Authenticated Encrypted Relay Network (AERN)

Revision: 1.0
Date: October 2025
Author: John G. Underhill
Document Type: QRCS Executive Summary
Keywords: AERN, Authenticated Encrypted Relay Network, Multi-Party Cryptography, Post-Quantum Secure Networking, Encrypted Relay Systems

1. Mission and Context

The **Authenticated Encrypted Relay Network (AERN)** establishes a **quantum-resistant, authenticated, and anonymous communications framework** designed to supersede legacy anonymizers such as TOR.
Where traditional systems rely on public volunteer nodes, non-authenticated peers, and pre-quantum cryptography, AERN introduces a domain-controlled, certificate-based relay infrastructure that ensures **verifiable trust, forward secrecy, and complete metadata erasure.**

Its mission is to provide a **future-proof foundation for secure, private, and high-performance data exchange** across government, enterprise, and humanitarian sectors in anticipation of post-quantum threats.

2. Problem Definition

Current anonymity and tunneling systems face three systemic limitations:

- **Untrusted Infrastructure:** Volunteer-based routing networks allow malicious nodes and metadata capture.
- **Cryptographic Obsolescence:** RSA/ECC schemes are vulnerable to quantum decryption, rendering confidentiality temporary.
- **Traffic Correlation Exposure:** Fixed routing and variable packet sizes enable surveillance agencies to perform flow correlation.

AERN resolves these through **authenticated domain membership, quantum-secure primitives,** and **per-packet randomized routing** that makes correlation statistically infeasible—even under global observation.

3. System Architecture

AERN operates as a **four-tier federated architecture**, built for modular deployment and cryptographic isolation.

1. AERN Root Security (ARS):
Offline trust anchor; signs domain certificates and defines the approved cryptographic configuration set.

2. AERN Domain Controller (ADC):
Manages registration, certificate validation, revocation, and synchronization; optionally proxy-signs certificates on behalf of the ARS.

3. AERN Proxy Servers (APS):
Authenticated nodes forming a **fully meshed symmetric tunnel network**. Each pair of proxies maintains bi-directional encrypted channels derived from PQ key exchanges.

4. AERN Client Devices (ACD):
Endpoints that initiate connections through random entry nodes, traversing randomized multi-hop routes (3–16 hops by default).

Core design attributes

- **Fixed packet size:** 1500 B (standard MTU) eliminates traffic fingerprinting.
- **Per-packet route randomization:** New circuit for every packet, breaking timing and flow correlation.
- **Zero persistent metadata:** No packet, route, or session data retained after teardown.
- **Symmetric data plane:** High-throughput RCS cipher ensures low-latency operation suitable for real-time voice/video.

4. Cryptographic Foundation

AERN's cryptosystem adheres strictly to **NIST post-quantum standards**.

Function	Algorithm Suite	Security Margin

Key Encapsulation	Kyber, McEliece	≥ 256-bit PQ
Digital Signature	Dilithium, SPHINCS+	≥ 256-bit PQ
Symmetric Encryption	**RCS** (wide-block Rijndael AEAD)	256-bit
KDF / MAC	**SHAKE-256, KMAC-256** (SP 800-185)	256-bit

Security disciplines

- **Forward + Post-Compromise Secrecy:** automatic re-key every ~1200 packets via cSHAKE/KMAC.
- **Replay & Injection Resistance:** UTC timestamps and sequence counters validated at each hop.
- **Administrative Isolation:** ARS air-gapped; ADC limited to proxy-signing channel.
- **Cryptanalytic transparency:** RCS design open to independent audit; AES-GCM fallback supported.

5. Applications and Use Cases

Government & Defense:
Secure classified communications over sovereign domains with verifiable node trust.

Financial and Enterprise Systems:
Confidential transaction tunnels, regulatory-compliant anonymity for internal or cross-border operations.

Critical Infrastructure / IoT / SCADA:
Authenticated encrypted relays between industrial and telemetry devices, resistant to traffic profiling.

Humanitarian and Civil Society:
Trusted anonymity infrastructure for journalists, NGOs, and citizens operating under surveillance or censorship.

Research and Healthcare Federations:
Cross-institution collaboration with end-to-end encrypted exchange, preserving confidentiality and identity verification.

6. Societal and Economic Value

AERN delivers quantifiable value across multiple dimensions:

- **Digital Sovereignty:** Enables nations and enterprises to deploy **independent, auditable privacy networks**.
- **Regulatory Confidence:** Maintains device authentication and accountability while preserving user anonymity.
- **Quantum Readiness:** Avoids future remediation costs associated with cryptographic obsolescence.
- **Operational Efficiency:** Symmetric tunnels reduce computational overhead by orders of magnitude compared to layered onion models.
- **Human Rights Enablement:** Protects communications vital to democracy, press freedom, and humanitarian coordination.

7. Comparative and Strategic Assessment

Dimension	TOR / VPN	AERN
Node Trust	Public / volunteer	**Authenticated domain nodes**
Cryptography	Classical (RSA/ECC)	**Post-Quantum secure**
Circuit Lifetime	Fixed (≈10 min)	**Per-packet randomized**
Packet Size	Variable	**Fixed 1500 B uniformity**
Metadata Retention	Partial / logged	**Zero retention**
Latency (typical)	200–400 ms	**< 80 ms (16 hops)**
Governance Model	Global volunteer	**Federated private domains**

Strategic Outlook

AERN stands as a **quantum-secure successor** to both TOR and conventional VPNs—offering authenticated anonymity, verifiable trust, and scalable deployment. Its design aligns with the QRCS principle of *practical cryptographic sovereignty*: enabling private, provable, and future-safe communication fabrics for institutional and civic resilience.

Prepared by: **Quantum-Resistant Cryptographic Solutions**
Contact: contact@qrcscorp.ca

©2025 QRCS Corporation. All rights reserved.