ETERNAKEYS LEGAL

Zero-Knowledge Architecture & Risk Disclosure

Version 1.1 · Effective 2026-04-14

Open PDF Download PDF Preview in page

1. Purpose

This document describes the zero-knowledge architecture of EternaKeys and discloses the inherent risks of a system designed so that the service provider cannot access user content.

2. How Zero-Knowledge Works at EternaKeys

EternaKeys uses a zero-knowledge architecture: vault content is encrypted on your device before transmission. The server stores only ciphertext and operational metadata necessary for the service to function.

2.1 Encryption

Vault content is encrypted with **AES-256-GCM** using per-item random nonces.

Encryption keys are derived from your vault passphrase using **Argon2id** key derivation.

Your vault passphrase never leaves your device — not during setup, not during use, not ever.

2.2 What the Server Stores

Ciphertext: Encrypted vault item content that cannot be decrypted without your passphrase.

Operational metadata: Item types, sizes, timestamps, account information, heir designations, audit logs, and session data. This metadata is necessary for the service to function but does not include plaintext vault content.

KDF parameters: Salt and configuration needed to re-derive your encryption keys from your passphrase on your device.

3. Risk Disclosure

3.1 Credential Loss — Account Access

Standard user accounts authenticate exclusively via passkeys (hardware keys or platform authenticators). If all registered passkeys are lost and no backup passkey is available, account access cannot be restored. EternaKeys does not store passwords for standard user accounts and cannot reset passkey credentials on your behalf.

3.2 Credential Loss — Vault Data

Your vault passphrase is the sole key to your encrypted data. Because we never receive your vault passphrase, we have no mechanism to reset it, recover it, or decrypt your data on your behalf. If your vault passphrase is lost, encrypted vault data is permanently and irreversibly inaccessible. This is a fundamental property of the zero-knowledge architecture, not an operational limitation.

3.3 Device Compromise

If your device is compromised by malware, an attacker could potentially intercept your vault passphrase or decrypted content. EternaKeys mitigates this risk through WebAuthn/passkey support and two-factor authentication, but cannot fully protect against a compromised device.

3.4 Metadata Visibility

While vault content is encrypted, operational metadata (item types, sizes, timestamps, and account information) is visible to the service. This metadata is necessary for functionality but could reveal information about your usage patterns.

3.5 No Absolute Guarantee

No security system can guarantee absolute protection. EternaKeys is designed to minimize risk through client-side encryption, but device compromise, credential loss, or implementation limitations remain relevant factors.

4. Your Responsibilities

Store your vault passphrase securely (e.g., in a physical safe or with a trusted person).

Register at least two passkeys (e.g., a hardware key and a platform authenticator) to protect against loss of a single credential.

Keep your devices secure and up to date.

If you are sharing vault access with heirs, ensure they have independent access to the vault passphrase through a secure offline method.

5. Acknowledgment

By creating a vault, you acknowledge that you have read and understood these risks. You accept that credential loss may result in permanent, irreversible loss of access to your encrypted data.