Plannelink Technical Security Whitepaper

Zero-Knowledge Architecture & Cryptographic Integrity Standards

Version: 1.0
Date: January 1, 2026
Classification: Public / Technical Disclosure
Author: Chief Security Officer (CSO), Plannelink

Sommario

1. Executive Summary

Plannelink is a high-assurance digital legacy management platform engineered to resolve the fundamental paradox of digital inheritance: the need for absolute data privacy during a user's lifetime and the guaranteed, secure transmission of that data upon their passing.

The cornerstone of the Plannelink security model is a **Zero-Knowledge Architecture**. Unlike traditional cloud storage or financial institutions that rely on server-side encryption and institutional trust, Plannelink utilizes **Client-Side Encryption (CSE)** via the W3C Web Crypto API. This ensures that sensitive data—including financial inventories, legal instructions, and private credentials—is transformed into ciphertext within the isolated execution environment of the user's browser BEFORE it is transmitted over any network.

Because the decryption keys are derived solely from the user's Master Password, which is never shared with Plannelink, the platform operates as a "Blind Orchestrator." We maintain the "safe," but we do not possess, nor can we generate, the key. This whitepaper details the mathematical rigor, cryptographic primitives, and threat modeling that underpin this architecture.

2. Theoretical Framework: Security by Mathematics, Not Trust

In the contemporary cybersecurity landscape, the "Trust Me" model of SaaS is increasingly obsolete. Data breaches are persistent, and insider threats remain a critical vulnerability. Plannelink shifts the security paradigm from *administrative policy* to *mathematical enforcement*.

2.1 The Zero-Knowledge Principle

A Zero-Knowledge system is defined by its inability to learn anything about the secret data it processes. In the context of Plannelink, this means:

1. **Zero Visibility:** No employee, administrator, or sub-processor can view the plaintext data.
2. **Zero Retrieval:** Plannelink cannot "reset" a master password or "recover" data if a key is lost.
3. **Zero Knowledge of Content:** Metadata and storage structures are decoupled from the encrypted payloads.

2.2 Proof of Sovereignty

The user maintains absolute sovereignty over their data. The encryption process uses a Symmetric-Key Algorithm where the key is transient—it exists only in the browser's volatile memory during an active session and is never persisted to any disk, local or remote.

3. Cryptographic Implementation Details

Plannelink's cryptographic suite is composed of industry-standard, peer-reviewed primitives that are resistant to modern cryptanalysis, including GPU-accelerated brute-force and side-channel attacks.

3.1 Key Derivation Function: PBKDF2-HMAC-SHA256

The security of a Zero-Knowledge system is only as strong as its key derivation. To transform a human-readable Master Password into a high-entropy 256-bit AES key, we employ the **Password-Based Key Derivation Function 2 (PBKDF2)**.

- **Computational Hardening:** We implement **600,000 iterations**. This exceeds the current recommendations from NIST and OWASP (which often suggest 210,000 to 310,000 for SHA-256). The high iteration count forces an adversary to perform a massive amount of hashing for every password guess, making it economically and computationally prohibitive to execute successful brute-force attacks.
- **Unique Salting:** Every user is assigned a unique, 16-byte cryptographically secure random **Salt** generated via `window.crypto.getRandomValues()`. This salt is stored in the database alongside the encrypted data but remains useless without the password. Its presence ensures that identical passwords across different users result in completely different derived keys, effectively neutralizing **Rainbow Table** attacks.
- **HMAC-SHA256:** We use SHA-256 as the underlying pseudo-random function, ensuring a collision-resistant and high-performing derivation phase.

3.2 Authenticated Encryption: AES-256-GCM

For the encryption of data payloads, Plannelink utilizes the **Advanced Encryption Standard (AES)** in **Galois/Counter Mode (GCM)** with a **256-bit key**.

- **Confidentiality:** AES-256 is the gold standard for symmetric encryption, currently approved by the NSA for "Top Secret" level information.
- **Integrity and Authenticity:** Unlike older modes like CBC, **GCM** is an **Authenticated Encryption with Associated Data (AEAD)** mode. It provides a

"Tag" that accompanies the ciphertext. During decryption, the Web Crypto API verifies this tag. If the ciphertext has been modified by even a single bit (by a malicious actor or due to storage corruption), the authentication check will fail, and the data will not be decrypted. This prevents **Chosen Ciphertext Attacks (CCA)**.

- **Initialization Vector (IV):** Every encryption operation uses a unique 12-byte IV. This ensures that even if a user saves the same asset twice, the resulting ciphertexts will be completely different, preventing **pattern recognition/frequency analysis** in the encrypted database.

4. Comprehensive Threat Model

We evaluate our security posture against three primary adversarial categories: The External Attacker, The Malicious Service Provider, and The MitM Actor.

4.1 Threat Baseline A: Total Server Compromise

In this scenario, we assume an adversary has gained `root` access to our production database and cloud storage.

- **Adversary Assets:** Access to all stored Base64 encrypted strings, Salts, and IVs.
- **Security Outcome:** The data remains secure. Because the adversary lacks the Master Password, they would need to crack a 256-bit AES key. Even with the world's fastest supercomputers, the time required to brute-force a single key is estimated to be longer than the remaining age of the universe. The offline attack on the KDF is similarly mitigated by the 600k iterations and unique salts.

4.2 Threat Baseline B: The Malicious Insider

We consider a scenario where a Plannelink developer or administrator attempts to access user data.

- **Internal Controls:** Our backend logic is designed to be "Blind." The APIs only accept and return encrypted blobs. No plaintext data ever touches our server RAM.
- **Security Outcome:** Even if an administrator manipulated the database, they could only see when a user was active, but never *what* they stored. The Zero-Knowledge boundary is a physical separation of concerns enforced by the client-side execution.

4.3 Threat Baseline C: Man-in-the-Middle (MitM) & Interception

We evaluate the risk of data interception during the transition from the browser to the cloud.

- **Transport Security:** All traffic is strictly enforced over **TLS 1.3**. We implement **HSTS (HTTP Strict Transport Security)** to prevent protocol downgrade attacks.
- **Security Outcome:** Even if the TLS layer were theoretically compromised (e.g., via a fraudulent Root CA), the adversary would only intercept the encrypted ciphertext. Since the encryption happened *before* the TLS wrapping, the data remains protected.

5. System Architecture & Data Sovereignty

The Plannelink architecture follows a distributed security model where the client is the primary cryptographic authority.

5.1 The Encryption Lifecycle

1. **Capture:** The user enters asset details (e.g., "Seed phrase in the red book") into the browser.
2. **Derivation:** The browser executes 600,000 PBKDF2 rounds using the Master Password and a local salt.
3. **Encapsulation:** The plaintext is encrypted using AES-256-GCM.
4. **Serialization:** The ciphertext, salt, and IV are converted to Base64.
5. **Transmission:** The Base64 bundle is sent via an authenticated HTTPS POST request to the Supabase backend.
6. **Persistence:** The data is stored as an encrypted string in a PostgreSQL database hosted in the **European Union (EU)** to ensure **GDPR** compliance.

5.2 Data Sovereignty & GDPR Compliance

By design, Plannelink is natively compliant with the most stringent data protection regulations, including **GDPR**.

- **Privacy by Design:** Since we do not possess the keys to read user data, we cannot "process" it in the traditional sense. The user remains the sole data controller.
- **Right to be Forgotten:** Deleting an account removes the encrypted blobs and associated salts from our servers, effectively destroying the data permanently.
- **Sovereignty:** Our servers are located within the European Union, ensuring compliance with local data residency requirements.

6. Failure Recovery & The "No Backdoor" Policy

One of the most critical security features of Plannelink is the **absence of a password recovery mechanism**.

In a traditional system, "Forgot Password" works because the server has the power to reset your access. In a true Zero-Knowledge system, this power is a vulnerability. If we could reset your password, we could also be forced by a court or an attacker to reset it and access your data.

The Reality of Zero-Knowledge:

- If a user loses their Master Password, the data in the vault is **irretrievably lost**.
- There is no "Master Key," no "Backdoor," and no "Recovery Code" stored on our servers.
- This extreme measure is the only way to guarantee that no one—not even Plannelink—can ever be compelled to provide access to your private information.

7. Open Source Verification & Transparency

The "Don't Trust, Verify" mantra is only possible with transparency. Plannelink provides its core cryptographic implementation for public audit. This allows security professionals to verify that:

1. Encryption is indeed happening client-side.
2. No "phone home" of the Master Password exists in the code.
3. The algorithms (AES-GCM, PBKDF2) are implemented correctly without weaknesses.

Public Audit Gist:
Verify Implementation: Plannelink Public Security Logic

8. Conclusion

Plannelink represents the state-of-the-art in digital legacy protection. By combining the **Web Crypto API**, **AES-256-GCM**, and a high-iteration **PBKDF2 KDF**, we have created a platform where users can store their most sensitive information with absolute confidence. Our Zero-Knowledge architecture ensures that privacy is a technical guarantee, not just a promise.

Institutional Disclaimer

This document is intended for technical evaluation and auditing purposes. The security claims herein are based on the current implementation of the Plannelink v1.1.37 platform. Periodic security updates and third-party audits are part of our continuous improvement lifecycle.