DIMS

Decentralized Identity Management System – DIMS Using Blockchain

Date: November 12, 2025

Supervisor:

Dr. Rashad M. Jillani

Co-Supervisor:

Muhammad Qasim Riaz

Group Members:

Ayesha Kashif 2022132

Mohammad Abdur Rehman 2022299

Noor ul Ain Islam 2022485

Faculty of Computer Sciences & Engineering

Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Pakistan

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 – Supervisor Muhammad Qasim Riaz – Co-supervisor

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.

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
PII	Personally Identifiable Information

Table 1. Terms used in this document and their description

2 OVERVIEW

2.1 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.

2.2 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.

2.2. PRODUCT FUNCTIONS

The major functions the product must perform are:

- **Secure Client Data Capture:** Collection of customer data and biometrics via Mobile App.
- **Mobile App Authorization:** User registration via **email** and securing access with Multi-Factor Authentication (MFA).
- **Identity Verification:** Real-time checking of collected data and biometrics against the NADRA API.
- **Rule Enforcement:** Automatic execution of Check Limit logic via Smart Contracts on the blockchain.
- **Immutable Record-Keeping:** Submission of the final, verified registration record for Write Block on the Distributed Ledger.
- **Fraud Logging:** Maintaining Limit Logs for all failed attempts and raising system Alerts.

2.3. USER CHARACTERISTICS

There are two primary roles for DIMS:

1. User
    - **Role:** These users are responsible for making a user account, generating a request for new sim, and managing sims previously issued against their CNIC.

- **Expertise:** Users will have varying level of technical proficiency but must possess basic understanding of using a smart device.
- **Access Control:** Each User will only be able to access data of the SIM(s) issued against their respective CNIC

2. Admin
    - **Role:** Admins are responsible for managing the backend server, handling SIM issuance requests, and responding to the system problems.
    - **Expertise:** High technical expertise; monitors security and operational logs; manages system configuration.
    - **Security:** Admins do not have direct access to user data, they just get to see the biometric output result based on which they process the requests.

2.3. CONSTRAINTS

- **Mandatory External Interface:** Must integrate with the NADRA API for primary identity verification.
- **Technology Constraint:** The Distributed Ledger must use an approved **Consortium Blockchain** protocol (e.g., Hyperledger).
- **Security Constraint:** All customer PII must be encrypted end-to-end. Biometric data must be securely hashed *before* any transmission or storage.
- **MFA Protocol Constraint:** The mobile app must use a secure, industry-standard MFA protocol (e.g., TOTP or push notification-based).

2.4. ASSUMPTIONS AND DEPENDENCIES

- **Assumption:** The NADRA API provides adequate uptime and response time to support real-time registration.
- **Dependency:** Continued availability and stability of the MNO's core SIM activation system.
- **Assumption:** The Mobile App can securely leverage built-in smartphone biometrics (e.g., Face ID, fingerprint scanner) for optional customer identity assurance.

3 STATE OF THE ART

3.1 Literature Review

This section will review contemporary research on decentralized identity (DID) systems, focusing on how Self-Sovereign Identity (SSI) models are applied in regulated industries. Key areas include the cryptographic principles of zero-knowledge proofs (ZKPs) and verifiable credentials (VCs) in blockchain.

Reference System/ Source	Core Problem Identified	Limitation Addressed by DIMS/DIMS-SR
Satybaldy et al. (2022) – Healthcare	Centralized e-health ID systems are vulnerable; limited user control.	Adaptation: DIMS studies and adapts DID/VC concepts for SIM registration in telecom.
ATIS (2023) – Telecom Industry	Fraud, spoofing, and weak subscriber KYC in telecom.	Technical Prototype: DIMS proposes and tests a technical prototype for a telecom DIMS, involving regulator and telco roles.
Konasani (2025) – Finance (KYC/AML)	KYC processes are slow, costly, and fraud prone.	Consortium Model: DIMS explores how a consortium model (telcos + regulator) could be applied in telecom.
Le et al. (2025) – General ID (BDIMS)	Identity fraud; no selective disclosure in centralized IDs.	Selective Disclosure: DIMS aims to demonstrate selective disclosure in telecom KYC, focusing on user privacy.

Table 2. Literature Review

3.2 Existing Systems

This section will detail existing SIM registration systems (traditional centralized MNO databases) and assess their limitations (e.g., fraud, lack of auditability) to justify the DIMS-SR's blockchain-based approach. It will also look at global examples of e-government or national ID systems that have successfully implemented blockchain or biometric verification.

Reference System/ Source	Core Problem Identified	Limitation Addressed by DIMS/DIMS-SR
Traditional Centralized Systems	High vulnerability to single points of failure, data breaches, fraud, and misuse.	DIMS shifts control to a decentralized network, achieving transparency and tamper-resistance via blockchain hashes.
SIM Registration Databases (MNOs)	Susceptible to fraud and lack of auditability.	DIMS-SR mandates a trustless limit check via Smart Contracts and uses the distributed ledger for an immutable record.
Estonia e-ID	Infrastructure is centralized despite its security.	DIMS eliminates central database reliance by using a distributed ledger and IPFS for identity anchoring.

Table 3. Existing Systems

4 USER/SYSTEM REQUIREMENTS

4.1 External Interface Requirements

4.1.1 User Interfaces

- **Mobile App UI:** Must be intuitive, adhere to native iOS/Android design standards, and clearly guide the user through the email registration and MFA setup processes.

4.1.2 Hardware Interfaces

- **Mobile App:** Must utilize the device's native network connection (cellular/Wi-Fi), and on-device biometric sensors (e.g., fingerprint/face) for local authentication if applicable.

4.1.3 Software Interfaces

- **NADRA API:** (Outbound) For identity and biometric verification.
- **SIM Registration Core API:** (Outbound) For the final SIM activation.
- **Blockchain Client/SDK:** (Outbound) For submitting transactions to the Smart Contracts and the Distributed Ledger.
- **MFA Provider API:** (Outbound/Inbound) For generating and verifying time-based one-time passwords (TOTP) or push notifications.

4.1.4 Communication Interfaces

- All communication channels (Client to Server)
- API/Blockchain) must use HTTPS/TLS for encryption.
- The Application Server must use the specific Consortium Blockchain Protocol for network transactions.
- The system must use SMTP/Secure Email Protocols for mobile user registration and a dedicated Push Notification Service for MFA prompts.

5 Functional Requirements

5.1 Functional Requirements with Traceability information

5.1.1 Allow User to Create a new account

Requirement ID	FR1			**Requirement Type**		Functional			**Use Case #**		1
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-			
Parent Requirement #	-										
Description	User provides email, CNIC, and password to create a profile.										
Rationale	Required for secure user identification and SIM self-service.										
Source					**Source Document**	-					
Acceptance/Fit Criteria	Account created and stored securely; confirmation sent.										
Dependencies	None										
Priority	***Essential***	X	***Conditional***	-	***Optional***	-					
Change History											

Table 4. Use Case 1

5.1.2 Allow User to Login with MFA

Requirement ID	FR2			**Requirement Type**		Functional			**Use Case #**		2
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-			
Parent Requirement #	FR1										
Description	User logs in using CNIC/Email and completes MFA										

Rationale	Provides secure Access to sim management and registration system							
Source				**Source Document**	-			
Acceptance/Fit Criteria	System verifies MFA success before providing success							
Dependencies	FR1							
Priority	***Essential***	X	***Conditional***	-	***Optional***	-		
Change History								

Table 5. Use Case 2

5.1.3 View Registered SIMs

Requirement ID	FR3		**Requirement Type**		Functional		**Use Case #**		3
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-	
Parent Requirement #	-								
Description	User view list of all sims issued under their CNIC								
Rationale	Allow transparency and user awareness their of active sims								
Source					**Source Document**	-			
Acceptance/Fit Criteria	User sees all sims linked to their CNIC								
Dependencies	FR1, FR2								
Priority	***Essential***	X	***Conditional***	-	***Optional***	-			
Change History									

Table 6. Use Case 3

5.1.4 Request SIM Issuance

Requirement ID	FR4		**Requirement Type**		Functional		**Use Case #**		4
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-	
Parent Requirement #	-								

Description	User initiates a request for new SIM registration							
Rationale	Allow mobile users to start the issuance workflow digitally							
Source			**Source Document**	-				
Acceptance/Fit Criteria	Request is generated and forwarded for biometric verification							
Dependencies	FR2							
Priority	***Essential***	X	***Conditional***	-	***Optional***	-		
Change History								

Table 7 Use Case 4

5.1.5 Check SIM limit status

Requirement ID	FR5		**Requirement Type**		Functional		**Use Case #**		5	
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-		
Parent Requirement #	-									
Description	System Checks how many SIMs are registered against user's CNIC.									
Rationale	Provides clarity before submitting new sim request.									
Source			**Source Document**	-						
Acceptance/Fit Criteria	System shows registered SIM count and remaining allowance.									
Dependencies	FR2									
Priority	***Essential***	X	***Conditional***	-	***Optional***	-				
Change History										

Table 8. Use Case 5

5.1.6 Deactivate an existing SIM

Requirement ID	FR6		**Requirement Type**		Functional		**Use Case #**		6	
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-		

Parent Requirement #	-							
Description	User requests deactivation of SIM(s) tied to their CNIC							
Rationale	Provides self-service control for fraud prevention							
Source			**Source Document**	-				
Acceptance/Fit Criteria	Deactivation request sent to backend and logged in blockchain							
Dependencies	FR2, FR3							
Priority	***Essential***	X	***Conditional***	-	***Optional***	-		
Change History								

Table 9 Use Case 6

5.1.7 View SIM activity and history

Requirement ID	FR7		**Requirement Type**	Functional		**Use Case #**	7		
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-	
Parent Requirement #	-								
Description	User views issuance details and recorded activity logs for their corresponding SIM(s)								
Rationale	Provides auditability and transparency to end users								
Source			**Source Document**	-					
Acceptance/Fit Criteria	User can view issuance date, activation logs, and recorded changes								
Dependencies	FR3								
Priority	***Essential***	X	***Conditional***	-	***Optional***	-			
Change History									

Table 10 Use Case 7

5.1.8 Update User Profile

Requirement ID	FR8	**Requirement Type**	Functional	**Use Case #**	8

Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-	
Parent Requirement #	-								
Description	User updates provided email, password or MFA configuration								
Rationale	Maintains secure and updated credentials								
Source					**Source Document**	-			
Acceptance/Fit Criteria	Updated record securely stored on server								
Dependencies	FR2								
Priority	***Essential***	X	***Conditional***	-	***Optional***	-			
Change History									

Table 11 Use Case 8

5.1.9 Receive alert/notifications

Requirement ID	FR9		**Requirement Type**		Functional		**Use Case #**		9
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-	
Parent Requirement #	-								
Description	User receives application notifications								
Rationale	Keeps users informed about the activities								
Source					**Source Document**	-			
Acceptance/Fit Criteria	Notifications appear in app								
Dependencies	FR1								
Priority	***Essential***	X	***Conditional***	-	***Optional***	-			
Change History									

Table 12 Use Case 9

5.1.10 View Pending Requests

Requirement ID	FR10			**Requirement Type**		Functional			**Use Case #**		10
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-			
Parent Requirement #	-										
Description	User can view all the pending SIM issuance requests										
Rationale	Keeps users informed about the request's progress										
Source						**Source Document**	-				
Acceptance/Fit Criteria	Pending request displayed										
Dependencies	FR4										
Priority	***Essential***	X	***Conditional***	-	***Optional***	-					
Change History											

Table 13 Use Case 10

5.1.11 Cancel Pending Request

Requirement ID	FR11			**Requirement Type**		Functional			**Use Case #**		11
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-			
Parent Requirement #	-										
Description	User can cancel a pending SIM issuance request										
Rationale	Gives control to withdraw unwanted request.										
Source						**Source Document**	-				
Acceptance/Fit Criteria	Request cancelled										
Dependencies	FR10										
Priority	***Essential***	X	***Conditional***	-	***Optional***	-					
Change History											

Table 14 Use Case 11

5.1.12 Manage Logged in Devices – Session Control

Requirement ID	FR12			**Requirement Type**		Functional			**Use Case #**		12
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-			
Parent Requirement #	-										
Description	User can view all the devices where their account is logged in and can remove sessions										
Rationale	Prevents unauthorized access and strengthen security										
Source					**Source Document**	-					
Acceptance/Fit Criteria	Selected sessions terminated										
Dependencies	FR2										
Priority	***Essential***	X	***Conditional***	-	***Optional***	-					
Change History											

Table 15 Use Case 12

5.1.13 Update Notification Preferences

Requirement ID	FR13			**Requirement Type**		Functional			**Use Case #**		13
Status	***New***	**X**	***Agreed-to***	-	***Baselined***	-	***Rejected***	-			
Parent Requirement #	-										
Description	User chooses which notifications to receive										
Rationale	Improves user control and reduces noise										
Source					**Source Document**	-					
Acceptance/Fit Criteria	Preferences updated										
Dependencies	FR9										
Priority	***Essential***	X	***Conditional***	-	***Optional***	-					

Change History	

Table 16 Use Case 13

6 Nonfunctional Requirements & Software System Attributes

6.1 Performance Requirements

- **PERF-1:** The combined latency for Verify Identity and Check Limit shall not exceed 5 seconds for a single transaction for 95% of transactions to ensure a fast customer experience.
- **PERF-2:** The network synchronization time for a Write Block transaction shall achieve finality across Blockchain Nodes in less than 10 seconds.
- **PERF-3:** The Mobile App must load and authorize the user (including MFA verification) within 2 seconds.

6.2 Security Requirements

- **SEC-1 (Authorization):** The Mobile App shall enforce MFA for all user logins and for critical actions like initiating a SIM registration request.
- **SEC-2 (Data-in-Transit):** All data transmitted from the Mobile App and BVS Client to the Application Server must use TLS 1.2 or higher.
- **SEC-3 (Integrity):** The Smart Contracts must be formally audited to prevent unauthorized alteration of the SIM limit logic.

6.3 Safety Requirements

- **SAFE-1:** The system shall never store raw biometric data in any persistent storage, only cryptographically secure hashes that comply with national privacy standards.

6.4 Software Quality Attributes

- **Usability:** The BVS Client UI must be easy to learn and operate by Retailers with minimal training.
- **Reliability:** The core Write Block feature must maintain 99% uptime.
- **Portability:** The Mobile App must be deployable on both major mobile platforms (Android and iOS).
- **Interoperability:** The Application Server must be able to securely communicate and exchange data with the NADRA API and the MNO Core Systems.
- **Availability:** The DIMS-SR system, including the Application Server and Blockchain Gateways, shall maintain 24/7 accessibility (excluding scheduled maintenance) and ensure continuous operation for all High Priority functions.

7 Project Design/Architecture

7.1. 4+1 ARCHITECTURE VIEW MODEL

7.1.1. Use Case View

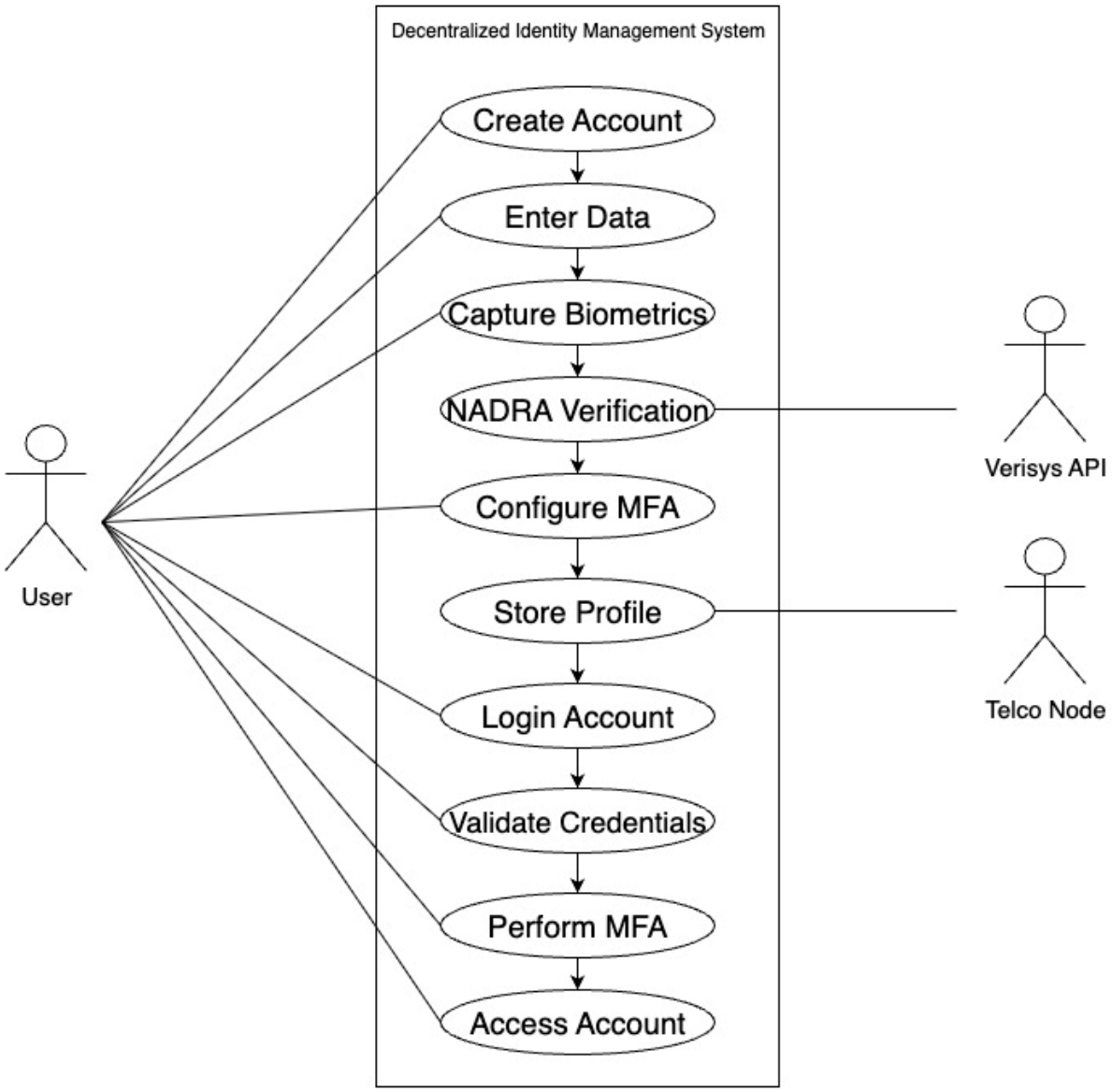

Figure 1. Create and Login Account Use Case Diagram

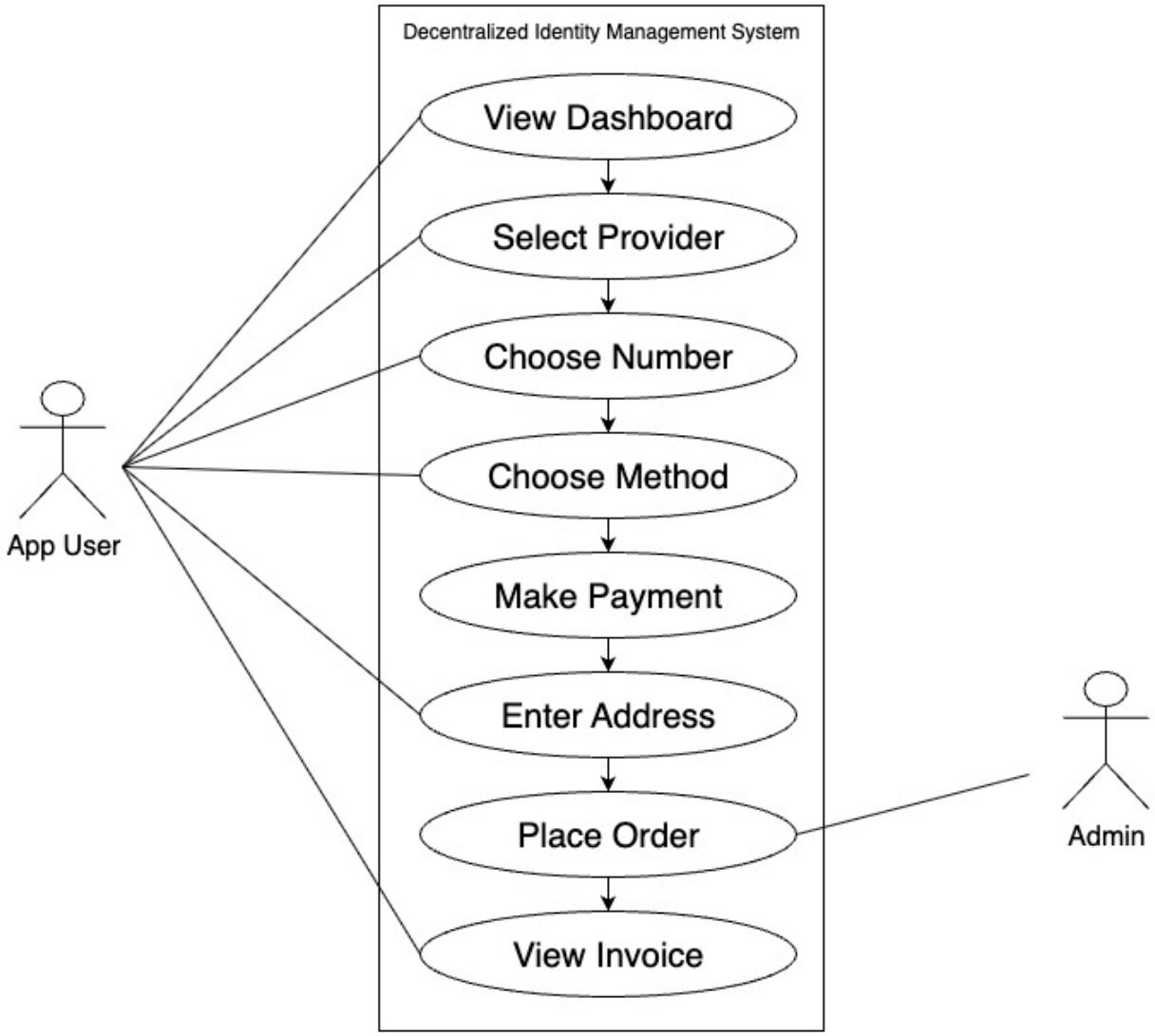

Figure 2. Registration Flow Use Case

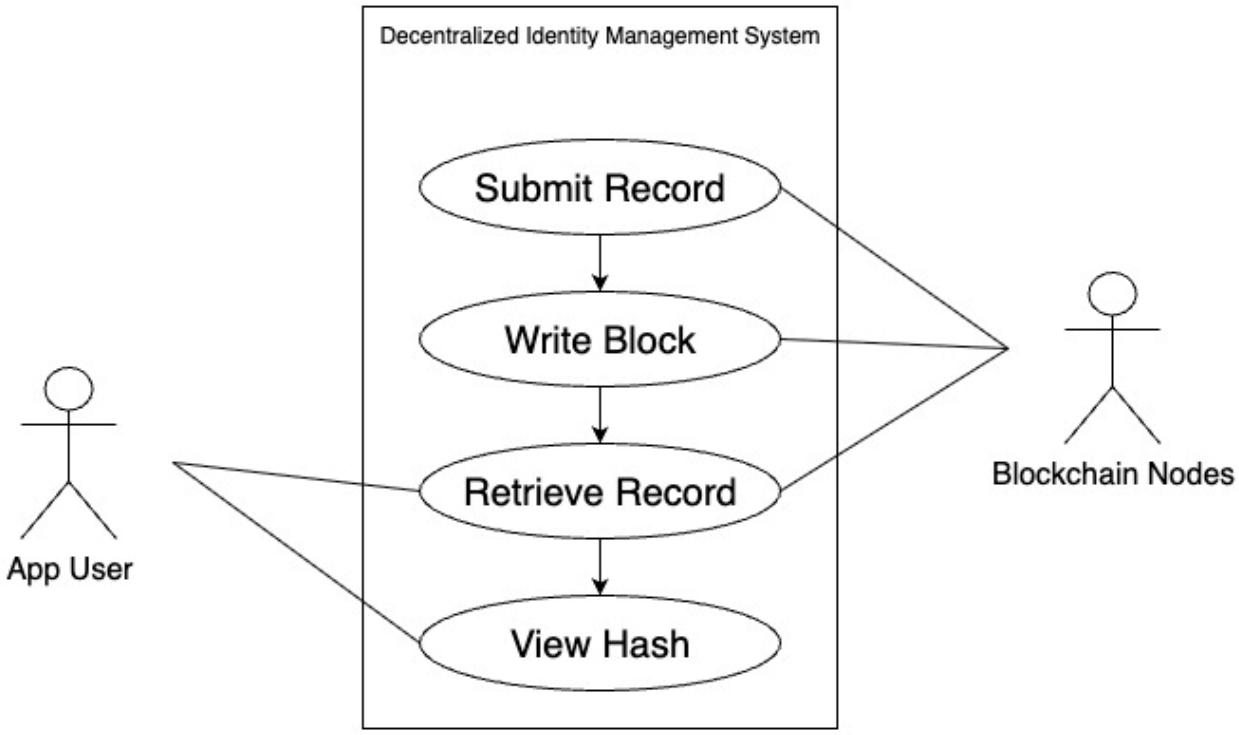

Figure 3. View Record Use Case

7.1.2. Logical View:

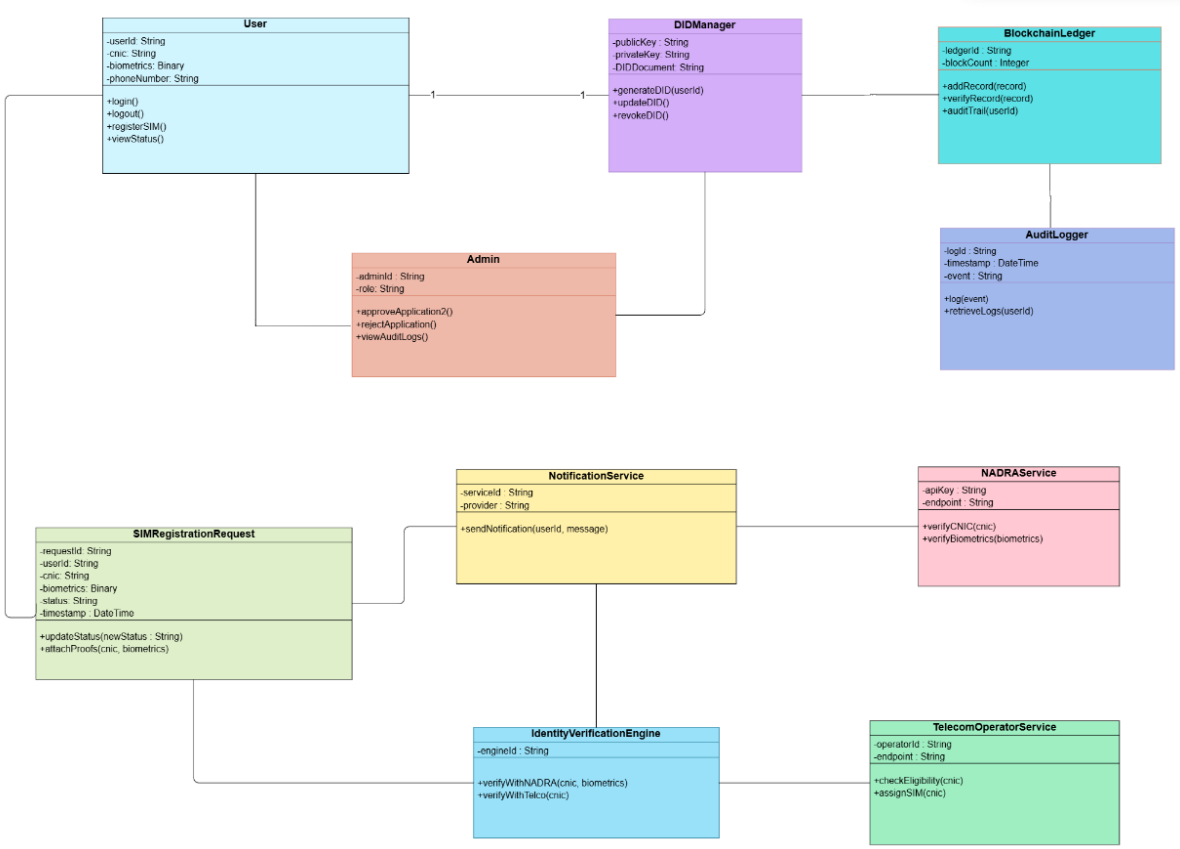

Figure 4. Logical View

7.1.3. Development View

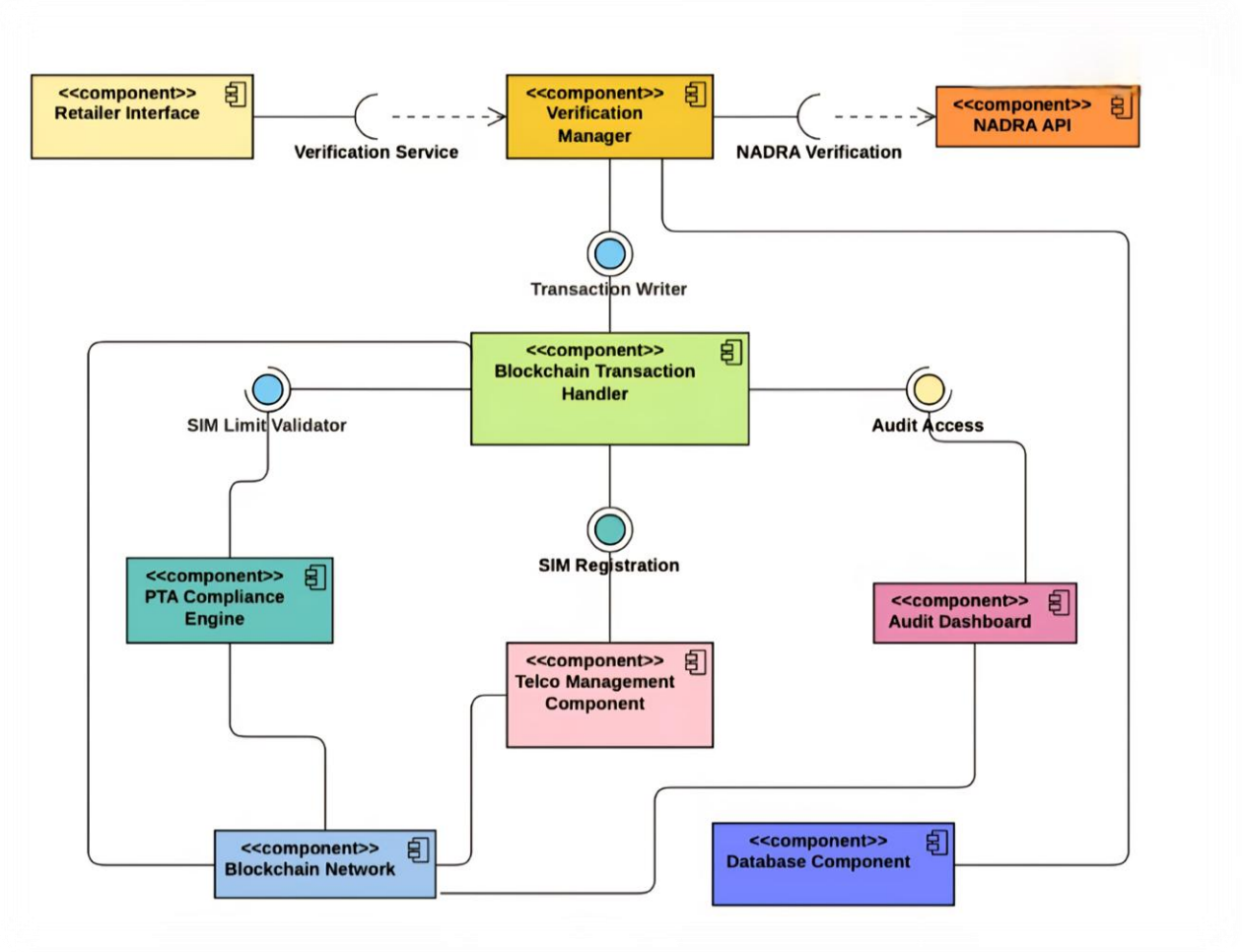

Figure 5. Development View

7.1.4. Process View

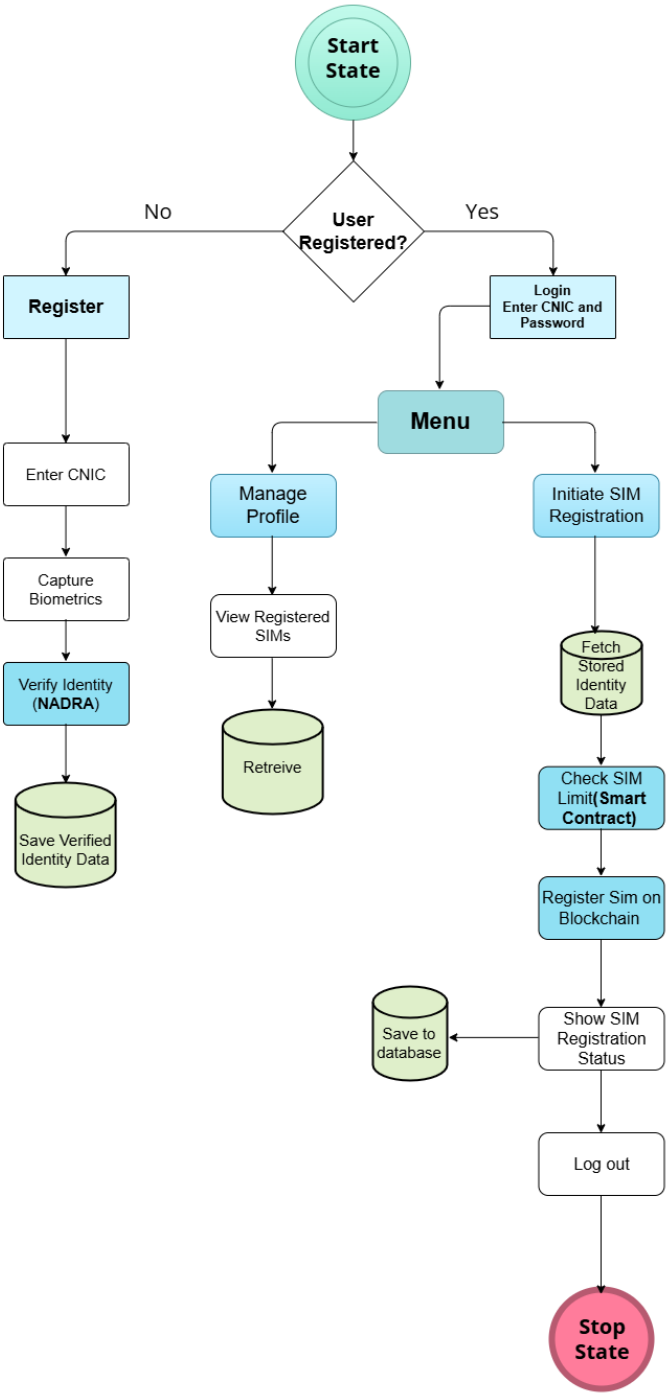

Figure 6. Process View

7.1.5. Physical View

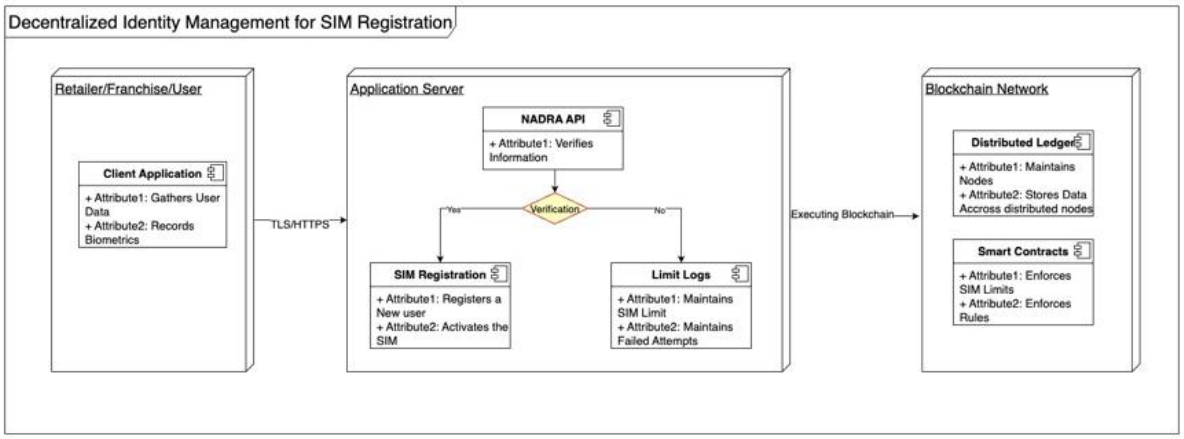

Figure 7. Deployment Diagram

7.1.6. User Interface Design

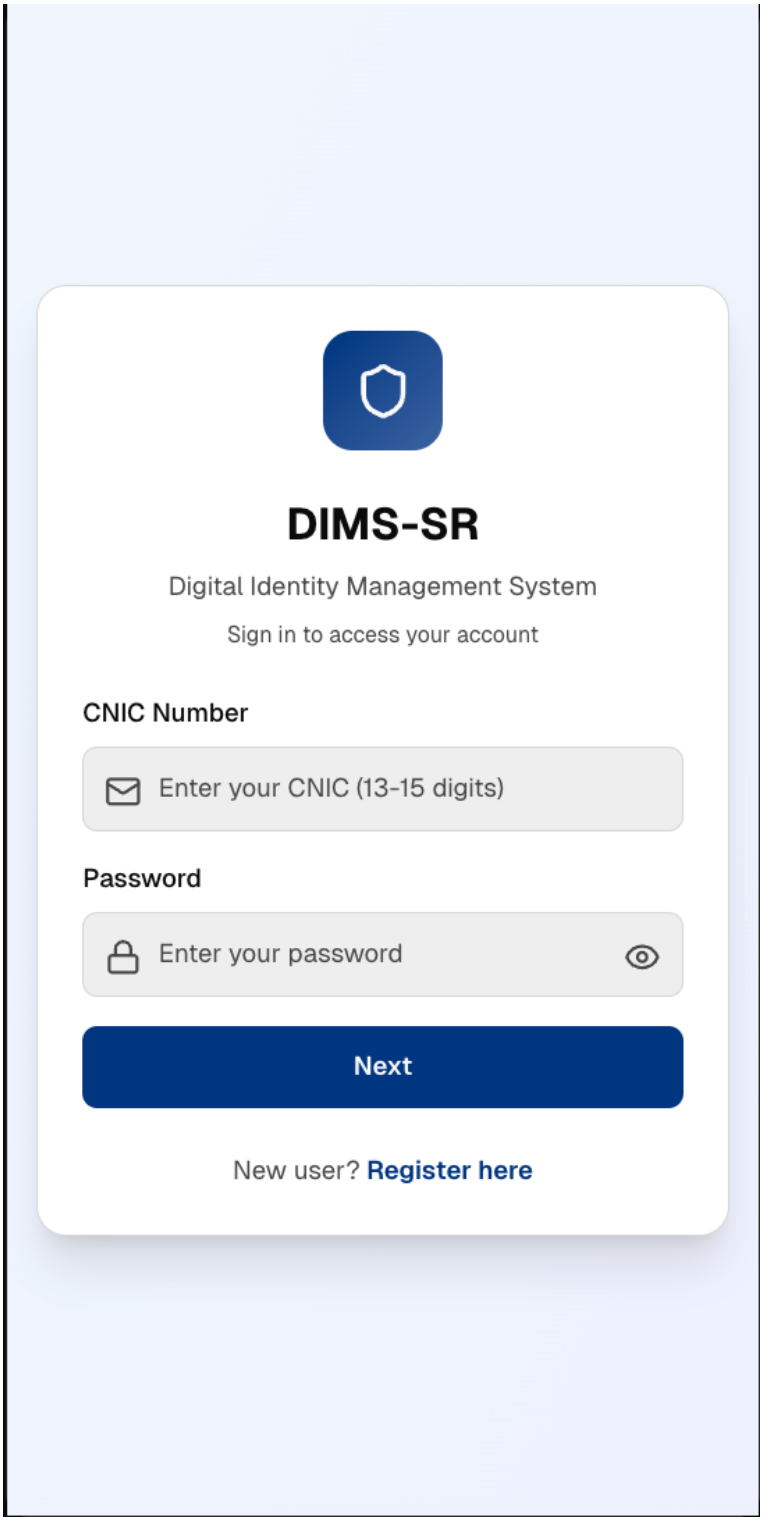

Figure 8. Login Page

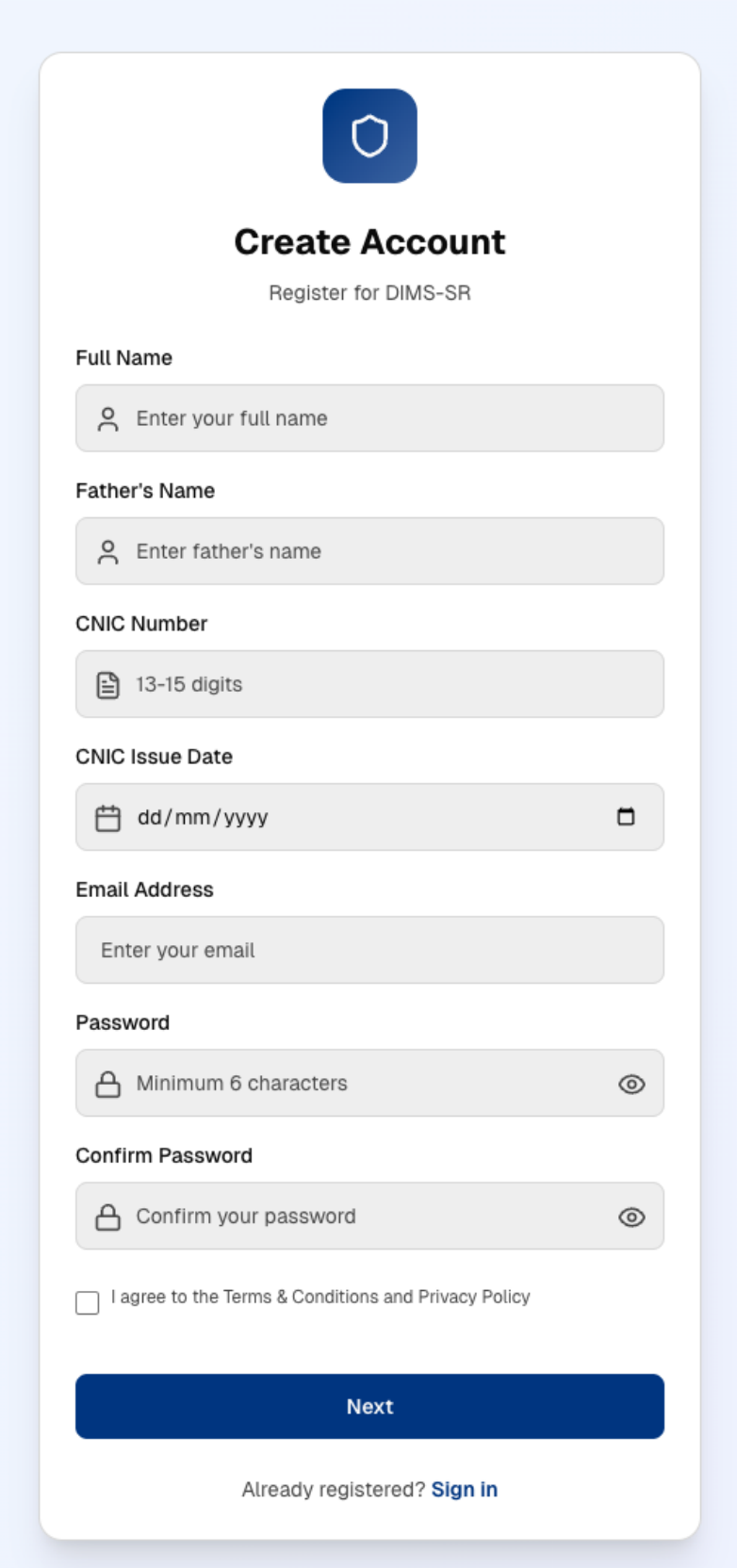

Figure 9. Create Account

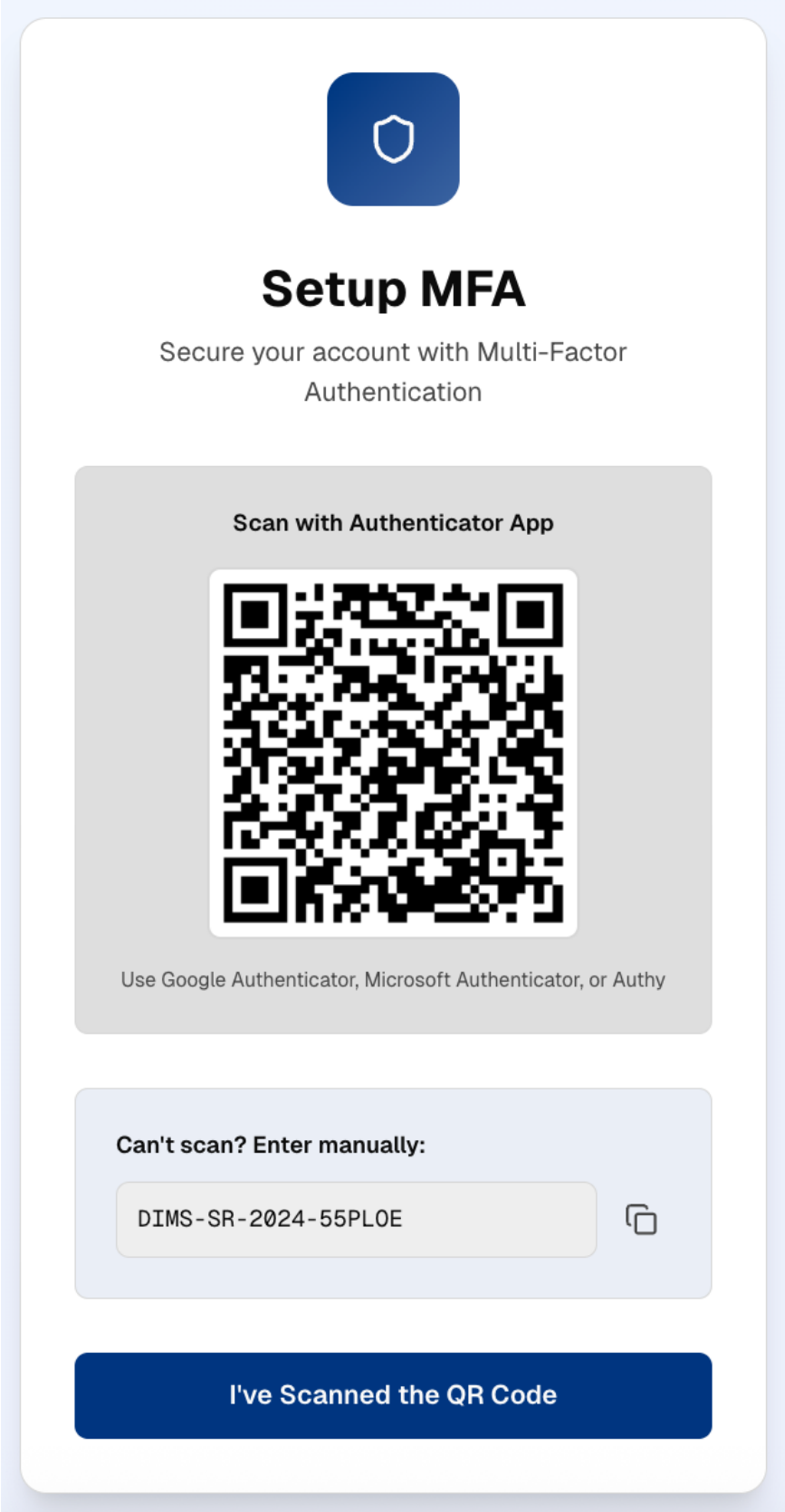

Figure 10. MFA Configuration Page

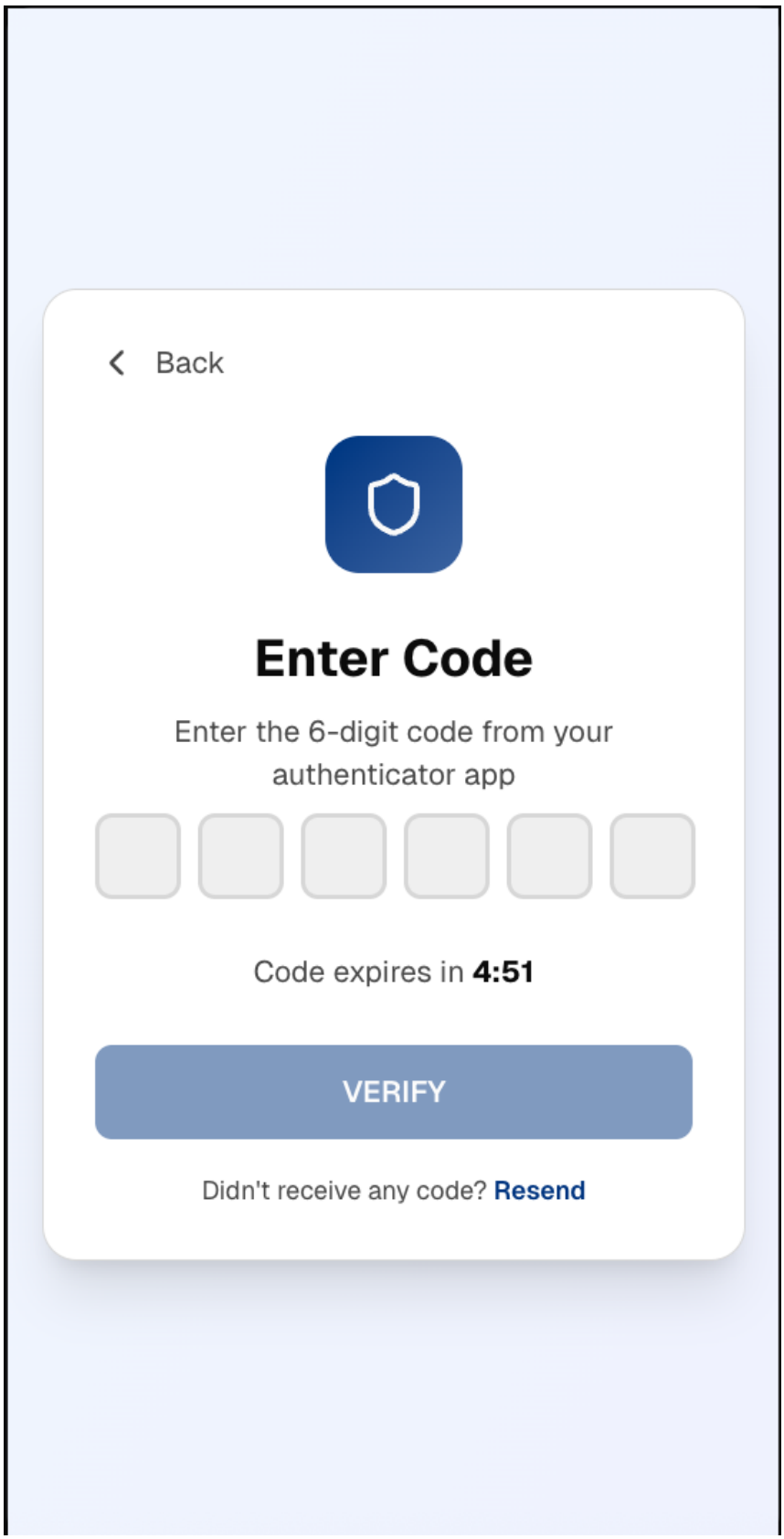

Figure 11. MFA Verification Page

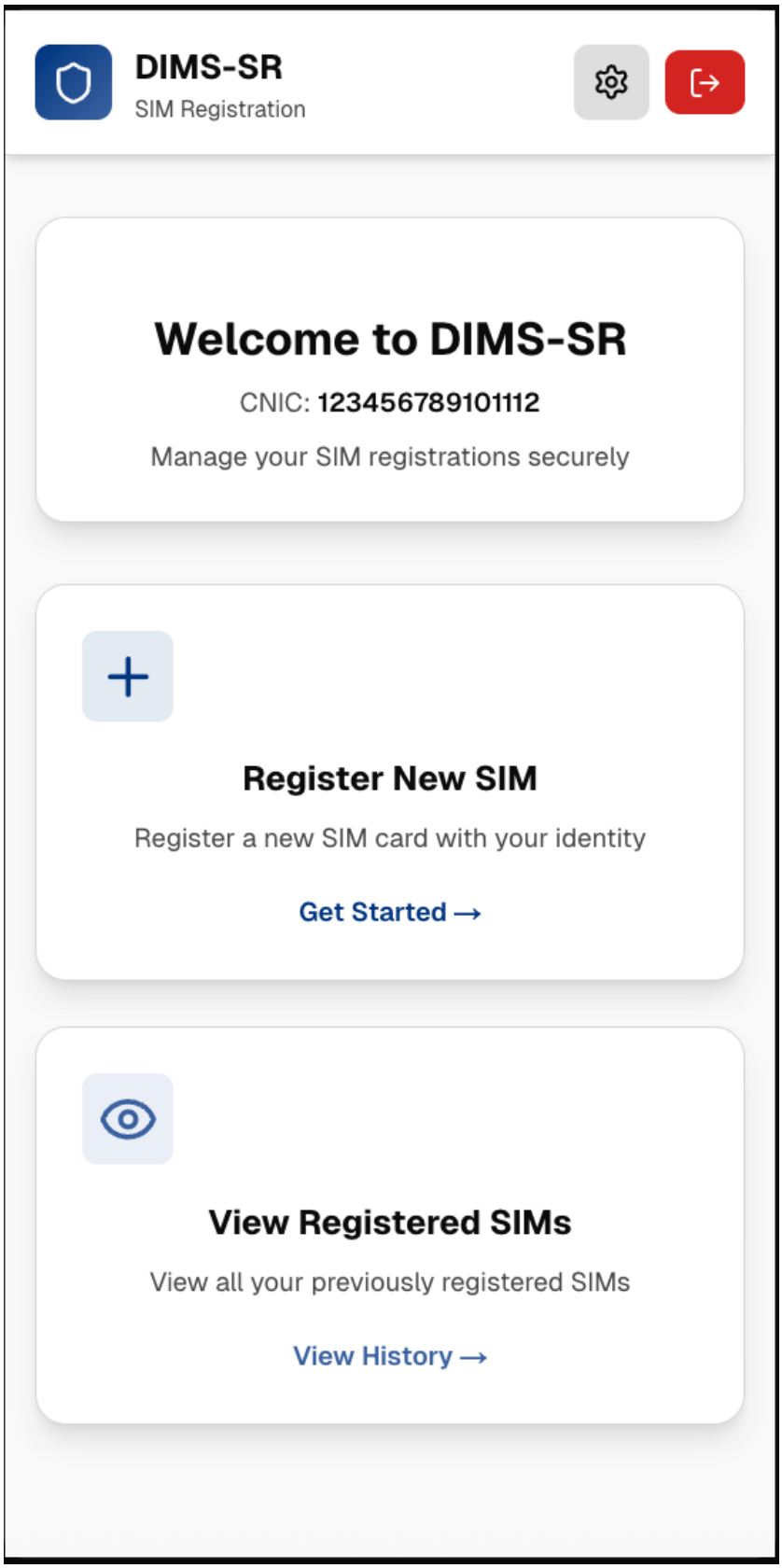

Figure 12. Home Page

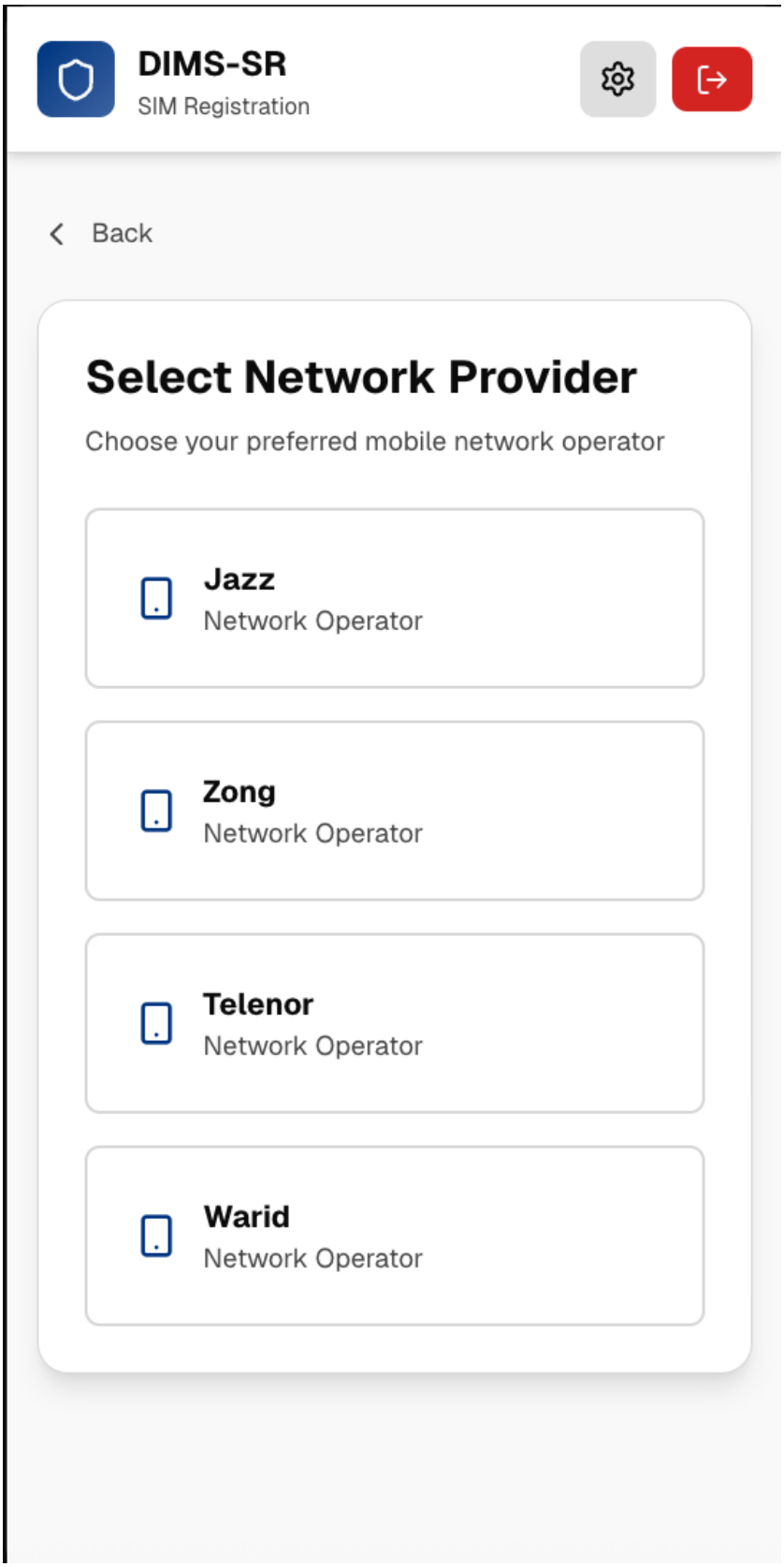

Figure 13 Register SIM

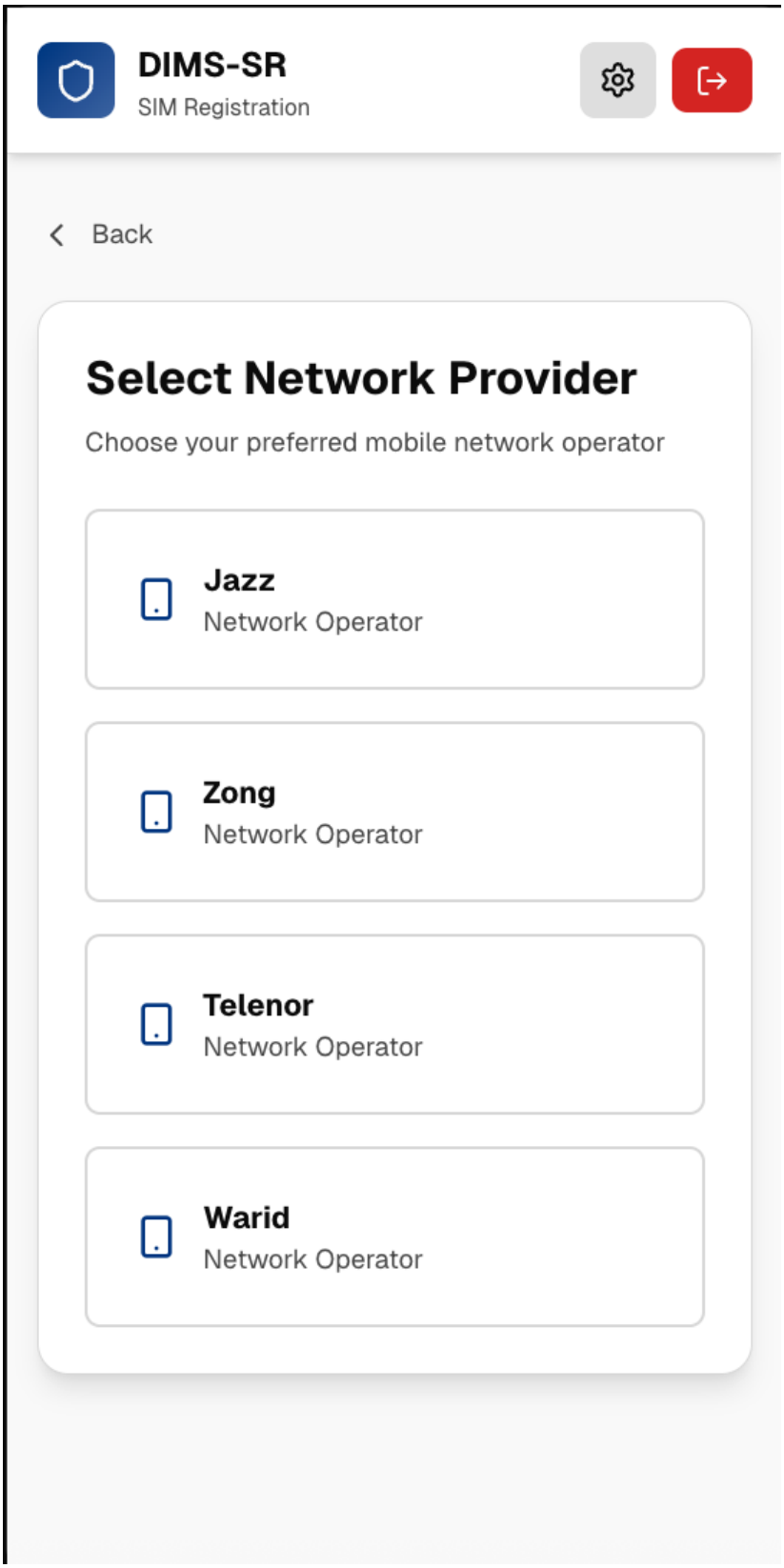

Figure 14. Register SIM - 1

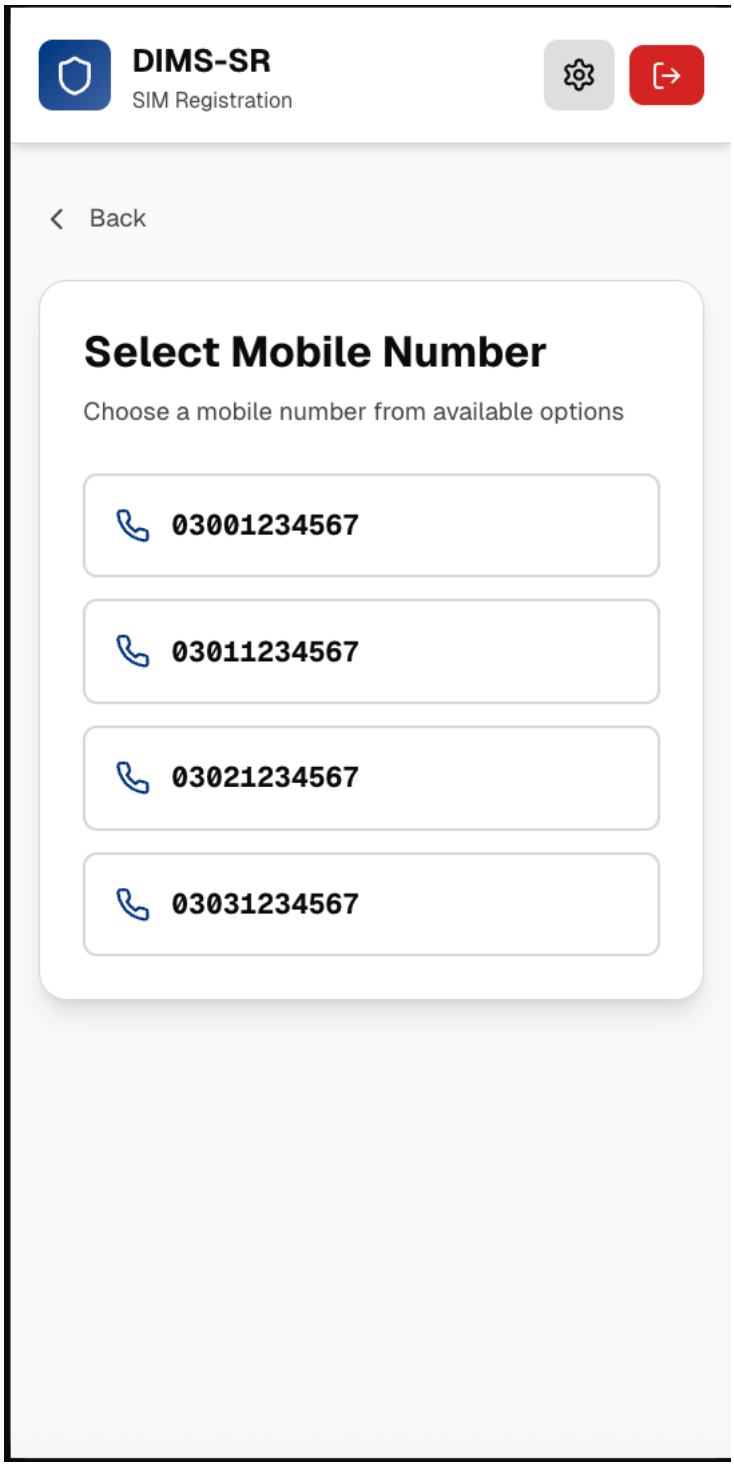

Figure 15. Register SIM - 2

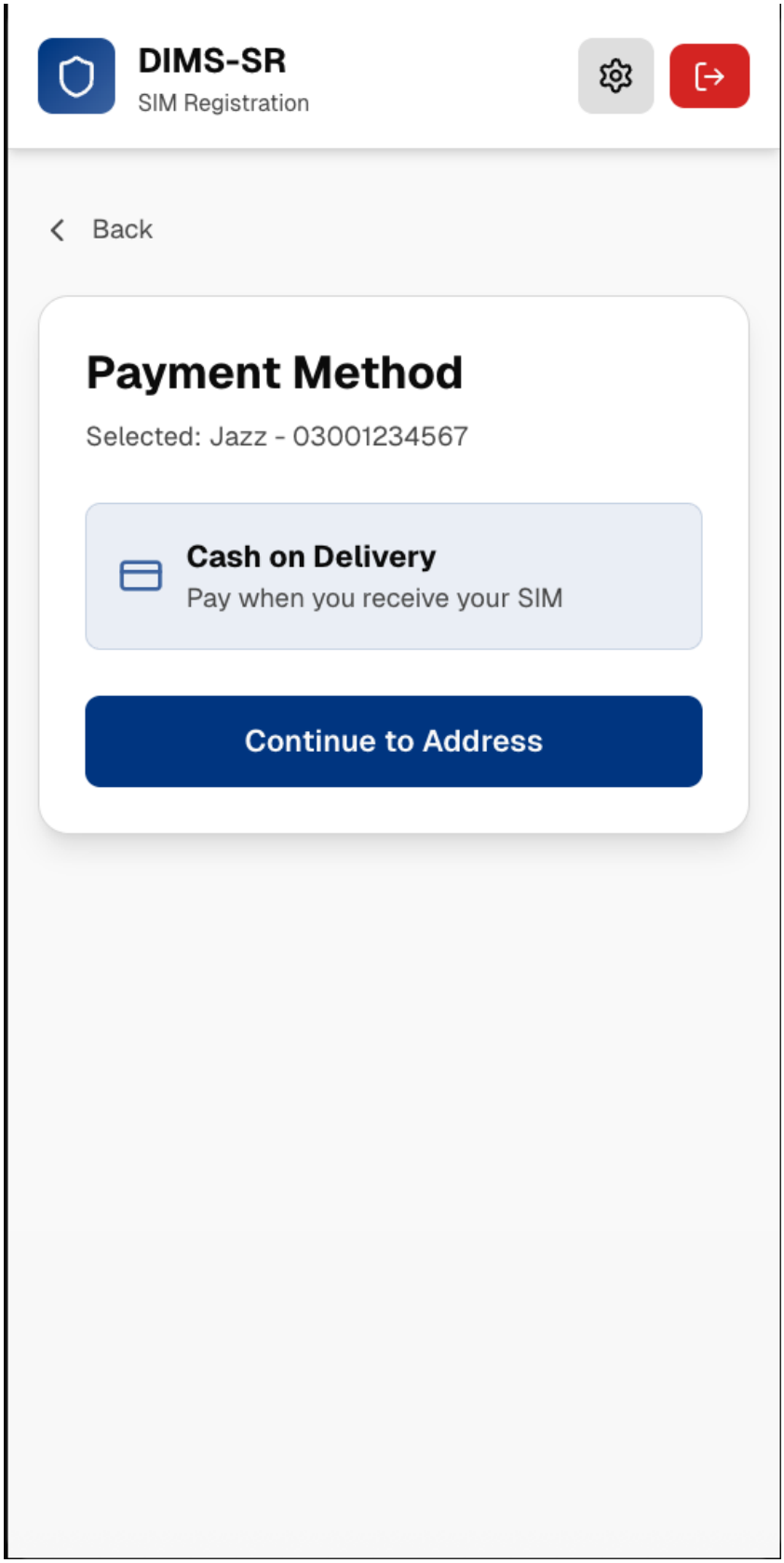

Figure 16. Register SIM - 3

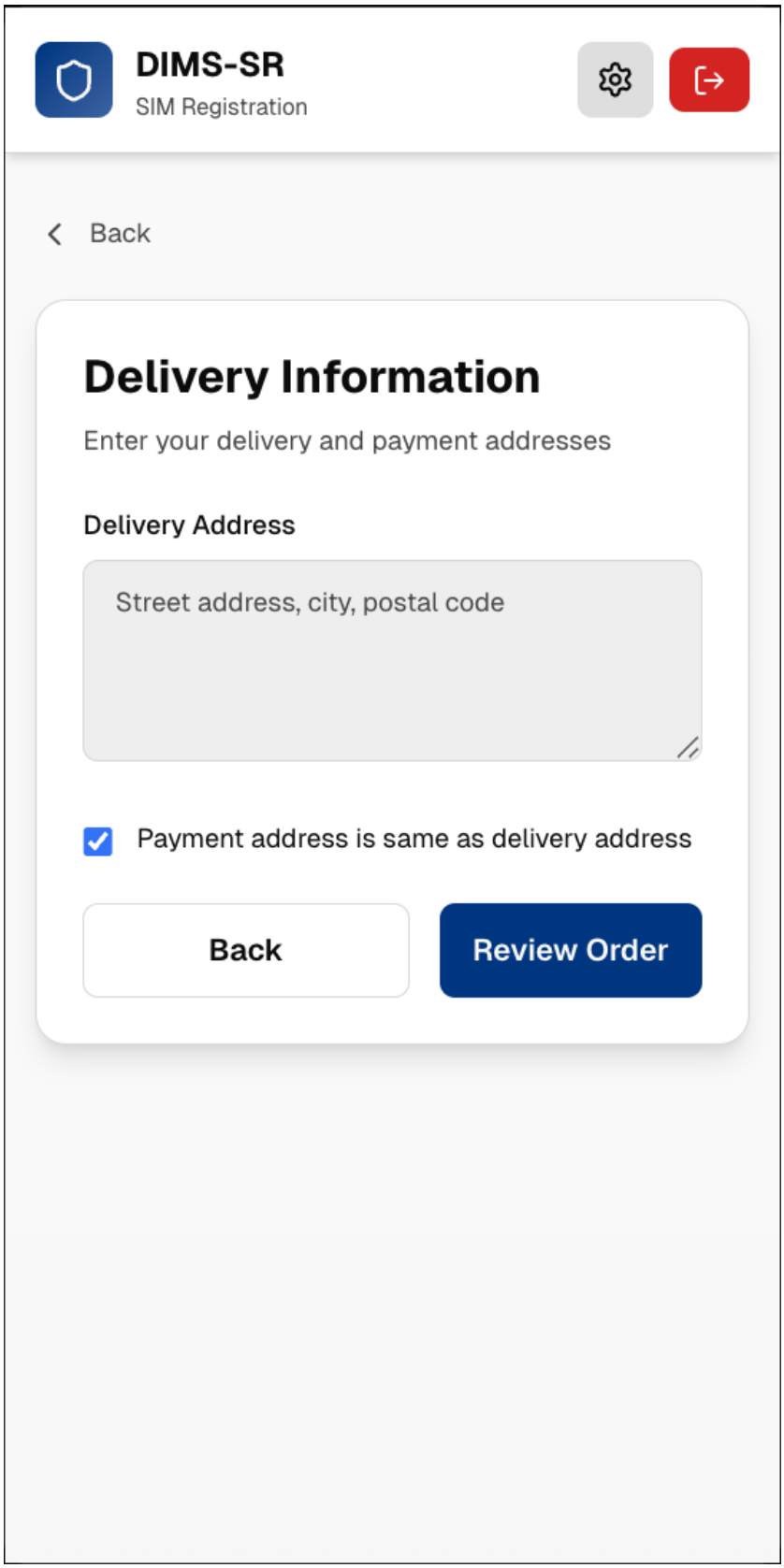

Figure 17. Register SIM - 4

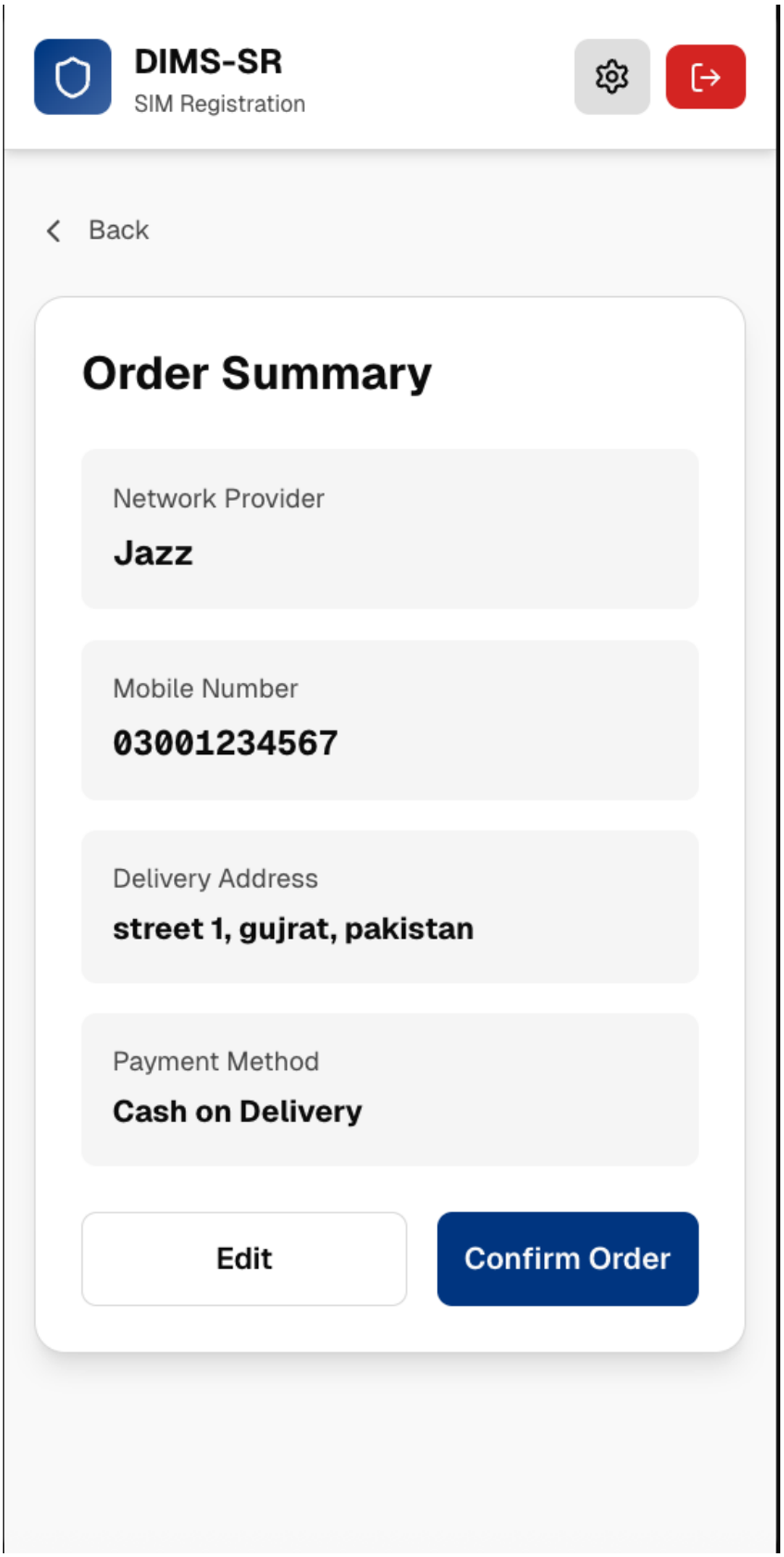

Figure 18. Register SIM - 5

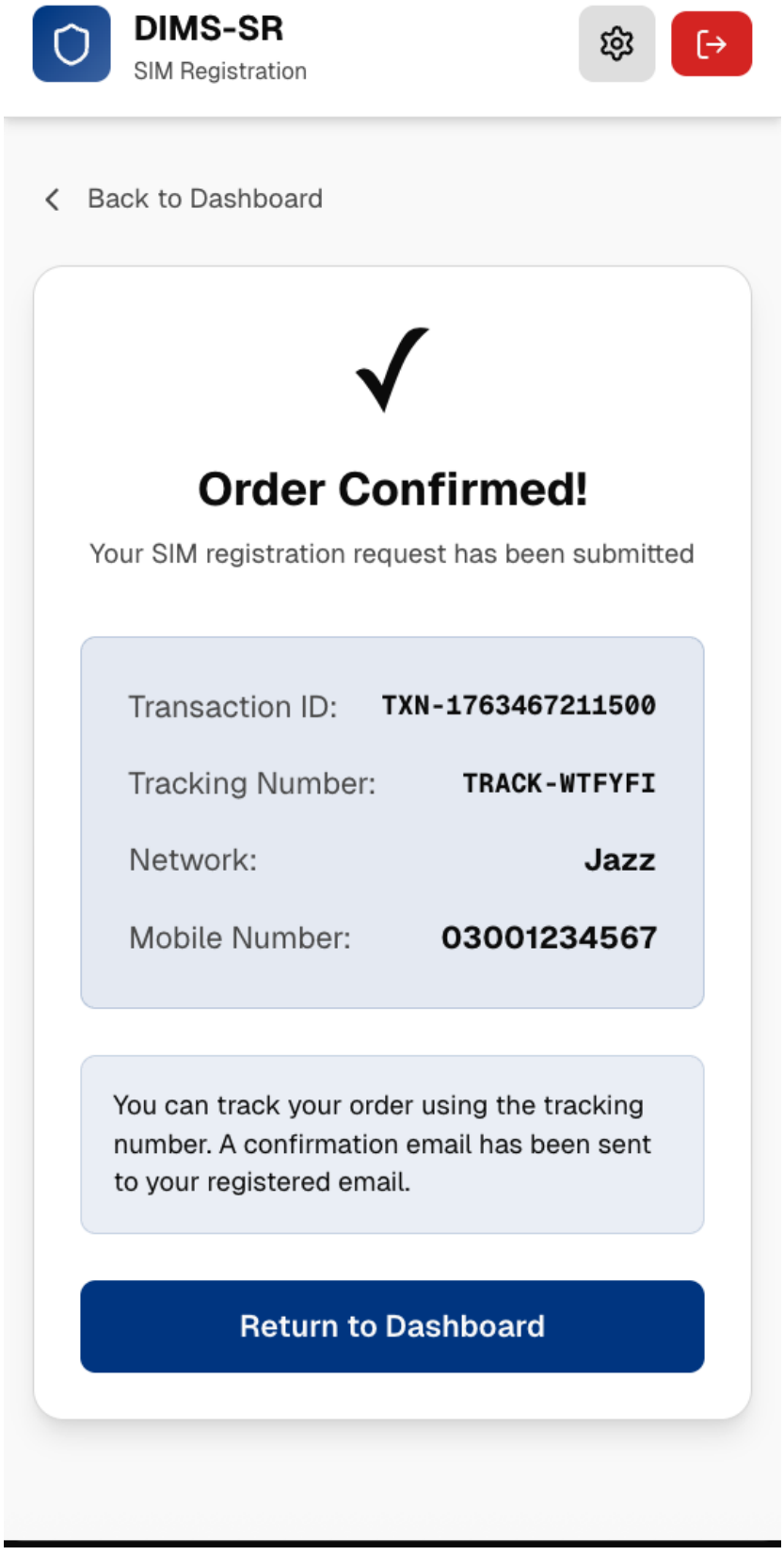

Figure 1109. Register SIM - 6

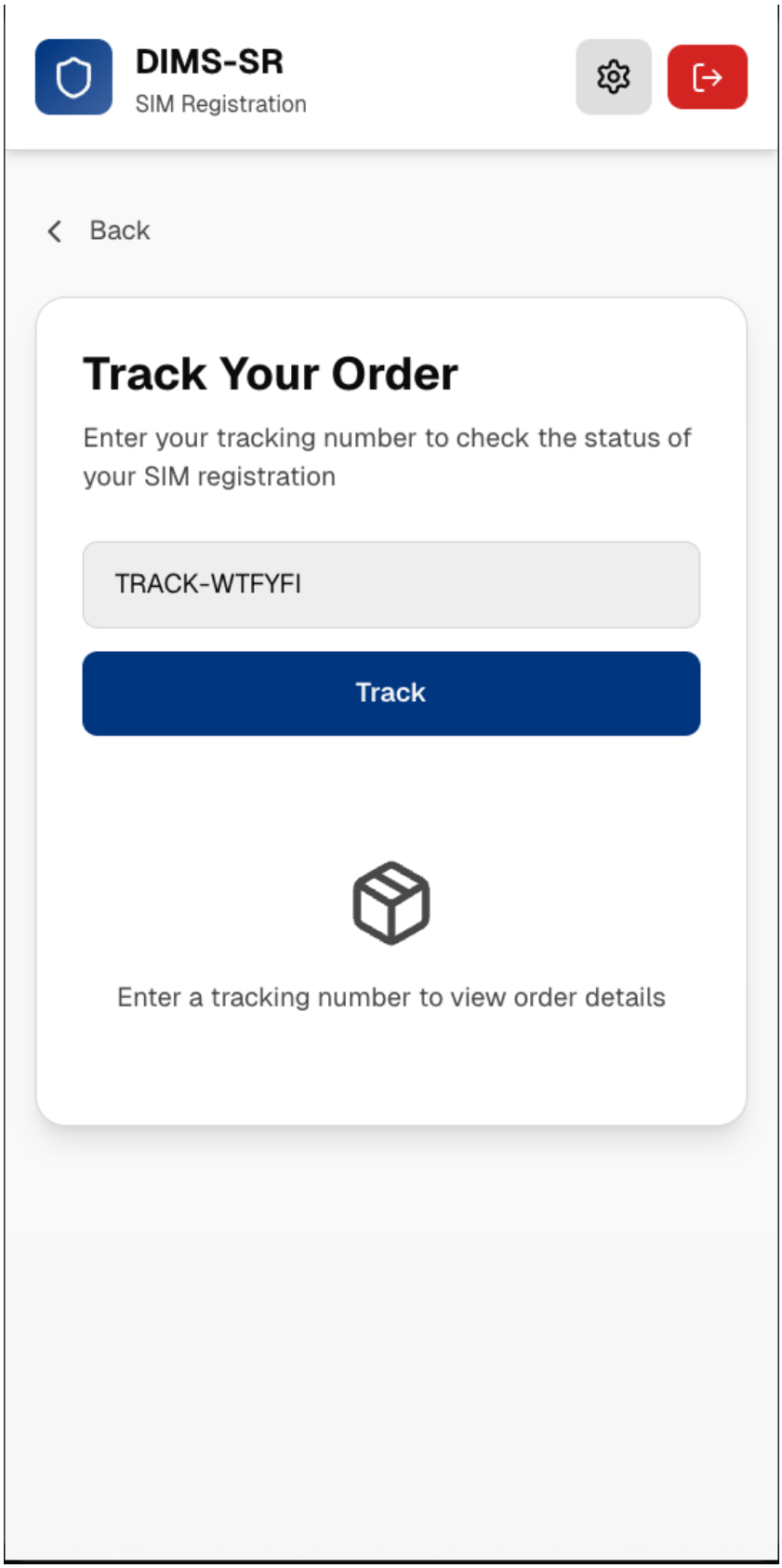

Figure 20. Track Order

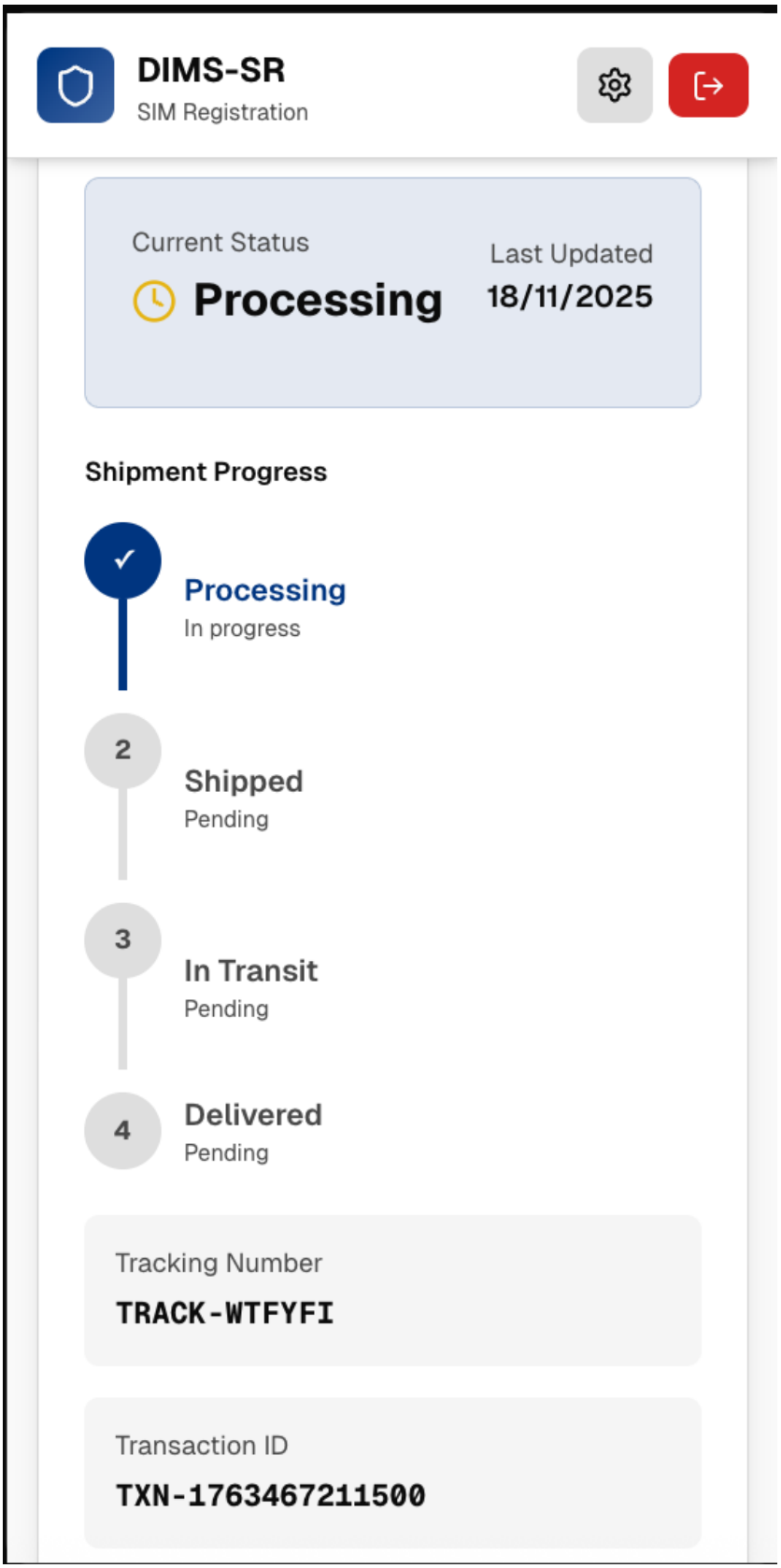

Figure 21. Track Order - 1

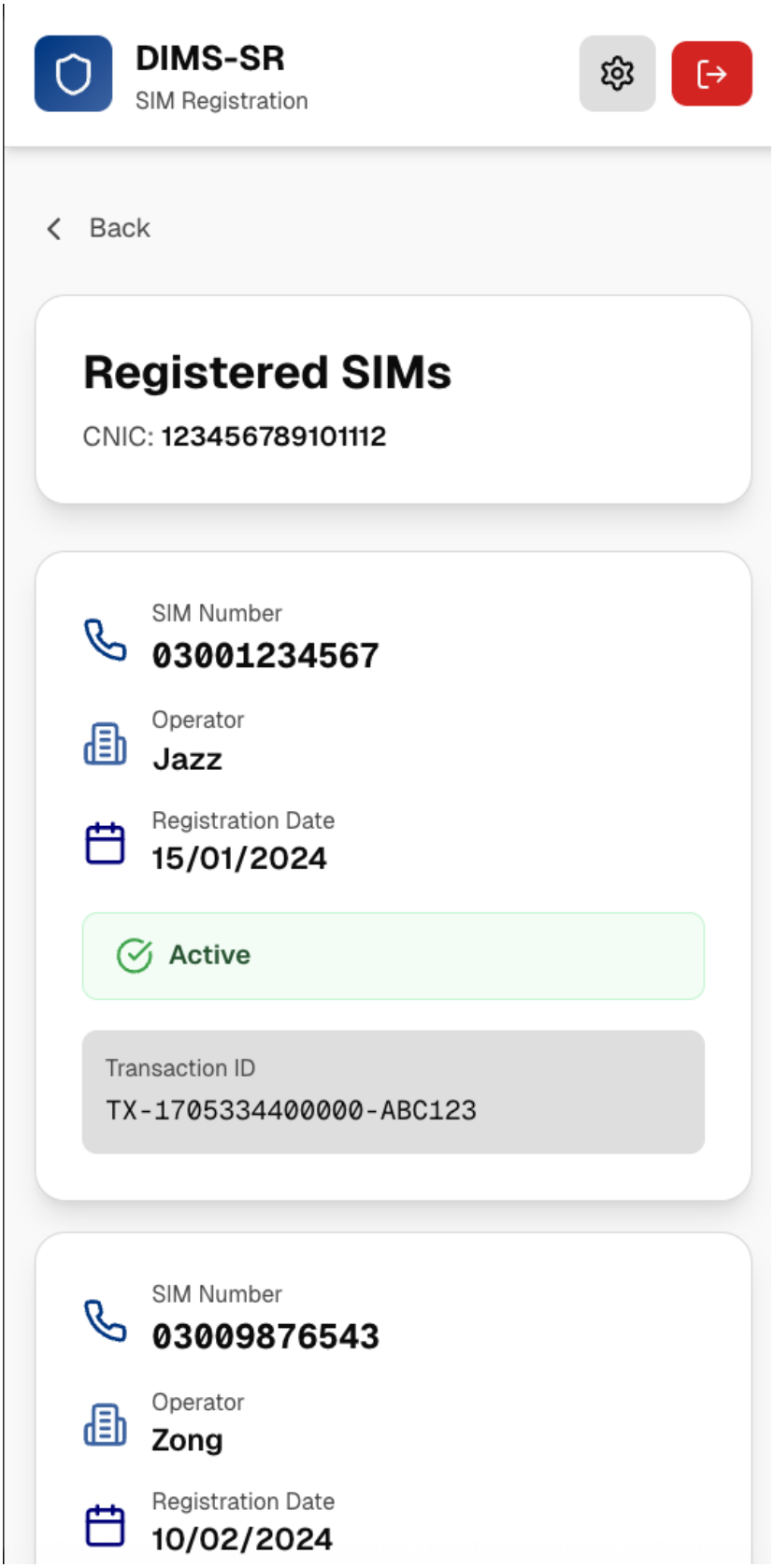

Figure 22. View SIM record

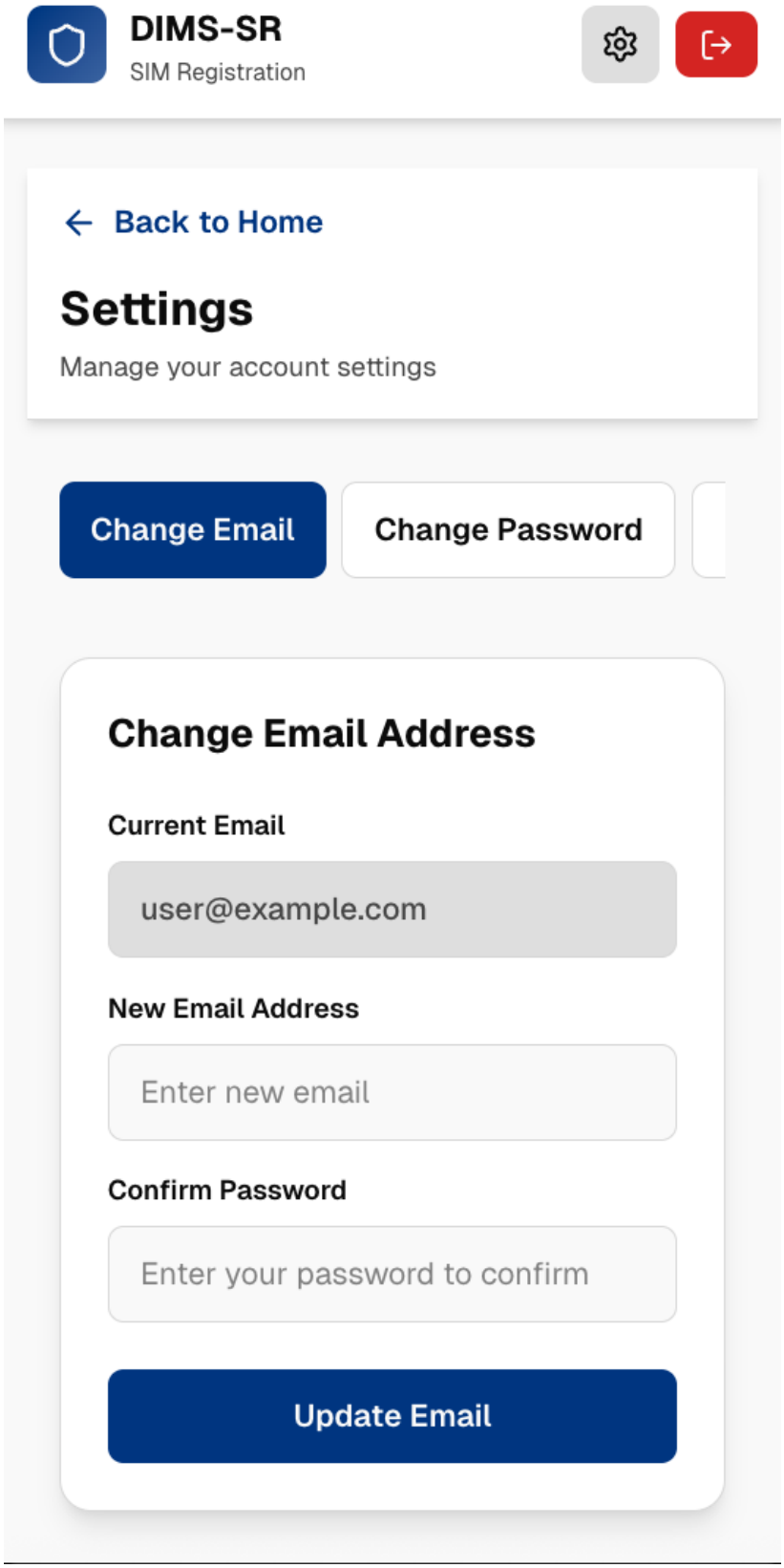

Figure 23. Settings Page