ARCHITECTURAL WHITEPAPER

Bonafide™

User-Sovereign Encrypted Data Vault Architecture

Open Specification for Quantized, Encrypted, Privacy-First Data Sovereignty

Sly Technologies Inc.

Version 1.0 — February 2026

Classification: Open Specification

Privacy by architecture, not by promise.

1. Executive Summary

Every major data breach of the last decade shares the same root cause: institutions store personal data in centralized databases protected by perimeter security. When the perimeter falls—and it always does—everything is exposed. Users bear 100% of the consequences with 0% of the control.

Bonafide is an open specification for a fundamentally different model. Instead of trusting institutions to protect your data behind their walls, Bonafide encrypts every piece of personal data independently, gives users the only master keys, and distributes encrypted fragments across the institutions that need them—with each institution able to see only what the user has authorized.

The core innovations:

- **Quantized encryption:** Personal data is decomposed into atomic units called quanta. Each quantum has its own encryption key, access policy, and tamper-proof audit trail. Compromise of one reveals nothing about any other.
- **Passwordless multi-factor authentication:** No passwords. No recovery phrases. No shared secrets. The user's multi-modal biometric is processed on-device within a hardware secure element, combined with a user-chosen root secret stored in the device's enclave. The entire derivation is stateless—there is no stored "correct answer," no error on failure, no oracle for an attacker to probe.
- **Composable authentication gestures:** The root secret can be derived from any combination of physiological gestures (a specific fingerprint, a facial expression, a spoken word), behavioral gestures (keystroke rhythm, tap pattern, device movement), or traditional knowledge inputs. An attacker doesn't even know what type of input to attempt.
- **Three-path key architecture:** User keys are sovereign (only the user holds them). Institutional keys are sacrosanct (licensed exclusively for authorized operations, architecturally incapable of third-party access). Third-party keys are purpose-specific (generated on demand for sharing, verification, legal access, or emergency).
- **Privacy classifications:** Every institutional deployment carries a transparent, auditable privacy grade (S/A/B/C/U) based on hardware isolation, operational behavior, and audit results. Users see the grade before authorizing access.
- **Compliance by design:** Open and Regulated compliance profiles support global deployment from privacy-favorable jurisdictions to regulated markets, with an explicit "no Surveillance Profile" commitment. No backdoors. No master keys. Lawful access through scoped, audited, purpose-specific mechanisms.
- **Open ecosystem:** Free specification, open-source reference implementations, certification program, three-phase governance evolution from corporate stewardship to community foundation.

Bonafide builds on cryptographic primitives already deployed in production within the ExaScale™ platform by Sly Technologies. The specification is open. Anyone can implement it.

2. The Problem

2.1 Broken Trust Model

A person's name, address, Social Security number, and financial history are duplicated across hundreds of institutional databases—each a potential breach target, each protected by the institution's own security decisions. When Equifax was breached, 147 million people lost control of data they never chose to share with Equifax in the first place. The user bears the consequences; the institution bears the headline.

2.2 Password Failure

Passwords are shared secrets: both the user and the service must know them. They are reused, phished, and stored in databases that get breached. Multi-factor authentication adds friction without addressing the root cause. Recovery phrases shift the burden to the user—lose your 24-word seed and your assets are gone. Neither model works for the general population.

2.3 No Revocation, No Accountability

When you close a bank account, your data doesn't leave with you. It persists in backups, analytics pipelines, and partner systems. GDPR's right to erasure is a legal construct with no technical enforcement. There is no mechanism for users to see who accessed their data, when, or why. Accountability is a policy promise, not a verifiable fact.

2.4 Redundant Identity Verification

Every institution independently verifies the same attributes. The user provides their name, address, date of birth, and government ID to their bank, their employer, their insurer, their landlord, their doctor—each performing its own KYC process, each storing its own copy, each creating its own breach surface.

3. How Bonafide Works

3.1 The Quantum — Atomic Data Unit

A quantum is the fundamental unit of the Bonafide vault. It is a self-contained, independently encrypted package: a single record, document, image, or assertion. Each quantum is encrypted with its own AES-256-GCM key, carries its own access policy, and has its own Merkle tree entry for integrity verification. Authorizing access to one quantum reveals nothing about any other. Revoking access to one leaves all others intact.

3.2 The Vault — Distributed Hierarchy

A user's vault is a tree of branches distributed across institutions. Chase Bank hosts the Chase branch. A hospital hosts the health branch. Neither institution can see the other's branch. The user's device holds the root key that unifies the tree. Branches contain channels (data streams within an institutional relationship), and channels contain quanta.

3.3 Composable Root Derivation

The Bio Root—the cryptographic root of the entire vault—is computed from three inputs:

$$\textbf{Bio Root} = \textbf{Hash}(\ \textbf{biometric}\ ||\ \textbf{root\_secret\_hash}\ ||\ \textbf{manual\_passphrase}\ )$$

The biometric is always required, processed on-device in a hardware secure element, never transmitted. The root secret is set once during vault creation from user-chosen gestures—a specific finger, a facial expression, a tap rhythm, a spoken word, or any combination—then stored in the device enclave and auto-appended transparently. The manual passphrase is optional, selecting alternate personas when present.

The derivation is stateless: there is no stored correct answer. Every input combination produces a valid-looking 256-bit key. The system never indicates whether the result was correct. An attacker searching with wrong inputs gets a key that decrypts nothing, and they cannot distinguish failure from success. This is unique to Bonafide—every other authentication system provides an oracle.

3.4 Ghost Quanta — Privacy-Preserving Data Use

Most institutional interactions do not require raw data. A credit check needs a yes/no, not the actual income. An age verification needs a confirmation, not the date of birth. Ghost quanta provide cryptographic proofs about data without exposing the data itself: zero-knowledge proofs, range proofs, set membership proofs, redacted summaries, and hashed confirmations. Institutions receive the answers they need without possessing the data.

3.5 Extensible Security Levels

Bonafide uses graduated security levels to protect data of varying sensitivity. The reference profile defines 10 levels—from Level 0 (public identifiers) through Level 9 (sovereign root material)—but deployments configure their own count. Each level determines key derivation depth, minimum device enclave tier, and minimum institutional privacy classification. A retailer accesses Levels 0–2. A bank reaches 0–4. A hospital reaches 0–5. Nobody except the user touches Level 8–9.

4. Three-Path Key Architecture

Bonafide defines three distinct key paths. Each has a strictly bounded purpose. No key path can serve another's function. This separation is enforced cryptographically.

4.1 User Key — Sovereign

Derived from the Bio Root through the key hierarchy. The user can access their data from any enrolled device without institutional cooperation. If an institution disappears, the user's data is still decryptable. The user key is never shared with any institution, third party, or the Bonafide network.

4.2 Institutional Key — Sacrosanct

Licensed exclusively for user-authorized institutional operations. No exceptions. The institution uses its key to process transactions, generate statements, and deliver services. The key cannot be used to facilitate third-party access—not for law enforcement, not for regulators, not for partners. On Classification A and S deployments, the key exists only in hardware-isolated memory. The institution cannot extract it.

This protects institutions from coercion. If a government agency demands customer data, the institution has a genuine defense: the protocol doesn't allow institutional keys to serve third-party access. The agency must use the third-party access protocol.

4.3 Third-Party Key — Purpose-Specific

Generated on demand by the Bonafide API for any authorized third-party access: sharing photos with a friend, verifying identity with a merchant, transferring medical records to a specialist, executing a court order. Each key is scoped to specific data, bound to a specific recipient, limited to a specific duration, and derived from the authorization that created it. Multiple third-party keys can coexist independently on the same data.

5. Third-Party Access

Third-party access is a first-class protocol operation—not a compromise of user or institutional keys.

5.1 User Sharing

Users share vault data by generating a link. The recipient clicks the link and sees the data in the Bonafide viewer—rendered with forensic watermarking, no download button, no copy-paste. Share modes include view-once, view-limited, time-bounded, revocable, and permanent. Recipients without a Bonafide vault can view shared data through the web viewer—share links are the onramp for new users.

5.2 Institutional Verification

When Merchant A needs Bank B to confirm a user's identity or account standing, the user's pre-configured verification rules authorize the exchange. Ghost quanta are the default—the merchant receives a cryptographic proof, not raw data. The two institutions' keys never meet. The Bonafide network mediates the entire exchange. The user can require real-time approval for sensitive verifications.

5.3 Legal and Audit Access

When a court orders access to specific data, the authority presents the legal instrument to the Bonafide API. The instrument is validated (authority registration, scope, jurisdiction, uniqueness). A purpose-specific key is generated, derived from the instrument's hash—binding the key to this specific legal order. Two access modes: snapshot (point-in-time forensic copy with its own Merkle root) and monitoring (real-time read access with hard expiration). Multiple agencies get independent keys. The institution is not involved—the protocol handles it.

Exported data can carry constraints: minimum privacy classification of the receiving system, enclave-only decryption, time-to-live, or ghost-only export.

5.4 Emergency Access

Users optionally configure an emergency profile: which data is accessible (medical conditions, allergies, emergency contacts), who can trigger access (certified first responders, designated agents), and how (device beacon, responder credential). Emergency keys are short-lived (24 hours, renewable once). Longer access transitions to the legal access path.

6. Privacy Classifications

Every institutional deployment carries a transparent, auditable privacy grade. Users see the grade before authorizing access.

Classification	Key Isolation	Plaintext Exposure	Revocation	Hardware
S — Sovereign	FPGA fabric	Never leaves enclave	Absolute	Dedicated FPGA / SE
A — Attested	Hardware TEE	Within TEE only	Effective	TEE-capable CPU or DPU
B — Bounded	Software process	In API responses	Operational	Optional HSM/TPM
C — Compliant	Runtime only	In application stack	Partial	None required
U — Unclassified	Not audited	Unknown	Unknown	Not verified

Classifications are not self-reported. They are determined by automated hardware attestation (continuous) and periodic integration and operational audits. Downgrades trigger user notifications. Users can set minimum classification requirements for their vault—a user requiring Classification A cannot peer with a Classification B institution regardless of willingness.

The privacy score (0–100) combines the structural baseline from classification with behavioral metrics: ghost quanta usage, revocation compliance, override frequency, and breach history. Institutions compete on privacy scores as a market differentiator.

7. Personas and Duress Protection

7.1 Multiple Identities

The manual passphrase component of the Bio Root formula enables multiple cryptographically independent personas from the same biometric. Each persona has its own vault tree, its own institutions, its own proxy addresses. No institution seeing one persona can correlate it to another. The existence of additional personas is undetectable—stateless derivation means there is nothing to enumerate.

7.2 Duress Protection

Under coercion, the user authenticates without a passphrase. The default persona opens—configured as a decoy with plausible but non-sensitive data. The real vault requires a passphrase the coercer doesn't know exists. Silent alerts optionally notify trusted contacts. The decoy has valid encryption, valid Merkle proofs, and realistic content—indistinguishable from a real vault.

7.3 Content Neutrality

The vault encrypts, authorizes, and audits. It does not inspect, filter, or classify content. No backdoors. No content scanning. Lawful access works through audited, scoped mechanisms—not circumvention. If a jurisdiction requires content scanning, Bonafide cannot be deployed there.

8. Blind Validation Network

Every vault operation is verified by independent validators who see cryptographic proofs, not data. Validators confirm that operations are authorized and correctly formed without learning what the data is, who the user is, or what institution is involved.

The network uses Byzantine fault tolerant consensus. Committee sizes scale with operation sensitivity (3 validators for routine operations, up to 9+ for legal access). Selection enforces organizational, geographic, and network diversity—no single entity can dominate any committee.

Trust scores (0–1000) track validator behavior. New validators start at 100 (probationary) and earn trust through 90+ days of correct operation. Scores below threshold trigger automatic suspension. Sybil resistance comes from certification cost, organizational diversity limits, and mentorship risk—an established validator vouching for a malicious node loses its own score.

9. Network Security

Bonafide defends against six attacker classes from opportunistic scanners to nation-states:

- **Transport:** Mutual TLS everywhere. TLS 1.3 with AEAD-only ciphers. No anonymous connections. Certificate pinning for all long-lived connections. Hardware-accelerated TLS termination on FPGA and DPU deployments.
- **Client authentication:** Device attestation required for every connection—cryptographic proof of enclave tier and software integrity. Guest enclave with restricted capabilities for unrecognized devices.
- **DoS defense:** Five-tier capacity architecture with isolated resource pools. Proof-of-work for unauthenticated requests. Anycast distribution. Backpressure propagation for graceful degradation.
- **Traffic analysis resistance:** Constant-rate padding, uniform request/response sizing, timing jitter, and optional ORAM for high-security deployments.
- **Anti-duplication:** Six layers—ghost quanta to minimize exposure, forensic watermarking for traceability, canary quanta for breach detection, privacy scoring for economic deterrence, API abstraction for technical enforcement, and contractual terms in peering agreements.
- **Incident response:** Trust scores as automated immune system. Certificate revocation within 60 seconds. Immutable forensic audit trail for every security-relevant event.

10. Enclave Architecture and Hardware

10.1 Device-Side Enclaves

Five enclave tiers from Tier S (FPGA, Level 9 access) to Tier 4 (software-only, Level 3). The tier is determined by hardware attestation, not self-report. Flagship phones (iPhone SEP, Pixel Titan M2) reach Tier 1. MacBook Apple Silicon reaches Tier 1. Windows with TPM reaches Tier 3. Every modern smartphone and laptop can participate; the tier determines the maximum security level accessible.

10.2 Server-Side Hardware

The Bonafide runtime's Hardware Abstraction Layer supports pluggable backends:

- **ExaForge FPGA (Classification S):** Keys in PUF, AES in fabric, ZK proofs in fabric. Plaintext never touches host memory.
- **NVIDIA H100 Confidential Computing, SmartNIC/DPU (Classification A):** TEE-equivalent isolation with hardware acceleration.
- **AWS Nitro Enclaves, Azure Confidential VMs (Classification A):** Cloud-native TEE—lowest barrier to Classification A.
- **HSM + QAT, TPM + GPU (Classification B):** Key storage in hardware, bulk crypto in accelerator.
- **Software only (Classification C):** Encrypted keyring, software AES. The starting point for incremental adoption.

Institutions start at Classification C and upgrade incrementally. The Bonafide runtime is the same software throughout—only the HAL backend changes.

10.3 Peripheral Devices

IoT devices (cameras, sensors, smart locks, medical monitors) participate as peripherals under delegated credentials from a vault holder. Three peripheral tiers (P1–P3) with credential lifetimes from 7 to 90 days depending on hardware security.

11. Compliance and Global Deployment

11.1 Compliance Profiles

The Open Profile is the canonical specification: full content neutrality, no backdoors, lawful access through the third-party protocol. The Regulated Profile adds configurable compliance controls for jurisdictions with lawful access requirements: pre-registered legal authorities, data residency enforcement, automated regulatory reporting. The core cryptographic architecture is unchanged.

The specification explicitly does not define and will never define a Surveillance Profile. Bulk access, real-time interception, content scanning, master keys, and silent access are outside the specification's design space. Any implementation adding these capabilities is non-compliant.

11.2 Global Market Tiers

Tier	Profile	Jurisdictions
Tier 1 — Open	Open Profile, no modifications	US, Canada, Switzerland, Japan, South Korea, Taiwan, Israel, Brazil, most of Latin America
Tier 2 — Regulated	Regulated Profile	EU (GDPR + eIDAS), UK, Australia, India, Singapore, France, Germany
Tier 3 — Institutional Only	Enterprise deployment	Russia, Turkey, UAE, Gulf States, Thailand
Tier 4 — Cannot Deploy	Specification prohibits	China, Iran, North Korea, Myanmar, Vietnam

Tier 1 and Tier 2 markets cover approximately 60% of global GDP. Tier 4 classification is not permanent—if legal frameworks evolve, jurisdictions can be reclassified.

11.3 Regulatory Framework Mapping

Bonafide meets or exceeds NIST 800-63 AAL2/AAL3, PSD2 Strong Customer Authentication, FIDO2/WebAuthn, GDPR Articles 5, 17, 20, 25, and 32, HIPAA, PCI-DSS v4.0, CCPA, and eIDAS 2.0. The specification maps each framework's requirements to specific Bonafide mechanisms.

12. What Existing Systems Cannot Do

Capability	Passwords / SSO	Crypto Wallets	Federated ID	Bonafide
No shared secrets	No — password is shared	Seed phrase risk	OAuth tokens	Biometric + root secret, on-device
No oracle on failure	Login succeeds/fails	Tx succeeds/fails	Token valid/invalid	Silence — no signal
Per-institution isolation	Central DB	N/A	Partial	Full — each branch independent
Granular revocation	All or nothing	All or nothing	Token revocation	Per-quantum, per-channel, per-branch
Verifiable audit trail	Server logs (mutable)	Blockchain (public)	No	Immutable ledger, privacy-scored
Institutional key separation	N/A	N/A	N/A	Sacrosanct — cannot serve 3rd-party
Third-party access protocol	N/A	N/A	N/A	Purpose-specific keys per authorization
Privacy classifications	N/A	N/A	N/A	Audited S/A/B/C/U grades, visible to users
Unlinkable personas	No	Multiple wallets	No	Cryptographic independence, undetectable
Content neutrality	Platform-dependent	Protocol-level	Platform-dependent	Specification requirement — no inspection

The critical difference is architectural. Bonafide does not improve the perimeter—it eliminates the need for one. Each quantum is its own fortress. Breaching an institution's network yields only ciphertext that cannot be decrypted without the user's biometric, the device's root secret, and the correct derivation path.

13. Open Ecosystem

13.1 What Anyone Can Build

The specification is free. Reference implementations are open source. Third parties build vault providers, validator nodes, relay operators, hardware devices, database integrations, consumer apps, institutional middleware, verification services, and privacy tools. Certification ensures interoperability.

13.2 Institutional Onramp

Institutions adopt incrementally: start with database encryption packages (Classification C), refactor to runtime API (Classification B), add TEE hardware (Classification A), deploy FPGA enclaves (Classification S). Each phase delivers compliance benefit. No flag-day migration required.

13.3 User Onramp

Users discover Bonafide through share links (a friend sends a photo, the recipient creates a vault to view it), institutional adoption (their bank deploys Bonafide), or direct download. The guest enclave flow bootstraps a new vault in minutes.

13.4 Governance Evolution

Phase 1 (current): Sly Technologies stewards the specification. Phase 2: an independent Bonafide Foundation takes ownership when the ecosystem reaches critical mass. Phase 3: fully community-governed with no single entity holding veto power. The specification's identity is preserved by a defined boundary: compliance features may evolve, but master keys, bulk access, and content scanning are never added.

13.5 Revenue Model

Sustainable revenue from Bonafide Cloud subscriptions, ExaScale integration, Bonafide Personal premium features, certification fees, and institutional subdomain registration. The specification is always free. Reference implementations are always open source. User data is never monetized—the network cannot see the data it protects.

14. Specification Reference

The Bonafide V1.0 specification is organized into 13 parts:

Part	Title	Scope
1	Foundation & Core Architecture	Vault hierarchy, quantum model, design principles, participation models, security levels, ledger
2	Cryptographic Foundation	Composable root derivation, gesture system, biometric processing, key hierarchy, encryption, Merkle integrity
3	Security Levels & Authentication	Level system, MFA compliance mapping, auth flows, elevation, session management, duress
4	PII Protection & Privacy	Proxy identity, privacy scoring, canary detection, watermarking, data minimization, erasure, portability
5	Blind Validation Network	ZK proof system, trust scoring, validator selection, BFT consensus, Sybil resistance
6	Infrastructure & Portfolio	Database packages, cloud coordination, ExaScale integration, namespace, products, revenue
7	Personas & Identity	Multi-persona architecture, duress protection, focus profiles, content neutrality, persona lifecycle
8	Open Ecosystem & Governance	Ecosystem philosophy, federated relay, certification program, governance evolution, adoption strategy
9	Network Security & Abuse Prevention	Threat model, transport security, DoS defense, validator protection, traffic analysis resistance
10	Enclave Architecture & Device Classes	Enclave tiers, device profiles, peripherals, biometric input, server hardware, cross-device sync
11	Privacy Classifications	S/A/B/C/U definitions, audit methodology, upgrade path, score integration
12	Institutional Runtime & Data Governance	Runtime architecture, three-path keys, third-party access, revocation, anti-duplication, HAL
13	Compliance Profiles & Global Deployment	Open/Regulated profiles, market tiers, regulatory mapping, data residency, compliance evolution

15. Vision

Bonafide exists because the current model is fundamentally broken. Institutions collect more data than they need, protect it with perimeter security that fails, and leave users with no control and no recourse. Passwords are a solved problem—they need to stop existing. Recovery phrases are a burden the general population cannot bear. Centralized identity databases are targets that cannot be defended indefinitely.

The answer is not higher walls around institutional databases. It is making the data itself sovereign—encrypted at the atomic level, keyed to the individual's biometric, distributed so that no breach exposes more than opaque ciphertext. The institution's role shifts from guardian of data to host of encrypted fragments whose content it cannot see without user authorization.

Bonafide makes this architecturally real. The specification defines the protocol. ExaScale provides the first production implementation. The ecosystem grows through institutional adoption, user activation, and third-party innovation. Privacy classifications create market pressure. Compliance profiles enable global deployment. The open governance model ensures the specification outlives any single company.

The end state is a world where your data is truly yours: encrypted with keys only you possess, shared only as you authorize, auditable at every step, and revocable at any time. No passwords. No centralized honeypots. No backdoors. No master keys. No more hoping institutions protect what they were never supposed to see in the first place.

Bonafide™ — Privacy by architecture, not by promise.

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