BONAFIDE™ SPECIFICATION V1.0 — PART 7

Personas & Identity

Multi-persona architecture, duress protection with plausible deniability, focus profiles, content neutrality, and persona lifecycle management

1. Purpose

This part defines Bonafide's persona system: the ability for a single user to maintain multiple cryptographically isolated identities within the same vault infrastructure. Personas enable privacy compartmentalization, duress protection, contextual identity management, and plausible deniability.

2. Persona Architecture

2.1 What a Persona Is

A persona is an independent vault identity derived from a unique Bio Root. Each persona has its own vault tree, its own branches, its own institutional peers, and its own security level assignments. Personas are cryptographically isolated: the keys for Persona A cannot access data in Persona B. No institution peered with Persona A can discover that Persona B exists.

2.2 Persona Derivation

Personas are derived from the manual passphrase component of the Bio Root formula:

Persona 0: Hash(biometric || root_secret_hash || "") → default persona

Persona 1: Hash(biometric || root_secret_hash || "work") → work persona

Persona 2: Hash(biometric || root_secret_hash || "private") → private persona

Each passphrase produces a completely different Bio Root, which produces a completely different key hierarchy. The personas share nothing cryptographically. An attacker who compromises Persona 0’s Bio Root cannot derive Persona 1’s Bio Root without knowing the passphrase “work.”

2.3 Persona Independence

Each persona is a full vault with all the capabilities defined in the specification:

- Independent institutional peers (Persona 0 might peer with Chase; Persona 1 with a different bank entirely).
- Independent security level configuration (the reference 10-level profile or a custom configuration).
- Independent proxy addresses (each persona has its own relay-assigned email, phone, and mail proxies).
- Independent privacy classification requirements (Persona 0 might accept Classification B peers; Persona 2 might require Classification A minimum).
- Independent emergency profile (or no emergency profile).
- Independent third-party sharing, verification rules, and access history.

3. Duress Protection

3.1 Threat Model

A user may be coerced into authenticating: at a border crossing, during a robbery, by an abusive partner, by a hostile government agent. The coercer demands the user unlock their device and show their vault. The user needs to comply without exposing their real data.

3.2 Duress Persona

The user configures a duress persona as their default (Persona 0, no passphrase required). This persona contains plausible but non-sensitive data: a modest bank account, routine medical records, innocuous communications. The real vault lives in a different persona protected by a passphrase.

When coerced:

- The user authenticates with biometric only (touch sensor). No passphrase.
- Persona 0 (duress) opens. It looks like a real, active vault.
- The coercer sees bank statements, some emails, normal documents. Everything appears legitimate.
- The coercer has no way to determine whether other personas exist. The stateless derivation produces no signal.
- The user’s real vault (Persona 1 or 2) is completely invisible.

3.3 Plausible Deniability

The stateless derivation property (Part 2) is the foundation of plausible deniability. There is no metadata indicating how many personas exist. There is no “persona list” to discover. There is no encrypted container whose existence implies hidden content. Each passphrase either produces a Bio Root that decrypts a real vault or it produces a Bio Root that decrypts nothing—and the system never indicates which. The user can truthfully say “this is my vault” while the coercer cannot prove otherwise.

3.4 Silent Alert

When the duress persona is activated, the vault can optionally trigger a silent alert:

- The alert is sent through the relay network to pre-configured contacts (attorney, family member, rights organization).
- No observable signal on the device. The coercer sees a normal vault opening.
- The alert includes: timestamp, device location (if available), and a configurable message.
- The alert mechanism is independent of the persona’s vault operations—it cannot be detected by monitoring the vault’s network traffic.

3.5 Duress and Emergency Interaction

The duress persona’s emergency profile can be configured independently. A user might include real medical data (allergies and medications are life-critical even during coercion) but synthetic identity information. This tradeoff is configured by the user during emergency profile setup.

4. Focus Profiles

4.1 Purpose

Focus profiles are lightweight persona variants that restrict the visible scope of the vault without changing the underlying persona. They are not separate personas with separate Bio Roots—they are views on an existing persona's vault, filtered by context.

4.2 Use Cases

- **Work focus:** Shows only work-related branches (employer, professional services, work email). Hides personal banking, medical, dating, and social branches. Used during work hours or when sharing a screen in a professional setting.
- **Travel focus:** Shows only branches relevant to travel (airline, hotel, rental car, passport). Hides domestic banking, medical, and personal branches. Used while traveling, especially across borders.
- **Medical focus:** Shows only health-related branches for a doctor's visit. Hides financial, employment, and social branches.
- **Child focus:** Shows only age-appropriate branches if a child is using the device. Hides all sensitive content.

4.3 Focus vs. Persona

Property	Persona	Focus Profile
Crypto isolation	Full: separate Bio Root, separate key hierarchy	None: same keys, filtered view
Institutional visibility	Institution sees only the persona it peered with	Institution sees its branch regardless of focus
Plausible deniability	Yes: no evidence of other personas	No: the data still exists, just hidden from the UI
Authentication	Requires different passphrase to switch	Toggleable from vault interface
Use case	Adversarial threats, identity separation	Convenience, context management, screen sharing

Focus profiles are for convenience and context. Personas are for security and adversarial threats. They serve different purposes and should not be confused.

5. Content Neutrality

5.1 Principle

The Bonafide vault is content-neutral. It encrypts, stores, authorizes, and audits data without inspecting, filtering, classifying, or judging the data’s content. The vault does not know whether a quantum contains a bank statement, a medical record, a political manifesto, a religious text, or a personal diary. It applies the same cryptographic protections to all content equally.

5.2 Why Content Neutrality Matters

Content inspection is the gateway to censorship. Any system that inspects content to “protect users” can be repurposed to suppress dissent, target minorities, or enforce ideological conformity. A data sovereignty system that examines content is not sovereign—it is a censor with encryption capabilities.

Content neutrality is not a political statement. It is an architectural requirement for trust. Users in authoritarian regimes need the same vault security as users in liberal democracies. Journalists, activists, whistleblowers, and ordinary citizens need confidence that the system protecting their data does not also evaluate it.

5.3 Content Neutrality and Legal Obligations

Content neutrality does not mean lawlessness. The specification provides lawful access through the third-party access protocol (Part 12). Courts can order access to specific data through validated legal instruments. The vault cooperates with lawful authority—it just refuses to be the authority. It does not decide what content is acceptable; it provides a mechanism for courts to make that determination.

5.4 Content Neutrality and Compliance Profiles

The Open Profile (Part 13) provides full content neutrality. The Regulated Profile maintains content neutrality while supporting scoped lawful access. No compliance profile includes content scanning, filtering, or classification. If a jurisdiction requires content scanning as a condition of deployment, Bonafide cannot be deployed there (Part 13, Section 2.3).

6. Persona Lifecycle

6.1 Creation

- The user creates a new persona by authenticating with a new passphrase.
- The new Bio Root is computed. A new vault tree is created.
- The user peers with institutions from the new persona.
- The new persona is fully independent. No link to existing personas.

6.2 Maintenance

- Each persona's branches, channels, and quanta are managed independently.
- Institutional peering, security levels, privacy requirements, and access policies are per-persona.
- Share links from one persona cannot access another persona's data.
- Focus profiles are per-persona: a work focus on Persona 0 and a work focus on Persona 1 are different configurations.

6.3 Destruction

- A persona is destroyed by deleting all its branch data and revoking all institutional peers.
- The user authenticates into the persona, initiates erasure on all branches, and confirms.
- All DEKs are destroyed. All institutional wrappings are removed. All Merkle leaves are tombstoned.
- The Bio Root derivation path (the passphrase) can be reused for a new persona or abandoned.
- There is no central "persona registry" to update. Destroying a persona is simply destroying all the data associated with that Bio Root.

6.4 Cross-Persona Operations

There are no cross-persona operations. Persona isolation is absolute. The user cannot query across personas, share between personas, or link personas. If the user wants data to exist in two personas, they must create it independently in each. This is by design: any cross-persona linkage would compromise the deniability property.

6.5 Persona Discovery

There is no persona discovery mechanism. The specification provides no API, no metadata, and no network protocol to enumerate, count, or detect personas. A validator, an institution, and an attacker all face the same reality: they know about the personas they have interacted with. They cannot know how many others exist or whether any others exist. This property is enforced by the stateless derivation: there is nothing to enumerate.

Bonafide™ — Privacy by architecture, not by promise.

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

V1.0 — February 2026