# GeSIM: World’s first on-chain MVNO

## A Cryptographically Verifiable and Programmable Telecom Layer

## Abstract

GeSIM proposes a novel architecture for Mobile Virtual Network Operator (MVNO) infrastructure, replacing the current trust-based telecom model with cryptographic proofs and automated smart contracts. The system decouples sensitive user data from settlement logic, utilizing **Zero-Knowledge Proofs (ZKPs)** to verify usage and service delivery without exposing raw Call Detail Records (CDRs). **ZK-TLS** is employed to ensure the verifiable authenticity of the provisioning server (SM-DP+), eliminating the risk of identity spoofing and SIM fraud. This framework establishes an **On-Chain Settlement Engine** compatible with emerging GSMA standards (BCE), providing near-instant reconciliation and creating a liquid, programmable market for telecommunication services.

# 1. Introduction & Problem Statement

## 1.1 Current Telecom Trust Model

The contemporary telecom ecosystem operates as a series of opaque, centralized monopolies bound by complex, manual trust agreements. The core MVNO stack—comprising BSS (Billing), OSS (Operations), and Roaming Settlement—is characterized by proprietary databases and vendor-locked systems. Trust is assumed, not proven. This results in high friction and systemic vulnerabilities.

## 1.2 Key Problems

- **SIM Fraud & Identity Risk:** The reliance on centralized subscriber databases (HSS/HLR) and provisioning servers (SM-DP+) makes them high-value targets. **SIM hijacking and profile cloning** lead to billions in annual losses and severe security risks for users.
- **Opaque Usage Accounting (The "Trust Tax"):** Roaming settlement is slow (30-60 days) and manual, based on exchanging non-auditable data files (TAP/BCE). This high cost of reconciliation is passed directly to the consumer as the "Trust Tax."
- **Unverifiable QoS/SLA:** Service Level Agreement (SLA) reporting relies on the MNO’s internal monitoring, creating a conflict of interest and leading to frequent disputes over service quality and conditional payments.
- **Fragmented Cross-Border Access:** Switching networks requires complex legal and technical agreements, hindering the realization of true global, interoperable mobile service.

## 1.3 Need for Cryptographic Verifiability

The GeSIM protocol replaces trust-based assumptions with **proof-based guarantees**. By anchoring critical identity, usage, and settlement events to an immutable ledger and validating them with Zero-Knowledge Cryptography, we introduce auditable, programmable logic to the telecom industry.

## 2. Design Goals

### 2.1 Verifiable Provisioning

To eliminate identity spoofing, the authenticity of the provisioning server (SM-DP+) must be proven cryptographically to the device before any profile is downloaded.

### 2.2 Privacy-Preserving Entitlement

Entitlements (data plans, service access) must be bound to the device's pseudonymous identifier (EID commitment) on-chain without revealing the raw EID, IMSI, or user PII.

### 2.3 ZK-Based Usage Accounting

Usage data must be verified for correctness and total sum (**proof of sum correctness**) via ZKPs, allowing settlement without exposing fine-grained, raw CDRs.

### 2.4 On-Chain Settlement

The entire wholesale reconciliation and settlement process must be automated by smart contracts, executing payment in near-real-time based on verified usage and SLA proofs.

### 2.5 GSMA Compatibility

The protocol must be built to integrate with current and emerging GSMA standards (e.g., BCE reporting, SM-DP+ APIs) to ensure seamless MNO onboarding.

### 2.6 Security + Privacy by Default

The architecture must minimize metadata leakage, guarantee data sovereignty for the user (User-Custodial Auth), and maximize cryptographic assurances against fraud and attack.

## 3. System Architecture

### 3.1 Actors

- **User/Subscriber:** Holds the cryptographic keys (wallet) controlling the service entitlement.
- **Device (eUICC/LPA):** The physical or embedded SIM containing the key material for authentication.
- **SM-DP+ (Legacy):** The existing provisioning server, now wrapped by the GeSIM ZK-TLS Gateway.
- **MVNO Contract:** The core set of smart contracts governing entitlements, escrow, and settlement logic.
- **Provers:** Off-chain, specialized machines (ZK Coprocessors) that compute and submit validity proofs (usage, SLA) to the contract.
- **MNO Partners:** The upstream network providers receiving settlement payments.
- **Indexers/Oracles:** Provide verifiable data feeds (e.g., DePIN network performance data).

### 3.2 System Components

- **High-Throughput Settlement Layer:** A smart contract platform optimized for low cost and high transaction finality, hosting the core escrow and reconciliation logic.
- **ZK-Optimized Verification Environment:** A dedicated computation layer (ZK Coprocessor) used solely for generating and verifying complex proofs of large datasets (CDRs).
- **User-Custodial Identity Module:** A cryptographic framework (e.g., TEE-secured HSS/HLR functions) that delegates key ownership to the user's device/wallet.
- **Tokenized Catalog:** A set of smart contracts defining and issuing service entitlements as Semi-Fungible Tokens (e.g., ERC-1155 derivative).

### 3.3 High-Level Architecture Diagram

The architecture is structured as a **Modular Stack**:

1. **Identity Layer:** User Wallet holds DID/Keys (User-Custodial Auth).
2. **Access Layer:** Device connects to ZK-TLS Gateway for verified provisioning.
3. **Data Layer:** Raw CDRs remain off-chain; Merkle Roots anchor usage.
4. **Verification Layer:** ZK Coprocessors prove usage sums and SLAs.
5. **Settlement Layer:** Smart Contracts execute automated payments to MNOs.

## 4. Cryptographic Foundations

### 4.1 zkTLS Provenance

We leverage a variant of **ZK-TLS** (Zero-Knowledge Transport Layer Security) to allow the device to cryptographically verify the identity and certificate chain of the SM-DP+ server **without exposing the session data or the server's private keys**. This proof is required before the profile download sequence begins, eliminating provisioning spoofing.

### 4.2 EID Possession Proofs

The Device proves to the MVNO Contract that it possesses a valid EID (eUICC Identifier) commitment tied to an entitlement **without revealing the raw EID**. This ensures binding without breaching privacy.

### 4.3 Usage Commitments

Raw Call Detail Records (CDRs) are aggregated into structured data batches. A **Merkle Tree** is constructed over each batch, and only the resulting **Merkle Root** (the Usage Commitment) is anchored on-chain. This provides an audit trail without storing private logs.

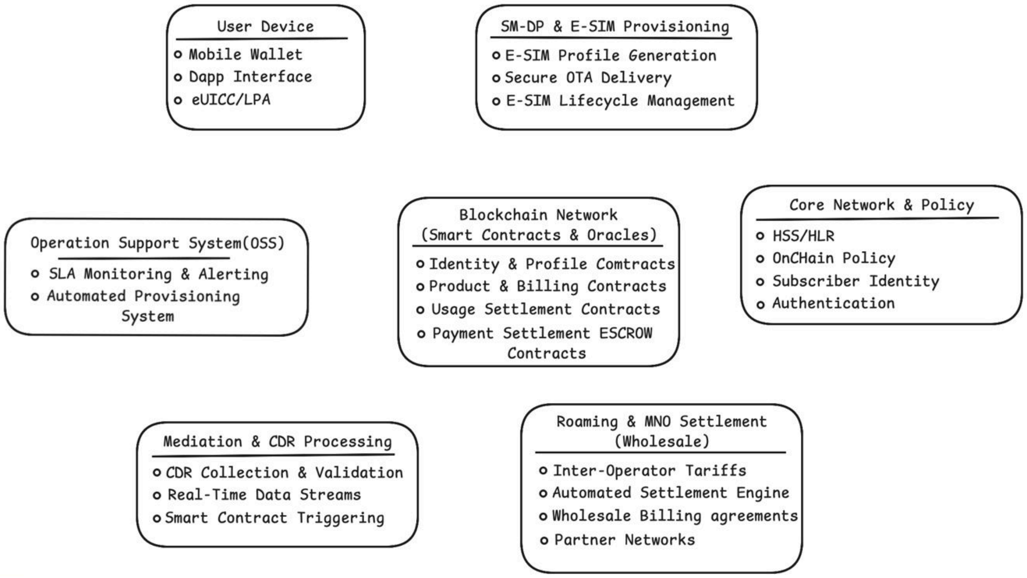
### 4.4 Zero-Knowledge Usage Proofs

Specialized **ZK Coprocessors** execute integrity-proofed queries against the off-chain Usage Commitments. The system generates a ZKP that validates the final settlement amount, specifically confirming: $Proof( \sum_{CDRs} (Usage) = InvoiceAmount)$. This proves the mathematical correctness of the billable sum.

### 4.5 On-Chain State Commitments

Product plans and entitlements are represented as **ERC-1155 derivative tokens**. The token's metadata contains the cryptographic commitment to the plan’s constraints (e.g., max quota, expiry), ensuring auditable pricing and usage rules.

## 5. Technical Architecture/Components


User Device
Mobile Wallet
Dapp Interface
eUICC/LPA
SM-DP & E-SIM Provisioning
E-SIM Profile Generation
Secure OTA Delivery
E-SIM Lifecycle Management
Operation Support System(OSS)
SLA Monitoring & Alerting
Automated Provisioning System
Blockchain Network (Smart Contracts & Oracles)
Identity & Profile Comtracts
Product & Billing Contracts
Usage Settlement Contracts
Payment Settlement ESCROW Contracts
Core Network & Policy
HSS/HLR
OnCHain Policy
Subscriber Identity
Authentication
Mediation & CDR Processing
CDR Collection & Validation
Real-Time Data Streams
Smart Contract Triggering
Roaming & MNO Settlement (Wholesale)
Inter-Operator Tariffs
Automated Settlement Engine
Wholesale Billing agreements
Partner Networks

## 6. Security Model

### 6.1 Threat Model

The primary threats addressed are:

- **SM-DP+ Spoofing:** A rogue server impersonating the provisioning entity.
- **EID Misbinding:** Linking a service entitlement to a device the user does not control.
- **Fraudulent Usage Reporting:** An MNO claiming excessive usage for fraudulent billing.
- **Replay Attacks:** Submitting the same ZK proof or provisioning request multiple times.

### 6.2 Telecom-Specific Protections

- **zkTLS:** Defends against SM-DP+ spoofing by cryptographically verifying the server's identity.
- **EID Proofs:** Prevents misbinding by enforcing proof-of-possession tied to the wallet.
- **TEE Security:** Authentication keys (Ki) are secured within Trusted Execution Environments (or user devices), preventing the single HSS honeypot risk.
- **ZK Non-Replay Circuits:** Proofs are constructed to include unique transaction nonces and timestamps, making them impossible to replay.

### 6.3 On-Chain Protections

- **Escrow Logic:** Funds are locked and released only upon the fulfillment of verified cryptographic proofs (SLA/Usage).
- **Verifier Checks:** The smart contract includes robust checks against the ZK proof validity, preventing fraudulent settlement.

### 6.4 Privacy Model

The system is built for pseudonymity: User PII is held off-chain (if at all). On-chain data consists only of cryptographic commitments (Merkle roots), proofs of computation, and pseudonymized wallet addresses. Raw CDRs are never broadcast.

## 7. Economic & Governance Model

### 7.1 Payment Flows

The system creates a transparent, three-party payment flow:

1. **User Payment:** User pays for the Plan in stablecoins.
2. **Escrow:** Funds are held by the Settlement Contract.
3. **MNO Payout:** Funds are released automatically to the MNO upon ZK-verified usage.
4. **MVNO Margin:** The predefined margin is extracted by the MVNO Contract before payout.

### 7.2 Refund Structure

ESCROW Contracts will be used to manage unhandled exceptions, where if there are any discrepancies in plan purchase/activation, the refund will be made directly via the Smart Contracts itself.

### 7.3 Incentive Layers

The protocol includes optional incentive layers to align network participation:

- **Prover Rewards:** Fees paid to ZK Coprocessor operators for computing high-volume proofs.
- **Indexer Rewards:** Payments to services that index the immutable ledger for easy querying.
- **DePIN Oracles:** Payments to users/devices for submitting verified, real-time network performance data (SLA proofs).

### 7.4 Governance Phases

The protocol adopts a progressive decentralization model:

- **Phase 1 (Centralized):** Initial development and contract deployment are centrally controlled (Multi-sig).
- **Phase 2 (DAO Oversight):** Key parameters (fee structure, MNO onboarding) are moved to a decentralized autonomous organization (DAO) controlled by token holders.
- **Phase 3 (Full Decentralization):** The protocol is self-sustaining, with the community managing all upgrades and economic parameters.

## 8. Implementation Roadmap

| Phase | Focus Area | Key Deliverable |
|---|---|---|
| **Phase 1** | Smart Contract Layer | Escrow and basic entitlement issuance (ERC-1155). Initial Ricardian Contract framework. |
| **Phase 2** | Cryptographic POC | Functional prototype of ZK-TLS verifiable provisioning and EID possession proofs. |
| **Phase 3** | MNO Integration & ZK Metering | Implementation of the ZK Coprocessor for high-volume BCE usage aggregation. First MNO pilot integration. |
| **Phase 4** | Security Hardening | Comprehensive security audits of all smart contracts and ZK circuits. Optimization of proving costs. |
| **Phase 5** | Multi-MNO Ecosystem Launch | Open APIs for onboarding additional MNOs. Implementation of multi-MNO roaming/clearinghouse logic. |

## 9. Related Work

### 9.1 Traditional MVNOs

GeSIM aims to replace the legacy clearinghouse model, which relies on proprietary vendor-locked solutions, with a transparent, open-source settlement layer.

### 9.2 DePIN Projects

GeSIM integrates DePIN principles by incentivizing users to become verifiable data oracles, securing the integrity of the network performance data used for SLA monitoring.

### 9.3 ZK in Telecom

Prior research focused on generic anonymous authentication. GeSIM moves beyond this to deploy ZKPs for the highly valuable, transactional layer: **verifiable provisioning and settlement**.

### 9.4 Positioning

GeSIM stands at the intersection of GSMA compatibility, cryptographic verification, and programmable finance. It is the first architecture designed to achieve **automated, trustless wholesale roaming settlement** while simultaneously establishing **User-Custodial Auth** as the default security model.

## 10. Conclusion

The GeSIM protocol offers a necessary and irreversible upgrade to global mobile telecommunications. By leveraging Zero-Knowledge Proofs, User-Custodial Identity, and programmable smart contracts, we eliminate the systemic vulnerabilities of centralized infrastructure and remove the billions of dollars lost annually to fraud and manual settlement costs. GeSIM creates a verifiable, privacy-preserving, and liquid telecom layer, paving the way for truly programmable, decentralized connectivity.

## Appendix

*(Note: These appendices would be graphical representations and detailed technical specifications in the final white paper.)*

- **A. Architecture Diagram:** Visual overview of the five layers (Identity, Access, Data, Verification, Settlement).
- **B. Provisioning Sequence Diagram:** Detailed flow from Device request to ZK-TLS verification and profile download.
- **C. Settlement Sequence Diagram:** Detailed flow from MNO usage reporting to ZK Proof submission and automated stablecoin payout.
- **D. Cryptographic Notation:** Formal specification of the ZK circuits used for usage and identity proofs.