BONAFIDE™ SPECIFICATION V1.0 — PART 8

Open Ecosystem & Governance

Ecosystem philosophy, federated relay architecture, third-party developer platform, certification program, governance evolution, and adoption strategy

1. Purpose

This part defines the Bonafide ecosystem: how the specification evolves from a single-vendor project to an open foundation, how institutions and developers participate, how the certification program ensures quality and interoperability, and how the federated relay provides proxy identity infrastructure.

2. Ecosystem Philosophy

2.1 Open by Design

The Bonafide specification is free and open. Anyone can implement it. Anyone can build on it. The protocol's value comes from network effects and interoperability, not from licensing or lock-in. The specification is designed to create an ecosystem, not a product.

2.2 ExaScale Relationship

Sly Technologies develops the Bonafide specification and the first production implementation through ExaScale. This gives Sly Technologies first-mover advantage but not permanent control. The specification is separate from any implementation. As the ecosystem matures, governance transitions to an independent foundation (Section 6).

2.3 Competing Implementations

The specification explicitly encourages competing implementations. A Bonafide-compliant vault provider from another vendor should interoperate with a Bonafide-compliant institution from Sly Technologies and vice versa. Certification (Section 5) verifies interoperability. Competition improves the ecosystem; lock-in destroys it.

3. Federated Relay Architecture

3.1 What Relays Do

Relays provide proxy identity services: email forwarding, phone forwarding, and physical mail forwarding. They enable users to interact with institutions and individuals without exposing their real contact information (Part 4, Section 2). Multiple relay operators can coexist, providing redundancy and choice.

3.2 Relay Federation

Relay operators are independent entities certified through the Bonafide Certified program. They operate their own infrastructure, maintain their own proxy address pools, and handle their own jurisdictional compliance. Users choose which relay operator to use, and can use different operators for different proxies.

3.3 Relay Operator Requirements

Requirement	Description
Certification	Must pass Bonafide Relay Certified audit (infrastructure, operational, privacy)
Privacy classification	Relay operators carry their own classification (Part 11), visible to users
No content inspection	Relays route messages; they do not read, scan, filter, or modify content
Jurisdictional compliance	Relay operator complies with laws of its operating jurisdiction
Availability SLA	Minimum 99.5% uptime for message routing
Retention policy	Messages forwarded within configurable window (default: 72 hours), then deleted
Transparency	Relay operator publishes privacy policy, audit results, and classification

3.4 Relay Revenue

Relay operators earn revenue through subscription fees from users (premium relay features: custom domains, priority routing, extended retention) and from the Bonafide network (per-message routing fees paid from the network's fee pool). Basic relay service is included in the Bonafide Personal free tier to ensure universal access to proxy identity.

4. Third-Party Ecosystem

4.1 Developer Platform

The Bonafide SDK and database packages are the developer platform. Third-party developers build applications, services, and integrations using these tools:

- **Vault-aware applications:** Apps that integrate with the user's vault to store and retrieve data. A health tracking app stores vitals as quanta in the user's health branch. A financial planning app reads (with permission) across the user's banking branches.
- **Institutional integrations:** Middleware that connects existing institutional systems to the Bonafide runtime. An EHR vendor integrates Bonafide into their hospital software. A banking platform adds Bonafide vault support.
- **Verification services:** Specialized services that perform institutional verifications (Part 12, Section 6) for specific industries: KYC providers, credit verification services, background check services.
- **Privacy tools:** Tools that help users understand and manage their vault: privacy dashboards, breach notification services, canary monitoring, exposure analytics.

4.2 App Certification

Third-party applications can be certified through the Bonafide App Certified program. Certification verifies that the app correctly uses the SDK, does not bypass the runtime, does not cache plaintext outside authorized scopes, and does not leak data through side channels. Certified apps display the Bonafide Certified mark and receive preferential listing in the ecosystem directory.

4.3 Hardware Ecosystem

Hardware vendors can certify devices and accelerators for Bonafide compatibility:

- Consumer devices: phone and laptop vendors certify their secure element implementations for specific enclave tiers (Part 10).
- Server hardware: FPGA, DPU, HSM, and TEE vendors certify for specific privacy classifications (Part 11).
- IoT devices: peripheral device vendors certify for specific peripheral tiers (Part 10).
- Biometric hardware: external biometric device vendors certify for Bonafide's multi-modal fusion requirements.

5. Certification Program

5.1 Certification Tiers

Tier	Target	Requirements	Benefits
Core Compliant	Institutions (Classification C/B)	Bonafide runtime deployed, SDK integration audit passed, basic operational audit	Ecosystem directory listing, privacy score eligibility
Hardware Certified (TEE)	Institutions (Classification A)	Core Compliant + TEE attestation verified, hardware audit passed	Classification A eligibility, preferential user trust
Hardware Certified (FPGA)	Institutions (Classification S)	Hardware Certified + FPGA/dedicated SE audit, side-channel assessment	Classification S eligibility, highest user trust
Validator Certified	Validator operators	Infrastructure audit, operational demonstration, uptime commitment	Network participation, fee eligibility
Relay Certified	Relay operators	Infrastructure audit, privacy audit, content neutrality verification	Relay federation participation, fee eligibility
App Certified	Third-party applications	SDK usage audit, no plaintext leakage, no side channels	Certified mark, ecosystem directory
Device Certified	Hardware vendors	Enclave tier verification, biometric capability audit	Certified mark, device compatibility listing

5.2 Certification Process

- Application: the candidate submits an application with infrastructure documentation and self-assessment.
- Technical audit: a certified auditor reviews the deployment, runs certification test suites (bonafide-cert), and verifies compliance.
- Operational audit: the auditor reviews operational practices, incident response procedures, and privacy controls.
- Certification decision: the auditor issues a certification or lists deficiencies for remediation.
- Annual re-certification: all certifications require annual renewal with re-audit.

5.3 Certified Auditors

Auditors are independent entities certified by Sly Technologies (Phase 1) or the Foundation (Phase 2) to perform certification audits. Auditor certification requires demonstrated expertise in cryptographic systems, data privacy regulation, and hardware security assessment. The auditor ecosystem grows with the Bonafide ecosystem—more deployments require more auditors.

6. Governance Evolution

6.1 Three-Phase Model

Phase 1 — Stewardship (current): Sly Technologies develops the specification, operates Bonafide Cloud, and manages the certification program. Decisions are made by Sly Technologies with community input. This phase prioritizes speed of development and coherence of vision.

Phase 2 — Foundation: Governance transitions to an independent Bonafide Foundation (bonafideid.org). The Foundation is a non-profit entity with a governing board composed of institutional members, technical contributors, user advocates, and Sly Technologies (as founding member with transitional veto). The Foundation owns the specification, operates the certification program, and manages bonafideid.org. Sly Technologies continues to develop ExaScale and Bonafide Cloud as commercial products within the ecosystem.

Phase 3 — Community: Sly Technologies' transitional veto expires. The Foundation operates as a fully community-governed entity. Specification changes require community consensus through a defined RFC (Request for Comments) process. The ecosystem is self-sustaining through certification fees, membership dues, and network operation fees.

6.2 Transition Criteria

Transition	Criteria
Phase 1 → Phase 2	At least 3 independent institutional deployments, at least 5 certified validators, at least 2 certified relay operators, specification stable for 6+ months
Phase 2 → Phase 3	At least 20 institutional deployments, at least 20 certified validators, at least 3 independent specification contributors, Foundation financially self-sustaining for 12+ months

6.3 Specification Change Process

- Phase 1: Sly Technologies publishes specification updates with community comment period (minimum 30 days).
- Phase 2: Changes submitted as RFCs. Technical committee reviews. Board approves. Sly Technologies retains veto on changes that compromise security architecture.
- Phase 3: Full RFC process with community vote. No single entity has veto power. Security-critical changes require supermajority (two-thirds).

7. Adoption Strategy

7.1 Institutional Onramp

Institutions adopt Bonafide incrementally:

- **Phase A — Database encryption:** Deploy bonafide-db packages on existing databases. Encrypt sensitive columns. No application changes. Immediate compliance benefit (data at rest encryption with audit trail). Classification C.
- **Phase B — Runtime integration:** Refactor application code to use Bonafide runtime API. Eliminate direct database access to encrypted columns. Add HSM for key storage. Classification B.
- **Phase C — Vault peering:** Enable user vault peering. Users can authorize the institution and manage their data. Ghost quanta for verification workflows. Full Bonafide participation.
- **Phase D — Hardware upgrade:** Deploy TEE or FPGA hardware for Classification A or S. Maximum privacy protection.

7.2 User Onramp

Users discover Bonafide through:

- **Share links:** A friend shares a photo album via share link. The recipient views the data through the Bonafide viewer and is offered the option to create their own vault.
- **Institutional adoption:** The user's bank or employer adopts Bonafide. The user creates a vault to peer with the institution.
- **Guest enclave:** The user downloads the Bonafide app and creates a vault directly. The guest enclave flow (Part 3, Section 4.4) bootstraps a new vault with the user's first device.
- **Privacy motivation:** Users concerned about data breaches, identity theft, or surveillance seek out Bonafide proactively.

7.3 Network Effect

Each institutional adoption makes Bonafide more valuable for users (more of their data is protected). Each user adoption makes Bonafide more valuable for institutions (more customers expect vault support). Share links create organic user growth. Privacy scoring creates competitive pressure for institutional adoption. The network effect compounds.

Bonafide™ — Privacy by architecture, not by promise.

An open specification by Sly Technologies Inc. | bonafide.id | bonafideid.org
V1.0 — February 2026