Zsub SSCM Roadmap

Version 0.1.9
Authored by the Zsub Team
Published Dec 28, 2025

This roadmap outlines the phased development of Self-Sovereign Cryptographic Mesh (SSCM) protocol suite. Each phase delivers independently functional protocols while building toward a complete decentralized identity, trust, and connectivity infrastructure.

- Already Shipping (Dec 2025) – Phase 0: Bootstrap Foundation [*] (live & used daily)
- Q1 2026 – Phase 1: Cryptographic Foundation (StarfortDB + Heavy WoT) ▸ in progress
- Q2 2026 – Phase 2: Basic Mesh Connectivity (Keel P2P + NAT traversal) ▸ polishing
- Q3 2026 – Phase 3: Application Integration (Virtual L2 + gated services)
- Q4 2026 – Phase 4: Ecosystem Scaling (Discovery + blind micro-payments)
- Q1 2027 – Phase 5: Secure Group Messaging (large-scale forward-secret groups)
- Q2 2027 – Phase 6: Privacy Hardening (onion routing + DPI evasion)

→ Complete SSCM by mid-2027, shipping at least every quarter

Phase 0: Bootstrap Foundation (Completed December 2025)

Deliverable: Working hierarchical key management system with secure memory handling, multi-tool integration, agent, CLI — bootstraps dogfooding and real-world user testing

A git-based subcommand system demonstrating hierarchical key management and per-context key derivation.

Architecture:

- Secure backend in Zig (zero dependencies)
- Python CLI interface
- Keys encrypted at rest (ChaCha20-Poly1305)
- Secrets decrypted into mlock()ed memory, zeroed after use
- PIN-protected key access

Capabilities:

- npub/nsec pair generation and management
- Git commit and tag signing
- SSH agent implementation
- Minisign-compatible build signing with embedded BIP-340 signatures
- Nostr event broadcasting (kinds 0, 1, 30617, 30618)

Source: https://codeberg.org/zsub/rebased

Technical validation: Confirms viability of hierarchical key derivation, per-context isolation, and secure memory handling in production use.

Purpose: Establish cryptographic foundation, prove secure implementation practices, and bootstrap real-world usage (dogfooding) to inform subsequent phases and enable early user testing in live workflows.

Status: Implemented and actively used (last update December 2025).

Phase 1: Cryptographic Foundation (Q1 2026)

Deliverable: Seed-derived private key database with multi-device sync and privacy-preserving trust proofs

StarfortDB

Hierarchical deterministic key database providing:

- Blake3-based key derivation with configurable context strings
- Per-relationship key isolation via hierarchical deterministic derivation
- Multi-device synchronization with branch healing
- Hardware security device support (YubiKey via PC/SC)
- Continuous cascading key rotation with configurable retention periods
- Threshold recovery via M-of-N Shamir secret sharing
- Three-tier access control (cool/warm/hot) with layered encryption
- Support for Ristretto255/Curve25519, Ed25519, and secp256k1

Heavy Web of Trust

Privacy-preserving trust verification protocol providing:

- Schnorr proofs of knowledge over Pedersen commitments
- Blake3 Merkle trees for revocation
- Minimal-disclosure attribute verification
- Configurable trust models (self-anchored, organizational, federated)
- Real-time revocation with ~358 byte path proofs
- ~0.8-1.3 ms verification time for 5-hop chains

Standalone Value

Application domain: Hierarchical key management and attribute verification for identity systems.

Use cases:

- Code signing and verification workflows
- SSH key management across devices
- Credential storage with automatic rotation
- Team access control with attribute-based policies

Independent utility: StarfortDB provides hierarchical deterministic key derivation with continuous rotation. Heavy enables privacy-preserving trust chains. Both operate independently of subsequent phases and address key management and trust verification requirements without requiring mesh connectivity.

Technical Milestone: Standalone credential and authentication protocols operational.

Specification: 1. Self-Sovereign Identity and Trust

Status: In progress — substantial foundations of StarfortDB coded.

Phase 2: Basic Mesh Connectivity (Q2 2026)

Deliverable: NAT-penetrating, double-ratchet encrypted P2P connections with blind peer rendezvous

Keel

UDP-based secure connection protocol providing:

- Double ratchet encryption (Blake3 symmetric, ECDH asymmetric)
- Zero-knowledge authentication via Heavy proofs
- Continuous key rotation at configurable intervals (default 1000 messages)
- Fast reconnection via proof tokens (±160 second window)
- ~5-15 ms handshake latency
- 473-byte payload limit (uniform 512-byte packets)

Skylight

NAT traversal protocol providing:

- ICE-like candidate exchange (host, server-reflexive, relay)
- Connectivity checks with authentication
- Asynchronous operation via dead drops
- ~100 ms check pacing

Rendezvous

Peer coordination protocol providing:

- Blind message relaying
- Message holding for offline peers
- Load balancing (round-robin, broadcast)
- ~5,000 peers per host capacity

Submerge

Message chunking protocol providing:

- Fragmentation to fit transport MTU
- Reordering and reassembly
- Adaptive timeouts (SRTT + 4*RTTVAR)
- Congestion control (slow-start, AIMD)

Standalone Value

Application domain: Secure peer-to-peer connectivity with forward and backward secrecy.

Use cases:

- Secure device-to-device synchronization
- Private file transfer
- Peer-to-peer communication channels
- Development environment access

Independent utility: Keel provides UDP-based connections with double ratchet encryption and continuous key rotation. Skylight enables NAT traversal. Rendezvous supports peer coordination without central servers. These protocols operate independently of overlay networks or service provisioning in later phases.

Technical Milestone: Direct peer-to-peer authenticated communications functional.

Specification: 2. Secure Connectivity

Status: In progress — initial Keel implementation mostly complete, polishing and testing. Benchmarks and public requests for comments coming soon.

Phase 3: Application Integration (Q3 2026)

Deliverable: Virtual overlay networks + cryptographically gated service provisioning (TAP interface ready)

Surface

Virtual layer 2 networking protocol providing:

- TAP interface integration for standard networking stacks
- MAC address derivation via SHA-256 hash of StarfortDB public keys
- IP address self-assignment with collision resolution
- OAuth2 adapter translating Heavy proofs to JWT format

Dock

Service provisioning protocol providing:

- 32-byte Service ID and Session ID identifiers
- Heavy proof-based access gating
- Session tracking with encrypted state
- ~51 ms provisioning latency
- Support for Utility Credit-based access control

Standalone Value

Application domain: Virtual layer 2 networking with cryptographic access control.

Use cases:

- Private network overlays for organizations
- Secure remote access to internal resources
- Application-level networking without VPN infrastructure
- Legacy application integration via standard OAuth2 flows

Independent utility: Surface creates virtual Ethernet networks over Keel connections. Dock provides service provisioning with Heavy proof-based authentication. The OAuth2 adapter enables standard applications to authenticate using Heavy proofs without modification. These components function independently of service discovery or economic incentives in later phases.

Technical Milestone: Virtual Ethernet and gated service provisioning operational.

Specification: 3. Overlays and Services

Phase 4: Ecosystem Scaling (Q4 2026)

Deliverable: Decentralized service discovery, reputation, and incentivized node network with blind Lightning micro-payments

Sonar

Service discovery protocol providing:

- Service advertisement and query (ServiceOffer/ServiceQuery)
- VRF-randomized queries for privacy
- Quality-of-service metric aggregation
- Reputation scoring integration

Reactor Core

Utility Credit issuance and redemption system providing:

- Blind Schnorr signatures (Ristretto255/Curve25519)
- Chaumian mint architecture with 1,048,576 bucket hash ring
- ~51 ms redemption latency
- Double-spending prevention via Seen hash sets
- Lightning Network integration for UC purchase

Fleet

Federated service infrastructure providing:

- Third-party operated relay and service nodes
- Lightning-based settlement for UC redemption
- Quality-of-service reporting and verification
- Economic incentive alignment for network operators

Standalone Value

Application domain: Service discovery and economic infrastructure for network operations.

Use cases:

- Service discovery with quality-of-service metrics
- Monetized relay and service nodes
- Incentivized network infrastructure operation
- Privacy-preserving micropayments via Lightning Network

Independent utility: Sonar enables discovery of services with reputation scoring. Reactor Core provides blind Chaumian microcredits for privacy-preserving payments. Fleet creates economic incentives for operating network infrastructure. These components enable sustainable, professionalized network services while preserving user privacy through blind signatures.

Technical Milestone: Service discovery and economic infrastructure operational.

Specification: 4. Discovery and Incentives

Status: In progress — Reactor Core HP in-memory database ring prototype complete, benchmarks at ~3000 rps per node.

Phase 5: Secure Group Messaging (Q1 2027)

Deliverable: Secure, forward-secret group messaging with attested membership (up to thousands of participants)

Coms

Secure group messaging protocol providing:

- Ratchet-based encryption with forward secrecy
- Heavy-attested membership verification
- Symmetric chain ratchet for group key updates
- VRF-based cycle key agreement
- ~0.1-0.2 ms message encryption
- Support for 1,000-5,000 members per group

Standalone Value

Application domain: Secure group messaging with cryptographic membership verification.

Use cases:

- Private team communication channels
- Secure group coordination
- Encrypted messaging with forward secrecy

Independent utility: Coms provides group messaging with ratchet-based encryption and Heavy-attested membership. Messages are encrypted with forward secrecy, and group membership is verified cryptographically. Offline message delivery is supported via Rendezvous dead drops.

Technical Milestone: Decentralized group messaging operational.

Specification: 5. Secure Messaging Utilities

Status: Specification complete and ready to implement.

Phase 6: Privacy Hardening (Q2 2027)

Deliverable: Multi-hop onion routing + traffic obfuscation to defeat DPI and correlation attacks

Ramp

Onion routing protocol providing:

- Multi-hop routing with layered ChaCha20-Poly1305 encryption
- Randomized path selection
- Request tracks (sender-selected) and response tracks (random)
- 16-byte random Waypoint IDs per message
- ~15-30 ms latency for 3-hop routing

Submerge+

Enhanced message handling providing:

- Path multiplexing (scattering across ≥2 channels)
- Session multiplexing (mixing multiple sessions)
- SHA-256 PRNG for random assignment
- Traffic pattern obfuscation

Standalone Value

Application domain: Anonymized routing with economic incentives.

Use cases:

- Anonymous communication channels
- Traffic pattern obfuscation
- Censorship circumvention
- Privacy-enhanced network access

Independent utility: Ramp provides multi-hop onion routing with randomized path selection. Submerge+ adds path multiplexing (scattering) and session multiplexing (mixing) for traffic analysis resistance. Economic incentives via Fleet ensure availability and quality of waypoint operators.

Technical Milestone: Anonymized routing with economic incentives operational.

Specification: 6. Privacy Enhancements

Status: Specification complete and ready to implement.

Ongoing: Cross-Cutting Components

These components develop in parallel across all phases:

Runtime Operations

Components: Hull (process isolation), Agent (key operations), Daemon (network I/O), Helm (interfaces)
Specification: A. Runtime Operations
Status: Ongoing development, bootstrapped and working in Rebased.

Secure Recovery

Component: Airlock (air-gapped key management)
Specification: B. Secure Recovery and Custody
Status: Fully specified and will contribute as SeedSigner patch or fork.

Security Analysis

Documentation: Threat modeling and mitigation strategies
Specification: C. Security and Threat Model

Performance Metrics

Documentation: Latency, bandwidth, and scalability benchmarks
Specification: D. Performance Characteristics

Future Development

Documentation: Post-quantum migration, protocol extensions
Specification: E. Future Work and Appendices

Design Principles

Modular Independence

Each phase delivers independently functional protocols. Early phases operate without later phases. Organizations may deploy subsets based on requirements.

Backward Compatibility

Later phases extend earlier protocols without breaking existing deployments. Phase 3 applications function identically in Phase 6 environments.

Incremental Development

Phased delivery validates each component before proceeding. Each milestone demonstrates technical feasibility.

Composable Architecture

Complete SSCM emerges from protocol composition rather than monolithic design. Components interoperate via well-defined interfaces.

System Integration

Phase 1 Capabilities

- Hierarchical key management
- Privacy-preserving trust verification
- Credential storage and rotation

Phase 1+2 Capabilities

- Secure peer-to-peer connectivity
- NAT traversal
- Device synchronization

Phase 1+2+3 Capabilities

- Virtual layer 2 networking
- Service provisioning
- Legacy application integration

Phase 1-4 Capabilities

- Service discovery
- Economic incentive layer
- Monetized network operations

Phase 1-5 Capabilities

- Group messaging
- Attested membership

Phase 1-6 Capabilities (Complete SSCM)

- Anonymized routing
- Traffic analysis resistance
- Privacy-preserving payments

Reference Documentation

- **Overview**: Zsub SSCM Overview
- **Current Implementation**: rebased (https://codeberg.org/zsub/rebased)
- **Development Timeline**: 18 months to complete SSCM (Q2 2027)