BONAFIDE™ SPECIFICATION V1.0 — PART 6

Infrastructure & Portfolio

Database packages, cloud coordination, ExaScale integration, namespace infrastructure, product portfolio, and revenue model

1. Purpose

This part defines the infrastructure components that enable Bonafide deployment: the database packages that provide transparent encryption within existing database systems, the cloud coordination layer, the ExaScale integration that serves as the first implementation, the namespace infrastructure at bonafide.id, and the product portfolio that maps specification components to deployable software.

2. Database Packages

2.1 Transparent Encryption Layer

Bonafide database packages provide per-quantum encryption within existing database systems. The institution's application code issues standard SQL queries. The Bonafide layer intercepts reads and writes, encrypts and decrypts through the runtime (Part 12), and manages key material and audit logging transparently. From the application's perspective, the database contains normal data. From the storage engine's perspective, it contains encrypted blobs.

2.2 Supported Databases

Database	Package Name	Integration Method	Notes
PostgreSQL	bonafide-db-postgres	Extension (pg_bonafide) + trigger-based encryption	Most mature reference implementation. Supports row-level and column-level encryption granularity.
Oracle	bonafide-db-oracle	PL/SQL packages + Virtual Private Database integration	Leverages Oracle's VPD for row-level access control alongside Bonafide encryption.
SQL Server	bonafide-db-sqlserver	CLR integration + Always Encrypted extension	Extends SQL Server's Always Encrypted with Bonafide key management and audit.
MySQL	bonafide-db-mysql	Plugin API + proxy layer	Plugin intercepts queries at the MySQL protocol level.
MongoDB	bonafide-db-mongodb	Client-Side Field Level Encryption integration	Extends MongoDB's CSFLE with Bonafide key hierarchy and multi-path wrapping.

2.3 Encryption Granularity

Database packages support three granularity levels:

- **Column-level:** Individual columns are encrypted. The application queries normally; the Bonafide layer encrypts/decrypts specified columns transparently. Indexes on encrypted columns use deterministic encryption for equality queries or are replaced with encrypted indexes.
- **Row-level:** Entire rows are encrypted as single quanta. The primary key and access-control columns remain in plaintext for routing; the payload columns are encrypted as a unit.
- **Document-level (MongoDB):** Individual fields within a document are encrypted independently. Each field can have a different security level and access policy.

2.4 Query Capabilities on Encrypted Data

Encrypted data presents query challenges. The database packages support:

- Equality queries on deterministically encrypted columns (same plaintext always produces same ciphertext). Note: deterministic encryption leaks frequency distribution and is appropriate only for low-sensitivity columns.
- Range queries through order-preserving encryption (OPE) for non-sensitive ordering. OPE leaks ordering information and is appropriate only for columns where the order is not itself sensitive.
- Full-text search through encrypted search indexes (using searchable symmetric encryption). The index reveals access patterns but not plaintext.
- For high-sensitivity columns, queries are performed in the runtime (decryption in memory, filter in memory, return results). This is slower but reveals nothing to the database engine.

3. Cloud Coordination

3.1 Bonafide Cloud

Bonafide Cloud is a managed service that provides the coordination layer for the Bonafide network. It handles validator orchestration, federation routing, relay management, certificate authority operations, and trust score computation. Bonafide Cloud is operated by Sly Technologies in Phase 1 and transitions to Foundation operation in Phase 2.

3.2 Cloud Components

Component	Function	Availability
api.bonafide.id	API gateway for all network operations. Tiered authentication, rate limiting, request routing.	Multi-region, anycast
val.bonafide.id	Validator coordination. Committee selection, consensus orchestration, trust score computation.	Multi-region, redundant
fed.bonafide.id	Federation layer. Cross-region sync, institutional peering coordination.	Multi-region
relay.bonafide.id	Relay coordination. Proxy address management, relay operator routing.	Multi-region
ca.bonafide.id	Certificate authority. Device certificates, institutional certificates, validator certificates.	High-security, HSM-backed
ledger.bonafide.id	Ledger service. Merkle root publication, ledger verification endpoints.	Multi-region, append-only

3.3 Cloud Independence

Bonafide Cloud is a convenience, not a dependency. The specification defines all protocols such that a fully self-hosted deployment is possible without using any Bonafide Cloud services. An institution can operate its own API gateway, run its own validator nodes, manage its own certificates, and maintain its own ledger. Bonafide Cloud provides the managed infrastructure for organizations that prefer not to operate their own.

4. ExaScale Integration

4.1 ExaScale as First Adopter

Sly Technologies' ExaScale™ platform is the first production deployment of the Bonafide specification. ExaScale provides high-performance data infrastructure for telecommunications, banking, and defense customers. Bonafide is integrated into ExaScale as the data sovereignty layer.

4.2 Sovereignty Sidecar

The ExaScale Sovereignty Sidecar is the migration path for existing ExaScale deployments. The sidecar sits alongside existing ExaScale data pipelines and transparently encrypts data into Bonafide vault format. Existing applications continue to operate normally; the sidecar intercepts data flows and applies per-quantum encryption, key management, and audit logging.

The sidecar approach enables adoption without application rewrite: the institution's existing ExaScale deployment gains Bonafide protection incrementally, one data stream at a time.

4.3 ExaForge Hardware Acceleration

ExaScale's ExaForge FPGA provides the Classification S enclave for Bonafide operations:

- PUF-based key storage: institutional master keys stored in FPGA physically unclonable function, non-extractable.
- In-fabric AES-256-GCM: quantum encryption and decryption at line rate within FPGA fabric.
- In-fabric HKDF: key derivation without keys leaving the fabric.
- In-fabric ZK proof generation: proof generation within hardware isolation.
- In-fabric TLS termination: unauthorized connections rejected at wire speed, CPU never sees rejected handshakes.
- Side-channel hardened: constant-time operations, power analysis resistance, fault injection detection.

4.4 ExaScale and Bonafide Independence

ExaScale is a Bonafide deployment, not Bonafide itself. The specification is independent of ExaScale. Any hardware vendor can implement Classification S with equivalent FPGA or secure processor capabilities. ExaScale's advantage is that it exists today and is deployed in production; the specification ensures competitors can emerge.

5. Namespace Infrastructure

5.1 Domain Architecture

Domain	Purpose	Phase
bonafide.id	Network infrastructure, API, services, user-facing namespace	Phase 1 (active)
bonafideid.org	Specification, governance, certification, community, documentation	Phase 2 (Foundation)

5.2 Service Namespace Zones

The bonafide.id domain is organized into service zones:

Zone	Purpose	Examples
api.bonafide.id	Core API endpoints	Authentication, vault operations, key generation
val.bonafide.id	Validator network	Consensus, trust scoring, proof verification
fed.bonafide.id	Federation layer	Cross-region sync, peering coordination
relay.bonafide.id	Relay services	Email proxy, phone proxy, address proxy
ca.bonafide.id	Certificate authority	Device certs, institutional certs, validator certs
ledger.bonafide.id	Ledger service	Merkle root publication, verification
docs.bonafide.id	Documentation	Specification, API reference, implementation guides
*.vault.bonafide.id	User vault subdomains (optional)	Personal vault namespace for direct addressing

5.3 Institutional Subdomains

Institutions deploying Bonafide can optionally register institutional subdomains under bonafide.id (e.g., chase.bonafide.id) for service discovery and trust signaling. Institutional subdomain registration requires certification (Part 8) and verification of the institution's legal identity. Subdomain registration is a revenue source for ecosystem sustainability.

6. Product Portfolio

The Bonafide ecosystem produces the following product categories. Some are developed by Sly Technologies (Phase 1); others are open for third-party implementation.

Product	Type	Description	Developer
Bonafide Spec	Document	Canonical specification (this document, Parts 1–13)	Sly Technologies → Foundation
Bonafide Core	Library	Reference implementation of vault protocol, key derivation, ledger, validation client	Sly Technologies (open source)
Bonafide DB	Packages	Database-native vault packages for PostgreSQL, Oracle, SQL Server, MySQL, MongoDB	Sly Technologies (open source)
Bonafide SDK	Libraries	Developer SDKs for JavaScript, Java, Python, Swift, Kotlin, Rust, Go, C	Sly Technologies (open source)
Bonafide Cloud	Service	Managed coordination infrastructure (API, validators, federation, relay, CA, ledger)	Sly Technologies
Bonafide Personal	App	Consumer vault application for iOS, Android, desktop, web	Sly Technologies
Bonafide Gateway	Service	API gateway with tiered authentication and rate limiting	Sly Technologies (open source)
Bonafide Validator	Service	Reference validator node implementation	Sly Technologies (open source)
Bonafide Relay	Service	Reference relay operator implementation	Sly Technologies (open source)
Bonafide Cert	Tool	Certification test suites for all compliance tiers	Sly Technologies (open source)
ExaScale + Bonafide	Product	Integrated high-performance data platform with Classification S vault	Sly Technologies

7. Revenue Model

7.1 Sustainability Principle

Bonafide is a privacy-first ecosystem that is commercially sustainable, not a commercial product that happens to have privacy features. The specification is free. Reference implementations are open source. Revenue comes from services, certification, and premium products—not from the protocol itself.

7.2 Revenue Sources

Source	Description	Payer
Bonafide Cloud subscriptions	Managed infrastructure for institutions that prefer not to self-host	Institutions
ExaScale integration	Classification S hardware + Bonafide integration for enterprise customers	Institutions
Bonafide Personal (premium)	Consumer vault app with advanced features (extended sharing, multi-persona, priority relay)	Users (freemium model)
Certification fees	Bonafide Certified program for validators, relay operators, hardware vendors, institutions	Ecosystem participants
Institutional subdomain registration	Branded subdomains under bonafide.id	Institutions
Foundation membership	Phase 2+ governance participation with voting rights	Institutions and organizations
Validator fees	Transaction fees for validation operations (paid to validators, network takes percentage)	Operations volume

7.3 What Is Never a Revenue Source

- User data. Bonafide never monetizes user data, metadata, or behavioral analytics. This is architectural—the network cannot see the data it protects.
- Advertising. Bonafide products do not display ads or sell attention.
- Protocol licensing. The specification is free and open. No one pays to implement it.
- Data brokerage. Bonafide exists to prevent data brokerage, not to participate in it.

Bonafide™ — Privacy by architecture, not by promise.

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