BONAFIDE™ SPECIFICATION V1.0 — PART 3

Security Levels & Authentication

Extensible security level system, passwordless multi-factor compliance mapping, authentication flows, elevation, quantum-level override, session management, and duress authentication

1. Purpose

This part defines the security level system in detail: how levels interact with the key hierarchy, how authentication maps to established regulatory frameworks, how elevation between levels works, how quantum-level overrides operate, and how sessions are managed across different trust tiers.

2. Security Level System

2.1 Extensible Architecture

A security level is an unsigned integer that determines three properties of any quantum assigned to that level:

- Key derivation depth: the number of HKDF rounds required to derive the quantum's DEK from the Bio Root.
- Minimum enclave tier: the lowest-tier device hardware that can access the quantum (Part 10).
- Minimum privacy classification: the lowest-classified institutional deployment that can host the quantum (Part 11).

The specification does not mandate a fixed number of levels. The reference profile defines 10 levels as a practical default. Deployments configure their own level count and mapping. A consumer note-taking app might define 3 levels. A defense deployment might define 50. The protocol is indifferent to the count—it cares only that each level maps to the three properties above.

2.2 Reference Profile: 10 Levels

Level	Name	Description	Examples
0	Public	Freely shareable, no sensitivity	Display name, public key, profile avatar
1	Basic	Low sensitivity, non-identifying	App preferences, language settings, notification config
2	Personal	Standard personal identifiers	Email, phone, mailing address, employer name
3	Confidential	Government-issued identifiers	SSN, passport number, driver's license, date of birth, tax ID
4	Sensitive	Financial and employment data	Bank accounts, income, credit score, employment history, tax returns
5	Protected	Medical and legal records	Diagnoses, prescriptions, lab results, contracts, insurance policies
6	Restricted	High-sensitivity personal data	Psychiatric records, genetic data, sealed legal proceedings, addiction history
7	Classified	Trade secrets and intelligence	Corporate IP, defense materials, investigative files, source identities
8	Critical	Authentication material	Biometric templates, root secret helper values, device attestation keys
9	Sovereign	Root cryptographic material	Bio Root derivatives, master key components, vault structure metadata

2.3 Level Constraints

Level	Min Enclave Tier	Min Institution Classification	Max Key Cache Duration
0–1	Tier 4 (Software)	C (Compliant)	24 hours
2–3	Tier 3 (TPM)	C (Compliant) / B (Bounded)	8 hours
4–5	Tier 2 (TEE)	B (Bounded)	4 hours
6–7	Tier 2 (TEE) / Tier 1 (Dedicated SE)	A (Attested)	1 hour
8	Tier 1 (Dedicated SE)	A (Attested)	Session only (no cache)
9	Tier S (FPGA)	S (Sovereign)	Never cached

These constraints are enforced cryptographically. A Tier 3 device cannot derive the key for a Level 6 quantum because the key derivation requires enclave capabilities (secure intermediate state storage, side-channel resistance) that Tier 3 hardware does not provide. The device does not receive an error—it simply cannot perform the derivation. The constraint is architectural, not policy.

3. Passwordless Multi-Factor Authentication

3.1 Factor Analysis

Bonafide's authentication model provides three distinct factors without requiring the user to manage passwords, tokens, or recovery phrases:

Factor	MFA Category	Bonafide Implementation	Properties
Biometric	Inherence (something you are)	Multi-modal biometric processed in device secure element	Cannot be phished, cannot be replayed, requires liveness, unique per individual
Device	Possession (something you have)	Attested secure element on enrolled device, root_secret_hash stored in enclave	Cannot be cloned, hardware-bound, remotely revocable, attestation-verified
Passphrase	Knowledge (something you know)	Optional manual passphrase selects persona at authentication time	Not required for default persona, adds persona separation when used

The first two factors are always active. The user touches a sensor (biometric) on their enrolled device (possession). The root secret stored in the device's enclave is automatically appended. This is two-factor authentication with zero friction—the user perceives a single action (touch sensor) but the system applies two cryptographically independent factors.

When the user adds a manual passphrase, the system becomes three-factor. This is optional and typically used for persona selection or elevated security contexts.

3.2 Regulatory Compliance Mapping

Framework	Requirement	Bonafide Mapping	Compliance Status
NIST 800-63 AAL1	Single factor	Biometric alone exceeds	Exceeds
NIST 800-63 AAL2	Two distinct factors	Biometric (inherence) + attested device (possession)	Meets
NIST 800-63 AAL3	Hardware crypto + two factors + verifier impersonation resistance	Tier 1/S enclave + biometric + attestation; stateless derivation prevents verifier impersonation	Meets
PSD2 SCA	Two of: knowledge, possession, inherence	Biometric (inherence) + device (possession); optional passphrase (knowledge)	Meets
FIDO2 / WebAuthn	Authenticator + user verification	Device SE as authenticator, biometric as user verification	Architecturally aligned
HIPAA	Reasonable and appropriate	Per-quantum encryption, audit trail, hardware-bound biometric	Exceeds

	safeguards	auth	
PCI-DSS v4.0	Multi-factor for cardholder data access	Biometric + device attestation + security level enforcement	Exceeds

4. Authentication Flows

4.1 Daily Authentication (Touch and Go)

The user's most common interaction with Bonafide is daily device unlock and vault access:

- User touches biometric sensor (fingerprint) or presents face (Face ID).
- Secure element processes biometric, extracts template, generates biometric hash.
- Enclave retrieves stored root_secret_hash and appends it automatically.
- Manual passphrase is empty (default persona selected).
- Bio Root is computed: Hash(biometric || root_secret_hash || "").
- Branch keys are derived for active sessions. Vault is accessible.
- Bio Root and intermediate keys are destroyed. Only session keys persist for the session duration.

Total user effort: one touch. Total factors applied: two (biometric + device). Total time: under one second on modern hardware.

4.2 Persona Selection

When the user wants to access an alternate persona:

- User touches biometric sensor AND enters a manual passphrase.
- Bio Root is computed: Hash(biometric || root_secret_hash || passphrase).
- The resulting Bio Root is different from the default persona's Bio Root.
- The alternate persona's vault tree is loaded. Different branches, different institutions, different identity.

An observer cannot tell whether the user entered a passphrase or not. The authentication flow looks identical from the outside—the user interacts with their device and the vault opens. Which persona opened is known only to the user.

4.3 New Device Enrollment

- User initiates enrollment from an existing vault holder device (or through guest enclave if first device).
- New device performs hardware attestation, proving enclave tier.
- User authenticates biometrically on the new device.
- User performs root secret gestures manually (the new device doesn't have root_secret_hash yet).
- New device computes Bio Root and verifies against vault.
- root_secret_hash is stored in new device's enclave. Future authentications are touch-and-go.
- Device certificate is issued and registered with the network.

4.4 Guest Enclave (First-Time User)

A user with no existing vault creates one through the guest enclave flow:

- User's device performs hardware attestation.

- User provides biometric input and chooses root secret gestures.
- Bio Root is computed and a new vault is created.
- The user peers with their first institution (the bootstrap institution—typically the institution that introduced them to Bonafide).
- Multi-institutional validation over time strengthens the vault's web of trust.

5. Elevation and Step-Up

5.1 Level Elevation

Some operations require access to quanta at a higher security level than the current session's default. Rather than authenticating at the highest level for every session (which would impose unnecessary friction), Bonafide supports level elevation: temporarily upgrading the session's access ceiling.

5.2 Elevation Triggers

- The user or application requests access to a quantum above the session's current ceiling.
- An institution requests an operation that requires a higher security level (e.g., changing account settings vs. viewing a balance).
- A time-based policy requires re-authentication after a configured interval at the current level.

5.3 Elevation Flow

- The runtime determines the target level and its authentication requirements.
- The user is prompted for the additional authentication factor(s) required by the target level.
- For moderate elevation (e.g., Level 3 to Level 5): biometric re-confirmation on the same device.
- For significant elevation (e.g., Level 3 to Level 7): biometric re-confirmation + manual passphrase.
- For maximum elevation (to Level 8-9): biometric + root secret gesture re-entry + device re-attestation.
- Upon successful elevation, the session's ceiling is raised to the target level for a configurable duration (default: 15 minutes for Level 7+, 1 hour for Level 4-6).
- After the elevation duration, the session's ceiling reverts to its default.

5.4 Elevation Limits

Elevation cannot exceed the device's enclave tier ceiling. A Tier 3 device cannot elevate to Level 6+ regardless of how many authentication factors the user provides—the hardware cannot perform the key derivation.

6. Quantum-Level Override

6.1 Per-Quantum Security Assignment

Individual quanta can be assigned a security level that differs from their branch or channel's default. A single sensitive document in an otherwise routine branch can be elevated. The override is cryptographic—the quantum's DEK is derived at the overridden level's depth. A device or institution below the overridden level's requirements cannot access that quantum even if they access everything else in the branch.

6.2 Override Operations

- **Elevate:** Raise a quantum's level above the branch default. The DEK is re-derived at the new depth and the quantum is re-encrypted. Access from lower-tier devices or lower-classified institutions is immediately revoked for that quantum.
- **De-elevate:** Lower a quantum's level (within the branch's minimum floor). The DEK is re-derived at the new depth. Access is broadened.
- **Override audit:** Every override is recorded in the ledger with the old level, new level, the authorizing user or policy, and the timestamp.

6.3 Institutional Override

Institutions can request quantum-level overrides within their branch, subject to the user's authorization policy. A bank might auto-elevate quanta containing wire transfer authorizations to Level 4 while keeping balance queries at Level 2. These policies are configured during peering and enforced by the runtime.

7. Session Management

7.1 Session Types

Session Type	Authentication	Default Duration	Renewal
User device → vault	Biometric + root_secret (auto)	1 hour	Biometric re-confirmation
User device → elevated	Biometric + passphrase or gesture re-entry	15 min (Level 7+), 1 hour (Level 4-6)	Full re-authentication
Institution → runtime	Institutional certificate + runtime attestation	8 hours	Certificate re-validation
Third-party → shared data	Share key or verification key	Per authorization (seconds to days)	Not renewable (new authorization required)
Validator → federation	Validator certificate + trust score	24 hours	Automatic re-keying
Guest enclave	Device attestation only	24 hours	Must elevate to permanent or re-attest

7.2 Session Integrity

All sessions enforce the integrity mechanisms defined in Part 9:

- Request nonces: 128-bit cryptographic random per request, preventing replay.
- Monotonic sequence numbers: detecting dropped or reordered messages.
- TLS channel binding: session tokens bound to the TLS connection, preventing token theft.
- Concurrent session detection: the same session token appearing in two locations triggers immediate invalidation and alert.

7.3 Session Termination

Sessions terminate on: explicit user logout, duration expiration, device lock/sleep (configurable), network disconnection beyond a configurable timeout, detection of anomalous behavior (location change, device attestation failure), or revocation of any credential in the session's trust chain.

8. Duress Authentication

8.1 Purpose

Duress authentication allows a user who is being coerced to authenticate into a decoy persona that appears legitimate while protecting the real vault. This is specified in detail in Part 7. This section defines the security level interaction.

8.2 Duress and Security Levels

The duress persona has its own vault tree with its own branches, its own institutional peers, and its own security level assignments. From the perspective of the security level system, the duress persona is indistinguishable from any other persona. It has the same level architecture, the same enclave requirements, and the same session management. The coercing party sees a fully functional vault at whatever levels the duress persona was configured with.

8.3 Silent Alert

When duress authentication occurs, the vault can optionally trigger a silent alert to pre-configured contacts or authorities. The alert is sent through the relay network and does not produce any observable signal on the device. The coercing party sees a normal vault opening. The alert mechanism operates outside the security level system—it is a separate, parallel channel that does not affect key derivation or session management.

Bonafide™ — Privacy by architecture, not by promise.

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

V1.0 — February 2026