SIGNAVA

SECURITY STANDARDS

Signava Advisory

Document: v4.5.1 · **Last updated:** September 19, 2026

Detailed overview of the methodologies, hardware procurement, and architectural principles defining the Signava Sealed Device. Engineered specifically for the elevated threat models of Family Offices, Legal Counsel, Politicians, Celebrities, Journalists, Tech Executives.

1. Zero-Knowledge Architecture

1.1 Local Device Configuration

All initial cryptographic seeding, key generation, and architectural hardening procedures are executed strictly locally on the physical device. We ensure that secret material is never transmitted across external networks during the provisioning phase.

1.2 Cloud Independence

The Sealed Device is engineered to operate with total cloud independence. Native vendor cloud synchronization (e.g., iCloud, Google Drive) is systemically severed at the routing level. Any encrypted backup architectures implemented at the Principal's behest utilize dedicated, zero-knowledge storage silos wholly independent of the base operating system vendor.

1.3 No Remote Access

Signava Advisory categorically refuses to install, support, or utilize remote desktop or remote support backdoors. Post-delivery, our engineers have zero technical capacity to remotely access the device filesystem, intercept application execution, or read display contents.

1.3.1 Emergency Remote Wipe

Where a device management profile is applied, an emergency remote wipe capability is present. This payload is mathematically restricted to a binary destructive command. As detailed in Terms of Engagement (ToS) §15.1, this capability is executed only upon direct, authenticated authorization by the Principal via secure channels in the event of suspected device compromise.

1.3.2 Legally Compelled Disable

In strict accordance with Terms of Engagement (ToS) §24.3, should Signava Advisory receive a valid, final, and unappealable court order compelling cooperation, we reserve the right to trigger a device disablement payload. This capability exists to satisfy legal obligations regarding the cessation of service provision to explicitly unlawful actors, while remaining structurally incapable of extracting data.

2. Encryption Standards

All data at rest is secured utilizing industry-standard full-disk encryption (FDE) tightly bound to the device's hardware secure enclave (e.g., Secure Enclave Processor, Titan

M). Data in transit relies exclusively on End-to-End Encryption (E2EE) utilizing robust, peer-reviewed cryptographic primitives (e.g., AES-256, ChaCha20, Curve25519) and perfect forward secrecy (PFS). Client-controlled keys ensure that neither Signava Advisory nor any intermediate transit provider can decrypt payloads. We explicitly prohibit the implementation of key escrow systems.

3. Architectural Blindness

Our assertion of zero telemetry is not theoretical; it is Deterministically Verified via Wireshark and tcpdump packet analysis during the engineering phase. We actively intercept and analyze the egress routing of the baseline operating system to guarantee that all vendor-specific analytics, telemetry "pings," and background diagnostic channels are completely blackholed prior to device handover.

4. Jurisdictional Sovereignty

While MB Signava leverages independent, privacy-respecting Swiss providers (Threema, Proton, Infoguard) for secure communication and security-auditing frameworks, our organizational backend, legal domicile, and data center infrastructure operate under Lithuanian (EU) jurisdiction. This decoupling ensures that no single geopolitical entity possesses holistic leverage over both the technological stack and the advisory legal entity. Reputation Management* protocols are provided as an additional architectural defense for elite deployments.

5. Human-Verified Integrity

5.1 Manual Engineering

Every device provisioned by Signava Advisory is subjected to a rigorous, manual engineering process. We do not rely on mass-deployment cloning tools which could propagate subtle vulnerabilities across a fleet.

5.2 Prohibition of AI

We maintain a strict prohibition against the integration of Generative AI, automated configuration scripts, or machine-learning-driven threat analytics in our provisioning pipeline. The introduction of non-deterministic, probabilistic AI models introduces unacceptable variances in the security posture.

5.3 Deterministic Verification

The integrity of the device relies on human engineers executing deterministic, step-by-step verification protocols, ensuring that the final output perfectly matches the audited baseline.

5.4 Strict Auditing

To maintain the "Sealed" designation, the device must undergo an annual integrity audit by Signava Advisory personnel. This audit verifies the persistent lockdown of the bootloader, the integrity of the management profile enforcements, and the absence of unverified binary execution.

6. Privacy Standards

6.1 GDPR Compliance

Our operational ethos is governed by the EU General Data Protection Regulation (GDPR), emphasizing extreme data minimization and explicit, informed consent.

6.2 GDPR Principles

We structurally enforce the principles of Privacy by Design and Privacy by Default. The device assumes an inherently hostile network environment out of the box, requiring explicit whitelist permissions for external connectivity.

6.3 Neutrality of Technology

Signava Advisory provides dual-use, privacy-enhancing technology. We enforce strict technological neutrality, ensuring that our architectural implementations are completely agnostic to the content of the Principal's data.

6.4 No Institutional Certification

We intentionally bypass traditional, bureaucratic institutional certifications which often mandate "lawful intercept" backdoors or telemetric compliance tracking as a prerequisite for certification. Our standard is absolute mathematical and physical verification, not bureaucratic rubber-stamping.

7. Technical Inquiries

Signava Advisory maintains a dedicated secure channel for highly technical inquiries, architectural audits, and threat-modeling consultations. We commit to a 48-hour response standard for all authenticated communications from active Principals.

Direct technical inquiries securely to:

`hnwi@signava.co`

*Reputation Management includes strategic consultation and protocol design. Execution of removal campaigns is facilitated via third-party partners at additional cost.

> **Third-Party Independence Disclaimer**
>
> Signava Advisory is an independent boutique consultancy. We are not owned, operated, or supported by Cryptnox, Infoguard, Proton Mail, Proton VPN, Threema GmbH, or any other third-party provider. The use of these tools does not imply endorsement, affiliation, or shared liability. All services are provided exclusively by Signava Advisory.