BONAFIDE™ SPECIFICATION V1.0 — PART 11

Privacy Classifications

Institutional deployment grading, user-facing transparency, audit methodology, upgrade paths, and privacy score integration

1. Purpose

Privacy is not binary. An institution deploying Bonafide can provide dramatically different levels of actual data protection depending on their hardware, integration depth, and operational practices. Users deserve to know what level of protection they are getting before they authorize an institutional peer to access their vault.

This part defines the Bonafide Privacy Classification system: a transparent, auditable, comparable grading of how well each institutional deployment protects user data. Classifications are displayed to users during peer authorization, feed into privacy scoring, and map directly to certification tiers.

The governing principle is sunlight. Every classification explicitly states what it guarantees and what it does not. No classification claims absolute security. Each represents a defined set of protections with known boundaries.

2. Classification Definitions

2.1 Classification S — Sovereign

The highest privacy classification. All data operations execute inside a hardware-isolated enclave (FPGA fabric, dedicated secure processor, or equivalent) where keys and plaintext never exist outside the isolation boundary.

- **Key management:** All DEKs are derived, used, and destroyed within enclave fabric. The institution's host operating system, administrators, and privileged users cannot extract key material at any point in the lifecycle.
- **Data exposure:** All data returned to the institution's application layer is ghosted—zero-knowledge proofs, redacted summaries, hashed confirmations, or enclave-rendered displays. The institution's software stack never processes plaintext.
- **Revocation:** Absolute. When a user revokes access, the enclave purges all key material and cached plaintext. No residual data exists outside the enclave to survive revocation.
- **Hardware requirement:** Dedicated cryptographic enclave with hardware isolation (ExaForge FPGA, or equivalent with side-channel hardening and hardware PUF key storage).
- **What S does NOT guarantee:** Protection against physical attacks on the enclave hardware itself (decapping, probe station). Protection against a court order served on the institution's key path.

2.2 Classification A — Attested

Strong privacy with hardware-attested isolation. Data operations execute inside a Trusted Execution Environment (TEE) where the host system cannot access enclave memory during operation.

- **Key management:** DEKs are derived and used within a TEE (Intel SGX/TDX, AMD SEV-SNP, ARM TrustZone, AWS Nitro Enclave, NVIDIA Confidential Computing, or SmartNIC/DPU isolated cores). Keys exist in TEE memory but share silicon with the main processor.
- **Data exposure:** Ghost quanta used for most operations. Plaintext may exist within TEE memory for processing but is not accessible to the host OS. Some operations may return plaintext to the application layer when required for the institution's core function.
- **Revocation:** Effective. DEKs are purged from TEE on revocation. Re-encryption of stored quanta is triggered. Cached plaintext within the TEE is destroyed.
- **Hardware requirement:** CPU or accelerator with hardware-attested TEE capabilities. Attestation chain verifiable by the Bonafide network.
- **What A does NOT guarantee:** Protection against physical attacks on the CPU die. Protection against TEE implementation vulnerabilities (e.g., historical SGX side-channel attacks). Guarantee that no plaintext ever existed outside the TEE if the institution's application layer received plaintext responses.

2.3 Classification B — Bounded

Good privacy through API abstraction. Data operations go through the Bonafide runtime but without hardware enclave isolation. The institution integrates through the SDK and never handles DEKs directly, but key material exists in application memory during operations.

- **Key management:** DEKs are derived and managed by the Bonafide runtime in process memory. The institution's application code calls the runtime API and never touches keys directly. Keys are protected by software isolation (separate process, encrypted memory pages) but not hardware isolation.
- **Data exposure:** The institution receives plaintext through the Bonafide API for operational purposes. The Bonafide database packages encrypt data at rest transparently. The institution's application layer processes plaintext during active use.
- **Revocation:** Operational. The Bonafide runtime stops serving data and triggers re-encryption of stored quanta. Plaintext that existed in application memory or transient caches during prior operations is outside Bonafide's control.
- **Hardware requirement:** None beyond standard server hardware. Optional HSM or TPM for institutional master key storage (recommended).
- **What B does NOT guarantee:** Protection against a privileged attacker with access to the host system's memory during active operations. Guarantee that plaintext was never cached, logged, or persisted by the institution's application stack.

2.4 Classification C — Compliant

Minimum viable Bonafide deployment. The institution uses Bonafide for encrypted storage and access control. Data at rest is encrypted. Access is audited. Revocation removes data from the Bonafide layer. But the institution's application stack handles plaintext conventionally during active use.

- **Key management:** Institutional master key stored in the Bonafide runtime or HSM. DEKs derived on demand. The institution may cache decrypted data in their own systems for processing.
- **Data exposure:** Plaintext flows through the institution's conventional application stack. The Bonafide layer provides encryption at rest and access control at the API boundary.
- **Revocation:** Partial. Bonafide-managed storage is re-encrypted and access is cut. Copies of plaintext that the institution persisted in their own systems are outside Bonafide's control. Canary detection and watermarking provide forensic traceability for unauthorized copies.
- **Hardware requirement:** None.
- **What C does NOT guarantee:** That the institution has not duplicated plaintext data outside the Bonafide layer. That revocation removes all copies. That the institution's internal systems meet any particular security standard.

2.5 Classification U — Unclassified

The institution has deployed Bonafide infrastructure but has not been audited or has failed to meet the requirements for Classification C. The system is technically operational but no privacy guarantees are asserted. Users are warned during peer authorization that this institution has not been classified.

3. Classification Comparison

Property	S — Sovereign	A — Attested	B — Bounded	C — Compliant
Key isolation	Hardware fabric	Hardware TEE	Software process	Runtime only
Plaintext exposure	Never leaves enclave	Within TEE only	In API responses	In application stack
Ghost quanta usage	All operations	Most operations	Where feasible	Optional
Revocation strength	Absolute	Effective	Operational	Partial
Duplication risk	None	Minimal	Moderate (API only)	Significant
Hardware required	FPGA / dedicated SE	TEE-capable CPU or DPU	Optional HSM/TPM	None
Forensic controls	Watermark + canary + ledger	Watermark + canary + ledger	Watermark + canary + ledger	Canary + ledger
Certification tier	Hardware Certified (FPGA)	Hardware Certified (TEE)	Core Compliant+	Core Compliant

4. User-Facing Classification Display

4.1 Authorization Moment

When an institution requests to peer with a user's vault, the authorization prompt displays the institution's privacy classification alongside their privacy score. The user sees:

- Institution name and verified identity
- Privacy classification (S, A, B, C, or U) with a plain-language summary of what it means
- Privacy score (numerical, derived from behavioral history)
- Requested branch scope and security level ceiling
- Comparison to the user's other institutional peers (e.g., "Higher than 3 of your 5 current peers")

The classification is a fact about the institution's deployment, not a recommendation. The user decides whether to authorize based on the classification, the institution's reputation, and the sensitivity of the data involved.

4.2 Ongoing Visibility

The classification is visible at all times in the user's vault management interface. If an institution's classification changes (upgrade or downgrade after re-audit), the user is notified. A downgrade triggers an explicit notification with the option to revoke the peer relationship.

4.3 Classification Restrictions

Users can set minimum classification requirements for their vault:

- Allow all classifications (default for maximum compatibility)
- Require Classification B or above (exclude C and U deployments)
- Require Classification A or above (require hardware TEE)
- Require Classification S only (require hardware enclave isolation)

Minimum classification requirements are enforced during peer authorization. An institution below the user's minimum cannot complete peering regardless of the user's willingness. This allows privacy-conscious users to set a floor while maintaining compatibility for users who prioritize convenience.

5. Classification Audit

5.1 Audit Methodology

Privacy classification is not self-reported. It is determined through a combination of automated verification and periodic audit:

- **Hardware attestation (automated):** The Bonafide runtime on the institution's infrastructure reports its execution environment through remote attestation. FPGA fabric attestation for Classification S. TEE attestation (SGX, TDX, SEV-SNP, Nitro) for Classification A. Software environment report for Classification B. This is verified continuously, not just at audit time.
- **Integration audit (periodic):** Certified auditors verify that the institution's application code integrates through the Bonafide API correctly, does not bypass the runtime for direct data access, and does not persist plaintext outside the Bonafide-managed layer (for Classifications B and above).
- **Operational audit (periodic):** Review of access patterns, override frequency, revocation compliance, and incident response history. This feeds the behavioral component of the privacy score.

5.2 Audit Frequency

Classification	Hardware Attestation	Integration Audit	Operational Audit
S — Sovereign	Continuous (every session)	Annual	Annual
A — Attested	Continuous (every session)	Annual	Annual
B — Bounded	N/A (no hardware attestation)	Semi-annual	Annual
C — Compliant	N/A	Annual	Annual
U — Unclassified	N/A	Not audited	Not audited

5.3 Classification Downgrade

An institution's classification is downgraded immediately if hardware attestation fails (A or S drops to B), the integration audit reveals API bypass or unauthorized plaintext persistence (any classification drops one tier), or the operational audit reveals systematic non-compliance (any classification drops one tier).

Downgrade notifications propagate to all users peered with the institution. Users have a configurable grace period (default: 30 days) to decide whether to maintain or revoke the peer relationship at the new classification level.

6. Institutional Upgrade Path

Classifications are designed to support incremental adoption. An institution enters at any classification and upgrades over time as they invest in infrastructure and process maturity.

6.1 Typical Progression

Entry at C: The institution deploys Bonafide database packages and integrates through the SDK. Data at rest is encrypted, access is audited. This is the minimum deployment that provides compliance benefits over unencrypted storage. Most institutions start here.

Upgrade to B: The institution refactors application code to use the Bonafide runtime API exclusively, eliminating direct database access to encrypted columns. Adds HSM or TPM for institutional master key storage. Passes integration audit confirming no API bypass.

Upgrade to A: The institution deploys hardware with TEE capabilities (SmartNIC/DPU, cloud TEE instances, or TEE-capable servers). The Bonafide runtime executes inside the TEE. Hardware attestation is enabled and verified by the network.

Upgrade to S: The institution deploys dedicated cryptographic enclave hardware (ExaForge FPGA or equivalent). All data operations execute within enclave fabric. Ghost quanta become the default for all API responses. Plaintext never leaves the enclave.

6.2 Incentive Structure

Higher classifications provide tangible benefits beyond user trust:

- **Privacy score boost:** Classification level is a direct input to the institution's privacy score. Higher classification means higher baseline score.
- **Regulatory advantage:** Classification S and A may satisfy data protection requirements that Classification B and C cannot (e.g., certain GDPR Article 32 interpretations, healthcare data handling under HIPAA).
- **Insurance reduction:** Cyber insurance underwriters can assess risk more precisely when data handling is classified and audited. Hardware-isolated deployments carry demonstrably lower breach risk.
- **Competitive differentiation:** Users comparing institutions during peer authorization see classifications side by side. An A-classified bank competing against a C-classified bank has a visible trust advantage.
- **Reduced liability:** At Classification S, the institution never possesses plaintext. In the event of a breach, there is nothing to leak. The institution's legal exposure is fundamentally reduced.

7. Classification and Security Levels

Privacy classification interacts with the security level system. Higher-security data may require higher-classification deployments:

7.1 Configurable Security-Classification Floor

The specification allows security level policies to include a minimum classification requirement. For example, a vault configuration might specify:

- Levels 0–3 (public/basic): accessible from any classification
- Levels 4–6 (personal/sensitive): require Classification B or above
- Levels 7–8 (protected): require Classification A or above
- Levels 9–10 (restricted/sovereign): require Classification S

These floors are configurable per vault, per institution, or per regulatory profile. They are not hardcoded in the specification. The reference profile suggests the mapping above as a sensible default.

7.2 Institutional Ceiling Interaction

An institution’s security level ceiling (assigned during peering) cannot exceed what their classification supports. A Classification B institution cannot be granted a Level 9 ceiling even if the user explicitly authorizes it—the Bonafide runtime enforces the classification constraint. This prevents users from inadvertently exposing high-security data to insufficiently protected deployments.

8. Privacy Score Integration

The privacy classification is the structural component of an institution's privacy score. The behavioral component comes from operational history (Part 4). The combined score is what users see.

8.1 Score Composition

- **Structural baseline (classification):** Classification S starts at 90/100. Classification A at 75. Classification B at 55. Classification C at 35. Classification U at 0. This baseline reflects the technical protection level irrespective of institutional behavior.
- **Behavioral adjustment:** Operational history adjusts the score up or down from the baseline. Low override frequency, prompt revocation compliance, clean audit history, and low breach count push the score toward 100. Frequent overrides, slow revocation, audit findings, and breach events push it toward 0.
- **Combined score:** The user sees a single number (0–100) plus the letter classification. A Classification A institution with perfect behavior might score 95. A Classification A institution with poor operational history might score 60.

8.2 Score Visibility

Privacy scores are visible to users during peer authorization, in vault management, and through the public ecosystem directory. Institutions can display their score and classification as a trust signal in their own marketing and customer communications. The score is verifiable by any Bonafide participant—it is computed from ledger data and attestation records, not self-reported.

Bonafide™ — Privacy by architecture, not by promise.

An open specification by Sly Technologies Inc. | bonafide.id | bonafideid.org

V1.0 — February 2026