Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 31, 2026

L.J. Reilly
Independent

September 27, 2025

Reilly Resilience Protocol (RRP): Tamper-Evident Proof of System Resilience
draft-reilly-resilience-protocol-00

Abstract

The Reilly Resilience Protocol (RRP) standardizes a verifiable method to prove that IT systems, cloud infrastructures, and AI pipelines are continuously exercised and resilient. RRP turns resilience claims into cryptographically signed evidence persisted in immutable storage and batched into a daily Merkle root that is publicly time-anchored on blockchains. The protocol outputs an executive Resilience Scorecard backed by independently verifiable receipts. RRP composes with the Reilly EternaMark (REM) protocol to ensure dual-layer digital permanence using both DOI archival and blockchain timestamping.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

1. Introduction

Organizations often claim "high availability," "recoverability," and "compliance," but outages, failed restores, configuration drift, and silent AI degradation continue to occur. Traditional logs and dashboards can be edited, omitted, or lack objective time validity.

RRP closes this trust gap by producing daily, tamper-evident proof that critical controls executed successfully. Evidence MUST be signed, persisted in immutable storage, and anchored into a public blockchain Merkle root for time attestation. The protocol defines a Resilience Scorecard that SHOULD be consumable by executives, while remaining fully verifiable by auditors.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 and RFC 8174 when, and only when, they appear in all capitals, as shown here.

3. Protocol Principles

* Test restores, not backups. Recovery MUST be demonstrated by an actual restore + validation.

* Evidence over narrative. Every resilience claim MUST map to signed, immutable evidence.

* Minimum on-chain. Only Merkle roots MUST be anchored. Sensitive artifacts MUST remain off-chain.

* Composable. Existing monitoring and testing systems SHOULD be wrapped to produce standardized evidence records.

4. Architecture

RRP consists of the following roles:

* Collectors: MUST generate normalized evidence JSON/CBOR for each control check.

* Signer: MUST sign evidence digests with a private key (Ed25519 or ECDSA P-256) stored in a KMS/HSM.

* Evidence Store: MUST preserve full JSON and supporting artifacts in WORM/immutable storage.

* Aggregator: MUST validate signatures, construct a Merkle tree, and compute the root daily.

* Anchor: MUST publish the Merkle root to a public blockchain (Bitcoin/OpenTimestamps or Ethereum/L2).

* Scorecard: SHOULD compute weighted pillar scores and present a PDF or dashboard for executives.

5. Operations

Step 1: Define Controls and SLOs
: Implementers MUST define 5-12 critical controls with measurable SLOs (e.g., Restore <= 30 min).

Step 2: Collect Evidence
: Collectors MUST execute active checks (e.g., DB restore, TLS expiry, AI drift scan) and emit canonical evidence.

Step 3: Sign Evidence
: Each evidence JSON MUST be hashed (SHA-256) and signed using a per-collector key.

Step 4: Store Evidence
: Evidence and artifacts MUST be stored in immutable object storage with retention and versioning.

Step 5: Aggregate and Anchor
: Aggregators MUST compute the Merkle root over all results once per day and MUST anchor it into a public chain.

Step 6: Publish Scorecard
: Scorecard SHOULD provide a 0-100 RRP score. Stale evidence MUST decay the score. Critical FAILS MUST cap a pillar at 60.

Step 7: Independent Verification
Auditors MUST be able to re-derive digests, validate collector signatures, verify Merkle inclusion proofs, and validate anchor receipts without vendor trust.

6. Security Considerations

* Multiple chains SHOULD be used to mitigate correlated blockchain risk.

* Keys MUST be rotated periodically (at least annually).

* Verifiers MUST treat all evidence inputs as untrusted until hashes, signatures, and inclusion proofs are validated.

7. Relationship to REM

RRP specifies how to generate daily, verifiable resilience evidence. The REM protocol specifies how to preserve that evidence permanently via DOI archival + blockchain timestamping. RRP evidence packages SHOULD integrate with REM by publishing batch metadata as DOI-archived objects, embedding Merkle roots and anchor receipts.

8. IANA Considerations

This document has no IANA actions.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, July 2017.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 5652, September 2009.

[RFC9162] Laurie, B., et al., "Merkle Tree Proofs", RFC 9162, December 2021.

[RFC8259] Bray, T., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 8259, December 2017.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 8949, December 2020.

9.2. Informative References

Reilly, L.J., "Reilly EternaMark (REM) Protocol - Dual-Layer Digital Permanence Using DOI Archiving and Blockchain Timestamping", Work in Progress, draft-reilly-rem-protocol-00, September 2025.

Reilly, L.J., "The Reilly Resilience Protocol (RRP) Whitepaper v2", Zenodo, DOI: 10.5281/zenodo.17100703, September 2025.

Author’s Address

Lawrence John Reilly Jr.
Independent Researcher
Email: lawrencejohnreilly@gmail.com