SafePass Security Whitepaper

Technical Architecture & Data Sovereignty Protocol

1. Encryption Standards

SafePass implements AES-256 encryption in GCM (Galois/Counter Mode) [cite: SecurityHubView.swift]. This symmetric encryption standard is recognized globally by governmental and financial institutions for securing top-secret data. The GCM mode ensures both data confidentiality and integrity, preventing unauthorized tampering with stored vault items [cite: SecurityHubView.swift].

2. Zero-Knowledge Architecture

Our architecture follows a strict Zero-Knowledge principle. Encryption and decryption processes are performed exclusively on the user's local device [cite: AddItemView.swift]. Plaintext data never leaves the volatile memory (RAM) of the iPhone or iPad [cite: AddItemView.swift]. The developer does not operate centralized databases or master keys, ensuring that even in the event of a service compromise, no user data is accessible [cite: SafePassApp.swift, StoreManager.swift].

3. The Guardian 2-Key Protocol

To resolve the dilemma of digital legacy without compromising security, SafePass utilizes a mathematical secret-sharing protocol [cite: EmergencySetupView.swift]. The recovery backup is split into two distinct digital fragments. Neither Guardian A nor Guardian B can access the vault individually [cite: EmergencySetupView.swift, SettingsView.swift]. Only when both fragments are cryptographically combined can the vault be reconstructed, providing a fail-safe mechanism for emergency access [cite: EmergencySetupView.swift].

4. Private iCloud Infrastructure

All encrypted data is stored within the user's private iCloud container [cite: SafePassApp.swift]. This leverages Apple's multi-billion dollar security infrastructure, including end-to-end encryption and two-factor authentication (2FA). SafePass does not share data with third-party trackers or external cloud providers [cite: SafePassApp.swift].

5. Hardware-Level Security

Access to the SafePass application is gated via hardware-backed biometrics, specifically FaceID and TouchID [cite: ContentView.swift]. Cryptographic keys are securely managed within the Apple Keychain, protected by the device's Secure Enclave [cite: StoreManager.swift].