BONAFIDE™ SPECIFICATION V1.0 — PART 10

Enclave Architecture & Device Classes

Enclave tier system, device class profiles, peripheral model, biometric input across devices, server-class hardware for institutional deployments, cross-device synchronization, and device lifecycle

1. Purpose

This part defines the enclave architecture for both user devices and institutional servers: the hardware security requirements for participating in the Bonafide network, the enclave tier system, device class profiles, the peripheral device model, cross-device synchronization, device lifecycle management, and server-class hardware for institutional deployments.

2. Enclave Requirements

2.1 Core Properties

A Bonafide enclave provides four properties:

- **Isolated key storage:** Cryptographic keys stored within the enclave are not accessible to the host operating system, application software, or privileged users.
- **Isolated cryptographic computation:** Encryption, decryption, key derivation, and signing operations execute within the enclave. Intermediate values (plaintext keys, partial derivations) never appear in host-accessible memory.
- **Remote attestation:** The enclave can produce a cryptographic proof of its identity, configuration, and integrity that a remote verifier can check. Attestation proves the enclave is what it claims to be.
- **Tamper resistance:** Physical or logical attempts to extract key material from the enclave are detectable or prevented. The level of tamper resistance varies by tier.

2.2 Participation Models

Model	Enclave Role	Requirements	Examples
Vault holder	Computes Bio Root, derives branch keys, performs vault operations	Must have enclave for key isolation and biometric processing. Minimum Tier 4.	Phones, laptops, desktops, tablets
Peripheral	Produces or consumes data under delegated credentials	May have enclave (peripheral tiers P1–P3). Credentials scoped by vault holder.	IoT cameras, sensors, smart locks, medical monitors
Institutional server	Runs Bonafide runtime, manages institutional keys, performs bulk crypto	Enclave tier determines privacy classification (Part 11). Minimum: software-only.	Data center servers, cloud instances, edge appliances

3. Enclave Tier System

3.1 Five Tiers

Tier	Name	Hardware	Max Security Level	Tamper Resistance
S	FPGA / Dedicated SE	ExaForge FPGA, dedicated secure processor with PUF, side-channel hardening	Level 9 (Sovereign)	Physical + logical + side-channel
1	Dedicated Secure Element	Apple SEP, Google Titan M2, Samsung Knox, dedicated hardware SE	Level 8 (Critical)	Physical + logical
2	Trusted Execution Environment	Intel SGX/TDX, AMD SEV-SNP, ARM TrustZone, AWS Nitro Enclave	Level 7 (Classified)	Logical (hardware-attested isolation)
3	TPM / Basic Hardware	TPM 2.0, basic hardware key storage without full TEE	Level 5 (Protected)	Key storage only (limited computation)
4	Software Only	OS-level keychain, encrypted memory, no hardware isolation	Level 3 (Confidential)	None (software isolation only)

The tier determines the maximum security level a device can access. A Tier 3 device cannot access Level 6+ data regardless of the user's authentication. This is cryptographic enforcement: the key derivation for Level 6+ requires enclave capabilities that Tier 3 hardware does not possess.

3.2 Tier Determination

A device's tier is determined by its hardware attestation during enrollment. The Bonafide network verifies the device's attestation against known hardware roots of trust (Apple's attestation service, Google's key attestation, TPM manufacturer CAs). The tier is not self-reported—it is cryptographically verified.

4. Device Class Profiles

4.1 Mobile Devices

Device	Enclave Tier	Max Level	Biometric Input	Notes
iPhone (Face ID + SEP)	Tier 1	Level 8	3D face (strong) + optional finger	SEP provides dedicated SE. Best consumer enclave.
Pixel (Titan M2)	Tier 1	Level 8	Fingerprint (strong) + face	Titan M2 is independent secure processor.
Samsung Galaxy (Knox)	Tier 1	Level 8	Ultrasonic fingerprint + face	Knox provides hardware-backed SE.
Mid-range Android (TrustZone only)	Tier 2	Level 7	Optical fingerprint + 2D face	TrustZone TEE, no dedicated SE.
Budget Android (no SE/TEE)	Tier 4	Level 3	Basic fingerprint or face	Software-only. Limited vault capabilities.

4.2 Laptops and Desktops

Device	Enclave Tier	Max Level	Biometric Input	Notes
MacBook (Apple Silicon)	Tier 1	Level 8	Touch ID (strong)	Apple Silicon SE equivalent to SEP.
MacBook (Intel + T2)	Tier 2	Level 7	Touch ID via T2	T2 chip provides TEE-level isolation.
Windows (TPM 2.0 + SGX)	Tier 2	Level 7	Windows Hello (face/finger)	SGX provides TEE. TPM for key storage.
Windows (TPM 2.0 only)	Tier 3	Level 5	Windows Hello or external	TPM for key storage, no TEE.
Windows (no TPM)	Tier 4	Level 3	External biometric device	Software-only. Recommend external FIDO2.
Linux (TPM 2.0)	Tier 3	Level 5	External biometric device	TPM via tpm2-tools. External biometric.
Linux (no TPM)	Tier 4	Level 3	External biometric device	Software-only. External biometric required.

4.3 Other Devices

Device	Enclave Tier	Max Level	Role	Notes

iPad / Android tablet	Tier 1–2	Level 7–8	Vault holder	Same tier as phone equivalent
Chromebook	Tier 3–4	Level 3–5	Vault holder (limited)	Depends on TPM presence
Apple Watch / Wear OS	Tier 2	Level 7	Peripheral (biometric delegate)	Biometric input for paired phone
Raspberry Pi 5 + OP-TEE	Tier 2	Level 7	Personal vault server	OP-TEE provides TrustZone TEE
Raspberry Pi 5 + TPM HAT	Tier 3	Level 5	Personal vault server	TPM HAT for key storage
FIDO2 security key	Tier 2	Level 7	Enclave fallback	External SE for devices without built-in enclave

5. Peripheral Device Model

5.1 What Peripherals Are

Peripherals are devices that produce or consume Bonafide-protected data without holding vault keys. IoT cameras generate video quanta. Medical sensors generate vitals quanta. Smart locks consume access authorization quanta. Peripherals operate under delegated credentials from a vault holder, scoped to specific branches, channels, and operations.

5.2 Peripheral Tiers

Tier	Hardware	Credential Renewal	Max Level	Examples
P1	Dedicated secure element (e.g., ATECC608B)	90 days	Level 5	Medical monitors, high-security cameras, smart locks
P2	Encrypted storage, no SE	30 days	Level 3	Environmental sensors, basic cameras, smart home devices
P3	Minimal (no encryption at rest)	7 days	Level 1	Simple sensors, beacons, low-cost IoT

5.3 Peripheral Credential Delegation

- The vault holder enrolls the peripheral through a pairing flow (NFC tap, QR scan, Bluetooth pairing).
- The vault holder generates a delegated credential scoped to specific branch/channel/operations.
- The credential has a renewable lifetime (7–90 days depending on peripheral tier).
- The peripheral uses the credential to sign data it produces and to decrypt data it consumes.
- The vault holder can revoke the peripheral's credential at any time.

5.4 Peripheral Lifecycle

- **Pairing:** Vault holder establishes a trusted connection and issues the initial delegated credential.
- **Operation:** Peripheral produces or consumes data within its authorized scope.
- **Renewal:** Credential is automatically renewed before expiration if the vault holder and peripheral are reachable.
- **Decommissioning:** Credential is revoked. Peripheral's cached data (if any) becomes inaccessible. Factory reset recommended.

6. Biometric Input Across Devices

6.1 Modality Availability

Device Class	Fingerprint	Face	Iris	Voice	Multi-Modal Fusion
Flagship phone	Ultrasonic (strong)	3D structured light (strong)	Some models	Via microphone	Two strong modalities available
Mid-range phone	Optical (medium)	2D + IR (medium)	Rare	Via microphone	Two medium modalities
MacBook	Touch ID (strong)	No	No	Via microphone	One strong + one medium
Windows laptop	Some models	Windows Hello IR (medium)	No	Via microphone	Varies by model
Linux desktop	External USB	External USB	External USB	Via microphone	Requires external devices
Raspberry Pi	External USB	External USB camera	No	Via microphone	Requires external devices

6.2 Multi-Modal Requirements

Vault holders require a minimum of two biometric modalities (one strong or two medium). Devices that cannot meet this requirement through built-in sensors can use external biometric peripherals (USB fingerprint readers, external cameras with IR) to reach the required modality count.

6.3 External Biometric Devices

External biometric devices (USB fingerprint readers, standalone iris scanners) must be certified through the Bonafide Device Certified program. Certification verifies that the device performs biometric processing in its own secure element (not on the host CPU), provides liveness detection, and does not retain biometric data after template extraction.

7. Server-Class Hardware

This section defines the hardware landscape for institutional Bonafide deployments. The Bonafide runtime's Hardware Abstraction Layer (Part 12, Section 11) maps these hardware platforms to privacy classifications.

7.1 FPGA Enclaves (Classification S)

ExaForge FPGA and equivalent dedicated cryptographic processors provide the highest isolation tier. Keys are stored in physically unclonable functions (PUFs). All cryptographic operations execute in FPGA fabric. Plaintext never exists in host-accessible memory. Side-channel hardening (constant-time operations, power analysis resistance) is mandatory. This is the only hardware class that achieves Classification S.

7.2 GPU Acceleration

NVIDIA CUDA GPUs accelerate specific Bonafide operations:

- **Bulk AES-256-GCM:** Hundreds of gigabytes per second across thousands of concurrent streams. Ideal for initial vault population, bulk migration, and re-encryption during key rotation.
- **ZK proof generation:** GPU parallel arithmetic accelerates polynomial and number-theoretic transforms required for SNARK/STARK generation.
- **Merkle tree computation:** Massively parallel leaf hashing and bottom-up tree construction.

Standard GPUs are not secure enclaves (keys in GPU memory are host-accessible). NVIDIA H100 with Confidential Computing mode provides TEE-equivalent isolation, enabling Classification A with GPU acceleration.

7.3 SmartNICs and DPUs (Classification A)

NVIDIA BlueField, AMD Pensando, and Intel IPU provide programmable network processors with isolated ARM cores and dedicated crypto engines. The Bonafide runtime runs entirely on the DPU, isolated from the host OS. The host server never sees keys or plaintext. This achieves Classification A at lower cost than FPGA and with standard server hardware.

7.4 HSMs (Classification B+)

Hardware Security Modules (Thales Luna, Entrust nShield, AWS CloudHSM) provide FIPS 140-3 certified key storage and cryptographic operations. HSMs are natural homes for institutional master keys. The HSM stores keys and performs wrapping/unwrapping; bulk encryption is offloaded to the CPU or an accelerator card. HSM + accelerator combinations achieve Classification B; HSM within a TEE context can approach Classification A.

7.5 Cloud TEE Instances (Classification A)

AWS Nitro Enclaves, Azure Confidential VMs (AMD SEV-SNP), and GCP Confidential VMs provide hardware-attested TEE environments in the cloud. An institution running the Bonafide runtime in a Nitro Enclave achieves Classification A using only cloud infrastructure—no on-premises hardware required. This is the lowest-barrier path to Classification A for cloud-native institutions.

7.6 Crypto Accelerator Cards (Classification B)

Intel QuickAssist Technology (QAT) and similar PCIe accelerators offload AES-GCM and hash operations at line rates up to 400 Gbps. These are throughput accelerators, not security enclaves. Combined with HSM or TPM for key storage, they provide Classification B with high-performance bulk encryption.

8. Cross-Device Vault Synchronization

8.1 Per-Device Key Derivation

Every enrolled device derives the same Bio Root (because every enrolled device has the same root_secret_hash in its enclave and the user provides the same biometric). Therefore, every enrolled device produces the same branch keys and can access the same data. There is no device-specific key at Level 1—this is critical for institutional interoperability (institutions expect the same branch key regardless of which device the user authenticates from).

8.2 Tier-Aware Sync

Not all devices can access all data. A Tier 3 laptop cannot access Level 6+ quanta. The synchronization layer is tier-aware: it replicates only quanta that the target device's enclave tier can access. A Tier 3 device never receives ciphertext for Level 6+ quanta because it cannot derive the keys to decrypt them.

8.3 Conflict Resolution

When the same quantum is modified on two devices simultaneously (offline scenario), the conflict is resolved by last-writer-wins with ledger arbitration. The ledger timestamp determines which write is canonical. The losing write is preserved as a version history entry accessible to the user.

8.4 Offline Operation

Vault holder devices can operate offline with locally cached data. The cache contains only quanta at or below the device's tier ceiling. Offline operations are queued and synchronized when connectivity is restored. Re-authentication windows are configurable: the device can operate offline for a configured duration (default: 24 hours for Level 0–3, 4 hours for Level 4–5) before requiring biometric re-confirmation.

9. Device Lifecycle

9.1 Enrollment

- New device performs hardware attestation, establishing its enclave tier.
- User authenticates biometrically and performs root secret gestures (for new devices).
- root_secret_hash is stored in the new device's enclave.
- Device certificate is issued by ca.bonafide.id.
- Device begins tier-aware sync of cached vault data.

9.2 Deauthorization

- User initiates deauthorization from any other vault holder device.
- The target device's certificate is revoked.
- All sessions from the target device are terminated.
- The device's local cache is marked for destruction (next power-on erases cached vault data).
- root_secret_hash in the device's enclave is marked for destruction.

9.3 Loss / Theft Recovery

- User deauthorizes the lost/stolen device from any remaining vault holder device.
- If no other vault holder device exists, the user initiates recovery through the guest enclave flow: biometric + root secret gestures + multi-institutional validation to elevate to permanent vault holder.
- The lost device's cached data is inaccessible without biometric authentication. The root_secret_hash in the enclave is protected by the SE and cannot be extracted.
- Even if the attacker bypasses the device lock, they lack the user's biometric. Even if they spoof the biometric, the root_secret_hash combined with their spoofed biometric produces the wrong Bio Root (the attacker doesn't know this—the system produces a valid-looking key that decrypts nothing).

9.4 Device Upgrade

When a user replaces a device (new phone, new laptop), the upgrade path is: enroll the new device (attestation + biometric + root secret gestures), verify the new device accesses the vault correctly, deauthorize the old device. The new device's tier may differ from the old device's tier, which may change the user's maximum accessible security level. The user is notified if the new device has a lower tier than the old one.