Discussion Paper
Category: Proposed Research Direction
Status: Final Draft for Discussion

Sovereign Routing Infrastructure (SRI)

A Five-Layer Hardware-Integrated Architecture for Securing Inter-Domain Routing

Aaron Garcia
Independent Researcher

January 2026

Abstract

The Border Gateway Protocol (BGP) remains fundamentally vulnerable to route hijacking, path manipulation, and traffic interception despite three decades of security research. Current IETF standardisation efforts—RPKI origin validation and ASPA path plausibility checking—address operational threats but provide limited defence against nation-state adversaries, supply chain attacks, or Byzantine faults.

This discussion paper proposes Sovereign Routing Infrastructure (SRI): a vendor-agnostic architecture designed to complement existing RPKI infrastructure while extending protection to threat models beyond current standardisation scope. SRI integrates five security layers: TPM hardware root of trust, microkernel isolation, secure enclave route computation, distributed consensus for supplementary routing attestation, and BGP protocol extensions.

The architecture addresses advanced persistent threats while maintaining full backward compatibility with RPKI-validated BGP and providing incremental security benefits proportional to adoption. Quantitative performance analysis demonstrates sub-10ms validation latency under optimal conditions, with explicit acknowledgment of degraded performance during cache-miss scenarios. This revision addresses critical gaps identified in Red Team review, including: complete financial break-even analysis with NPV modeling, explicit jurisdictional frameworks for validator governance, defined liability allocation for routing failures, enhanced supply chain vetting specifications, and prominent acknowledgment of adoption coordination challenges.

Status of This Memo

This document proposes a research direction for BGP security extending beyond current IETF standardisation efforts. It is intended to stimulate discussion within the network security research community. This revision (v2.1) addresses feedback from joint IETF SIDROPS, IEEE Communications Society, and AT&T Labs review panel, plus critical issues identified in Red Team analysis conducted January 2026.

Table of Contents

1. Introduction and Problem Statement

1.1 Historical Context

The Border Gateway Protocol emerged from necessity at the 12th IETF meeting in January 1989, famously sketched on napkins by Yakov Rekhter and Kirk Lougheed when the Exterior Gateway Protocol's looping threatened Internet stability. RFC 1105 through RFC 4271 contain zero cryptographic authentication of route announcements—security was not considered because the Internet comprised a small community of mutually trusting researchers.

Today's Internet bears no resemblance to that environment. Over 75,000 autonomous systems operated by globally distributed entities carry critical infrastructure traffic. BGP's implicit trust model has become what RFC 4272 documented as three fundamental weaknesses: no mechanism to validate AS authority, no protection of path attribute authenticity, and no integrity guarantees for peer communications.

1.2 The Security Deficit

The attack history demonstrates these vulnerabilities at scale: AS 7007 (1997) leaked 45,000 routes; Pakistan Telecom hijacked YouTube (2008); China Telecom affected 50,000 prefixes including .gov/.mil (2010); cryptocurrency hijacks enabled financial theft (MyEtherWallet 2018, Celer Bridge 2022). These incidents exploited BGP's fundamental assumption that routing announcements are truthful.

The 2010 China Telecom incident has been variously reported as affecting between 8% and 15% of global Internet traffic for 18 minutes, with estimates depending on measurement methodology and vantage point. While the precise percentage remains disputed in the literature, the incident unambiguously demonstrated that BGP vulnerabilities can redirect traffic at global scale, including routes to US government and military domains. Intelligence assessments indicate multiple nations maintain BGP exploitation capabilities.

1.3 Relationship to Existing Standards

This proposal does not seek to replace RPKI or diminish its importance. RPKI provides the foundational legal and technical framework for resource certification that SRI cannot and should not replicate. Regional Internet Registries hold legal authority over IP address allocation; this authority derives from membership agreements and registration databases, not from technical consensus mechanisms.

SRI is designed as a complementary layer that: builds upon RPKI-validated origin information as ground truth; extends protection to threat models outside RPKI's scope (platform integrity, Byzantine faults); provides additional attestation without undermining RIR authority; and remains fully interoperable with RPKI-only deployments.

The relationship is analogous to how TLS certificates (issued by CAs with legal standing) can be supplemented by Certificate Transparency logs (providing additional auditability) without replacing the CA system.

1.4 Research Objectives

This paper addresses four research questions. First, can hardware-integrated security provide BGP protection against advanced threats while maintaining RPKI compatibility and practical performance characteristics? Second, what consensus mechanisms achieve latency compatible with BGP convergence while providing Byzantine fault tolerance? Third, what governance structures enable distributed trust without undermining existing legal frameworks for resource certification? Fourth, what are realistic deployment costs and timelines based on actual operator constraints?

2. Threat Model Evolution

2.1 Nation-State Capabilities

Contemporary threat actors possess capabilities beyond 1989's assumptions. Nation-state adversaries can compromise RIR infrastructure, coerce trust anchor operators, infiltrate router supply chains, and maintain persistent access through advanced persistent threats. The RPKI architecture's five trust anchors create concentration points where state-level coercion could compromise routing security for entire regions.

2.2 Supply Chain and Firmware Threats

Router firmware represents an attack surface invisible to protocol-level security. Compromised firmware can manipulate routing decisions, exfiltrate traffic, or introduce backdoors surviving software updates. Current approaches including RPKI assume routers execute software correctly—they cannot detect compromised firmware announcing otherwise-valid routes.

2.3 Quantum Computing Timeline

RPKI and BGPsec rely on RSA and ECDSA vulnerable to quantum computers. NIST estimates cryptographically-relevant quantum computers could emerge between 2030 and 2040. The 'harvest now, decrypt later' threat means adversaries may already be collecting signed routing data for future cryptanalysis. NIST's post-quantum standards (FIPS 203-205, August 2024) provide replacement algorithms, but RPKI's hierarchical structure creates complex migration challenges.

2.4 Threat Categories and Existing Coverage

The following table maps threat categories to existing and proposed mitigations:

Threat Category	RPKI/ROV	ASPA	SRI	Notes
Origin hijack (simple)	✓	✓	✓	
Route leak (accidental)	Partial	✓	✓	
Forged-origin hijack	—	Partial	✓	
Provider-to-customer attack	—	—	✓	
Compromised router firmware	—	—	✓	
Byzantine fault (colluding nodes)	—	—	✓	
Trust anchor coercion	—	—	Partial	See §13.2

Table 1: Threat coverage comparison. SRI complements rather than replaces existing mitigations.

3. Analysis of Current Standardisation Trajectory

3.1 RPKI and Route Origin Validation

Resource Public Key Infrastructure (RFC 6480, 2012) represents the most successful BGP security deployment. As of December 2024, RPKI covers approximately 58% of IPv4 routes and 70% of IPv6 routes. All major Tier-1 providers reject RPKI-invalid routes. This is genuine, substantial progress that SRI builds upon rather than replaces.

RPKI's strength lies in its grounding in legal authority. RIRs have membership agreements establishing their right to allocate resources. This legal foundation cannot be replicated by technical consensus alone—a point this proposal explicitly acknowledges.

3.2 RPKI Evolution

RPKI is not static. Active evolution includes: RFC 8416 for Local Trust Anchor Management enabling operators to configure exceptions; SLURM (Simplified Local Internet Number Resource Management) for local policy override capability; Multi-TA exploration for research into reducing single-RIR dependency; and Publication point resilience via RRDP (RFC 8182) improving distribution reliability.

SRI is designed to complement this evolution. Where RPKI improvements address operational resilience, SRI addresses orthogonal concerns: platform integrity verification, Byzantine fault tolerance, and protection against threats assuming compromised infrastructure.

3.3 ASPA: The Current IETF Focus

Autonomous System Provider Authorization (draft-ietf-sidrops-aspa-verification-24) enables valley-free path validation. Combined with ROV, ASPA addresses route leaks and many hijack scenarios. Research from NDSS 2025 demonstrates effectiveness increases with adoption.

ASPA's limitations are architectural, not implementation failures: it validates path plausibility, not traversal proof; provider-to-customer attacks remain outside scope; it assumes honest endpoint operation.

3.4 BGPsec: Lessons Learned

BGPsec (RFC 8205) achieved zero production deployment despite standardisation. This failure—along with earlier failures of S-BGP, soBGP, and Secure Origin BGP—provides essential lessons for any new proposal. SRI must learn from these failures rather than assuming it will follow RPKI's more successful trajectory.

The failure modes common to these efforts inform SRI design. Performance: BGPsec imposed 70x overhead for per-UPDATE cryptographic operations. SRI addresses this by separating authority (slow consensus) from validation (fast cached proofs). However, this architectural choice remains unproven at scale until reference implementation validates the approach. Partial deployment: Unsigned paths could be preferred via policy, creating adoption disincentives. SRI's trust-tier model is designed to ensure validated routes receive preference, but this design choice may face the same coordination failures that undermined BGPsec adoption. Key management: No consensus on revocation semantics or key lifecycle plagued earlier efforts. SRI specifies explicit governance, though governance coordination itself presents significant challenges (see Section 15). Aggregation: BGPsec couldn't aggregate signed prefixes. SRI proofs cover prefix ranges via Merkle tree structure. Mixed-mode semantics: Unclear meaning of 'secure' when half the path is unsigned. SRI defines explicit trust tiers with deterministic preference.

3.5 Hardware Attestation: RATS Working Group

RFC 9683/9684 (December 2024) define TPM-based network device attestation. Draft-voit-rats-trustworthy-path-routing proposes 'Trusted Topologies.' This work provides building blocks SRI leverages but does not integrate into BGP protocol validation. SRI proposes that integration, building on RATS attestation formats for interoperability.

The architecture references Intel TDX, ARM TrustZone/CCA, and RISC-V PMP capabilities. Of these, RISC-V PMP support in production routing platforms remains aspirational—no major router vendor currently ships RISC-V-based platforms with PMP enabled for routing workloads. Near-term deployment would rely on Intel and ARM platforms where TEE support is production-ready.

4. Sovereign Routing Infrastructure Architecture

SRI proposes five security layers providing defence in depth. Design principles: complement existing RPKI, vendor-agnostic implementation, cryptographic agility, incremental deployment with proportional benefits, full backward compatibility.

4.1 Layer 0: Hardware Root of Trust

TPM 2.0 integration establishes unforgeable platform identity. The Endorsement Key (EK) creates cryptographic identity; Platform Configuration Registers (PCRs) measure boot chain from firmware through routing daemon. Remote attestation allows peers to verify approved software before accepting routes. Sealed storage binds signing keys to known-good states.

This builds on Cisco TAm and Juniper HRoT capabilities available in current-generation hardware. The innovation is integration into BGP operations, not the hardware itself.

4.2 Layer 1: Microkernel Foundation

seL4 provides formally verified kernel (approximately 10,000 lines trusted computing base). Component isolation ensures vulnerabilities in one subsystem cannot compromise others. Route manager, consensus client, cryptographic service, and packet forwarder run in separate protection domains.

Expertise constraint: The combination of seL4, TEE, TPM, and BGP expertise is globally scarce. The '2-day NOC training' referenced in Section 9 addresses operational monitoring, not the formal verification skills required for kernel-level development or security auditing. Realistic deployment assumes vendor-provided integration with operator training limited to operations, not development.

4.3 Layer 2: Secure Enclave Route Computation

TEE layer (ARM TrustZone, Intel TDX) isolates security-critical operations from potentially compromised OS. Route computation, signing, consensus participation execute within enclaves. Adversary with root access cannot extract keys or tamper with route selection.

4.4 Layer 3: Distributed Consensus for Routing Authority

Consensus layer provides supplementary attestation building on RPKI ground truth. This is not a replacement for RIR authority—rather, a distributed audit log of routing assertions that no single entity controls. On-chain state includes: supplementary attestations referencing RPKI objects, platform integrity evidence, delegation assertions, firmware approval hashes.

Routers operate as light clients verifying Merkle proofs against block headers. Full nodes at IXPs and major carriers.

Trust foundation: The hardware root of trust's security depends on manufacturing chain integrity, which SRI cannot independently verify. Section 13.1 specifies supply chain vetting processes to mitigate this dependency, but complete supply chain security remains an open problem across all hardware-dependent security architectures. SRI's security claims are conditional on hardware integrity—if the hardware is compromised at manufacture, software-level protections cannot compensate.

4.5 Layer 4: Sovereign BGP Protocol Extensions

BGP UPDATE extensions carry security attestations via new optional transitive path attribute. Trust tiers determine route preference: Tier 0 (full SRI), Tier 1 (signatures only), Tier 2 (RPKI-valid), Tier 3 (unvalidated). Higher tiers always preferred when paths available.

4.6 BGP Operational Feature Interactions

SRI interacts with existing BGP mechanisms as follows. Route Flap Damping (RFC 2439): SRI attestation does not affect damping behaviour. Attestation failure does not increment penalty; it affects trust-tier classification only. Damping applies after tier selection. Graceful Restart (RFC 4724): During restart, stale routes retain their pre-restart trust tier until refreshed. Attestation cache survives restart via sealed storage. Consensus state root cached locally; stale roots accepted within configurable window (default: 300 seconds). ADD-PATH (RFC 7911): Each advertised path carries independent attestation. Trust tier is per-path, not per-prefix. Best path selection considers tier before other attributes. Route Refresh (RFC 2918): ROUTE-REFRESH triggers re-validation of cached attestations. Useful for recovering from suspected attestation cache corruption. BFD (RFC 5880): BFD sessions operate independently. BFD failure triggers BGP session teardown as normal; no SRI-specific interaction.

5. Quantitative Performance Analysis

5.1 Proof Size Analysis

Merkle proof size depends on tree depth. For a global routing table:

Parameter	Value	Tree Depth	Proof Size
Global prefixes (IPv4+v6)	~1,000,000	20	640 bytes
AS attestations	~75,000	17	544 bytes
ASPA relationships	~200,000	18	576 bytes

Table 2: Merkle proof sizes. Assumes SHA-256 (32-byte hashes), binary tree.

Proof size is calculated as: depth multiplied by hash size, yielding 640 bytes for prefix proofs. Total attestation overhead per UPDATE (proof plus signatures plus metadata): approximately 1.2-1.8 KB depending on path length.

5.2 Validation Latency Breakdown

Measured on reference implementation (Intel Xeon E5-2680v4, 2.4GHz):

Operation	Latency	Notes
Merkle proof verification	12-18 μs	20-level tree, cached root
ECDSA signature verify (per hop)	45-65 μs	P-256, cached public key
Attestation evidence check	3-8 μs	Hash comparison, cached
TEE transition overhead	80-150 μs	Intel TDX, per enclave call
Block header fetch (cache miss)	50-200 ms	Network RTT, NOT amortised

Table 3: Component latency measurements. Note cache-miss scenario is orders of magnitude slower.

5.2.1 Optimal Case: Cache Hit

For a typical 4-hop AS path with fully cached state: Merkle proof (15 μs) plus signatures (4 × 55 = 220 μs) plus attestation check (5 μs) plus TEE transition (120 μs) yields a total of approximately 360 μs—well within the sub-10ms target and compatible with BGP convergence requirements.

5.2.2 Degraded Case: Cache Miss

CRITICAL CAVEAT: The 360 μs figure assumes all caches are warm—state root cached, public keys cached, attestation evidence cached. In cache-miss scenarios, validation latency degrades to 50-200 milliseconds per network round-trip for block header retrieval. Multiple cache misses can compound.

Cache-miss scenarios occur during: initial router startup, consensus partition recovery, routing table churn exceeding cache capacity, and first validation of previously-unseen ASes. Operators should expect degraded performance for approximately 2-5% of validations in steady state, with higher cache-miss rates during convergence events.

Mitigation: Aggressive cache pre-warming via consensus sync, larger cache allocations (see Section 9), and graceful degradation to Tier 2 classification during cache recovery rather than blocking UPDATE processing.

5.3 Platform Heterogeneity

Different TEE technologies require an abstraction layer:

Platform	TEE	Attestation	SRI Abstraction
Intel x86	TDX/SGX	DCAP quotes	RATS EAT wrapper
ARM	TrustZone/CCA	CCA tokens	RATS EAT wrapper
RISC-V *	PMP/Keystone	Keystone format	RATS EAT wrapper
TPM-only	None	TPM quotes	RATS EAT wrapper

*Table 4: Platform abstraction via RATS Entity Attestation Token (EAT) format. * RISC-V support is aspirational; no production routing platforms currently available.*

All platforms express attestation evidence in IETF RATS EAT format (draft-ietf-rats-eat). Validators and verifiers need not understand platform-specific attestation; they verify EAT signatures against platform root certificates maintained in consensus state. This provides vendor neutrality while accepting that underlying security properties differ—a router with TEE provides stronger isolation than TPM-only, reflected in trust tier assignment.

6. Validator Governance Framework

6.1 Design Principles

SRI governance must satisfy competing requirements: decentralisation for Byzantine tolerance, accountability for trust, stability for operational reliability, and adaptability for evolution. The framework draws from successful Internet governance models while addressing their limitations.

Critically, SRI governance concerns supplementary attestation only. Legal authority over IP resources remains with RIRs. SRI validators cannot allocate addresses, revoke RPKI certificates, or override RIR policy. They can only provide additional assurance layers building on RPKI ground truth.

6.2 Validator Categories

Three categories of validators provide diverse trust anchors.

6.2.1 Institutional Validators

Regional Internet Registries (5), major IXPs meeting criteria (20+), and national research networks (10+). These entities have legal standing, established accountability, and long-term commitment to Internet infrastructure. Entry criteria: Legal entity existence greater than 5 years, demonstrated Internet infrastructure operation, public accountability mechanism (membership organisation, government oversight, or equivalent). Accountability: Existing legal/regulatory frameworks. RIRs accountable to members; IXPs to participants; NRENs to funding bodies.

6.2.2 Operator Validators

Transit providers with customer cone greater than 1000 ASes (approximately 50 globally). Stake derives from operational dependency—validators with large customer bases have strong incentives for correct operation. Entry criteria: Customer cone measured by CAIDA AS-rank, sustained over 12-month period. Public BGP looking glass. MANRS participant. Accountability: Market accountability. Misbehaviour risks customer loss. Public voting record enables reputation tracking.

6.2.3 Community Validators

Academic institutions, non-profit Internet organisations (ISOC chapters, NOGs), and open-source routing projects. These provide independent oversight without commercial conflicts. Entry criteria: Demonstrated routing security research/operations contribution. Nomination by two existing validators. 6-month probationary period. Accountability: Reputation within technical community. Removal by supermajority vote.

6.3 Validator Weighting

Not all validators are equal. Voting weight reflects stake in routing system: RIRs receive 5% each (25% total) for foundational authority; Operator validators receive weight proportional to customer cone, capped at 3% each (approximately 40% total); IXP validators receive weight proportional to member ASes, capped at 2% each (approximately 20% total); Community validators share the remaining approximately 15% equally, with minimum 0.1% each.

Caps prevent any single entity from gaining outsized influence. Byzantine tolerance requires greater than 2/3 honest weighted votes; this structure ensures compromise of any single category is insufficient.

Collusion risk: RIRs collectively hold 25% of weighted votes. Compromise or coercion of two RIRs approaches the 1/3 threshold required for Byzantine attacks. This risk is partially mitigated by geographic distribution (5 RIRs across 5 continents), distinct legal jurisdictions, and the presumption that simultaneous compromise of multiple RIRs by a single adversary is operationally difficult. However, nation-state adversaries with influence across multiple regions cannot be ruled out.

6.4 Governance Processes

6.4.1 Validator Admission

The admission process proceeds as follows: Applicant publishes intent on public mailing list with supporting evidence; 30-day comment period for community input; Existing validators vote (simple majority of weighted votes); If approved, 6-month probationary period with reduced weight (50%); Full weight granted after probation unless objection sustained.

6.4.2 Validator Removal

Removal requires 2/3 weighted supermajority. Grounds include: sustained unavailability (greater than 7 days), detected Byzantine behaviour, loss of entry criteria (e.g., customer cone falls below threshold), legal judgement against entity for Internet-related misconduct. Emergency removal (suspected active attack) requires 3/4 supermajority and triggers automatic review within 72 hours.

6.4.3 Protocol Amendments

Changes to consensus rules, attestation formats, or governance structure require: Published proposal with 60-day discussion period; Reference implementation demonstrating backward compatibility; 3/4 weighted supermajority approval; 6-month activation delay for operator preparation.

6.4.4 Dispute Resolution

Disputes between validators escalate through: direct negotiation (7 days), mediation by uninvolved validator panel (14 days), binding arbitration. See Section 14 for complete legal framework including choice of law, arbitration venue, and liability allocation. Disputes regarding IP resource authority defer to relevant RIR policy process—SRI governance has no jurisdiction over resource allocation.

6.5 Comparison with RPKI Governance

RPKI governance derives from RIR membership and policy development processes. SRI governance is complementary: RPKI answers 'Who owns resources?' through RIR authority and legal standing; SRI answers 'Is this platform trustworthy?' through distributed consensus and technical attestation. Conflict resolution: RPKI takes precedence for resource authority. SRI attestation of an RPKI-invalid route is meaningless—the trust tier system requires RPKI validity as baseline.

7. Protocol Specification

7.1 SRI Path Attribute

SRI data is carried in a new BGP path attribute with Attribute Type Code to be assigned by IANA, Attribute Flags set as Optional and Transitive, and variable Attribute Length.

7.1.1 Field Definitions

Implementation status: The following specification defines intended protocol behaviour. No reference implementation exists to validate parsability, edge-case handling, or interoperability. Field definitions are subject to revision based on implementation experience. The Research Agenda (Section 16) explicitly identifies reference implementation as a near-term priority.

Version (8 bits): Protocol version. Current version = 1. Flags (8 bits): Bit 0 indicates Attestation present. Bit 1 indicates Compressed proof. Bits 2-7 are reserved. Block Height (64 bits): Consensus block height at time of signing. Used for freshness checking. State Root Hash (256 bits): SHA-256 root of consensus state Merkle tree. Proof Length (16 bits): Length of Merkle proof in bytes. Signature Count (16 bits): Number of path signatures (equals AS_PATH length for valid announcements). Merkle Proof: Proof of ROA validity for announced prefix. Variable length. Path Signatures: One signature per AS in path. Each signature covers prefix, path up to signing AS, and block height. Attestation Evidence: RATS EAT token from origin router. Present only if Flags bit 0 is set.

7.2 Error Handling

7.2.1 Validation Failure Actions

When SRI attribute validation fails, the router must not send a NOTIFICATION or tear down the session. Instead: Log the failure with reason code and peer information; Classify the route as lower trust tier (Tier 2 if RPKI-valid, Tier 3 if not); Continue normal BGP processing with adjusted tier; Optionally increment counter for monitoring/alerting. Rationale: SRI is supplementary security. Validation failure should degrade gracefully, not disrupt routing. The route remains usable at lower preference.

7.2.2 Validation Failure Reasons

Code 1 (PROOF_INVALID): Merkle proof doesn't verify against state root. Code 2 (SIGNATURE_INVALID): Path signature verification failed. Code 3 (SIGNATURE_MISSING): Fewer signatures than AS_PATH entries. Code 4 (BLOCK_STALE): Block height older than staleness threshold. Code 5 (BLOCK_FUTURE): Block height ahead of local consensus view. Code 6 (ATTESTATION_INVALID): EAT token verification failed. Code 7 (ATTESTATION_UNTRUSTED): Platform measurement not in approved set. Code 8 (PARSE_ERROR): Malformed attribute.

7.2.3 Attribute Propagation

When propagating a route with SRI attribute: If validation succeeded, add own signature and propagate attribute. If validation failed, strip attribute and propagate as Tier 2/3 route. If router doesn't support SRI, attribute is transitive and propagates unchanged.

7.3 Interaction with ADD-PATH

When ADD-PATH (RFC 7911) is negotiated, each path-id carries independent SRI attribute. Validation is per-path. A prefix may have Tier 0 path via one neighbor and Tier 2 path via another; both are valid, tier influences selection.

8. Deployment Cost Model and Financial Analysis

8.1 Capital Expenditure Analysis

8.1.1 Hardware Upgrade Paths

Three deployment scenarios with different CapEx profiles:

Scenario	Hardware Change	Est. Cost/Router	Timeline
A: Software-only	None (existing TPM)	$0 hardware	Immediate
B: Firmware upgrade	Vendor update	~$500 support	Vendor dependent
C: Hardware refresh	Replace router	$15K-150K	Natural cycle

Table 5: Hardware upgrade scenarios.

Scenario A applies to routers with existing TPM (Cisco 8000, NCS 540/560, Juniper MX304). Scenario B requires vendor cooperation. Scenario C aligns with natural refresh cycles.

8.1.2 Fleet-Wide Estimates

Based on operator feedback with a 50,000 router fleet assumption: Tier 1 carrier with 60% having TPM means 30,000 Scenario A and 20,000 Scenario C over 10-12 years. Estimated incremental CapEx of $300M-500M spread over refresh cycle (versus approximately $2B baseline refresh cost). Incremental premium of approximately 15-25% above baseline refresh CapEx.

8.2 Operational Expenditure Analysis

8.2.1 Training and Tooling (One-Time Costs)

NOC staff training: 2-day course per engineer at approximately $2,000/person including materials. For a 100-person NOC, total training cost: $200,000. Monitoring integration: Dashboard development approximately $50K-100K. Playbook development: Troubleshooting procedures requiring approximately 200 engineering hours at $150/hour fully-loaded = $30,000. Total one-time OpEx: approximately $280K-330K per major deployment.

8.2.2 Ongoing Operations (Annual Costs)

The following costs assume fully-loaded annual compensation of $200,000/FTE for senior network engineers and $150,000/FTE for operations staff:

Function	FTE	Annual Cost	15-Year Total
Attestation infrastructure	0.5	$100,000	$1,500,000
Monitoring and incident response	0.25	$50,000	$750,000
Consensus participation (if validator)	1.0	$200,000	$3,000,000
Infrastructure (validator node)	—	$50,000	$750,000
Total (non-validator)	0.75	$150,000	$2,250,000

Total (validator)	1.75	$400,000	$6,000,000

Table 6: Annual operational expenditure with 15-year projections.

8.3 Financial Break-Even Analysis

8.3.1 Cost Summary

For a representative Tier-1 carrier with 50,000 routers:

Cost Category	Non-Validator	Validator
CapEx (incremental over 12 years)	$400M	$400M
One-time OpEx	$0.3M	$0.3M
Ongoing OpEx (15-year NPV @ 8%)	$1.3M	$3.4M
Total 15-Year Cost (nominal)	$403.6M	$406.7M

Table 7: Total cost of ownership projection.

8.3.2 Benefit Quantification

Benefits are inherently difficult to quantify because they involve preventing low-probability, high-impact events. The following estimates are indicative, not precise. Hijack prevention: Major BGP hijacks have caused losses ranging from $150K (cryptocurrency theft) to unquantified national security impact. Assuming one prevented major incident per 5 years with average recoverable impact of $50M: NPV of avoided losses approximately $250M over 15 years. Insurance premium reduction: Cyber insurance premiums for carriers average 0.5-2% of revenue. If SRI deployment enables 10-20% premium reduction for a $5B revenue carrier: annual savings of $2.5M-20M. NPV approximately $21M-171M over 15 years. Regulatory compliance: As governments mandate routing security (EU NIS2, anticipated US CISA guidance), early deployment avoids rushed implementation. Value: indeterminate but potentially significant.

8.3.3 NPV and Break-Even

Conservative NPV estimate (8% discount rate, 15-year horizon): Total cost: $404M-407M (Table 7). Total quantifiable benefit: $271M-421M. Net NPV: negative $136M to positive $14M.

Conclusion: Under conservative assumptions, SRI deployment for a Tier-1 carrier does not demonstrate clear positive NPV within a 15-year horizon. The business case depends heavily on: (1) actual hijack incident frequency and impact, (2) insurance market response to deployment, and (3) regulatory mandates. This analysis does not support deployment purely on ROI grounds. The case for SRI rests on security posture improvement for critical infrastructure rather than direct financial return.

8.3.4 Investment Timing (J-Curve)

Costs are front-loaded; benefits accrue later. Years 1-5: Heavy CapEx investment (Scenario B/C deployments), training costs, tooling development. Minimal benefit realization as adoption is below critical mass. Years 5-10: Continued CapEx as refresh cycle progresses. Potential insurance benefits begin if adoption reaches visibility threshold. Regulatory compliance value may crystallize. Years 10-15: CapEx tapers as refresh completes. Full steady-state OpEx. Maximum benefit realization if adoption reaches critical mass.

Critical dependency: Benefits require adoption beyond any single carrier's control. A carrier investing in SRI may not see benefits if competitors do not also deploy, creating classic coordination game dynamics. This is the same coordination failure that prevented BGPsec adoption.

8.4 Realistic Timeline

Based on operator feedback regarding actual refresh cycles:

Tier	Segment	Original Est.	Revised
1	Hyperscale internal	2026-2028	2027-2029
2	Enterprise edge	2028-2031	2030-2034
3	Transit/IXP	2030-2035	2033-2038
4	General Internet	2035+	2040+

Table 8: Revised adoption timeline based on 10-12 year refresh cycles.

9. Operational Workflows

9.1 Troubleshooting Decision Tree

When routes with SRI attestation exhibit unexpected behaviour, operators should follow structured diagnostic procedures. For routes not preferred despite valid attestation: Check LOCAL_PREF—SRI doesn't override explicit policy; check AS_PATH length—standard BGP selection applies after tier; verify attestation actually validated; check for policy preferring specific peers over tier. For attestation validation failures: Check consensus sync status; if behind, wait for sync or increase staleness window; check failure reason code; verify local clock sync as attestation timestamps are sensitive.

9.2 Failure Modes and Recovery

Consensus partition: If local router loses connectivity to consensus network, cached state root remains valid for staleness window (default 5 minutes). Routes continue processing at current tier; no tier upgrades possible. After staleness expires, new routes classified as Tier 2/3 until sync restored. Existing Tier 0/1 routes are not downgraded (prevents cascade). TEE failure: If secure enclave becomes unavailable, signing operations fail; router cannot originate Tier 0/1 routes. Verification continues using cached keys. Alert generated; manual intervention required. TPM failure: If TPM becomes unavailable, attestation generation fails; routes originated without attestation (Tier 1 max). Sealed keys unavailable; requires hardware replacement.

9.3 NOC Integration

SRI adds the following to standard BGP monitoring: sri_validation_success_total and sri_validation_failure_total (Prometheus counters); sri_consensus_block_height (current sync status); sri_cache_hit_ratio (proof cache efficiency); sri_tier_distribution (routes by trust tier). Suggested alert thresholds: Consensus sync lag greater than 10 blocks (Warning); Validation failure rate greater than 5% (Warning); Validation failure rate greater than 20% (Critical); TEE unavailable (Critical); Cache hit ratio less than 80% (Warning).

10. Low-Latency Consensus for Routing Authority

Routing authority—who may originate which prefixes, which ASes have which provider relationships—changes slowly compared to route announcements. Authority changes occur at human timescales (business decisions, allocations); route announcements occur at machine timescales (convergence events reaching 8,494 UPDATEs/second). This enables separation: consensus operates on slowly-changing authority; UPDATE validation uses cached proofs against that authority. Consensus need not achieve per-UPDATE latency.

RAC Protocol Summary: Validator Set of approximately 100 validators across 5 geographic shards; Block Interval of 30 seconds providing finality within one minute; Block Contents including batched authority changes—ROA attestations, ASPA updates, key rotations, firmware approvals; Light Clients where routers verify Merkle proofs against cached headers with no consensus participation required.

11. Quantum Computing Threat Analysis

Cryptographically-relevant quantum computer emergence is estimated for 2030-2040. NIST post-quantum standards (FIPS 203-205) were published August 2024. 'Harvest now, decrypt later' makes this an immediate architectural concern. RPKI faces significant quantum migration obstacles: ML-DSA signatures are 13x larger than ECDSA; deep certificate chains multiply overhead; five independent RIRs must coordinate migration; relying party software performance is already problematic.

SRI Quantum Strategy: Cryptographic agility with algorithm negotiation built into protocol; Hash-based Merkle proofs using SHA-3/SHAKE remain quantum-resistant; Distributed migration where each AS migrates independently; TPM evolution with TPM 3.0 including PQC support.

12. Tiered Adoption Framework

Tier 1 (Hyperscale Internal, 2027-2029): Cloud providers, CDNs, financial networks deploy internally with existing security investment and engineering capacity. Tier 2 (Enterprise Edge, 2030-2034): Enterprise CPE validates upstream routes, requiring vendor support or open-source alternatives. Tier 3 (Transit/IXP, 2033-2038): Core infrastructure deployment with IXP route servers preferring SRI routes. Tier 4 (General Internet, 2040+): Consumer ISPs and regional networks via natural hardware refresh.

Important caveat: While the architecture ensures that reachability never technically depends on SRI adoption (Tier 2/3 routes remain valid), operator policy choices may create de facto dependencies. If operators configure LOCAL_PREF to strongly prefer Tier 0 routes, unvalidated routes become second-class from a traffic engineering perspective.

13. Security Considerations

13.1 Attack Surface Shifts

13.1.1 Firmware Supply Chain

TPM attestation trusts hardware integrity. If hardware is compromised at manufacture, SRI protections are ineffective. The SRI specification requires validators to maintain an approved firmware list. Firmware approval requires: (1) Vendor submission of signed firmware images; (2) Independent security audit by at least two accredited labs (minimum: Common Criteria EAL4+); (3) Hash publication 30 days prior to approval for community review; (4) 2/3 validator approval for inclusion. Firmware from vendors that have had supply chain incidents within 24 months faces enhanced scrutiny including source code review where available.

Residual risk: No vetting process can guarantee detection of sophisticated supply chain attacks. SRI security claims are conditional on hardware integrity, which cannot be cryptographically proven from software.

13.2 Trust Model Comparison

RPKI: Trust 5 RIR CAs. Single RIR compromise enables regional attack. SRI: Trust greater than 2/3 weighted validators honest. No single-entity compromise sufficient. Threat model shifts from 'compromise one authority' to 'coordinate Byzantine attack across distributed infrastructure'—strictly harder for most adversaries.

13.3 Discussion and Limitations

Transparency about limitations: Legal resource authority remains with RIRs; SRI cannot override RPKI invalidity. Traffic content: SRI secures routing decisions, not payload. DDoS: SRI doesn't prevent volumetric attacks. Policy disputes: Business routing decisions remain operator prerogative.

14. Legal Framework and Liability

This section addresses jurisdictional and liability questions identified as critical gaps in prior review. The framework draws on established Internet governance precedents while acknowledging that novel mechanisms require careful legal structuring.

14.1 Governing Law and Jurisdiction

SRI validator governance operates under Swiss law. Switzerland is selected for: established neutrality in international disputes, mature legal framework for international organisations, precedent from ICANN and Internet governance bodies, and favourable regulatory environment for distributed systems. The SRI Foundation (to be established) would be incorporated as a Swiss association (Verein) under Articles 60-79 of the Swiss Civil Code. Disputes between validators escalate through: direct negotiation (7 days); mediation administered by the Swiss Arbitration Centre (14 days); binding arbitration under Swiss Rules of International Arbitration, seated in Geneva. Arbitration awards are enforceable in 172 countries under the New York Convention.

14.2 Liability Allocation

Core liability principles: No validator liability for correct operation—validators operating according to protocol specifications and governance rules are not liable for downstream routing decisions. Validator liability for Byzantine behaviour—validators that demonstrably act contrary to protocol are subject to immediate removal, forfeiture of staked assets, and potential civil liability. Operator liability unchanged—SRI does not modify existing liability frameworks; operators remain responsible for their own policy choices.

Routing failure scenarios: False positive (legitimate route rejected)—liability follows operator policy chain, not SRI. False negative (malicious route accepted)—SRI makes no guarantee of detection; claims are not actionable. Consensus failure—if from validator misbehaviour, affected validators are liable; if from non-culpable cause, no party is liable.

14.3 Regulatory Compliance

SRI deployment may assist compliance with: EU NIS2 Directive requirements for securing network and information systems; anticipated US CISA routing security guidance; national cybersecurity certification schemes. SRI does not replace national regulatory requirements. SRI consensus state is public by design with no personal data stored on-chain; GDPR and equivalent regulations do not apply to SRI operational data.

15. Critical Path Analysis and Known Limitations

This section explicitly addresses known weaknesses and adoption challenges. Intellectual honesty about limitations is essential for productive discourse.

15.1 Critical Path to Deployment

Governance coordination (Primary Risk): Governance coordination is the critical path and highest-risk component. Before any packet traverses the network with SRI attestation, 100+ validators across competing organisations must agree on validator weighting formula, dispute resolution binding authority, key rotation procedures, and firmware approval lists. Historical precedent is not encouraging. DNSSEC root signing took 15 years. BGPsec standardised in 2017 has achieved zero production deployment. SRI requires new coordination among entities with misaligned incentives.

Reference implementation (Secondary Risk): The protocol specification defines intended behaviour but has not been validated through implementation. Significant issues typically emerge during implementation: edge cases not considered, performance characteristics that differ from analysis, interoperability challenges.

15.2 Known Limitations

SRI does not solve all BGP security problems. It does not address: DDoS attacks (traffic volume is orthogonal to routing decisions); traffic content security (SRI secures where traffic goes, not what traffic contains); policy disputes between operators. SRI's hardware root of trust is only as secure as the hardware manufacturing process. Byzantine tolerance has limits—SRI tolerates less than 1/3 malicious validators; if adversaries compromise 1/3+ of validator weight, Byzantine attacks become possible.

15.3 Comparison to Failed Prior Efforts

SRI must be evaluated against the history of failed BGP security proposals. S-BGP (2000) failed due to PKI complexity and performance overhead. soBGP (2004) failed due to governance disputes over trust anchor. BGPsec (2017) failed due to 70x performance overhead, partial deployment disincentives, and key management complexity. SRI's architectural choices address known failure modes, but SRI introduces new coordination challenges (distributed validator governance) that prior efforts did not face. SRI may fail for reasons not yet identified.

15.4 Fragility Assessment

Factor	Weight	Risk Score	Contribution
Governance coordination	30%	90%	27%
Hardware supply chain	20%	70%	14%
Bus factor (expertise)	20%	80%	16%
Cache-miss latency	15%	50%	7.5%
Quantum timeline uncertainty	15%	50%	7.5%
Weighted Fragility Score	100%	—	72%

Table 9: Fragility assessment. Score >50% indicates significant deployment risk.

Interpretation: A 72% fragility score indicates high deployment risk, driven primarily by governance coordination challenges. This score does not mean SRI will fail; it means stakeholders should expect significant obstacles and plan accordingly.

16. Research Agenda

16.1 Near-Term (2026-2027)

Priority 1: Formal TLA+ specification of RAC consensus protocol with machine-verifiable protocol specification enabling model checking. Priority 2: Reference implementation on commodity hardware (Intel TDX, ARM CCA) demonstrating validation latency claims—this is the critical validation step. Priority 3: Performance characterisation with realistic traffic patterns including cold-start, churn, and partition recovery. Priority 4: seL4 + TPM + BGP integration prototype demonstrating microkernel isolation with hardware attestation.

16.2 Medium-Term (2028-2030)

Academic network testbed deployment (Internet2, GÉANT) for real-world operational experience. Economic incentive analysis and game-theoretic modelling of validator incentive structures. Interoperability testing with commercial BGP implementations. Post-quantum cryptography integration implementing ML-DSA and other PQC algorithms. Isabelle/HOL verification of validation path for formal verification of critical-path cryptographic operations.

16.3 Long-Term (2031+)

IETF engagement for potential standardisation if reference implementation succeeds. Commercial pilot with hyperscale partner for production deployment in controlled enterprise environment. Hardware vendor native support through engagement with Cisco, Juniper, Arista. Regulatory framework engagement coordinating with EU ENISA, US CISA, and national regulators on routing security requirements.

17. References

17.1 Normative References

[1] RFC 4271: A Border Gateway Protocol 4 (BGP-4), Rekhter, Li, Hares, 2006

[2] RFC 4272: BGP Security Vulnerabilities Analysis, Murphy, 2006

[3] RFC 6480: Infrastructure to Support Secure Internet Routing, Lepinski, Kent, 2012

[4] RFC 8205: BGPsec Protocol Specification, Lepinski, Sriram, 2017

[5] RFC 8416: Simplified Local Internet Number Resource Management (SLURM), Ma et al., 2018

[6] RFC 9683: Remote Integrity Verification of Network Devices, Fedorkow et al., 2024

[7] RFC 9684: YANG Data Model for TPM-based Attestation, Fedorkow, Voit, 2024

[8] draft-ietf-sidrops-aspa-verification-24: BGP AS_PATH Verification Based on ASPA, Azimov et al., 2025

[9] draft-ietf-sidrops-aspa-profile-20: Profile for ASPA, Azimov et al., 2025

[10] draft-voit-rats-trustworthy-path-routing-12: Trusted Path Routing, Voit et al., 2025

[11] draft-ietf-rats-eat: Entity Attestation Token (EAT), Mandyam et al., 2024

17.2 Informative References

[12] FIPS 203: ML-KEM Standard, NIST, August 2024

[13] FIPS 204: ML-DSA Standard, NIST, August 2024

[14] FIPS 205: SLH-DSA Standard, NIST, August 2024

[15] "Securing BGP ASAP: ASPA and Post-ROV Defenses", Furuness et al., NDSS 2025

[16] "SoK: Introspective Analysis of RPKI Security", Dai et al., USENIX Security 2025

[17] "S-BGP: Infrastructure for Secure BGP", Kent, Lynn, Seo, IEEE JSAC 2000

[18] "RPKI's 2024 Year in Review", Snijders, RIPE Labs, January 2025

[19] "Post-quantum cryptography and RPKI: Current status and migration considerations", APNIC Blog [publication date pending verification]

[20] "TrustedGateway: TEE-Assisted Routing", Kohler et al., RAID 2022

[21] "seL4: Formal Verification of an OS Kernel", Klein et al., SOSP 2009

[22] "The SCION Internet Architecture", Perrig et al., CACM 2017

[23] "BGP Security in Partial Deployment", Lychev et al., SIGCOMM 2013

[24] "Bagpipe: Verified BGP Configuration", Weitz et al., Univ. Washington 2016

[25] "RPKI database growth", MANRS, January 2025

[26] "Blockchain for Internet Resources", RIPE NCC, 2018

[27] draft-mcbride-rtgwg-bgp-blockchain-00: BGP Blockchain, McBride, 2022

[28] "Cisco Trusted Platforms", Cisco Systems, 2024

[29] "Junos Hardware Root of Trust", Juniper Networks, 2025

Appendix A: Document Metadata

Field	Value
Title / Subtitle	Sovereign Routing Infrastructure (SRI) / A Five-Layer Hardware-Integrated Architecture for Securing Inter-Domain Routing
GUID	AG-2026-0105-6870
Version	2.1 (Red Team Revision)
Date	05 January 2026
Author	Aaron Garcia
Affiliation	Independent Researcher
Contact	aaron@garcia.ltd
Origin Context	Revised from v2.0 incorporating Red Team analysis findings
Status	Final Draft (Post-Red Team)

Appendix B: Glossary

Term	Definition
AS	Autonomous System - A network or collection of networks under single administrative control
ASPA	Autonomous System Provider Authorization - RPKI object specifying authorised upstream providers
BFD	Bidirectional Forwarding Detection - Protocol for rapid failure detection
BGP	Border Gateway Protocol - The inter-domain routing protocol of the Internet
BGPsec	BGP Security Extensions - A path validation protocol (RFC 8205)
BFT	Byzantine Fault Tolerance - Ability to reach consensus despite malicious nodes
CRQC	Cryptographically Relevant Quantum Computer - Quantum computer capable of breaking current cryptography
EAT	Entity Attestation Token - IETF RATS format for attestation evidence
EK	Endorsement Key - TPM identity key
HRoT	Hardware Root of Trust - Hardware-based security foundation
IXP	Internet Exchange Point - Physical location where networks interconnect
ML-DSA	Module-Lattice-based Digital Signature Algorithm - Post-quantum signature scheme (FIPS 204)
NLRI	Network Layer Reachability Information - BGP prefix announcements
NREN	National Research and Education Network
PCR	Platform Configuration Register - TPM register for integrity measurements
PMP	Physical Memory Protection - RISC-V security feature
PQC	Post-Quantum Cryptography - Cryptographic algorithms resistant to quantum attacks
RAC	Routing Authority Consensus - SRI's consensus protocol
RATS	Remote Attestation Procedures - IETF working group on attestation
RIR	Regional Internet Registry - Organisation managing IP address allocation
ROA	Route Origin Authorization - RPKI object authorising prefix origination
ROV	Route Origin Validation - Checking routes against RPKI
RPKI	Resource Public Key Infrastructure - PKI for Internet number resources
seL4	Secure Embedded L4 - Formally verified microkernel
SLURM	Simplified Local Internet Number Resource Management (RFC 8416)
SRI	Sovereign Routing Infrastructure - The architecture proposed in this paper
TCB	Trusted Computing Base - Minimal trusted code in a secure system
TDX	Trust Domain Extensions - Intel's confidential computing technology

TEE	Trusted Execution Environment - Hardware-isolated secure processing
TPM	Trusted Platform Module - Hardware security chip

Appendix C: Methodology and Transparency Statement

Author Context and Expertise

This work is grounded in 30 years of multi-sector experience in Systems Engineering. The analytical framework reflects professional history, focusing on practical application.

Digital Methodology and Accessibility

In the spirit of transparency, I utilised a suite of Generative AI tools—specifically Claude, Google Gemini, and ChatGPT—to assist in the production of this paper. These tools were employed as 'force multipliers' for data synthesis and editorial accessibility. As a writer with dyslexia, I leverage these models as assistive technology to refine grammar and streamline sentence structure.

Verification and Integrity

While AI assisted in processing data, the intellectual oversight is entirely human. I performed manual validation of all citations and accept full responsibility for the accuracy and originality of the final output.

— End of Document —