password

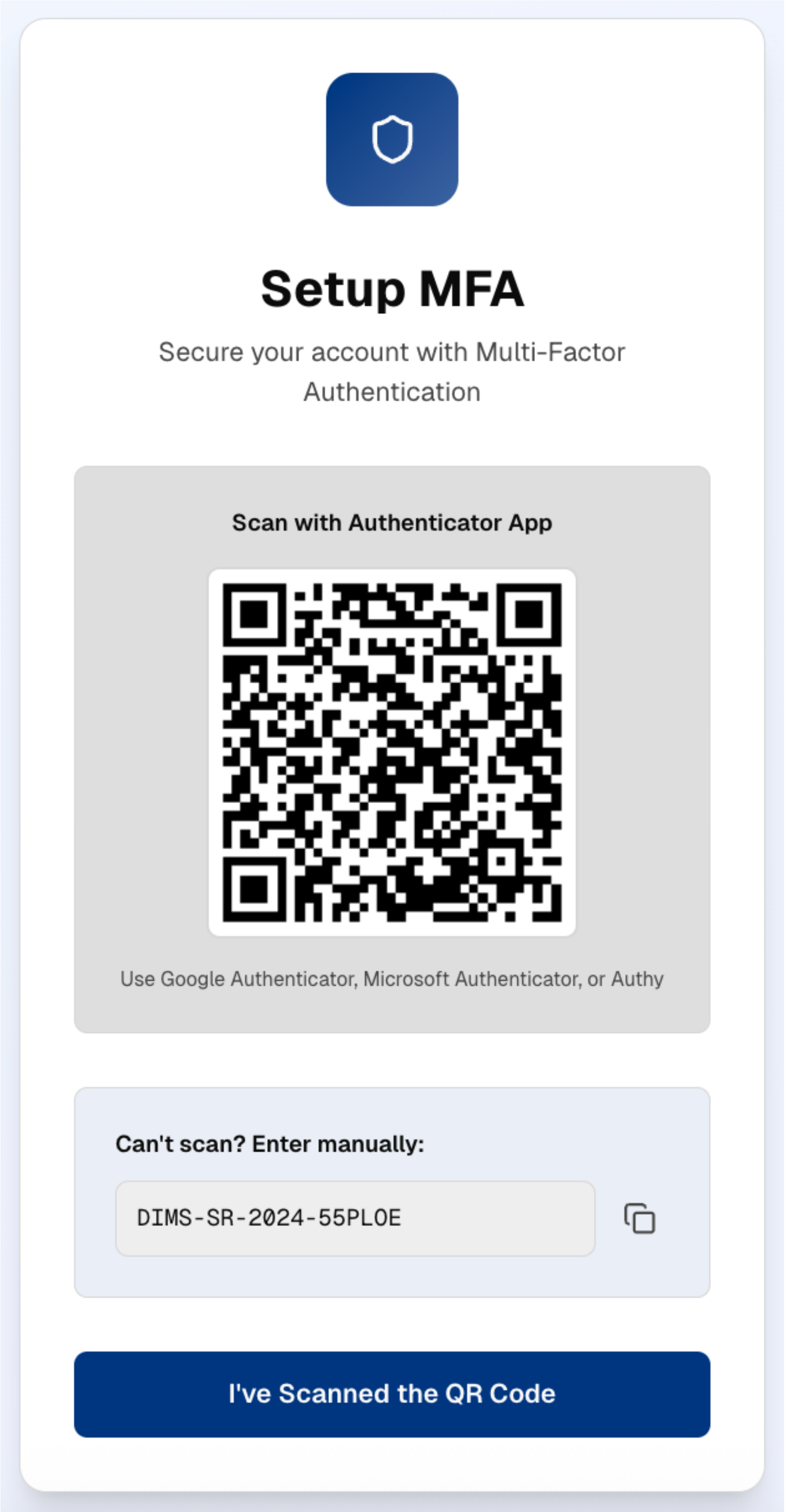
Confirm your password

□ I agree to the Terms & Conditions and Privacy Policy

Next

Already registered? Sign in

Figure 12 Create Account



Setup MFA

Secure your account with Multi-Factor Authentication

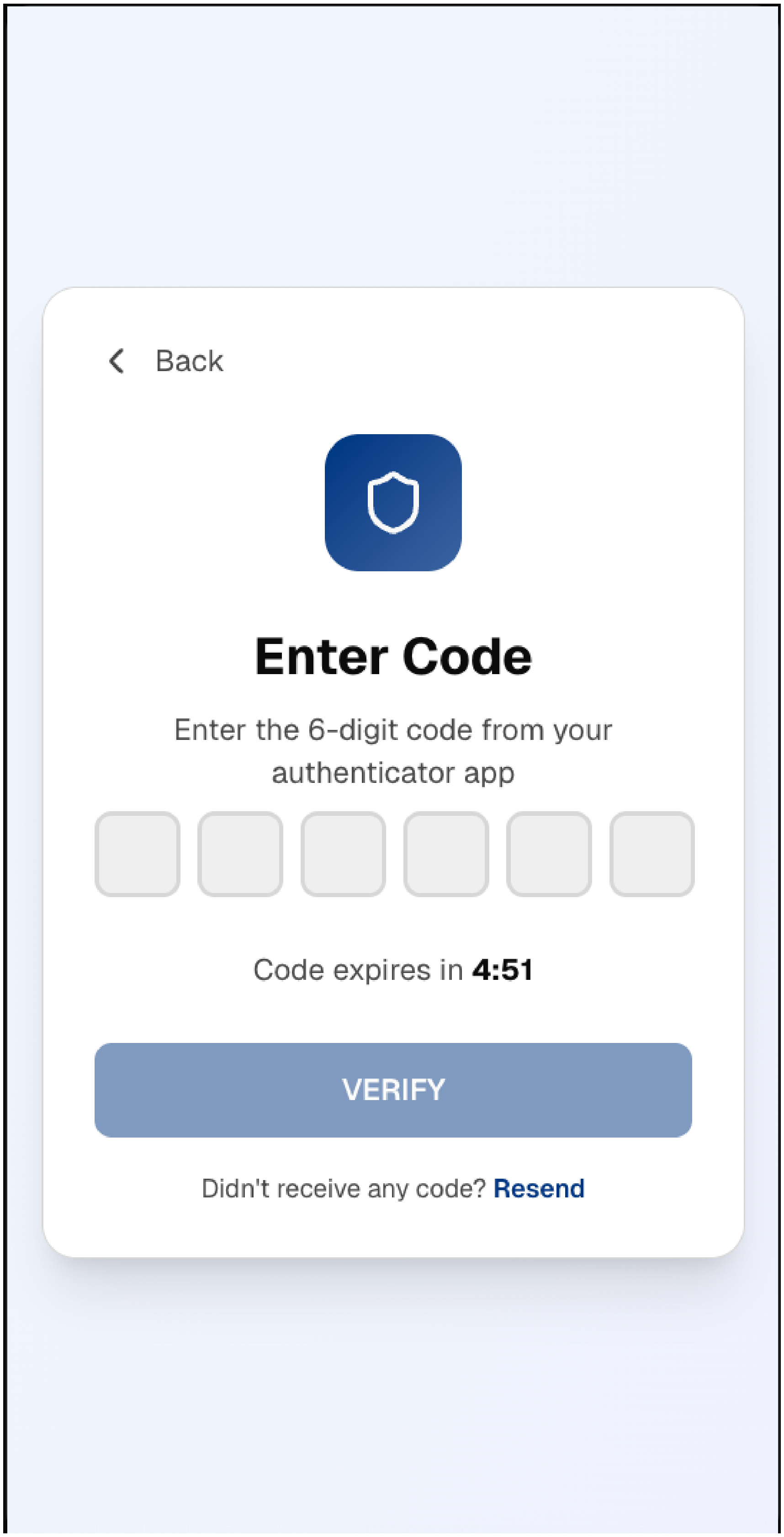
Scan with Authenticator App

Use Google Authenticator, Microsoft Authenticator, or Authy

Can't scan? Enter manually:

DIMS-SR-2024-55PLOE

Figure 13 MFA Configuration Page



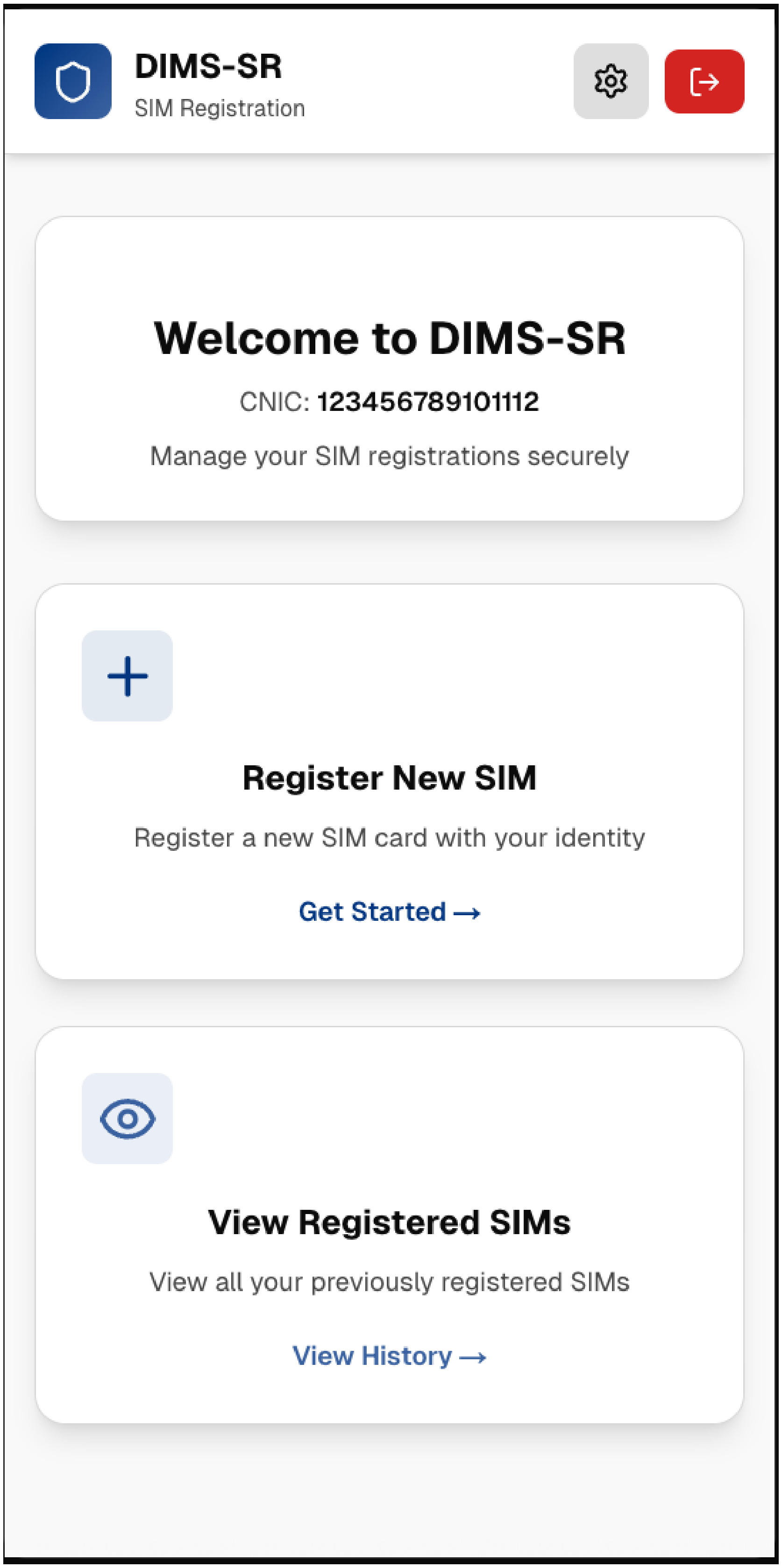
Enter Code

Enter the 6-digit code from your authenticator app

Code expires in **4:51**

Didn't receive any code? **Resend**

Figure 14 MFA Verification Page



Welcome to DIMS-SR

CNIC: 123456789101112

Manage your SIM registrations securely

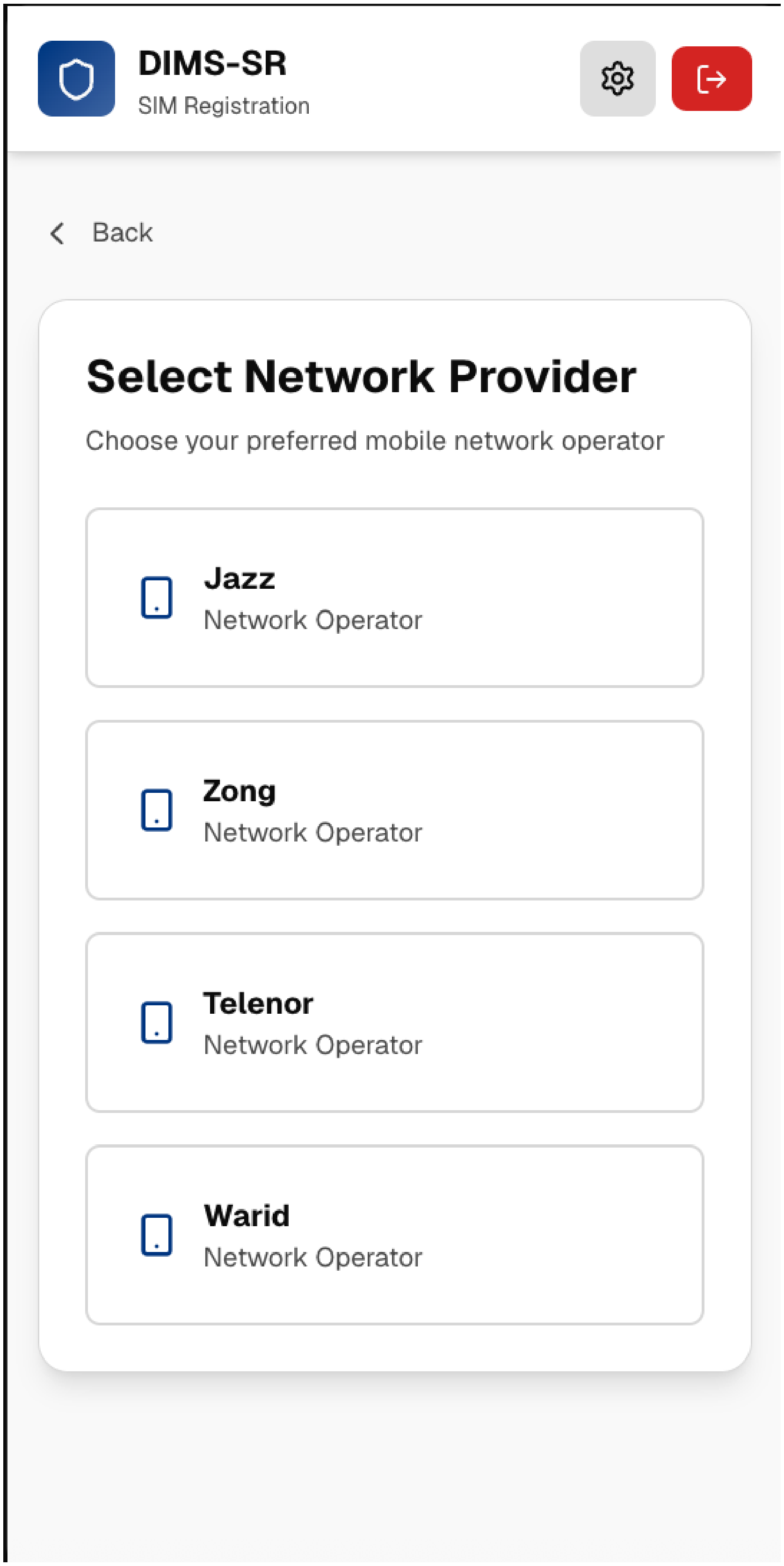
Register New SIM

Register a new SIM card with your identity

View Registered SIMs

View all your previously registered SIMs

Figure 15 Dashboard



DIMS-SR

SIM Registration

Back

Select Network Provider

Choose your preferred mobile network operator

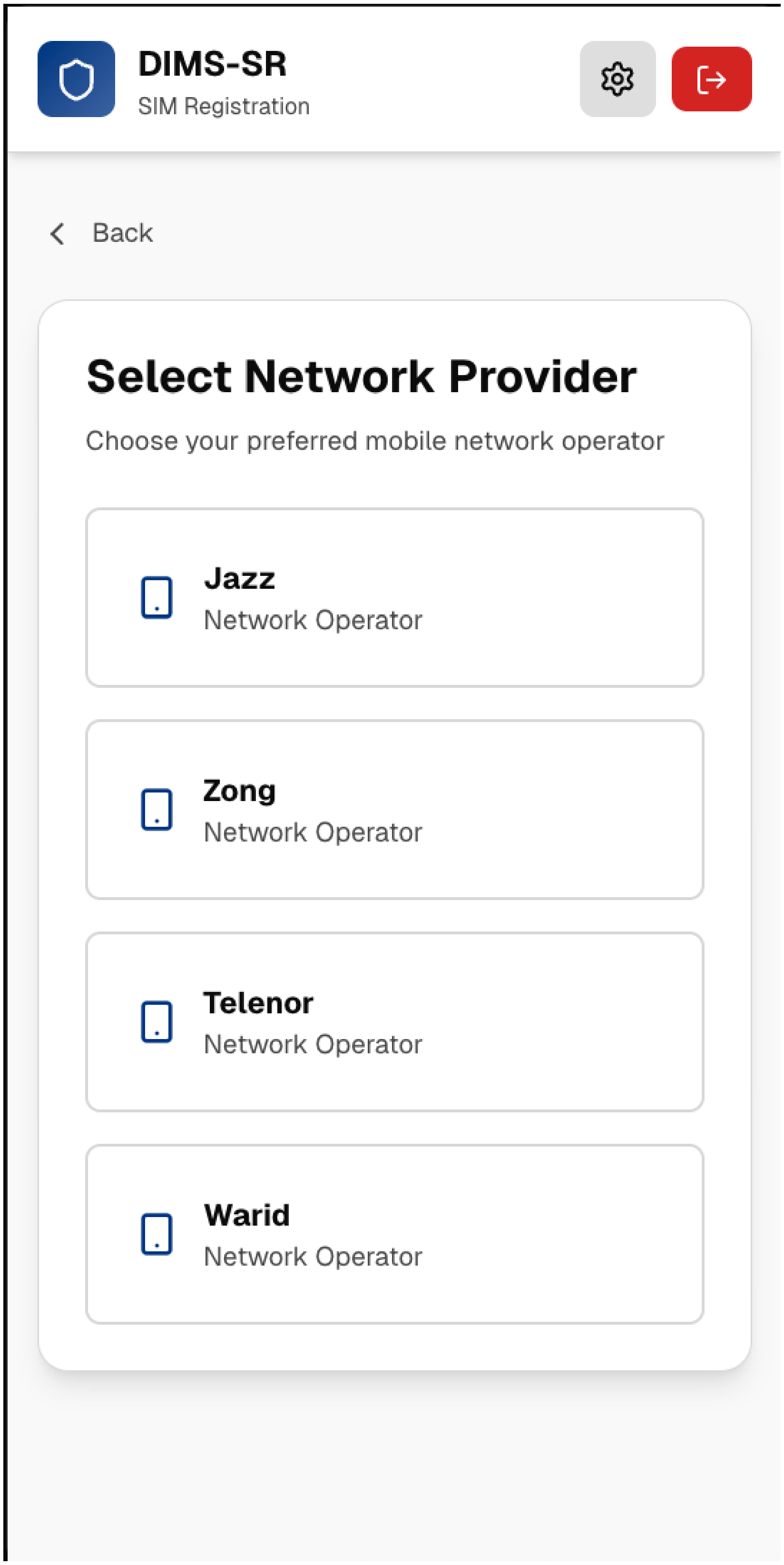
Jazz
Network Operator

Zong
Network Operator

Telenor
Network Operator

Warid
Network Operator

Figure 16 Register SIM



Select Network Provider

Choose your preferred mobile network operator

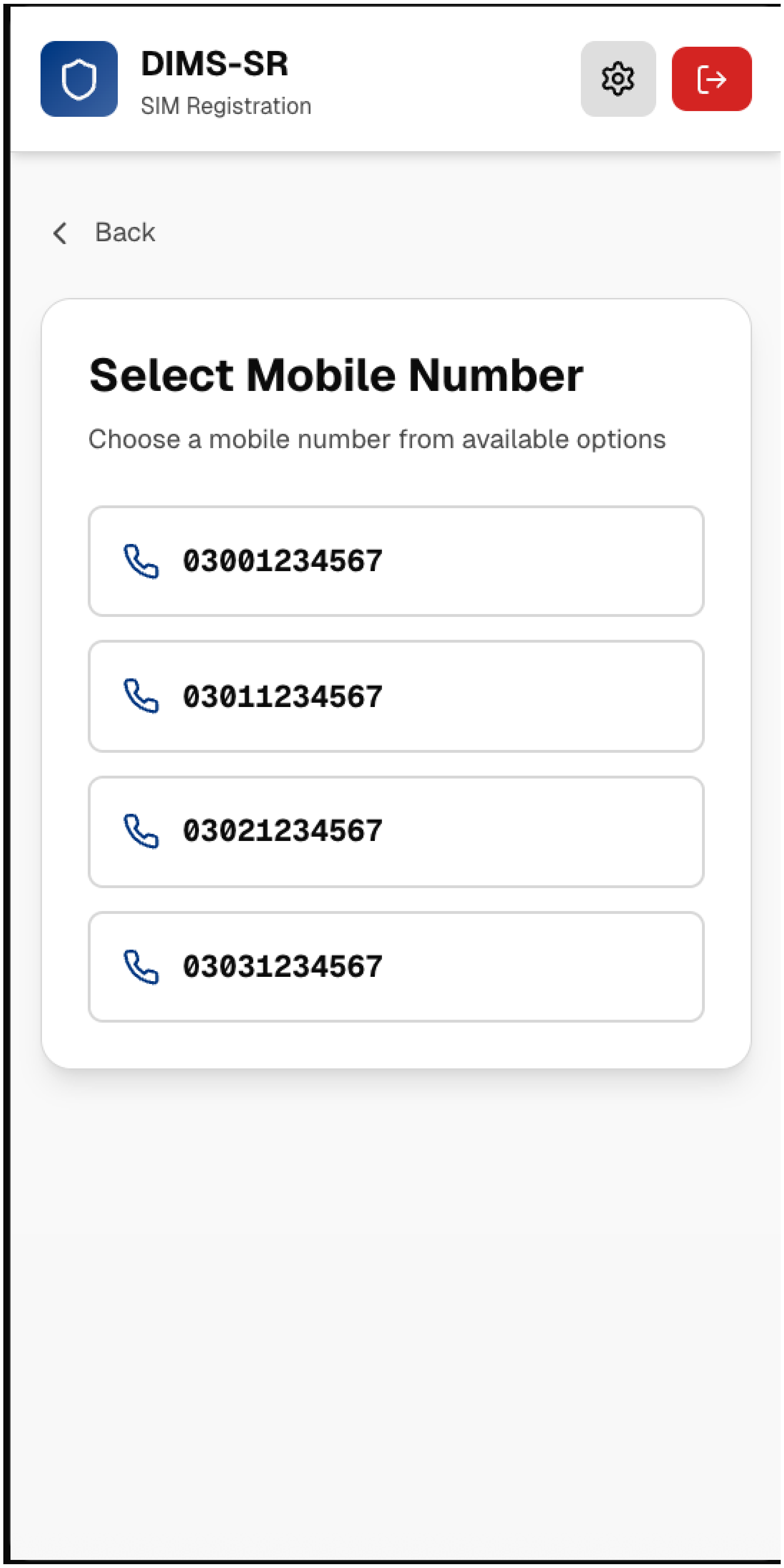
Jazz
Network Operator

Zong
Network Operator

Telenor
Network Operator

Warid
Network Operator

Figure 17 Register SIM - 1



DIMS-SR

SIM Registration

Back

Select Mobile Number

Choose a mobile number from available options

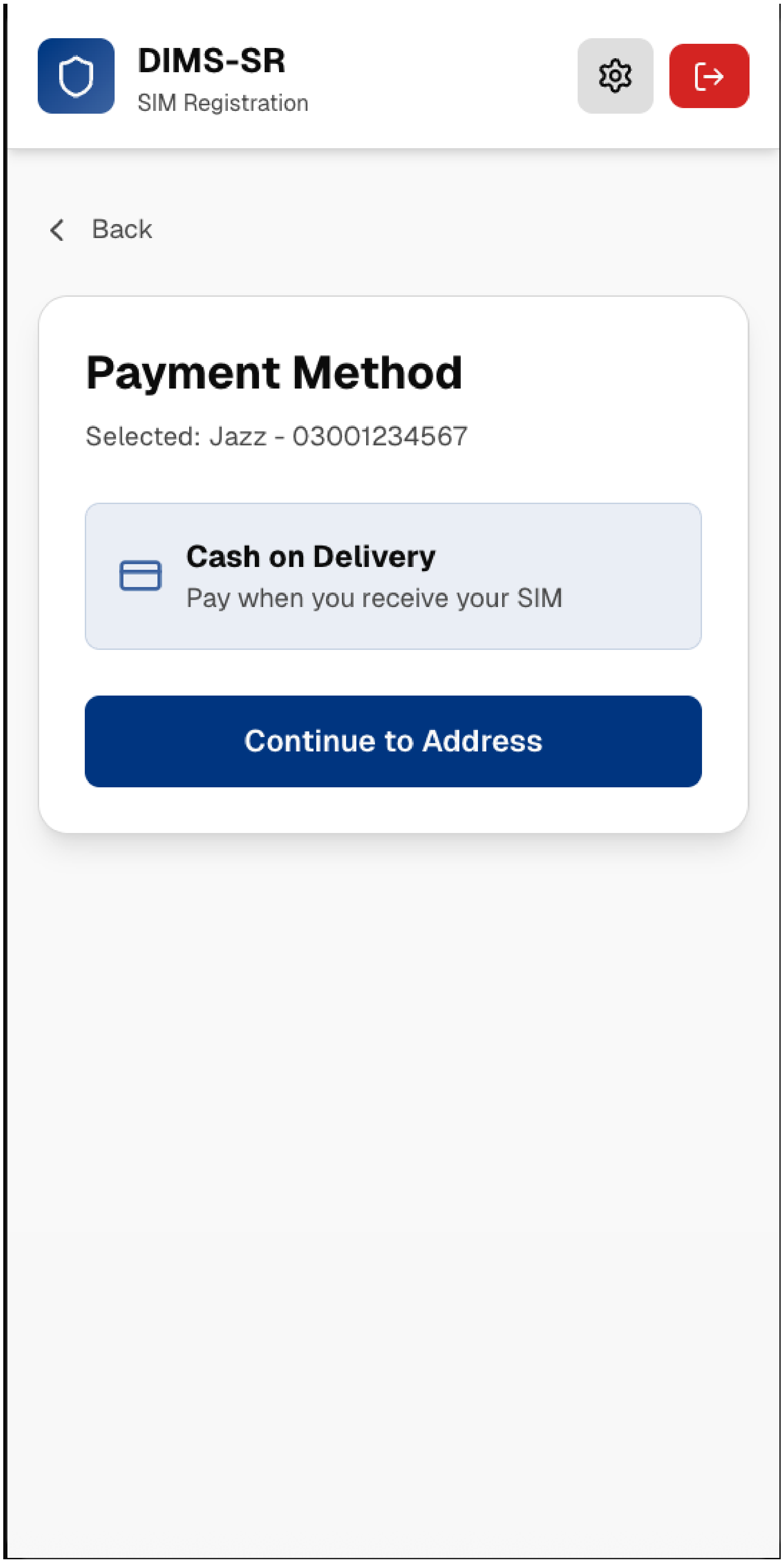
☎ 03001234567

☎ 03011234567

☎ 03021234567

☎ 03031234567

Figure 18 Register SIM - 2



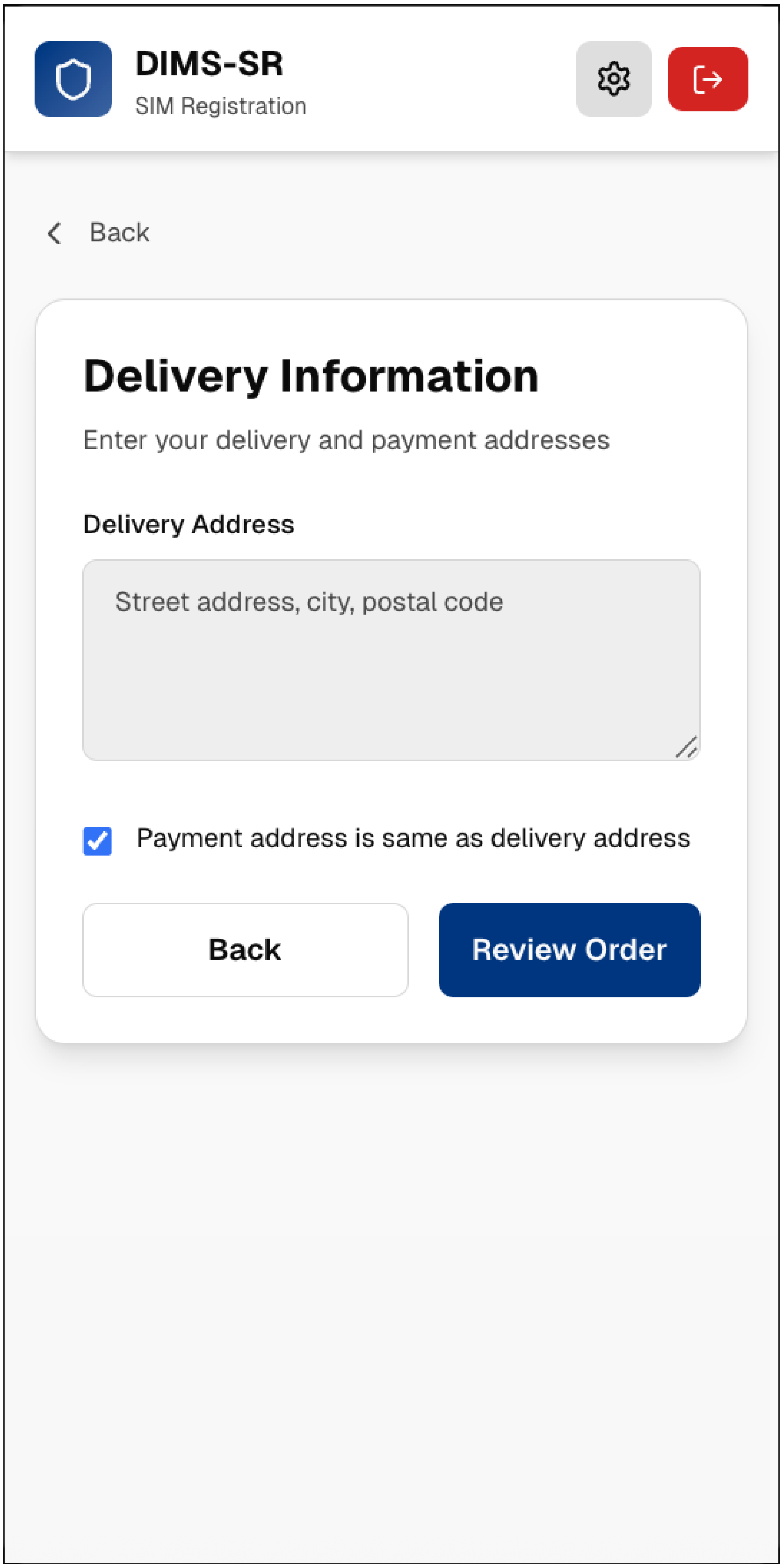
Payment Method

Selected: Jazz - 03001234567

Cash on Delivery

Pay when you receive your SIM

Figure 19 Register SIM - 3



DIMS-SR

SIM Registration

Back

Delivery Information

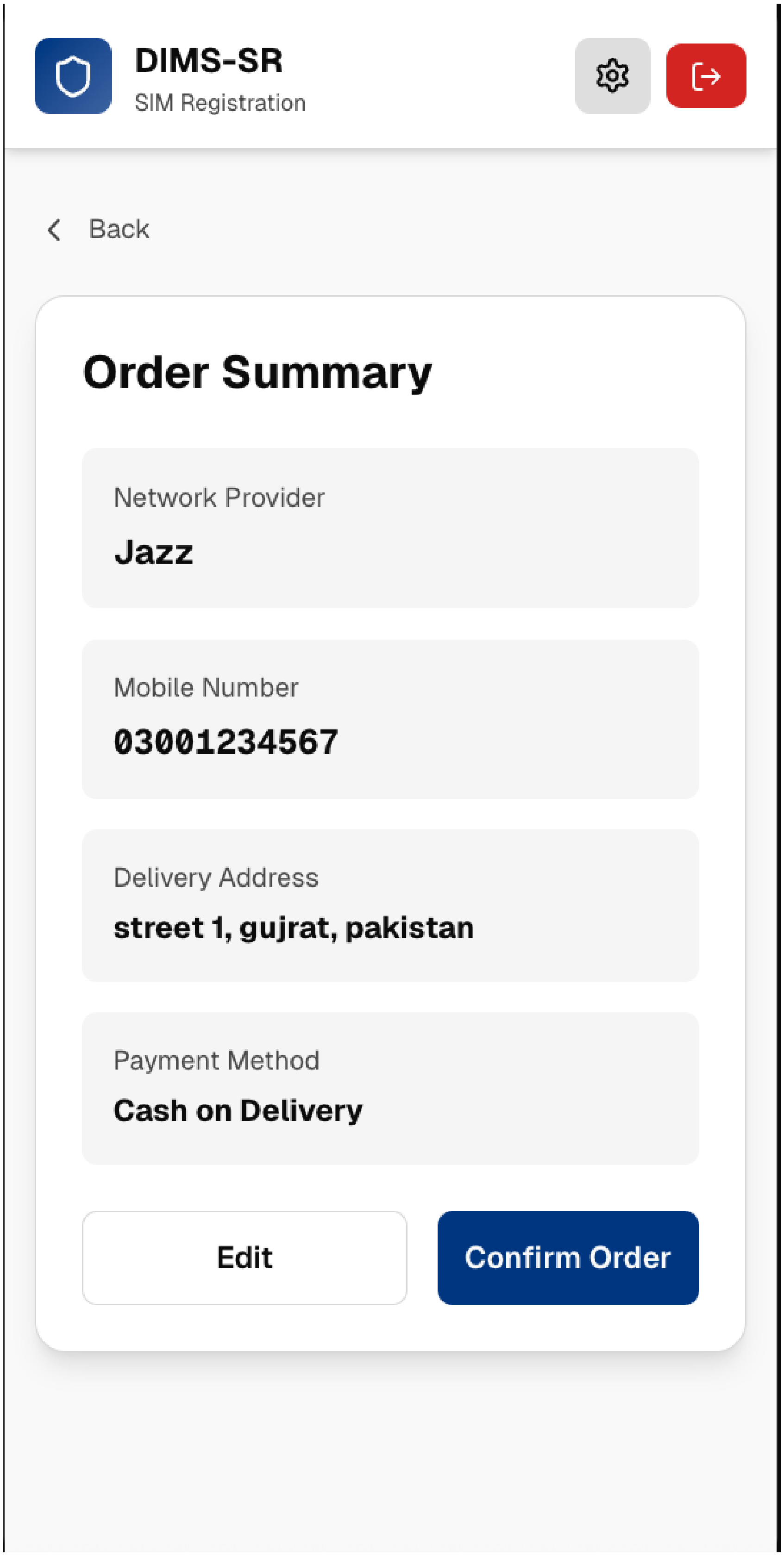
Enter your delivery and payment addresses

Delivery Address

Street address, city, postal code

☑ Payment address is same as delivery address

Figure 20 Register SIM - 4



Order Summary

Network Provider

Jazz

Mobile Number

03001234567

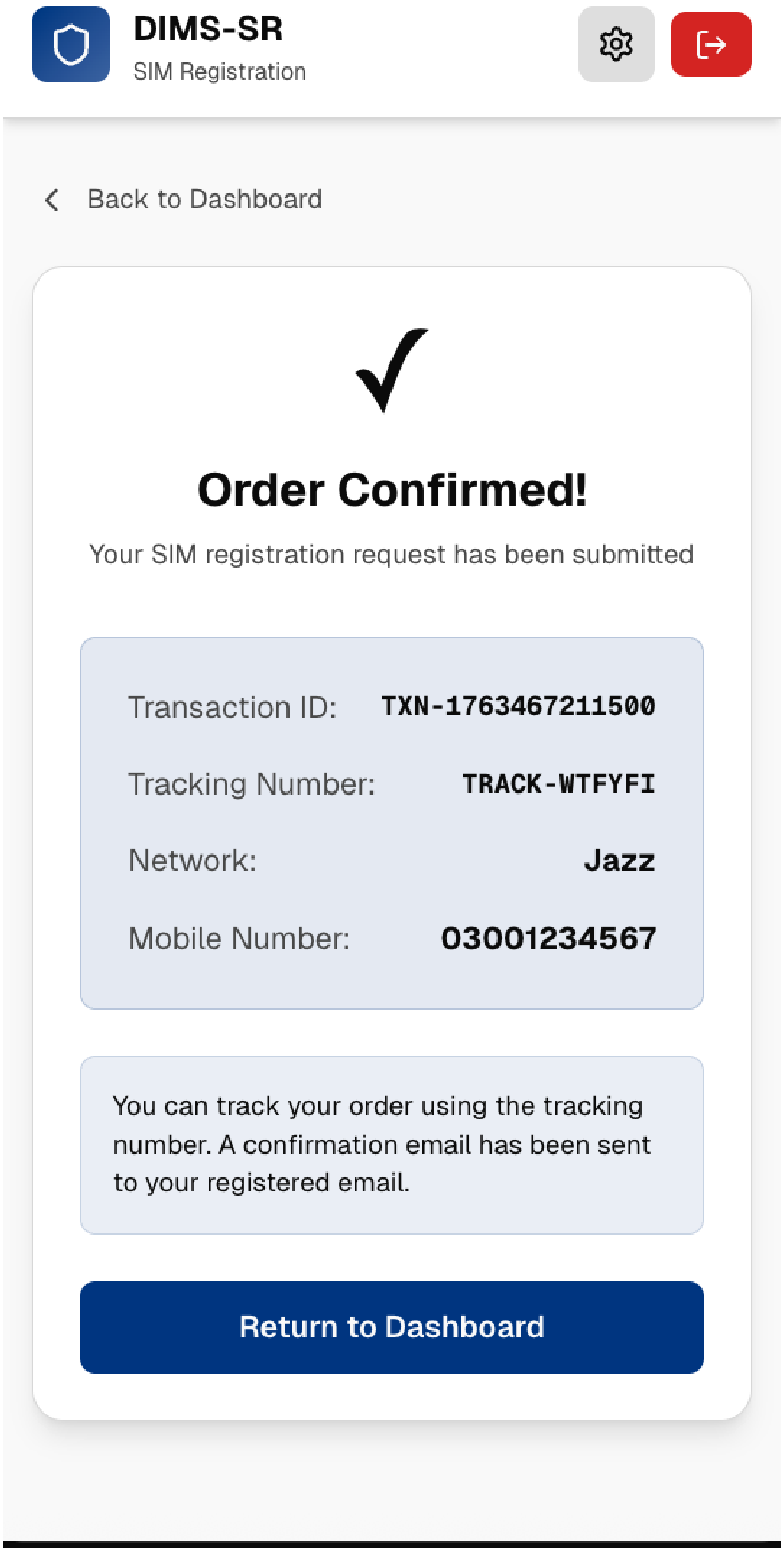
Delivery Address

street 1, gujrat, pakistan

Payment Method

Cash on Delivery

Figure 21 Register SIM - 5



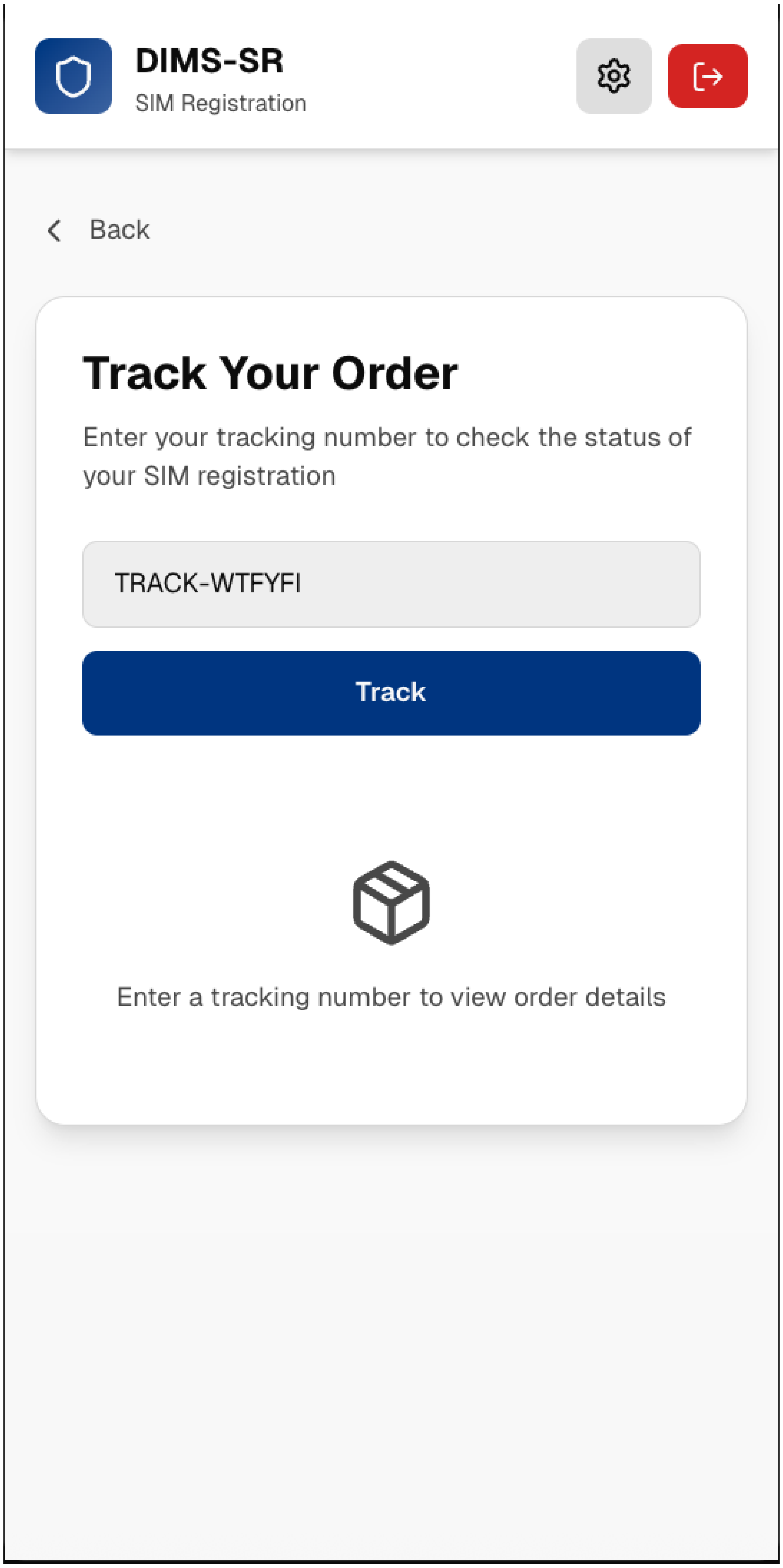
Order Confirmed!

Your SIM registration request has been submitted

Transaction ID:	TXN-1763467211500
Tracking Number:	TRACK-WTFYFI
Network:	Jazz
Mobile Number:	03001234567

You can track your order using the tracking number. A confirmation email has been sent to your registered email.

Figure 22 Register SIM - 6



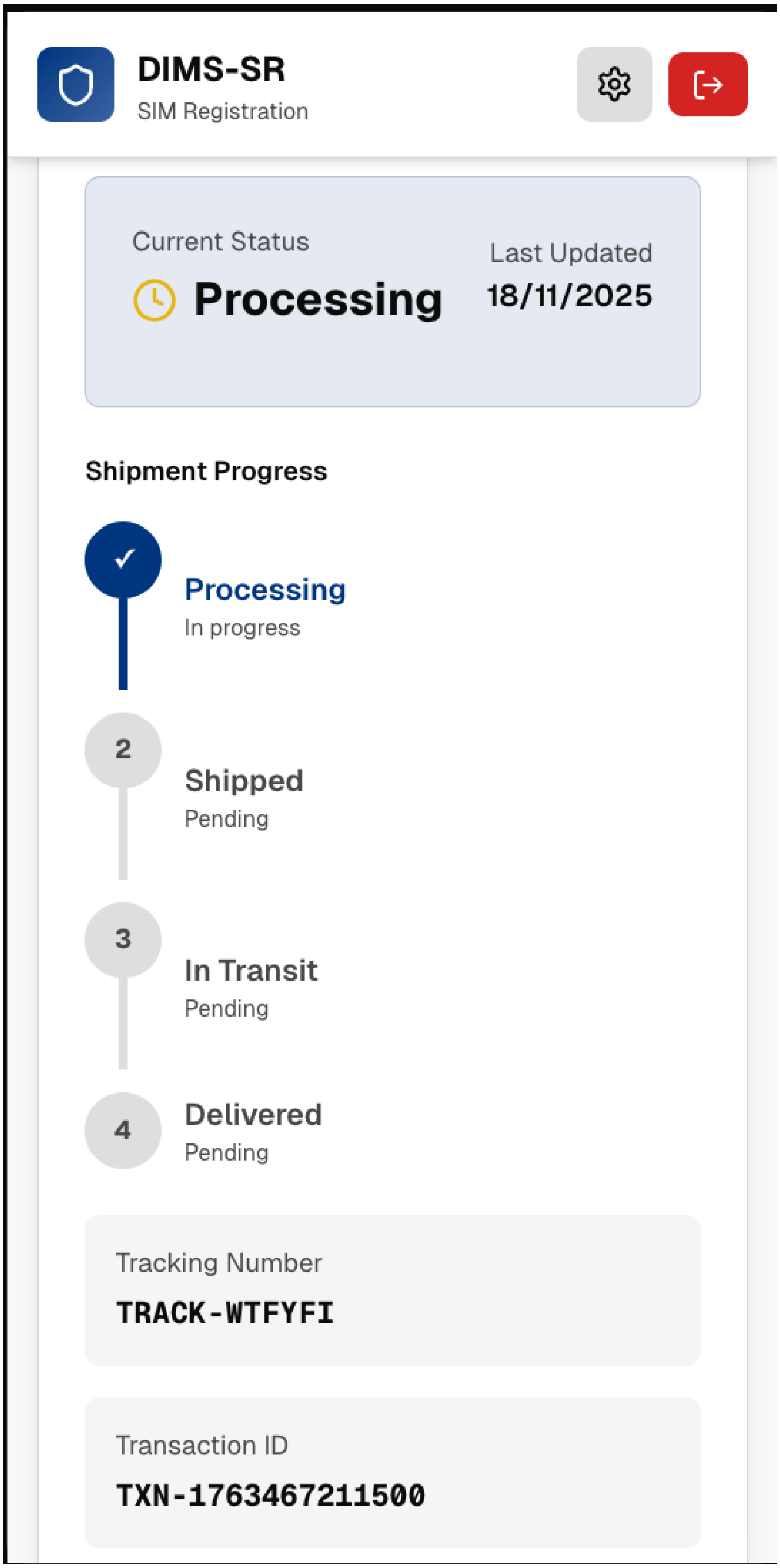
Track Your Order

Enter your tracking number to check the status of your SIM registration

TRACK-WTFYFI

Enter a tracking number to view order details

Figure 23 Track Order



Current Status

Processing

Last Updated

18/11/2025

Shipment Progress

✓ Processing
In progress

2 Shipped
Pending

3 In Transit
Pending

4 Delivered
Pending

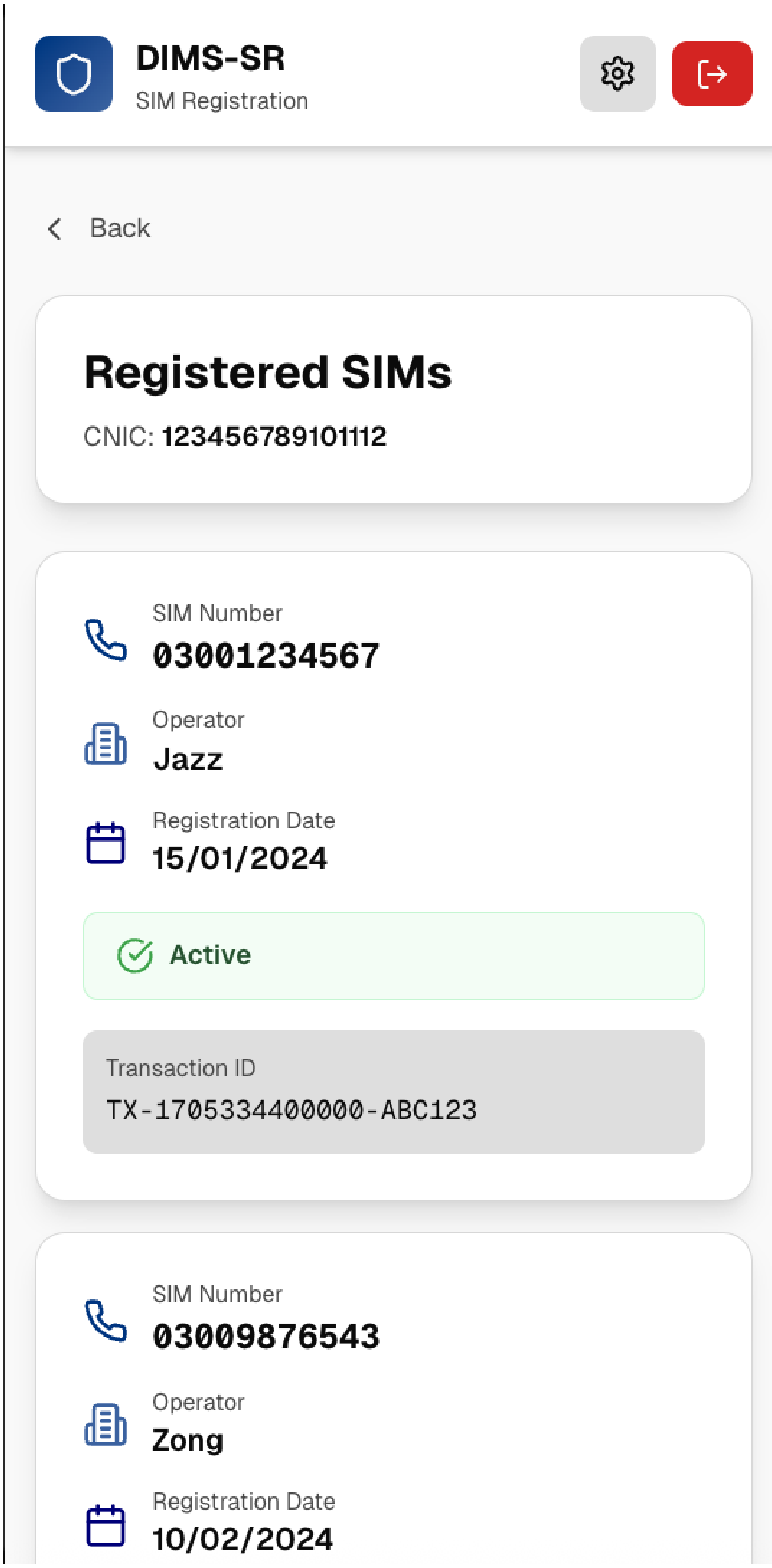
Tracking Number

TRACK-WTFYFI

Transaction ID

TXN-1763467211500

Figure 24 Track Order - 1



DIMS-SR

SIM Registration

Back

Registered SIMs

CNIC: 123456789101112

SIM Number

03001234567

Operator

Jazz

Registration Date

15/01/2024

Active

Transaction ID

TX-1705334400000-ABC123

SIM Number

03009876543

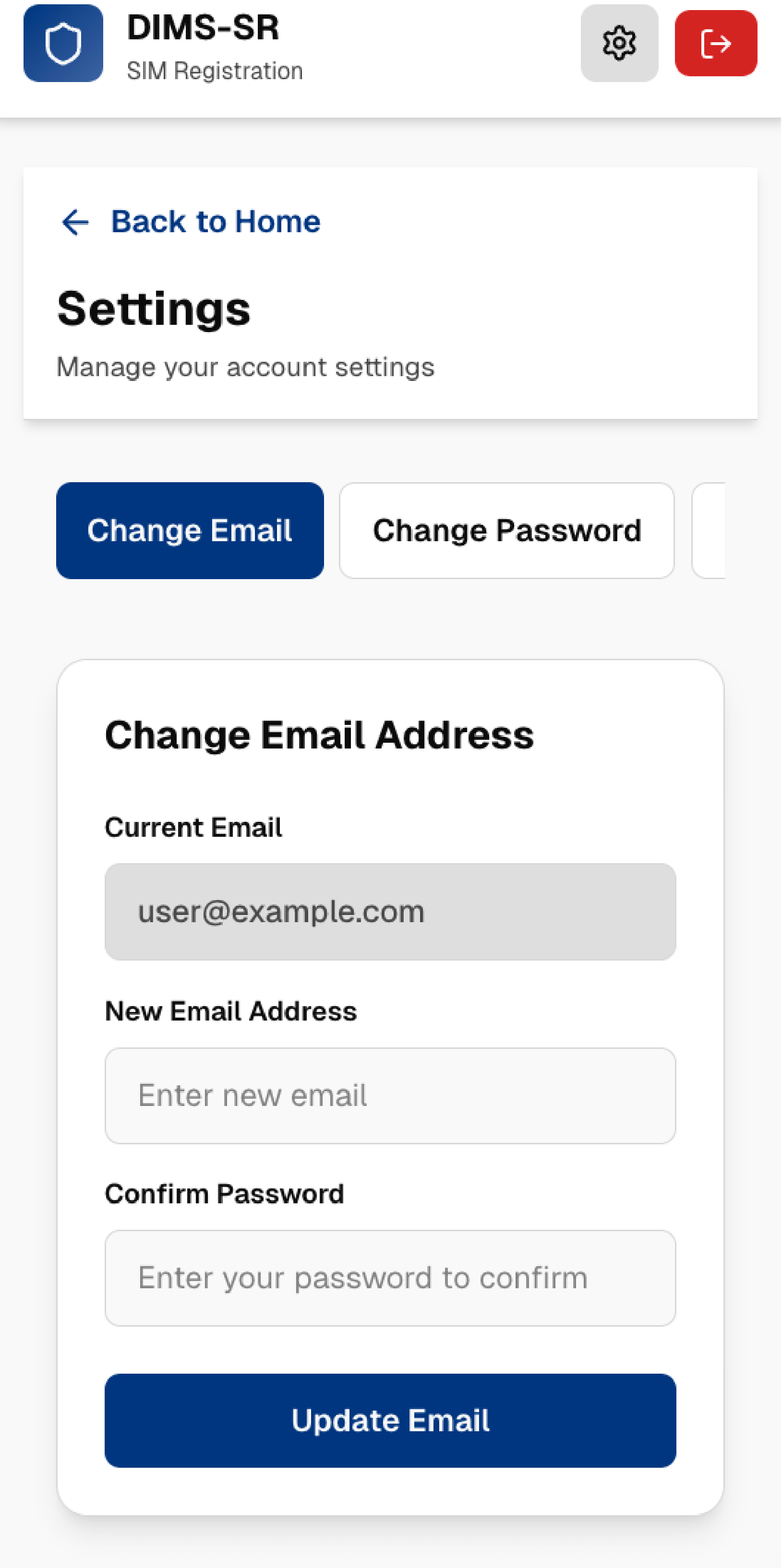
Operator

Zong

Registration Date

10/02/2024

Figure 25 View SIM record



Settings

Manage your account settings

Change Email Address

Current Email

user@example.com

New Email Address

Enter new email

Confirm Password

Enter your password to confirm

Figure 26 Setting Page