Secure Legion – Complete Architecture v3 (with Ping-Pong Wake System)

Private by Design • Serverless • Blockchain Integrated • Cold Storage Identity

1) Overview

Secure Legion is a **fully decentralized messaging and identity system** that combines a blockchain-based directory, hardware-encrypted wallets, a serverless wake-and-alarm communication system, and the innovative **Ping-Pong Wake Handshake** to deliver encrypted messages only when both devices are online. This architecture guarantees zero metadata exposure and no dependency on centralized servers.

2) Ping-Pong Wake Handshake

The Ping-Pong Wake System is Secure Legion's signature innovation. It ensures reliable, private, and serverless message delivery. Unlike conventional systems that depend on permanent relays, this design coordinates delivery only when both peers are awake and authenticated.

Flow Diagram (Textual Representation):

+----------------+ +----------------+ | Sender Device | | Receiver Device | +----------------+ +----------------+ | (1) Encrypt message, store in local queue | |-->| | (Ping Token) | |<--| | (2) Receiver wakes, authenticates user | | (3) Sends Pong acknowledgment (auth-signed) | |-->| | (4) Sender releases queued message securely | | (5) Receiver decrypts and confirms delivery | |<--|

Key Security Benefits:

- Messages never leave sender's device until receiver confirms readiness.
- No permanent relay or third-party storage required.
- All Ping and Pong tokens are encrypted and nonce-protected to prevent replay attacks.
- Local queues are AES-GCM encrypted with keys derived from the user's wake key.
- AlarmManager periodically re-arms Ping cycles until Pong is received.

3) Message Download Flow (Wake → Fetch → Decrypt)

1. Wake Receipt: Device receives encrypted wake via socket, alarm, or UnifiedPush.
2. Authenticate User: App unlocks hardware key after biometric/PIN verification.
3. Secure Fetch: Connects through Tor/WebSocket, retrieves ciphertext only.
4. Decrypt: Hardware key unwraps DEK, decrypts in RAM, displays local notification.
5. Auto-Wipe: DEK erased; message removed after viewing or timeout.

4) Duress PIN & Distress Wipe

- Entering duress PIN wipes private keys, session data, and message caches.
- Broadcasts signed revocation across peers to purge queued messages.
- Easy-to-guess PINs (e.g., 123456) can be configured as automatic duress triggers.
- App resets to onboarding state post-wipe, offering recovery from seed phrase.

5) Blockchain Directory (Solana + IPFS)

Each user publishes an encrypted contact card pointer to the blockchain. The contact card is encrypted with a passcode-derived key and stored on IPFS. Handles are hashed client-side with Argon2id to prevent scraping or brute-forcing. Registration costs are negligible (~0.000006–0.00007 SOL per entry).

6) Cold Storage Wallet Integration

- Keys stored in StrongBox/Secure Enclave, used for identity and message signing.
- No hot storage; wallet operates in read-only mode unless unlocked.
- Supports multiple burner identities; rotation possible per chat session.

7) Cross-Chain Bridge

A lightweight bridge mirrors Solana directory entries to BNB/Ethereum. It uses cryptographic proofs to link ed25519 and secp256k1 identities, allowing users from other chains to locate and message each other.

8) Security Overview

Feature	Method	Purpose
Encryption	XChaCha20 + Ed25519 Signatures	Protects data at all layers
Wake Privacy	Opaque Ping/Pong tokens	Prevents metadata exposure
Offline Resilience	AlarmManager + Queue Reconnect	Guarantees message delivery
Identity Storage	Cold wallet hardware key	Unforgeable and offline
Cross-chain Proof	Dual-curve signature mapping	Verifiable multi-chain identity

9) Summary

Secure Legion v3 unites blockchain-based discovery, cold storage identities, a serverless wake/alarm engine, and the Ping-Pong Wake System for the world’s first decentralized, metadata-free messaging protocol. Every component — from Solana directory lookups to local wake pings — is encrypted, ephemeral, and verifiable.