BONAFIDE™ SPECIFICATION V1.0 — PART 1

Foundation & Core Architecture

Vault hierarchy, quantum data model, design principles, participation models, extensible security levels, and immutable ledger

1. Introduction

Bonafide is an open specification for user-sovereign encrypted data vaults. It defines a protocol in which every piece of personal data is independently encrypted, secured by passwordless multi-factor authentication with hardware-bound biometrics, and distributed across institutions that can see only what the user authorizes.

This part establishes the foundational architecture: the vault hierarchy, the quantum data model, the core design principles, and the participation models that define how users, institutions, and the network interact.

1.1 What Bonafide Is

- An open specification, not a proprietary product. Anyone can implement it.
- A data sovereignty framework. Users own their data; institutions host encrypted fragments they cannot read.
- A passwordless authentication architecture. No passwords, no recovery phrases, no shared secrets.
- A privacy-first ecosystem designed for extensibility and third-party buildout.

1.2 What Bonafide Is Not

- Not a payment system or financial rails.
- Not a messaging protocol or communications platform.
- Not a blockchain or distributed ledger (though it uses Merkle trees for integrity).
- Not a product tied to any single vendor, hardware platform, or cloud provider.

2. The Problem

2.1 Broken Trust Model

The current model for personal data is: the user gives their data to an institution, and the institution promises to protect it. The institution stores the data in centralized databases, behind perimeter security that eventually fails. Every major breach—Equifax, Marriott, Yahoo, T-Mobile, Change Healthcare—follows the same pattern: perimeter breached, plaintext accessed, millions of records exposed.

Users bear 100% of the consequences (identity theft, financial loss, reputational damage) with 0% of the control. They cannot revoke access. They cannot audit who viewed their data. They cannot limit exposure to the minimum necessary. They cannot even discover what data an institution holds about them without filing regulatory requests.

2.2 Password Failure

Passwords are the weakest link in every security architecture. They are reused across services. They are stolen in phishing attacks. They are exposed in breaches. They are shared in sticky notes. Password managers mitigate but do not solve the problem—they centralize credentials behind a single master password, creating a high-value target. Multi-factor authentication adds friction without addressing the root cause: shared secrets that can be intercepted, replayed, or coerced.

2.3 No Revocation

Once a user shares data with an institution, they have no technical mechanism to revoke access. “Delete my account” is a request, not a command. The institution may retain copies in backups, analytics pipelines, data warehouses, and partner systems. GDPR and CCPA create legal obligations but provide no technical enforcement. The user must trust that the institution complied.

2.4 Redundant Identity Verification

Every institution independently verifies the same identity attributes. The user provides their name, address, date of birth, government ID, and biometric to their bank, their employer, their insurer, their landlord, their doctor—each institution performing its own KYC process, each storing its own copy of the verified data, each creating its own breach surface. The user’s identity is fragmented across dozens of institutions with no coordination, no deduplication, and no user control.

3. Design Principles

The Bonafide specification is governed by seven design principles. Every architectural decision traces back to one or more of these principles.

3.1 User Sovereignty

The user is the sole authority over their data. No institution, government, or network operator can access vault data without either the user's authorization or a validated legal instrument processed through the third-party access protocol (Part 12). The user's Bio Root—derived from their biometric—is the only master key, and it exists only ephemerally during authentication.

3.2 Quantized Encryption

Data is decomposed into atomic units (quanta) that are independently encrypted. Compromise of one quantum reveals nothing about any other. There is no bulk decryption—accessing N quanta requires N independent decryption operations, each authorized separately.

3.3 No Shared Secrets

The system contains no passwords, no recovery phrases, no master keys, no API keys that unlock data. Authentication is biometric, processed on-device within a hardware secure element, combined with a user-chosen root secret stored in the device enclave. The authentication factors never leave the device and are never transmitted over any network.

3.4 Institutional Separation

Each institution holds only its own branch of the user's vault. No institution can see other branches, discover which other institutions the user peers with, or infer the vault's overall structure. The institutional key is sacrosanct—licensed exclusively for user-authorized operational use and architecturally incapable of serving third-party access (Part 12).

3.5 Graduated Security

Not all data requires the same protection. Security levels provide cryptographic graduation from public identifiers to sovereign biometric roots. The number of levels is extensible—the reference profile defines 10 levels, but deployments can configure fewer or more. The level determines the encryption depth, the minimum enclave tier required for access, and the minimum privacy classification of the hosting institution.

3.6 Content Neutrality

The vault encrypts, authorizes, and audits. It does not inspect, filter, or classify content. No backdoors. No master keys. No content scanning. Lawful access is supported through audited, scoped mechanisms—not circumvention.

3.7 Transparency

Every operation is recorded in an immutable ledger. Every institutional deployment carries a visible privacy classification (Part 11). Every third-party access event is auditable. The user can

see who accessed their data, when, under what authority, and what they saw. Sunlight is the governing principle.

4. Vault Hierarchy

4.1 Structure

A user's vault is a tree of branches, channels, and quanta distributed across institutions. The tree is not stored in any single location—each institution holds only its own branch. The user's vault holder device maintains the tree's structure and can navigate across branches.

Vault: The root of the tree. One per user identity (one per persona, for users with multiple personas). The vault is an abstract container—it has no physical storage location. It exists as the set of branches the user has peered with institutions.

Branch: One per institutional peer. When a user peers with Chase Bank, a branch is created. The branch contains all data relevant to the user-institution relationship. Branches are cryptographically isolated—Chase's branch keys cannot access the hospital's branch.

Channel: A data stream within a branch. A banking branch might have channels for transactions, statements, account details, and communications. Channels organize data logically and can carry independent access policies.

Quantum: The atomic unit of data. A single record, document, image, measurement, or assertion. Every quantum is independently encrypted with its own DEK, carries its own security level, and has its own entry in the Merkle tree.

4.2 Vault Topology

The vault is a peer graph, not a centralized store. Each branch is hosted on the institution's infrastructure. The user's device knows the topology (which institutions host which branches) but the institutions do not know each other. Chase does not know the user also has a branch at Mount Sinai Hospital. The topology itself is private.

4.3 Cross-Branch Operations

Some operations span multiple branches: aggregating financial data across banks, combining medical records from multiple providers, or performing identity verification using attributes from different institutions. Cross-branch operations are mediated by the user's device, which holds the keys for all branches. The institutions never communicate directly about the user—the user's vault holder is the bridge.

5. Quantum Model

5.1 Quantum Structure

A quantum is the atomic unit of the Bonafide vault. Every quantum contains:

Field	Description	Encrypted?
Quantum ID	Globally unique identifier	No (required for addressing)
Payload	The actual data (text, binary, document, image, structured record)	Yes (AES-256-GCM with quantum-specific DEK)
Security level	The level assigned to this quantum (determines key derivation depth)	No (required for access control)
Metadata	Creation timestamp, last modified, size, content type	Configurable (can be encrypted or plaintext)
Access policy	Who can read, write, share; retention duration; permitted use	No (required for runtime enforcement)
DEK wrappings	User wrapping, institutional wrapping, third-party wrapping(s)	N/A (wrappings are encrypted keys)
Merkle leaf	Hash of the encrypted payload, linking the quantum to the integrity tree	No (required for verification)
Forensic watermark template	Session-unique watermark configuration applied during plaintext rendering	Yes (invisible to data consumers)

5.2 Quantum Independence

Every quantum is encrypted with its own DEK. There is no shared key across quanta. Compromising one quantum's DEK reveals only that quantum's payload. An attacker who obtains the encrypted contents of an entire branch and somehow cracks one DEK has gained exactly one quantum—and must repeat the effort independently for every other quantum.

5.3 Ghost Quanta

A ghost quantum is a derived representation of a quantum that proves something about the data without exposing the data itself. Ghost quanta are the primary mechanism for privacy-preserving institutional interactions (Part 12). Types include:

- **Zero-knowledge proofs:** Cryptographic proof that a statement about the data is true without revealing the data. "Account balance exceeds $5,000" without revealing the actual balance.
- **Redacted views:** A quantum with selected fields removed or replaced. A medical record with the diagnosis visible but the patient's name replaced with a pseudonym.

- **Hashed confirmations:** A hash of the data that a verifier can check against a known value without seeing the original. “This SSN hash matches the hash on file.”
- **Range proofs:** Proof that a numeric value falls within a range without revealing the exact value. “Income is between $50,000 and $100,000.”
- **Set membership proofs:** Proof that a value belongs to a defined set without revealing which element. “Country of citizenship is an EU member state.”

6. Participation Models

6.1 Vault Holders

A vault holder is a device that computes or caches Bio Root material, derives branch keys, and can perform vault operations. Vault holders require a hardware secure element for key isolation and biometric processing. Phones, laptops, desktops, tablets, and dedicated Bonafide hardware devices are vault holders. Part 10 defines the enclave tiers and device compatibility.

6.2 Institutions

An institution is any organization that peers with a user's vault to provide services. Banks, hospitals, employers, government agencies, schools, insurers, and merchants are institutions. Institutions deploy the Bonafide runtime on their infrastructure (Part 12) and interact with user data exclusively through the runtime API. Their privacy classification (Part 11) is visible to users.

6.3 Peripherals

A peripheral is a device that produces or consumes data within the Bonafide network without holding vault keys. IoT devices (cameras, sensors, smart locks, medical monitors) are peripherals. They receive delegated credentials from a vault holder and operate under scoped authority. Part 10 defines the peripheral model.

6.4 Validators

Validators are independent nodes in the blind validation network that verify operations without seeing data. They confirm quantum integrity, verify access authorization, and maintain trust scores. Validators are certified through the Bonafide Certified program (Part 8) and are selected for operations based on trust score, geographic diversity, and organizational diversity.

6.5 Relay Operators

Relay operators provide federated proxy services for email, phone, and physical address. They allow users to communicate through Bonafide proxy addresses without exposing their real contact information. Relay operators are certified and carry their own privacy classifications.

6.6 Third Parties

Any entity authorized to access vault data through the third-party access protocol (Part 12). Friends receiving shared photos, doctors receiving transferred records, law enforcement executing warrants, auditors performing compliance reviews, and emergency responders accessing medical profiles are all third parties. Each receives a purpose-specific, time-bounded key that is independent of both the user's key and the institution's key.

7. Security Level Architecture

7.1 Extensible Levels

Bonafide uses graduated security levels to control access to data of varying sensitivity. The number of levels is not fixed—it is an unsigned integer. The reference profile defines 10 levels as a sensible default for most deployments. Institutions can configure fewer (a simple consumer app might use 3) or more (a defense deployment might use 50).

The security level determines three properties: the key derivation depth (higher levels require deeper key chains), the minimum enclave tier required for device access (Part 10), and the minimum privacy classification of the hosting institution (Part 11).

7.2 Reference Profile (10 Levels)

Level	Classification	Description	Min Enclave Tier	Min Institution Classification
0	Public	Publicly shareable identifiers, display name, public key	Tier 4 (software)	C
1	Basic	Non-sensitive personal info (preferences, settings)	Tier 4 (software)	C
2	Personal	Contact info, address, phone, email	Tier 3 (TPM)	C
3	Confidential	Government IDs, date of birth, tax identifiers	Tier 3 (TPM)	B
4	Sensitive	Financial records, employment data, income	Tier 2 (TEE)	B
5	Protected	Medical records, legal documents, insurance	Tier 2 (TEE)	B
6	Restricted	Psychiatric records, genetic data, sealed legal	Tier 2 (TEE)	A
7	Classified	Intelligence, defense, trade secrets	Tier 1 (Dedicated SE)	A
8	Critical	Biometric templates, root secret material	Tier 1 (Dedicated SE)	A
9	Sovereign	Bio Root derivatives, master key material	Tier S (FPGA)	S

This is a reference profile, not a mandate. A healthcare deployment might define 15 levels with fine-grained distinctions between medical data categories. A consumer note-taking app might use 3 levels (public, personal, private). The protocol supports any configuration.

7.3 Quantum-Level Override

Individual quanta can be assigned a security level that differs from the default for their branch or channel. A single highly sensitive document in an otherwise routine branch can be elevated to a

higher level. The override is cryptographic—the quantum's DEK is derived at the overridden level's depth, not the branch's default depth. A device or institution that lacks the enclave tier for the overridden level cannot access that specific quantum even if they can access everything else in the branch.

8. Immutable Ledger

8.1 Purpose

The Bonafide ledger (QuantaLedger) is an immutable, append-only record of every operation performed on the vault. It provides the evidentiary foundation for user transparency, institutional accountability, regulatory compliance, and forensic investigation.

8.2 What the Ledger Records

- Every quantum creation, modification, and deletion
- Every access event (read, write) with the key path used (user, institutional, third-party)
- Every peering event (new institution, revocation)
- Every third-party authorization (sharing, verification, legal, emergency)
- Every security level change and quantum-level override
- Every key rotation and DEK re-encryption
- Every trust score change for validators and institutions
- Every privacy classification audit result
- Every revocation and its re-encryption confirmation

8.3 Merkle Integrity

The ledger is structured as a Merkle tree. Each entry is hashed and linked to the previous entry. The Merkle root provides a single hash that verifies the integrity of the entire ledger history. Tampering with any entry changes the root, making alteration detectable. The root is periodically published to the blind validation network for independent verification.

8.4 Privacy of the Ledger

The ledger records that operations occurred, not the content of the data involved. An access event records the quantum ID, the key path (user/institutional/third-party), and the timestamp—not the quantum's payload. The ledger itself is encrypted at rest and accessible only to the vault owner and to entities with valid third-party access keys that include ledger scope.