Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 26 March 2026

L.J. Reilly
Independent

September 27, 2025

Reilly Banking Integrity Protocol (RBIP)
draft-reilly-banking-integrity-00

Abstract

This document defines the Reilly Banking Integrity Protocol (RBIP), a compliance-grade architecture for generating immutable, auditor- and regulator-verifiable evidence trails in banking operations. RBIP combines cryptographic anchoring (e.g. blockchain timestamping) with archival DOI issuance to produce permanent, tamper-evident records. RBIP addresses three core domains: Proof-of-Reserves & Liquidity (PRL), Loan Origination & Collateral Chain (LOC), and KYC/AML Evidence Ledger (KAL).

RBIP is intended to help financial institutions satisfy requirements from Basel III/IV, SOX, BSA/AML, ISO/IEC 42001:2023, and other relevant regulations while preserving privacy, accountability, and auditability.

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."

Table of Contents

1. Introduction

Financial regulators and auditors require trustworthy, tamper-evident audit trails of bank operations. Conventional centralized logs or database snapshots suffer the risk of undetectable alteration or retrospective deletion. The Reilly Banking Integrity Protocol (RBIP) is designed to provide cryptographic guarantees and public verifiability while preserving the ability for selective disclosure to auditors or regulators.

RBIP realizes this by combining two orthogonal mechanisms:

* Deep archival of evidence artifacts with persistent identifiers (e.g. DOIs)
* Cryptographic anchoring (e.g. blockchain timestamping) to fix the chronological order and integrity of those artifacts

The result is an audit trail that is permanent, tamper-evident, and regulator-verifiable.

This document describes RBIP's architectural modules, workflows, interfaces, security obligations, and how it helps satisfy regulatory standards.

2. Requirements Language

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 BCP 14, RFC 2119 and RFC 8174.

3. Design Overview

3.1 Architecture & Modules

RBIP is composed of three cooperating modules:

* Proof-of-Reserves & Liquidity (PRL)
* Loan Origination & Collateral Chain (LOC)
* KYC/AML Evidence Ledger (KAL)

Each module records discrete events or milestones. Each event is assigned a unique Evidence Item with metadata and a digest of the underlying data. Bundles of Evidence Items are periodically archived and anchored.

A high-level architecture:

```
Bank Core Systems -> RBIP Evidence Generator ->
   -> DOI Archival Service
   -> Blockchain Anchoring Service
```

-> Auditor / Regulator Query Interface
-> Optional Public Transparency Interface

3.2 Threat Model

RBIP assumes adversaries may attempt:

* Retrospective deletion or modification of archived evidence
* Reordering of event chronology
* Collusion between internal operators and log managers
* Disclosure of sensitive customer data

RBIP counters these by requiring cryptographic binding, end-to-end chain-of-custody, and selective encryption or redaction.

4. Data Model and Event Types

4.1 PRL Module Events

* ReserveSnapshot
* LiquidityStressTest
* ReserveAttestation

4.2 LOC Module Events

* LoanApplication
* UnderwritingDecision
* CollateralBinding
* CollateralRevaluation
* LoanDisbursement
* PaymentReceipt
* DefaultEvent / RecoveryEvent

4.3 KAL Module Events

* IdentitySubmission
* IdentityVerificationResult
* TransactionMonitorAlert
* SARSubmission
* CaseEscalation
* CaseClosure

Each Event is represented by a JSON or CBOR object with mandatory fields including evidence_id, module, event_type, timestamp, prev_digest, data_digest, and metadata.

5. Protocol Workflow

5.1 Evidence Generation

1. Event data serialized into canonical form (JSON/CBOR).
2. SHA-256 digest computed.
3. Linked to prior digest.
4. Evidence Item emitted.

5.2 DOI Archival Step

1. Bundles of Evidence Items hashed to bundle_root_digest.
2. DOI minted for bundle.
3. Metadata stored.

5.3 Blockchain Anchoring / Timestamping

1. bundle_root_digest submitted to blockchain.
2. Transaction ID and block timestamp recorded.

5.4 Evidence Verification & Audit

Auditors check digests, Merkle paths, DOI records, and blockchain anchors to validate evidence.

6. Interfaces and APIs

6.1 Internal Bank Systems Interface

REST/gRPC API for event submission.

6.2 Regulator / Auditor API

APIs for evidence retrieval, bundle metadata, and anchor verification.

6.3 Public Transparent API

Optional limited disclosure interface.

7. Security Considerations

RBIP mitigates insider collusion and tampering by using HSMs, access controls, atomic event capture, backups, and key rotation.

8. Privacy and Confidentiality Considerations

RBIP enforces selective disclosure, encryption of sensitive data, and controlled access to prevent exposure of customer information.

9. Compliance with Regulatory Standards

RBIP helps satisfy Basel III/IV, SOX, BSA/AML, ISO/IEC 42001:2023, and related frameworks.

10. IANA Considerations

This document makes no IANA requests.

11. Acknowledgments

Thanks to the financial cryptography and auditing communities.

12. References

12.1 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.

12.2 Informative References

[Zenodo] Reilly, L.J., "Reilly Banking Integrity Protocol (RBIP): Ensuring Permanent and Regulator-Verifiable Audit Trails", Zenodo, 2025. Available: https://zenodo.org/records/17114424

Author’s Address

Lawrence John Reilly Jr.
Independent Researcher
Email: lreilly250@gmail.com