Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 10 July 2026

D. Wang
F. Liu
Y. Jiang
J. Zhang
Huawei

6 January 2026

Distributed Remote Attestation
draft-wang-rats-distributed-remote-attestation-02

Abstract

In many deployments, remote attestation is performed within separate administrative and trust domains. Each domain typically operates its own management plane and a Remote Attestation Service (RAS) to obtain verifier inputs (e.g., endorsement material and reference values) and produce attestation results. At scale, cross-domain scenarios face two recurring challenges: (1) enabling policy-controlled transparency so that verifiers or relying parties in one domain can discover and retrieve selected attestation artifacts from other domains; and (2) supporting many-to-many distribution and reuse of verifier inputs and verifier outputs without requiring point-to-point integrations.

This document describes Distributed Remote Attestation (DRA) patterns that use a shared publication channel for selected artifacts with provenance and access control in mind. A Distributed Ledger (DL) is discussed as one concrete instantiation of such a publication channel, including an option to host verification logic on the DL. The described patterns are intended to complement existing RATS procedures and conceptual messages, and can be realized by other tamper-evident publication channels with comparable properties.

This Internet-Draft will expire on 10 July 2026.

Table of Contents

1. Introduction 2
2. Requirements Language 4
3. Conventions and Definitions 4
3.1. Abbreviations 4
3.2. Additional Definitions 4
4. DRA Patterns 5
4.1. DL publication with off-chain attestation and verification 5
4.2. DL publication with optional on-chain verification . . . 6
5. Discussion 8
5.1. Freshness and Reuse 8
5.2. Access Control and Provenance 8
6. IANA Considerations 9
7. Security Considerations 9
8. References 9
8.1. Normative Reference 9
8.2. Informative References 9
Acknowledgments 9
Authors' Addresses 9

1. Introduction

Remote attestation is increasingly deployed in federated and multi-operator environments where devices, services, and management systems span multiple administrative and trust domains. In practice, each trust domain often operates its own Remote Attestation Service (RAS) integrated into that domain's management plane, and exposes attestation capabilities and artifacts according to local policies.

Cross-domain deployments expose a gap that is not primarily about the attestation evidence format or the appraisal function itself, but about _how attestation artifacts are discovered, distributed, and reused_ across domains at scale. Two pain points are repeatedly observed:

* _Cross-domain attestation transparency:_ A verifier or relying party in domain-A may need to obtain endorsement material, reference values, or attestation results that originate in domain-B. Direct point-to-point integration between operational sites does not scale, and is often infeasible due to operational domains and policy constraints. Deployments therefore need a policy-consensus controlled channel to publish and retrieve selected artifacts with clear provenance.

* _Many-to-many distribution and reuse of security artifacts:_ Verifiers appraising heterogeneous attesters need to obtain endorser public keys, endorsements, and reference values from multiple providers. Conversely, providers need to distribute artifacts to multiple verifiers across domains. Similar many-to-many scaling issues apply when attestation results are shared for reuse by other verifiers or relying parties. Without a shared publication channel, each integration becomes a bespoke, brittle dependency.

This document proposes a set of DRA patterns that make selected attestation artifacts more reusable across multiple verifiers and domains by introducing a shared publication channel. The publication channel is used to distribute: (a) verifier inputs such as endorser public keys, endorsements, and reference values; and (b) verifier outputs such as attestation results (or pointers/digests).

A Distributed Ledger (DL) is discussed as one concrete instantiation of the publication channel. DLs provide tamper-evidence and append-only provenance, and can be deployed in permissioned settings with authenticated writes and controlled reads. Where appropriate, a DL can additionally host verification logic (e.g., smart contracts) to record appraisal outcomes in a shared, auditable manner. The patterns in this document are not limited to DLs and can also be realized using other tamper-evident publication channels with comparable integrity and availability properties.

The rest of this document is organized as follows: Section 3 defines terminology and abbreviations; Section 4 specifies two DRA patterns (off-chain attestation/verification with on-channel publication, and an option for on-channel verification); and Section 5 discusses freshness, access control, governance, and privacy considerations.

2. Requirements Language

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 [RFC2119] .

3. Conventions and Definitions

This document uses roles and concepts defined by the RATS Architecture [RFC9334] (e.g., Attester, Verifier, Endorser, Reference Value Provider, and Relying Party).

3.1. Abbreviations

DL: Distributed Ledger.

DRA: Distributed Remote Attestation (the patterns described in this document).

RAS: Remote Attestation Service (deployment-specific service performing verifier functions or mediating access to verifier inputs/outputs).

RV: Reference Value (as in [RFC9334]).

AE: Attestation Evidence (as in [RFC9334]).

AR: Attestation Result (as in [RFC9334]).

3.2. Additional Definitions

Artifact Publisher: An entity that publishes selected attestation artifacts to the publication channel, such as an Endorser publishing endorsement material, a Reference Value Provider publishing RVs, or a Verifier publishing ARs (or pointers/ digests).

Artifact Consumer: An entity that retrieves artifacts from the publication channel, such as a Verifier retrieving RVs/ endorsements, or a Relying Party retrieving ARs for decision-making.

Publication Channel: A shared channel used to publish and retrieve selected attestation artifacts with provenance. A DL is one concrete instantiation; other tamper-evident channels may also be used.

4. DRA Patterns

This section describes two common patterns for using a DL-backed RAS as a publication channel for attestation artifacts. Both patterns assume that RVs and Endorser material (e.g., public keys and endorsement metadata) can be published to, and retrieved from, the DL under suitable access control policies.

4.1. DL publication with off-chain attestation and verification

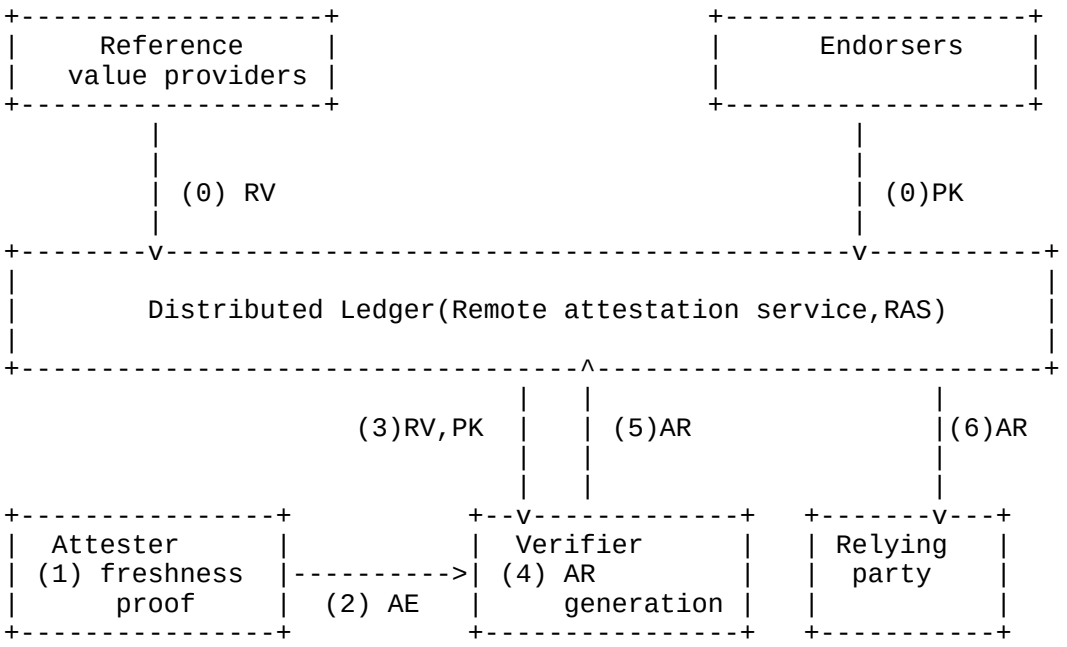

Figure 1 on-chain-based publication and off-chain-based attestation/verification

Figure 1: DL publication with off-chain attestation and verification

As shown in Figure 1, attestation evidence exchange and appraisal follow existing RATS flows, while the DL is used to publish and retrieve verifier inputs and verifier outputs:

0) _Registration/publication of inputs:_ Reference Value Providers publish RVs to the DL/RAS. Endorsers publish endorsement-related artifacts (e.g., endorser public keys (PK) and/or endorsements) to the DL/RAS. Access control and provenance mechanisms (e.g., permissioning, signatures) are deployment-specific.

1) _Freshness proof preparation:_ A freshness challenge/context may

be issued by the Verifier, RP, or another authorized requester acting under policy (e.g., a domain management function). The challenge can take different forms depending on deployment (e.g., a nonce, an epoch identifier, a timestamp requirement, or a context string bound to an intended appraisal). The Attester uses the received challenge/context to construct a _freshness proof_ that will be included in AE (see step (2)).

2) _Evidence (off-chain):_ The Attester generates AE, incorporating the freshness proof required by the Verifier, and sends AE to the Verifier over an authenticated and integrity-protected channel.

3) _Retrieval of appraisal inputs:_ The Verifier retrieves RVs and Endorser artifacts (e.g., PK) from the DL/RAS (or from caches populated from it), and uses them as appraisal inputs.

4) _Result generation and publication:_ The Verifier appraises AE using the retrieved RV/PK, and generates AR.

5) _Publication of results:_ The Verifier publishes AR (or a pointer/digest to AR) to the DL/RAS for cross-domain discovery and potential reuse, subject to policy, privacy, and confidentiality constraints.

6) _Reuse:_ RP retrieves AR from the DL/RAS and decides whether to reuse it based on provenance, freshness/validity window, and local policy.

4.2. DL publication with optional on-chain verification

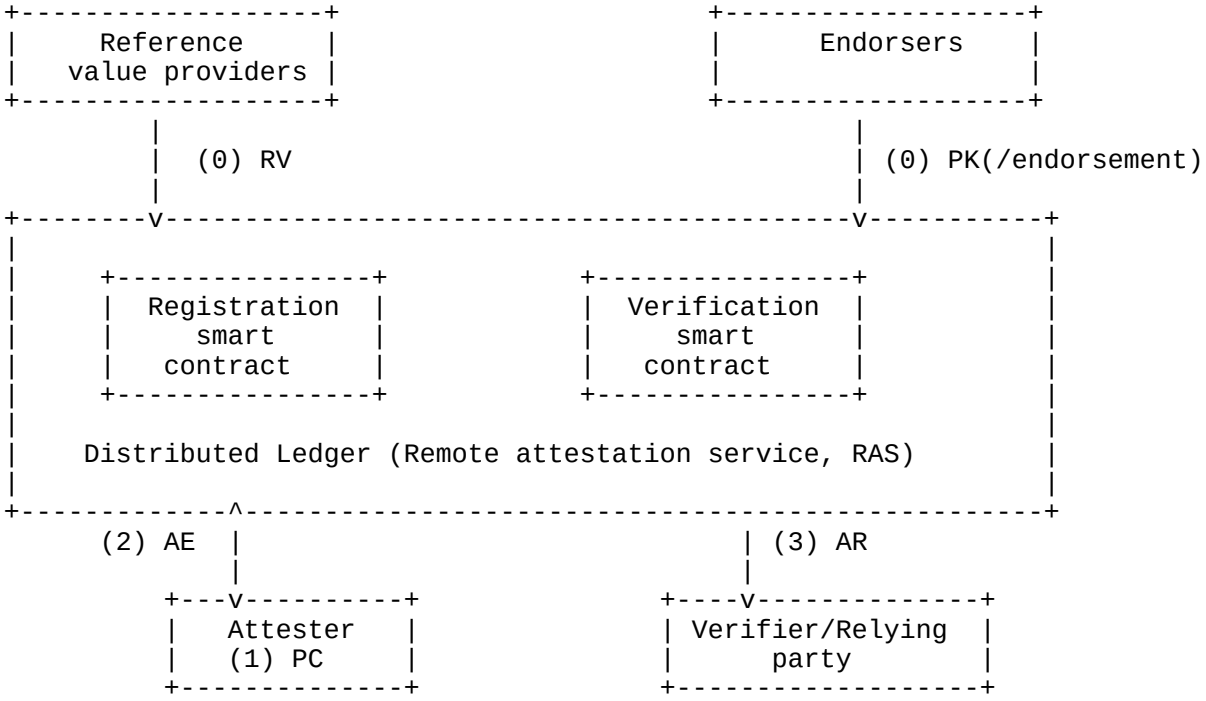

Figure 2 on-chain-based publication/attestation/verification

Figure 2: DL publication with optional on-chain verification

As shown in Figure 2, it can be beneficial to verify and/or record appraisal outcomes in a shared, tamper-evident way. In this pattern, the DL is used for publication as in the previous pattern, and hosts verification logic (e.g., smart contracts) or record verifiers' appraisal outcomes.

0) _Registration/publication of inputs:_ RVs and Endorser artifacts (e.g., PK/endorsements) are published to the DL/RAS. The _Registration smart contract_ supports publication authorization, schema/version checks, and governance rules.

1) _Evidence publication:_ The Attester generates AE and submits it to the DL/RAS via the Registration smart contract. AE could include a freshness proof suitable for publication and reuse (e.g., timestamp or epoch ID). The Attester may also obtain/ derive a public challenge (PC) value to support freshness/ unpredictability of the subsequent evidence. A common realization is to use a DL-derived value such as a recent block hash (or other consensus-derived header material). The block-generation process

(consensus, timestamps, and transaction sets) makes future block hashes hard to predict in advance, and the one-way property of hash functions prevents an attacker from predefining a desired hash by reverse-engineering corresponding block contents. Such selected PC is incorporated into AE in step (2).

2) _Verification and result recording (on-chain):_ The _Verification smart contract_ (or other on-chain verification logic) verifies AE using RVs and Endorser artifacts available from the DL/RAS, and checks freshness according to configured policy (e.g., acceptable time window / epoch constraints). The appraisal outcome is recorded as AR (or an appraisal log entry) on-chain. Triggering may be initiated by a Verifier, a Relying Party, or automatically upon AE submission, subject to policy.

3) _Result retrieval:_ The Verifier/RP queries the DL/RAS and obtains AR for decision-making and/or reuse.

5. Discussion

5.1. Freshness and Reuse

For the DRA service, the blocks of the DL need to be generated at appropriate time intervals, such as every few seconds. The consensus rules trigger the new block generation process periodically through preset time parameters. Even if there is no transaction data within a specific period, nodes will still generate an empty block containing basic information like the hash of the previous block and timestamps according to established algorithms. This approach aims to maintain the continuity of the DL chain structure and the orderliness of timestamps, thereby ensuring the freshness and validity of PC.

Artifact Consumers evaluates whether retrieved artifacts are fresh enough for their own threat model and acceptable staleness window. When ARs are published for reuse, it is recommended that ARs include time-of-appraisal and a validity interval, so that downstream consumers can make an informed decision.

5.2. Access Control and Provenance

The publication channel enforces authorization for publication. Consumers validates provenance and integrity (e.g., signatures, trust anchors) for retrieved RVs, endorsement material, and ARs. Deployments further defines governance for artifact update/rollback and caching policies.

6. IANA Considerations

This document has no IANA considerations.

7. Security Considerations

TODO

8. References

8.1. Normative Reference

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

8.2. Informative References

[RFC9334] Thaler, D., Richardson, M., Smith, M., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", January 2023, <https://datatracker.ietf.org/doc/rfc9334/>.

Acknowledgments

TODO

Authors' Addresses

Donghui Wang
Huawei
Email: wangdonghui124@huawei.com

Faye Liu
Huawei
Email: liufei19@huawei.com

Yuning Jiang
Huawei
Email: jiangyuning2@h-partners.com

Jun Zhang
Huawei
Email: junzhang1@huawei.com