Zero Lock Security Whitepaper v1.0

Website: https://zerolock.online
Protocol Version: 5.0
Date: January 2026
Identity: Zero Lock Intelligence Group

---

1. Executive Summary

Zero Lock is a high-security, zero-knowledge password manager designed for absolute data sovereignty. This document details the cryptographic primitives, threat models, and architectural controls that ensure user data remains unreadable to all parties except the vault owner. Our primary mission is the elimination of trust in central authorities through mathematical certainty.

---

2. Cryptographic Architecture

2.1 The Sealing Protocol (AES-256-GCM)

Zero Lock utilizes **AES-256 in Galois/Counter Mode (GCM)** for all data at rest and in transit.

- **Primitive:** NIST SP 800-38D standard.
- **Integrity:** GCM provides authenticated encryption, ensuring that any ciphertext mutation (bit-flipping) results in a decryption failure rather than corrupted plaintext.
- **Local Generation:** 256-bit encryption keys are generated strictly within the local secure context using high-entropy CSPRNG sources.

2.2 Key Hardening (PBKDF2-100K)

To prevent brute-force and rainbow-table attacks, Zero Lock applies massive computational hardening to the Master Password.

- **Algorithm:** PBKDF2-HMAC-SHA256.
- **Iterations:** 100,000 rounds.
- **Salting:** Every vault is assigned a unique, high-entropy salt based on the User ID (UID), ensuring that identical passwords yield unique derived keys.

- **Hardware Resistance:** The iteration count is tuned to be computationally expensive for ASICs and GPUs while maintaining sub-second performance on modern consumer hardware.

---

3. Data Flow & Persistence

3.1 Blind Relay Sync

Zero Lock operates as a **Zero-Insight Relay**.

1. **Localized Sealing:** Data is encrypted on the client device.
2. **Ciphertext Transmission:** Only the encrypted blob (ciphertext) is transmitted to the cloud.
3. **Blind Storage:** Our infrastructure (Google Firebase) stores these blobs indexed by a non-reversible cryptographic hash of the user identity.
4. **No Master Keys:** Zero Lock servers, Google employees, and third-party attackers physically cannot access the plaintext secrets.

3.2 Volatile Session Management

To mitigate persistent memory attacks:

- **Volatile Storage:** The derived Session Key is stored exclusively in RAM.
- **Self-Destruct:** The secure context is purged immediately upon browser tab closure, manual logout, or session timeout.
- **Zero Persistence:** No cryptographic keys are ever written to the local disk or persistent browser storage (IndexedDB/LocalStorage).

---

4. Threat Model & Mitigation

Threat Vector	Mitigation Strategy
Server-Side Breach	Servers only contain unreadable ciphertext and public salts. No plaintext or keys exist in the cloud.
Brute-Force Attack	PBKDF2-100K makes local cracking computationally prohibitive.

Bit-Flipping/Tampering	AES-256-GCM authentication tags detect any data modification.
Rainbow Table Attack	Unique per-vault salting ensures pre-computed hashes are useless.
Insider Threat	Zero-knowledge architecture removes the possibility of administrative access.

---

5. Compliance & Engineering Pillars

Zero Lock follows the **Radical Transparency** model. Our engineering is guided by the following:

- **Mathematical Sovereignty:** Security is derived from math, not corporate promises.
- **Open Disclosure:** All cryptographic primitives used are industry-standard and peer-reviewed.
- **Human-Centric Design:** Security defaults favor the user even in the event of total platform compromise.

---

6. Incident Response

While the architecture minimizes the impact of a breach, the **Zero Lock Intelligence Group** maintains a rigorous vulnerability disclosure program. Technical findings can be reported via our secure communication channels.

---

7. Conclusion

Zero Lock provides a provably secure environment for digital asset management. By moving the encryption boundary to the local hardware edge and utilizing verified cryptographic standards, we deliver absolute privacy by design.

Zero Lock Intelligence Group