SCITT
Internet-Draft
Intended status: Standards Track
Expires: 2 November 2026

J. Hillier
Certisyn, Inc.

1 May 2026

Attestation Reconciliation Protocol
draft-hillier-scitt-arp-00

Abstract

This document specifies the Attestation Reconciliation Protocol (ARP), a deterministic, bilateral, zero-knowledge-capable mechanism for reconciling verification claims against a plurality of sovereign authoritative registers without raw register records leaving their data-residency jurisdiction. ARP extends the SCITT (Supply Chain Integrity, Transparency, and Trust) architecture to cross-sovereign claim reconciliation. A reconciliation server canonicalises a structured claim, projects it through register-specific controlled projection functions producing the greatest-lower-bound predicate supported by each addressed register, transmits register-specific ciphertexts, receives partial attestations whose payload discloses only a verdict and an optional divergence axis, aggregates the partial attestations through either homomorphic or hash-linkage aggregation, and seals the resulting reconciliation output against a policy-version hash. An append-only cross-jurisdictional settlement-layer ledger records only hashes, with no content. The protocol supports retroactive re-evaluation of historical reconciliations under updated pattern libraries or policy versions without bilateral renegotiation, and a cryptographic-primitive-upgrade path including post-quantum primitives.

Table of Contents

1. Introduction

Sovereign authoritative registers record facts that are treated as conclusive within their jurisdiction. Examples include beneficial-ownership registers (such as the United States FinCEN Beneficial Ownership Secure System, the United Kingdom People with Significant Control register, and the European Union beneficial-ownership registers under the Anti-Money-Laundering Directives), corporate registries, consolidated sanctions lists, export-control registers, foreign-ownership-and-control-or-influence registers, maritime vessel registrations, flag-state registers, aviation registrations, land-title registries, customs declarations, and multilateral biometric registers.

Institutional decision-makers -- including export-control compliance officers, anti-money-laundering review functions, foreign-investment screening review functions, sanctions-screening operators, multilateral aid distribution authorities, and platform-owned verification infrastructure -- routinely require reliance on facts recorded across two or more sovereign registers simultaneously.

Existing computer-implemented approaches to such cross-sovereign reliance suffer from three structural and technical deficiencies that this protocol is specifically designed to overcome:

1. *Raw-record disclosure.* Existing approaches require the raw register record either to leave its data-residency jurisdiction or to be re-disclosed in plaintext to a relying party in another jurisdiction. Sovereign registers under data-protection regimes are jurisdictionally constrained against such re-disclosure.

2. *Non-reconcilable register outputs.* Each sovereign register exposes a different schema, a different signing chain, a different verdict semantic, and a different statutory access regime. A relying party that requires a deterministic combined verdict over n sovereign registers therefore faces n parallel verification problems.

3. *Non-auditable settlement.* Cross-sovereign reliance, where it occurs at all, occurs without a settlement-layer audit trail consumable by sovereign regulators.

This document specifies ARP, a protocol that addresses all three deficiencies in combination, and is layered atop the SCITT architecture [I-D.ietf-scitt-architecture] and the RATS architecture [RFC9334].

2. Conventions and Definitions

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.

The following terms are defined for use throughout this document:

Sovereign Register: An authoritative data store maintained by or on behalf of a sovereign and treated as conclusive within that sovereign’s jurisdiction for the predicates the register is empowered to record.

Register Operator: The entity that operates the Sovereign Register and is contractually empowered to bind the register’s attestations.

Bilateral Register Agreement: A negotiated contractual instrument between the operator of the reconciliation server and a Register Operator, declaring the permitted-predicate set, supported cryptographic primitives, supported aggregation capability, statutory-regulator-access scope, and cryptographic-primitive-upgrade path. Each Bilateral Register Agreement carries an Agreement Hash committing to its canonicalised content.

Canonical Claim: A deterministic structured representation of a verification claim, comprising at least a subject identifier, a predicate, an attested value, an applicable-regimes set, and an evidentiary provenance manifest. Canonicalisation comprises lexicographic sorting of object keys, preservation of declared array order, Unicode Normalization Form C of string fields, canonical JSON [RFC8259] number rendering, and stripping of undefined values.

Predicate Taxonomy: A controlled hierarchical classification of predicates that may be the subject of reconciliation, enabling taxonomic prefix match in projection.

Per-Register Claim Projection: The narrowest structured query

sufficient to elicit the required Partial Attestation under a register's Bilateral Register Agreement, computed by the controlled projection function as the greatest-lower-bound predicate within the register's permitted-predicate set.

Partial Attestation: A cryptographically signed output produced by a Sovereign Register in response to a Per-Register Claim Projection. The Partial Attestation payload SHALL disclose only a Reconciliation-Verdict field and an OPTIONAL Divergence-Axis field; it SHALL NOT disclose any register record.

Divergence Axis: A controlled descriptor identifying the structural reason for a non-match verdict, drawn from a controlled set including identity-mismatch, jurisdictional-scope-mismatch, temporal-mismatch, ownership-threshold-mismatch, sanctions-list-match, register-record-absent, claim-predicate-unsupported, and claim-projection-narrowed-beyond-attestation-scope.

Reconciliation Output: A data structure aggregating Partial Attestations from a single reconciliation event, sealed against a Policy-Version Hash.

Verdict Arithmetic: The operator governing how per-register verdicts combine into the Combined Verdict, drawn from a controlled set including conjunction, disjunction, threshold-count, and source-class-quorum.

Homomorphic Aggregation: A cryptographic aggregation of Partial Attestations under a homomorphic primitive permitting verdict combination without decommitment of intermediate per-register outputs.

Hash-Linkage Aggregation: An aggregation of Partial Attestations in which the per-register attestations are canonical-hashed, ordered, committed to a Merkle tree, and emitted with a Merkle root and a per-register verdict band.

Policy-Version Hash: A cryptographic commitment to the canonical verification-policy state in force at the moment of reconciliation, including reconciliation rules, threshold parameters, pattern-library version, applicable-regimes precedence, verdict-arithmetic selection, and the Bilateral-Register- Agreement Hashes of the addressed registers.

Settlement-Layer Ledger: An append-only cross-jurisdictional log retaining only hashes of reconciliations, with no content-bearing fields. Each entry comprises a sequence number, the reconciliation hash, the policy-version hash, the addressed-

registers identifier set, an aggregation-method descriptor, an optional Merkle root, a timestamp, a prior-entry hash, and a self-entry hash.

3. Architecture

ARP comprises eleven subsystems arranged as a deterministic pipeline:

1. Canonical Claim Ingestion
2. Adversarial Pre-Transmission Test
3. Per-Register Projection Function
4. Per-Register Encryption
5. Partial-Attestation Reception
6. Aggregation (Homomorphic or Hash-Linkage)
7. Policy-Version-Hash Sealing
8. Settlement-Layer Ledger Write
9. Regulator Portal
10. Retroactive Evaluation
11. Cryptographic-Primitive-Upgrade Path

Given an identical Canonical Claim, an identical Addressed-Registers Identifier Set, identical Bilateral-Register-Agreement Hashes for the addressed registers, an identical Pattern-Library Version Identifier, and an identical Policy-Version Identifier, the system MUST produce bit-for-bit identical Reconciliation Outputs and Settlement-Layer Ledger entries.

3.1. Canonical Claim Ingestion

A Canonical Claim comprises:

* Subject Identifier
* Predicate (drawn from the controlled Predicate Taxonomy)
* Attested Value (in the canonical type for the Predicate)
* Applicable-Regimes Set

* Evidentiary Provenance Manifest

* Claim Timestamp (RFC 3339 UTC)

* Claim Hash (computed over the canonical serialisation)

Two semantically-equivalent claims MUST produce the same canonical form and the same Claim Hash. The Claim Hash is the index on the Settlement-Layer Ledger and the key for retroactive re-evaluation.

3.2. Adversarial Pre-Transmission Test

Before any Per-Register Claim Projection is produced, the Adversarial Pre-Transmission Test Subsystem applies the current Pattern Library to the Canonical Claim. The Pattern Library enumerates known nation-state evasion patterns including projection-narrowing-evasion, predicate-substitution- evasion, attested-value-bracketing-evasion, addressed-register-cherry-picking, agreement-staleness-injection, and pattern-library-version-pinning.

The Subsystem emits either a Pass result or a Remediation Advisory. The Per-Register Encryption Subsystem MUST architecturally withhold external transmission until a Pass result has been emitted or until an authorised operator has explicitly overridden the outcome.

3.3. Per-Register Projection Function

For each addressed register, the controlled projection function MUST inspect the Canonical Claim against the permitted-predicate set declared in the Bilateral Register Agreement. Where the Canonical Claim’s Predicate is directly a member of the permitted-predicate set, the Projected Predicate equals the Canonical Claim Predicate.

Where it is not, the projection function resolves the Predicate through taxonomic prefix match: walking the Predicate Taxonomy upward from the Canonical Claim Predicate until reaching a Predicate that is a member of the permitted-predicate set. The narrowing operation MUST be recorded in the Narrowed-From field of the Per-Register Claim Projection.

3.4. Per-Register Encryption

Each Per-Register Claim Projection MUST be encrypted under the addressed register’s public-key material declared in the Bilateral Register Agreement. The encryption operation MUST bind the Bilateral-Register-Agreement Hash and the Pattern-Library Version Identifier into the ciphertext as authenticated additional data, such that a register attempting to decrypt under a stale Bilateral-

Register-Agreement Hash or Pattern-Library Version Identifier fails at the authenticated-additional-data verification step.

3.5. Partial Attestation Reception

A Partial Attestation comprises:

* Register Identifier
* Reconciliation-Verdict Field (match, no-match, partial-match, or indeterminate)
* OPTIONAL Divergence-Axis Field
* Bilateral-Register-Agreement Hash
* Policy-Version Hash
* Cryptographic Signature over the canonical payload of the foregoing
* Freshness Timestamp

The Partial Attestation payload SHALL NOT contain any register-record field, any pre-image of the register record, or any field beyond those enumerated. The architectural absence of register-record content is the specific technical mechanism by which ARP avoids raw-record disclosure.

3.6. Aggregation

Where every addressed register declares Homomorphic capability, the aggregation subsystem operates in Homomorphic Aggregation Mode. Per-register encrypted verdict contributions are aggregated through a homomorphic operator sequenced according to the Verdict Arithmetic declared in the Applicable-Regimes Set. Intermediate values remain cryptographically committed.

Where any addressed register does not declare Homomorphic capability, the aggregation subsystem MUST operate in Hash-Linkage Aggregation Mode. Each Partial Attestation is canonical-hashed, ordered by sorted-leaf construction, committed to a Merkle tree, and emitted with a Merkle root and a per-register verdict band signed by the reconciliation-server sealing key. The per-register verdict band MUST commit each register’s verdict individually without disclosure of any other register’s payload.

3.7. Policy-Version-Hash Sealing

The Policy-Version Hash MUST commit to:

1. Reconciliation rules
2. Threshold parameters
3. Pattern-Library Version Identifier
4. Applicable-Regimes precedence
5. Verdict-Arithmetic selection
6. Bilateral-Register-Agreement Hashes of the addressed registers

The Policy-Version Hash MUST be reconstructible under audit from a canonical policy state persisted in a policy-epoch store.

3.8. Settlement-Layer Ledger

Each Settlement-Layer Ledger entry comprises only:

* Entry Sequence Number (monotonically increasing)
* Reconciliation Hash
* Policy-Version Hash
* Addressed-Registers Identifier Set (sorted in canonical lexicographic order)
* Aggregation-Method Descriptor
* OPTIONAL Merkle Root
* Reconciliation Timestamp
* Prior-Entry Hash
* Self-Entry Hash

The Ledger MUST NOT store Canonical-Claim content, register records, or Partial-Attestation payloads. The append-only constraint MUST be enforced at the storage interface layer; the Ledger interface MUST expose only an APPEND operation, with no UPDATE or DELETE operation exposed or implemented.

The Ledger MAY be distributed across a plurality of per-jurisdiction secondary stores under synchronous replication, each operated under the data-residency constraints of its host jurisdiction. The append-only derivation-chain invariant -- that every entry's Prior-Entry Hash equals the Self-Entry Hash of the immediately preceding entry -- MUST be preserved across all secondary stores.

3.9. Regulator Portal

The Regulator Portal Subsystem authenticates a sovereign regulator's jurisdictional credentials against a regulator-identity-provider trust anchor declared in at least one Bilateral Register Agreement. It restricts returned fields to those within the regulator's statutory scope as declared in the statutory-regulator-access scope of the Bilateral Register Agreements of the addressed registers. The scope restriction is computed as the union of per-agreement permitted-read-predicates entries scoped to the regulator's jurisdiction, intersected with the regulator's requested field set. Each access MUST be recorded in an append-only subpoena-grade audit trail.

3.10. Retroactive Evaluation

Upon publication of an updated Pattern Library or an updated Policy Version, the Retroactive Evaluation Subsystem MUST execute a deterministic re-application of the updated policy state to retained reconciliation metadata of historical Reconciliation Outputs sealed against a superseded Policy-Version Hash. Where permissible under the applicable Bilateral Register Agreements, partial attestations MAY be re-invoked.

The retroactive evaluation MUST be executable without re-negotiation of any Bilateral Register Agreement. A material change in a historical Combined Verdict -- defined as any transition into or out of a decisive verdict value (the decisive values being match and no-match) -- MUST trigger a Sovereign Re-Notification through the Regulator Portal.

3.11. Cryptographic-Primitive-Upgrade Path

Each Bilateral Register Agreement MUST declare a Cryptographic-Primitive- Upgrade Path comprising an ordered equivalence list for each of three primitive classes: claim-encryption, partial-attestation-signature, and sealing-signature. The equivalence list MUST include at least one post-quantum primitive for each class, drawn from a set including ML-KEM [FIPS203] for key encapsulation and ML-DSA [FIPS204] for signature operations.

A primitive rotation MAY be executed simultaneously across the three layers without bilateral renegotiation. The Settlement-Layer Ledger remains continuous across the rotation because Ledger entries commit to hashes of canonicalised content rather than to cryptographic identities.

4. Encoding

4.1. CBOR-COSE Encoding

The recommended encoding for ARP messages on the wire is CBOR with COSE [RFC9052] [RFC9053] envelopes. COSE_Sign1 is used for both Partial Attestations and the Sealing Signature. The protected header MUST include the Bilateral-Register-Agreement Hash and Policy-Version Hash as unregistered labels in the range 0x800 .. 0x8FF (Certisyn private use).

4.2. Verifiable Credentials Interop

A Reconciliation Output MAY be additionally serialised as a JSON-LD document conforming to the W3C Verifiable Credentials Data Model [W3C-VC-DM-2.0], with the Reconciliation Hash, Addressed-Registers Identifier Set, Bilateral-Register-Agreement Hash Set, and Policy-Version Hash included as credential subject fields. The COSE_Sign1 envelope is the normative form; the Verifiable Credential serialisation is an interop convenience for relying parties operating in W3C VC ecosystems.

5. Security Considerations

5.1. Service-Operator Containment

The reconciliation server operates under a service-operator entity standing in bilateral contractual relationship with each Register Operator. The service-operator entity MUST be architecturally prohibited from observing any register record or any Partial-Attestation payload beyond the verdict and divergence-axis fields. The service-operator entity MUST be structurally incapable of disclosing any register record irrespective of internal operator action.

5.2. Pattern-Library Integrity

The Adversarial Pre-Transmission Test gates onward transmission. The Pattern Library MUST be bound to a Pattern-Library Commitment Hash. Any modification to the Pattern Library MUST produce a new Pattern-Library Version Identifier, and the Adversarial Pre-Transmission Test MUST be re-executed against the new library before the change takes effect.

5.3. Bilateral-Register-Agreement Drift

Each Bilateral Register Agreement carries an Agreement Hash. Each Partial Attestation includes a reference to the Agreement Hash under which it was issued. Agreement drift is detectable by comparison of agreement-hash references across Partial-Attestation batches. Reconciliation MUST be suspended for an addressed register whose Agreement Hash deviates from the hash committed at the start of a reconciliation event.

5.4. Replay Defence

Each Partial Attestation MUST carry a Freshness Timestamp. The reconciliation server MUST verify the Freshness Timestamp against a freshness window declared in the Bilateral Register Agreement. Stale Partial Attestations MUST be rejected with a freshness-stale divergence axis.

5.5. Post-Quantum Migration

The Cryptographic-Primitive-Upgrade Path is the mechanism by which ARP deployments migrate to post-quantum primitives. ML-KEM-1024 [FIPS203] is RECOMMENDED for the claim-encryption primitive class. ML-DSA-65 [FIPS204] is RECOMMENDED for the partial-attestation-signature and sealing-signature primitive classes. Implementations MUST declare their chosen post-quantum primitives in the Bilateral Register Agreement.

5.6. Side-Channel Considerations

Per-register projection narrowing is observable to the addressed register through the Projected Predicate. Implementations MUST NOT use narrowing patterns to fingerprint individual subjects. The Predicate Taxonomy SHOULD be designed such that the set of permitted narrowings is small enough that narrowing observation does not materially weaken subject privacy.

6. IANA Considerations

This document requests IANA to register the following:

* A namespace for ARP-specific COSE protected-header labels in the range 0x800 .. 0x8FF, containing at least:
  - arp-bilateral-agreement-hash (label 0x801)
  - arp-policy-version-hash (label 0x802)
  - arp-pattern-library-hash (label 0x803)
  - arp-divergence-axis (label 0x804)
* A media type application/arp-reconciliation-output+cbor for the CBOR-encoded Reconciliation Output.
* A media type application/arp-reconciliation-output+json for the Verifiable Credentials JSON-LD form.

7. Acknowledgments

This document benefits from the SCITT Architecture [I-D.ietf-scitt-architecture], the SCITT Receipts specification [I-D.ietf-scitt-receipts], and the RATS Architecture [RFC9334].

8. References

8.1. Normative References

[I-D.ietf-scitt-architecture]
Birkholz, H., Delignat-Lavaud, A., Fournet, C., Deshpande, Y., and S. Lasker, "An Architecture for Trustworthy and Transparent Digital Supply Chains", Work in Progress, Internet-Draft, draft-ietf-scitt-architecture-22, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-scitt-architecture-22>.

[I-D.ietf-scitt-receipts]
"*** BROKEN 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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/rfc/rfc9334>.

8.2. Informative References

[FIPS203] "Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)", NIST FIPS 203, 2024, <https://csrc.nist.gov/publications/detail/fips/203/final>.

[FIPS204] "Module-Lattice-Based Digital Signature Standard (ML-DSA)", NIST FIPS 204, 2024, <https://csrc.nist.gov/publications/detail/fips/204/final>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/rfc/rfc7515>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/rfc/rfc7519>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/rfc/rfc8259>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/rfc/rfc9053>.

[W3C-VC-DM-2.0] "Verifiable Credentials Data Model 2.0", 2025, <https://www.w3.org/TR/vc-data-model-2.0/>.

Appendix A. Examples

A.1. Example: Three-register Sanctions Reconciliation

A relying party requests reconciliation of the predicate sanctions:any-list-match for subject identifier corp:DUNS:0123456789 against the OFAC SDN list, the EU consolidated list, and the UK OFSI list.

Each Bilateral Register Agreement permits the predicate. The projection function emits identical Per-Register Claim Projections to all three registers. All three return Partial Attestations with verdict no-match.

The Aggregation Subsystem operates in Homomorphic Aggregation Mode (all three registers declare homomorphic capability). The Verdict Arithmetic is disjunction. The Combined Verdict is no-match.

The Reconciliation Output is sealed against the current Policy-Version Hash. The Settlement-Layer Ledger entry comprises:

* Entry Sequence Number: 4,217,981
* Reconciliation Hash: <32 bytes>
* Policy-Version Hash: <32 bytes>
* Addressed-Registers Identifier Set: ["EU-CONSOLIDATED-2026-Q2", "UK-OFSI-2026-Q2", "US-OFAC-SDN-2026-Q2"]
* Aggregation-Method Descriptor: "homomorphic-disjunction"
* Reconciliation Timestamp: 2026-04-27T19:47:14Z
* Prior-Entry Hash: <32 bytes>
* Self-Entry Hash: <32 bytes>

No register record content is stored on the Ledger.

A.2. Example: Retroactive Re-evaluation

Six weeks after the above reconciliation, OFAC adds the subject to the SDN list as part of a new tranche. The OFAC register’s Partial-Attestation endpoint, on next invocation, would return verdict match with divergence-axis sanctions-list-match.

The Retroactive Evaluation Subsystem detects the new Pattern-Library and Policy-Version transition, re-invokes Partial Attestations on all historical reconciliations addressing OFAC under the superseded Policy-Version Hash, identifies the material verdict change, and emits a Sovereign Re-Notification through the Regulator Portal to the regulators whose statutory-regulator-access scope intersects the changed reconciliation. A new Reconciliation Output is appended to the Ledger referencing the superseded one in its Source-Reconciliation-Output Identifier field.

Appendix B. Composition with the SCITT Architecture

The SCITT Architecture [I-D.ietf-scitt-architecture] provides notarisation of supply-chain artefacts, including transparency receipts, transparent statements, and registries. ARP composes with SCITT in three ways:

1. SCITT receipts MAY be the input claim to ARP. A claim referencing a SCITT-anchored artefact (its hash and its registration receipt) is reconciled across registers without disclosing the underlying artefact.

2. ARP Reconciliation Outputs MAY be notarised into SCITT registries as transparent statements, enabling SCITT-aware relying parties to verify the cross-sovereign reconciliation event in the same way they verify any other supply-chain claim.

3. The SCITT Architecture’s Identity Manager and Issuer roles map cleanly to the Bilateral Register Agreement structure: each Sovereign Register acts as a SCITT Issuer for a constrained predicate set, and the reconciliation server acts as a SCITT Aggregator across multiple Issuers.

Appendix C. Composition with the RATS Architecture

The RATS Architecture [RFC9334] provides remote-attestation procedures for compute-substrate trust. ARP composes with RATS in two ways:

1. The Adversarial Pre-Transmission Test runs inside a confidential computing boundary attested under RATS. The reconciliation server’s integrity MAY be verified by relying parties through standard RATS verification flows.

2. Compute-attestation reconciliation across heterogeneous TEE / CC providers is the natural specialisation of ARP to the RATS evidence class. A separate document specifies that specialisation.

Author’s Address

Joel David Hillier
Certisyn, Inc.
Email: jhillier@certisyn.com