Remote ATtestation procedureS
Internet-Draft
Intended status: Standards Track
Expires: 11 August 2026

D. Condrey
Writerslogic Inc

7 February 2026

Evidence Revocation and Status Protocol for Proof of Process
draft-condrey-rats-witnessd-revocation-00

Abstract

This document specifies mechanisms for revoking and updating Evidence status in the witnessd Proof of Process framework. It defines how authors can mark Evidence as superseded or revoked, how device key compromise is handled, and how Verifiers can efficiently check Evidence validity.

The specification also defines an External Verifier Registry protocol that enables Relying Parties to discover trusted Verifiers and obtain federated verification services.

About This Document

This note is to be removed before publishing as an RFC.

This is a companion document to draft-condrey-rats-pop, which defines the core Proof of Process evidence framework. This document addresses Evidence lifecycle management after initial generation.

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."

This Internet-Draft will expire on 11 August 2026.

Table of Contents

1. Introduction

The Proof of Process (PoP) specification [I-D.condrey-rats-pop] defines how Attesters generate Evidence during document authorship. However, Evidence is not immutable once generated. Authors may need to:

* Mark old Evidence as superseded by newer Evidence

* Revoke Evidence if it was generated in error or under duress

* Update Evidence status after device key compromise

* Correct declarations or metadata errors

This document defines protocols for Evidence status management and revocation, as well as a Verifier registry enabling federated verification services.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Evidence Status Model

2.1. Status Values

Evidence packets may have the following status values:

active: Evidence is current and valid. This is the default status for newly generated Evidence.

superseded: Evidence has been replaced by a newer Evidence packet. The superseding packet-id is recorded. Superseded Evidence remains verifiable but should not be considered current.

revoked: Evidence has been explicitly revoked by the author. Revoked Evidence should not be trusted. A revocation reason is recorded.

suspended: Evidence is temporarily suspended pending investigation or dispute resolution. May transition to active, revoked, or remain suspended.

expired: Evidence has exceeded its validity period (if one was declared). Expired Evidence may still be verifiable for historical purposes but should not be considered current.

2.2. Status Update Structure

Status updates are CBOR-encoded structures signed by the original Evidence author. The following CDDL defines the status update format:

```
status-update = {
  packet-id: bstr,          ; Evidence packet being updated
  new-status: status-code,
  reason: reason-code,
  ? superseded-by: bstr,    ; For superseded status
  ? explanation: tstr,      ; Optional human-readable text
  timestamp: time,
  signature: bstr           ; Author signature over update
}

status-code = &(
  active: 0,
  superseded: 1,
  revoked: 2,
  suspended: 3,
  expired: 4
)

reason-code = &(
  unspecified: 0,
  key-compromise: 1,
  content-error: 2,
  metadata-error: 3,
  generated-in-error: 4,
  duress: 5,
  newer-version: 6,
  validity-expired: 7
)
```

Status transitions MUST follow these rules:

* active MAY transition to any other status

* superseded is terminal (no further transitions)

* revoked is terminal (no further transitions)

* suspended MAY transition to active or revoked

* expired MAY transition to revoked only

The signature MUST be created using the same key that signed the original Evidence packet. If the original key is compromised, the key compromise protocol in Section 3.2 applies.

3. Revocation Mechanisms

3.1. Author-Initiated Revocation

Authors may revoke their own Evidence by publishing a signed revocation statement. The statement includes:

* packet-id of the revoked Evidence
* Revocation reason code
* Optional explanatory text
* Timestamp of revocation
* Author signature (using same key that signed Evidence)

3.2. Key Compromise Handling

When a device signing key is compromised, all Evidence signed by that key may be affected. The key compromise protocol:

1. Author generates new device key
2. Author publishes key compromise notice (signed by new key + optional secondary authentication)
3. Notice specifies compromise window (earliest and latest possible compromise times)
4. Evidence within compromise window is marked as suspicious
5. Evidence outside window may be re-endorsed with new key

3.3. Revocation Distribution

Revocation information may be distributed through:

* Well-known URI: /.well-known/witnessd-revocations
* Revocation list embedded in Attestation Results

* Push notifications to subscribed Verifiers

* Blockchain or transparency log publication

4. External Verifier Registry

This section defines a protocol for discovering trusted Verifiers and obtaining federated verification services.

4.1. Verifier Discovery

Organizations may publish their trusted Verifiers at:

/.well-known/witnessd-verifiers

This endpoint returns a signed JSON document listing:

* Trusted Verifier identities and endpoints

* Verifier certificates

* Supported appraisal policies

* Service level agreements

4.2. Federated Verification

Federated verification enables Relying Parties in one organization to accept Attestation Results from Verifiers in another organization. The protocol operates as follows:

1. Relying Party receives Evidence packet from an author

2. Relying Party queries its organization’s trusted Verifier list

3. If the author’s organization has a trusted Verifier, the Relying Party forwards the Evidence to that Verifier

4. The remote Verifier appraises the Evidence and returns an Attestation Result

5. The Attestation Result is signed by the remote Verifier and includes the Verifier’s identity for accountability

6. The Relying Party validates the Attestation Result signature against the trusted Verifier list

Trust delegation allows organizations to designate other Verifiers as authoritative for specific author domains. Delegation statements are signed by the delegating organization and published in the Verifier registry.

Attestation Results from federated Verifiers MUST include:

* Original Evidence packet-id
* Verifier identity and organization
* Appraisal policy applied
* Timestamp of verification
* Result validity period

4.3. Verifier Accountability

Verifiers MUST maintain audit logs of all appraisal operations. Audit logs include:

* Timestamp of each appraisal request
* Evidence packet-id appraised
* Appraisal policy applied
* Result issued (without sensitive details)
* Requesting party identifier (if authenticated)

Audit logs MUST be retained for a minimum of 7 years to support legal and compliance requirements. Logs SHOULD be stored in append-only format to prevent tampering.

Misbehavior reporting enables Relying Parties to report Verifiers that issue inconsistent or incorrect Attestation Results:

1. Relying Party detects inconsistency (e.g., same Evidence receives conflicting results from same Verifier)
2. Relying Party submits misbehavior report to registry operator
3. Registry operator investigates and may revoke Verifier listing
4. Misbehavior reports are published for transparency

Organizations MAY implement reputation scoring for Verifiers based on consistency, availability, and misbehavior history. Reputation scores are advisory and do not replace explicit trust decisions.

5. Security Considerations

5.1. Revocation Freshness

Verifiers MUST check revocation status using fresh data. Cached revocation lists have a maximum validity period (RECOMMENDED: 24 hours for general use, 1 hour for high-security contexts).

5.2. Revocation Service Availability

Verifiers MUST handle revocation service unavailability gracefully. Two modes are defined:

Hard-fail mode: If revocation status cannot be determined, the Verifier MUST reject the Evidence as unverifiable. This mode is RECOMMENDED for high-security contexts where accepting potentially revoked Evidence poses significant risk.

Soft-fail mode: If revocation status cannot be determined, the Verifier MAY accept the Evidence with a warning flag indicating revocation status is unknown. The Attestation Result MUST clearly indicate this condition. This mode is acceptable for lower-risk contexts where availability is prioritized.

Verifiers SHOULD implement the following availability measures:

* Cache revocation lists with appropriate TTL

* Support multiple revocation distribution endpoints

* Implement exponential backoff for failed queries

* Monitor revocation service health proactively

Relying Parties MUST be informed of the Verifier’s failure mode and MAY override the default based on their risk tolerance.

5.3. Revocation Privacy

Revocation queries may reveal which Evidence packets a Verifier is checking, potentially leaking information about document verification patterns. The following mitigations apply:

* Verifiers SHOULD download complete revocation lists rather than querying individual packet-ids to prevent query correlation

* Revocation services MUST NOT log individual query patterns in a way that enables tracking specific Verifier behavior

* Batch queries SHOULD be supported to allow Verifiers to check multiple packet-ids in a single request, reducing metadata leakage

For high-privacy deployments, Verifiers MAY use Private Information Retrieval (PIR) techniques to query revocation status without revealing which packet-id is being checked. PIR support is OPTIONAL and deployment-specific.

Revocation lists MUST NOT include information beyond what is necessary for status determination. Specifically, revocation reasons are available only to authenticated parties with a legitimate need to know.

6. Privacy Considerations

This section addresses privacy implications of Evidence status management and Verifier registry operations.

6.1. Verifier Tracking Prevention

Verifiers process Evidence from multiple authors and may accumulate significant metadata about verification patterns. To prevent misuse:

* Verifiers MUST NOT correlate verification requests across different Relying Parties without explicit consent

* Verification logs MUST be purged of personally identifiable information after the retention period expires

* Verifiers MUST NOT share verification metadata with third parties except as required by law

6.2. Metadata Minimization

Status updates and revocation statements contain metadata that could be privacy-sensitive. Implementations MUST:

* Include only the minimum metadata necessary for status determination

* Avoid including IP addresses, device identifiers, or location data in status update structures

* Use opaque packet-ids that do not encode author identity

6.3. Anonymous Verification Mode

For privacy-sensitive contexts, Verifiers MAY support anonymous verification where:

* Relying Party identity is not required for verification
* No verification logs are retained
* Rate limiting is applied to prevent abuse

Anonymous verification provides weaker accountability guarantees and is not suitable for all deployment contexts. Verifiers MUST clearly document whether anonymous mode is supported.

7. IANA Considerations

This document requests registration of the following well-known URIs:

* URI suffix: witnessd-revocations
* URI suffix: witnessd-verifiers

Change controller: IETF

Specification document: [this document]

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

8.2. Informative References

[I-D.condrey-rats-pop]
Condrey, D., "Proof of Process: An Evidence Framework for Digital Authorship Attestation", Work in Progress, Internet-Draft, draft-condrey-rats-pop, <https://datatracker.ietf.org/doc/html/draft-condrey-rats-pop>.

Author's Address

David Condrey
Writerslogic Inc
United States
Email: david@writerslogic.com