BONAFIDE™ SPECIFICATION V1.0 — PART 5

Blind Validation Network

Zero-knowledge validation, proof system, trust scoring with bootstrapping, validator selection diversity, Byzantine fault tolerant consensus, Sybil resistance, and validator operations

1. Purpose

This part defines the blind validation network: a distributed system of independent validator nodes that verify Bonafide operations without seeing the data being validated. Validators confirm quantum integrity, verify access authorization, maintain trust scores, and provide the consensus mechanism that prevents any single entity—including Sly Technologies—from controlling the network.

2. Blind Validation Principle

2.1 What Validators See

Validators see cryptographic proofs, not data. When an operation is submitted for validation (a quantum write, an access authorization, a third-party key generation), the validator receives a zero-knowledge proof that the operation is authorized, correctly formed, and consistent with the vault's state—without learning what the data is, who the user is, or what institution is involved.

2.2 What Validators Verify

Operation	Validator Checks	Validator Does NOT See
Quantum write	Proof that the writer holds a valid key for the target branch/channel/level, Merkle consistency	Quantum payload, user identity, institution identity
Quantum read	Proof that the reader holds a valid key for the quantum's level, session validity	Quantum payload, what was read, who read it
Access authorization	Proof that the authorization is well-formed, scope is valid, duration is within policy	What data is being authorized, who the third party is
Key generation (3rd party)	Proof that the legal instrument hash is valid, authority is registered, scope is bounded	Instrument content, target user, accessing authority
Revocation	Proof that the revoking party holds the user key, scope is valid	What is being revoked, which institution
Trust score update	Behavioral metrics from ledger hashes, attestation results	Specific operations that generated the metrics

2.3 Why Blind Validation Matters

If validators could see the data or metadata they validate, the validation network would become a surveillance infrastructure. Every operation across the entire Bonafide ecosystem would flow through validators who could build complete profiles of every user's activity. Blind validation prevents this by design: validators are essential to the network's security but structurally unable to learn anything about the users or data they protect.

3. Zero-Knowledge Proof System

3.1 Proof Types

The Bonafide specification uses several ZK proof constructions depending on the operation:

- **Authorization proofs:** Prove that a key holder is authorized for a specific operation at a specific security level without revealing the key or the operation's content. Based on ZK-SNARKs for compact proof size and fast verification.
- **Merkle inclusion proofs:** Prove that a quantum exists in a branch's Merkle tree at a specific position without revealing the tree's structure or other quanta. Standard Merkle path proof with ZK wrapping.
- **Range proofs:** Prove that a value (trust score, duration, security level) falls within an acceptable range without revealing the exact value. Based on Bulletproofs for efficiency.
- **Set membership proofs:** Prove that an authority belongs to the set of registered authorities without revealing which authority. Used for third-party access validation.
- **Consistency proofs:** Prove that a new Merkle root is a valid extension of the previous root (append-only, no deletions except tombstones). Used for ledger integrity.

3.2 Proof Generation

Proofs are generated by the Bonafide runtime on the institution's infrastructure (for institutional operations) or on the user's device (for user-initiated operations). The proof generator has access to the actual data and keys; it produces a proof that validators can verify without that access.

Proof generation is computationally expensive—particularly ZK-SNARK generation, which involves polynomial arithmetic and number-theoretic transforms. The specification supports hardware acceleration:

- **GPU acceleration:** ZK proof generation maps well to GPU parallel arithmetic. CUDA-capable GPUs (NVIDIA A100, H100) can generate proofs at orders of magnitude higher throughput than CPU-only generation. Institutional deployments with high validation volume should use GPU acceleration.
- **FPGA acceleration:** ExaForge FPGA fabric can generate proofs within the enclave, keeping proof inputs (keys, data) in hardware-isolated memory throughout generation.
- **CPU fallback:** Software-only proof generation is supported for low-volume deployments and user devices. Performance is adequate for individual operations but not for institutional batch processing.

3.3 Proof Verification

Verification is fast—orders of magnitude faster than generation. A ZK-SNARK proof that takes 500ms to generate verifies in under 5ms. This asymmetry is critical: the expensive work happens at the proof generator (institution or device) while validators perform cheap verification at high throughput.

4. Trust Scoring

4.1 Purpose

Every participant in the Bonafide network—validators, institutions, relay operators—has a trust score. The trust score is a behavioral assessment derived from the participant's operational history. It is distinct from privacy classification (Part 11), which measures structural protection. Trust scoring measures how reliably and honestly the participant behaves over time.

4.2 Validator Trust Score

Validators earn trust through consistent correct behavior:

Behavior	Trust Impact	Detection
Correct proof verification (agrees with consensus)	Positive (gradual increase)	Consensus comparison
Incorrect proof verification (disagrees with consensus)	Negative (significant decrease)	Consensus comparison
High uptime, consistent availability	Positive (gradual)	Heartbeat monitoring
Downtime or unreachability	Negative (proportional to duration)	Heartbeat monitoring
Fast response time	Positive (minor)	Response latency metrics
Slow response or timeout	Negative (minor)	Response latency metrics
Attestation current and valid	Neutral (required baseline)	Continuous attestation
Attestation expired or failed	Negative (severe, immediate)	Continuous attestation

4.3 Score Range and Thresholds

Trust scores range from 0 to 1000. New validators enter at 100 (probationary). Thresholds:

Score Range	Status	Selection Frequency	Capabilities
0–49	Suspended	Never selected	Must re-certify to resume
50–199	Probationary	Rarely selected, low-sensitivity operations only	Limited to routine validations
200–499	Operational	Normal selection frequency	All operation types
500–799	Trusted	Preferential selection	All operations + consensus leadership eligibility

800–1000	Established	Highest selection frequency	All operations + consensus leadership + trust anchor for new validators

4.4 Trust Score Bootstrapping

New validators face a cold-start problem: they have no history to earn trust. The bootstrapping path:

- **Certification:** The validator passes the Bonafide Validator Certified program (Part 8). This proves infrastructure capability, not behavioral trust. Entry score: 100.
- **Probationary period:** Minimum 90 days. The validator is selected infrequently and only for low-sensitivity operations. Each correct validation increments the score.
- **Mentorship:** An established validator (score 800+) can vouch for a new validator, increasing its initial selection frequency during probation. The mentor’s score is partially at risk—if the new validator misbehaves, the mentor’s score is also penalized.
- **Graduation:** When the validator’s score crosses 200, it exits probation and enters normal operation. Typical time: 90–180 days with consistent correct behavior.

5. Validator Selection

5.1 Selection Algorithm

When an operation requires validation, the network selects a committee of validators. The selection algorithm balances trust (higher-scored validators are preferred) with diversity (no single organization, geography, or network can dominate the committee).

5.2 Diversity Constraints

- **Organizational diversity:** No two validators from the same organization on the same committee.
- **Geographic diversity:** Validators drawn from at least two distinct geographic regions per operation.
- **Network diversity:** No more than one validator per autonomous system (ASN) per committee.
- **Score-weighted random:** Within the diversity constraints, selection is weighted by trust score. Higher-scored validators are more likely to be selected but not guaranteed.
- **Minimum slot allocation:** A configurable percentage of committee slots (default: 10%) are reserved for probationary validators, ensuring new validators have opportunity to build scores.

5.3 Committee Size

Committee size scales with operation sensitivity:

Operation Type	Committee Size	Consensus Threshold
Routine read/write (Level 0–3)	3 validators	2 of 3 agree
Sensitive operations (Level 4–6)	5 validators	3 of 5 agree
Critical operations (Level 7–9)	7 validators	5 of 7 agree
Third-party key generation (legal)	9 validators	6 of 9 agree
Network-wide events (key ceremony, root rotation)	11+ validators	Two-thirds supermajority

6. Consensus Protocol

6.1 Byzantine Fault Tolerance

The validation network uses a Byzantine fault tolerant (BFT) consensus protocol. The network operates correctly as long as fewer than one-third of committee validators are malicious or faulty. With a committee of 9, up to 2 can be compromised without affecting the operation's outcome.

6.2 Consensus Flow

- The operation's proof is distributed to all committee members simultaneously.
- Each validator independently verifies the proof and produces a signed vote (valid or invalid).
- Votes are collected by the consensus coordinator (the highest-scored committee member).
- When the consensus threshold is reached, the result is finalized and signed by all agreeing validators.
- The consensus result is returned to the requesting party and recorded in the ledger.
- Dissenting validators' votes are recorded. Persistent dissent (disagreeing with consensus more than 5% of the time) degrades the dissenter's trust score.

6.3 Consensus Timing

Target consensus latency by operation type:

- Routine operations: under 200ms (validators are geographically distributed, network latency dominates).
- Sensitive operations: under 500ms (larger committee, more verification steps).
- Critical operations: under 2 seconds (largest committees, additional verification).
- Third-party key generation: under 5 seconds (instrument validation adds overhead).

6.4 Consensus Communication Security

Inter-validator communication uses the same mTLS foundation as all Bonafide traffic (Part 9). Additional constraints:

- Consensus messages are signed with the validator's certification key (non-repudiation).
- Ephemeral keys are generated per consensus round (forward secrecy).
- Validators communicate through the federation layer, not directly peer-to-peer.

7. Sybil Resistance

7.1 Threat

A Sybil attack involves an adversary operating many validator nodes to gain disproportionate influence over consensus outcomes. If an attacker controls one-third of a committee, they can prevent consensus. If they control two-thirds, they can forge consensus.

7.2 Defenses

- **Certification cost:** Each validator must pass the Bonafide Validator Certified program, requiring infrastructure audit, operational demonstration, and a fee. Certifying 50 validators costs 50 times the fee with 50 times the infrastructure.
- **Probationary period:** New validators start at score 100 and are selected infrequently for 90+ days. An attacker deploying 50 validators waits 90 days before they participate meaningfully.
- **Organizational diversity:** The selection algorithm limits each organization to one committee slot. Fifty validators under one organization get one slot, not fifty.
- **Diminishing returns:** Adding validators under the same organization, geography, or network does not increase selection frequency beyond the per-category cap.
- **Ongoing cost:** Validators must maintain infrastructure, pass annual re-certification, and sustain uptime SLAs. Dormant validators lose score and drop below selection thresholds.
- **Mentorship risk:** If an established validator vouches for a Sybil node and the node misbehaves, the mentor’s score is penalized. This creates social accountability within the validator community.

7.3 Economic Analysis

For an attacker to control one-third of a 9-validator committee, they need at least 3 validators from different organizations, geographies, and ASNs—each certified, each probationary for 90 days, each requiring real infrastructure. The cost in certification fees, infrastructure, and time vastly exceeds the value of corrupting a single validation operation. The attack does not scale: controlling one committee does not help with any other committee because selection is randomized per operation.

8. Validator Operations

8.1 Validator Infrastructure Requirements

Requirement	Minimum	Recommended
CPU	8 cores, modern x86 or ARM	16+ cores with AES-NI
Memory	32 GB	64+ GB
Storage	1 TB SSD	2+ TB NVMe
Network	1 Gbps symmetric, static IP	10 Gbps, redundant uplink
Uptime SLA	99.5%	99.9%+
TLS termination	Software	Hardware accelerated (QAT or HSM)
ZK verification	CPU	GPU accelerated (recommended for high-volume)
Attestation	Software environment report	TEE or FPGA attestation

8.2 Validator Revenue Model

Validators earn fees for validation operations. Fees are proportional to operation complexity and the validator’s trust score (higher-scored validators earn slightly higher fees as compensation for their demonstrated reliability). The fee structure is defined by the ecosystem governance (Part 8) and adjusted periodically based on network economics.

8.3 Validator Certification Lifecycle

- Initial certification: infrastructure audit, operational demonstration, fee payment. Entry at score 100.
- Annual re-certification: re-audit, updated infrastructure verification, continued fee.
- Score maintenance: consistent correct validation, uptime, attestation currency.
- Suspension: score drops below 50 due to misbehavior, downtime, or attestation failure. Must re-certify.
- Voluntary exit: validator notifies the network, completes pending validations, and gracefully departs. Score is preserved for 12 months in case of return.

Bonafide™ — Privacy by architecture, not by promise.

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