WHITE PAPER: The BioBridge Protocol (BBP)

Universal Hardware-Enforced Biometric Session Injection & JIT Identity Generation
Document Ref: BBP-WP-2026-01 | **Patent Pending:** SA #2026/03023

1. Executive Summary

The BioBridge Protocol (BBP) is a decentralized identity settlement layer designed to bridge the "Security Gap" between modern hardware-bound biometrics (WebAuthn L3) and legacy enterprise infrastructure (PHP/XHTML/Java). By utilizing **Just-In-Time (JIT) Identity Generation** and **Blind Switchboard Handshakes**, BBP eliminates the "Credential Honeypot" (centralised password databases) and replaces it with a hardware-verified session injection model.

2. The Problem: The "Legacy Wall"

Current Multi-Factor Authentication (MFA) solutions fail at the Fortune 2000 level because:

1. **High-Friction Deployment:** Traditional FIDO2/WebAuthn requires a total rewrite of legacy login controllers.
2. **Credential Dependency:** Even with MFA, the underlying "password" remains a static target in the vendor's database.
3. **Recovery Deadlocks:** Loss of a hardware key often results in permanent account lockout or insecure "social engineering" recovery paths.

3. The BioBridge Solution: Technical Architecture

3.1. Zero-Knowledge "Blind Switchboard"

Unlike traditional SSO (OIDC/SAML), BBP acts as a **Stateless Identity Router**.

- **Non-Custodial:** ArmerTech servers never receive, store, or process raw biometric templates or User PINs.
- **Cryptographic Isolation:** Biometric verification occurs exclusively within the device's **Trusted Execution Environment (TEE)** or **Secure Enclave**. ArmerTech only verifies the resulting RS256/ES256 digital signature.

3.2. JIT Identity & Auto-Provisioning

BBP leverages a "Registry-First" model. Upon a successful hardware handshake:

- The **Bridge Interface** (Client-side JS) captures a unique hardware rawId.
- The **Vendor API** (Server-side) checks for the user's existence.

- If absent, a skeleton record is generated **Just-In-Time**, mapping the hardware identity to a "Biometric User" flag in the legacy database, eliminating the need for pre-existing passwords.

3.3. Self-Healing Atomic Reset (SHAR)

To solve the "Lost Device" problem without compromising Zero-Knowledge integrity, BBP implements **SHAR**:

- **Client-Side Hashing:** During registration, a User PIN is combined with a salt (Email) and hashed locally using **SHA-256**.
- **Recovery Hash:** Only the hash is stored by ArmerTech.
- **Atomic Overwrite:** A user can "kill" an old hardware credential and bind a new one by proving possession of the PIN-hash, ensuring 100% availability without administrative intervention.

4. Security & Compliance Specifications

4.1. Authenticator Assurance Level 3 (AAL3)

BBP enforces **Resident Keys (Discoverable Credentials)**. The identity is physically bound to the user's silicon. This makes BBP inherently resistant to:

- **Phishing:** There is no "secret" for the user to type or an attacker to steal.
- **Man-in-the-Middle (MitM):** BBP utilizes **Session Pinning**, locking the biometric challenge to the specific Vendor Domain (armer_locked_site).

4.2. Cyber Insurance Arbitrage

By shifting the "Root of Trust" from a vulnerable software database to hardened hardware, BBP reduces the **Attack Surface Area** by >90%, directly justifying the **28% reduction in cyber insurance premiums** for Global Fortune 2000 entities.

5. Implementation: The "1-Line" Integration

BBP is designed for rapid deployment via a single-file drop-in and a Content-Security-Policy (CSP) whitelist.

- **The Bridge Interface:** Injects the biometric challenge into legacy HTML forms via an asynchronous JS layer.
- **The Verification Handshake:** A server-to-server cURL request validates the hardware "Proof" and triggers the session injection.

6. Conclusion

The BioBridge Protocol represents the final evolution of the identity layer. It removes the liability of stored secrets from the vendor and returns sovereignty to the user's hardware. For an acquirer, BBP is not just a tool; it is the **infrastructure for a passwordless world.**