Independent Submission
Internet-Draft
Intended status: Informational
Expires: 1 December 2026

C. Hopley
AlgoVoi

30 May 2026

Composite Trust Query Response Format for Agentic-Payment Audit Chains
draft-hopley-x402-composite-trust-query-01

Abstract

This document specifies a composite trust query response format for agentic-payment audit chains. The format records a verifier's categorical conclusion over an audit chain composed of compliance, settlement, cancellation, and refund receipts, in response to a stated query.

The response format uses a closed four-element enumeration of categorical outcomes (TRUSTED, PROVISIONAL, INSUFFICIENT_EVIDENCE, UNTRUSTED). The four-state enumeration captures the operationally-distinct decision space: proceed, proceed-with-caution, hold-pending-more-data, halt. Collapsing to three values loses the distinction between INSUFFICIENT_EVIDENCE ("we could not verify either way") and UNTRUSTED ("we verified and the answer is no"), which matters for operator dashboards, regulator reporting, and downstream automated decision-making.

The format is verifier-emitted and audit-chain-anchored. A verifier walks an audit chain composed of compliance receipts (draft-hopley-x402-compliance-receipt), settlement attestations (draft-hopley-x402-settlement-attestation), cancellation receipts (draft-hopley-x402-cancellation-receipt), and refund receipts (draft-hopley-x402-refund-receipt), applies a structured query identified by content-addressed reference, and emits a single composite-trust-claim response anchoring the chain by its content-addressed root.

The format composes above the four receipt formats under the same canonicalisation discipline (draft-hopley-x402-canonicalisation-jcs). Regulators, dashboards, and downstream agents consuming the response get a single byte-deterministic statement of the trust posture without re-walking the underlying chain. The chain remains independently verifiable at the response's chain_ref content-address.

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 1 December 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction 3
  1.1. Motivation 3
  1.2. Scope 4
  1.3. Relationship to other Internet-Drafts 5
2. Conventions and Definitions 6
  2.1. Notation 6
  2.2. Definitions 6
3. Response Format Specification 7
  3.1. trust_outcome 7
  3.2. chain_ref 7
  3.3. query_ref 8
  3.4. ctq_timestamp_ms 8
  3.5. jurisdiction_flags 8
  3.6. verifier_did 9
  3.7. canon_version 9
4. Canonicalisation 9
5. Audit Chain Composition 9
  5.1. CTQ Response as Chain Consumer 9
  5.2. CTQ Response as Chain Row 9
  5.3. Linkage Verification 10

6. Year-N Auditability Properties 10
7. Composition with Other x402 Substrate 10
7.1. Receipt Format Composition 11
7.2. Cryptographic Settlement Proofs 11
7.3. Non-Goals 11
8. IANA Considerations 11
8.1. URN Namespace Registration 11
8.2. Response Format Identifier 12
9. Security Considerations 12
9.1. Response Tampering 12
9.2. Verifier Compromise 12
9.3. Chain Reference Spoofing 12
9.4. Query Reference Spoofing 13
9.5. Stale Responses 13
9.6. Operator Continuity Loss 13
Appendix A. References 13
A.1. Normative References 13
A.2. Informative References 13
Appendix B. Appendix A. Examples (Informative) 14
B.1. A.1. TRUSTED over a settled-and-uncancelled chain . . . 14
B.2. A.2. PROVISIONAL over a settled-but-not-yet-final chain 14
B.3. A.3. INSUFFICIENT_EVIDENCE over an incomplete chain . . 15
B.4. A.4. UNTRUSTED over a settled-then-reversed chain . . . 15
Appendix C. Appendix B. Reference Implementations (Informative) 16
Appendix D. Known Adopters (Informative) 16
Appendix E. Acknowledgments 17
Author’s Address 17

1. Introduction

1.1. Motivation

Agentic-payment flows generate audit chains composed of multiple categorical receipt classes: admission (compliance receipt), each recurring execution (settlement attestation), termination (cancellation receipt), and refund (refund receipt where owed). Consumers of these chains include regulators auditing operator behaviour, dashboards rendering operator state, parent agents managing fleets of child tasks, and downstream automation deciding whether to proceed with onward actions.

These consumers typically do not want to walk the underlying chain themselves. They want a verified categorical answer to a structured question: "is this payment cleared for settlement under jurisdiction X?", "is this mandate currently active?", "is this chain free of compliance-forced terminations?", "is this refund obligation satisfied?". The chain itself is the evidence; the answer is the consumable.

This document specifies a verifier-side response format that records:

* The categorical conclusion the verifier reached (TRUSTED / PROVISIONAL / INSUFFICIENT_EVIDENCE / UNTRUSTED).
* The audit chain that was queried, referenced by content-addressed root (chain_ref).
* The query that was answered, referenced by content-addressed bytes (query_ref).
* The verifier identity (verifier_did).
* The timestamp of the response (ctq_timestamp_ms).
* The jurisdiction(s) under which the conclusion was reached (jurisdiction_flags).

The four-state enumeration is load-bearing under existing regulatory frameworks:

* Under MiCA (Regulation (EU) 2023/1114) Article 80 record-keeping, retained verifier conclusions over settlement audit chains are themselves evidence. The distinction between PROVISIONAL (settled but not yet finalised) and INSUFFICIENT_EVIDENCE (verifier could not reach a conclusion) is operationally material.
* Under PSD2 (Directive 2015/2366), refund-window decisions are triggered by settlement state plus elapsed time. A consumer reading a CTQ response over a refund-eligible chain needs to distinguish UNTRUSTED ("settled-then-reversed, no refund obligation attaches in this direction") from PROVISIONAL ("not yet final, re-query later") from INSUFFICIENT_EVIDENCE ("chain has gaps, cannot conclude").
* Under AML Directives 5 and 6, audit-chain verification by independent parties is itself a regulatory function. The verifier’s conclusion is the evidence the regulator retains.

A receipt format that collapses these distinctions loses the load-bearing operational separation between "the answer is no" and "we cannot conclude."

1.2. Scope

This document specifies:

* The canonical JSON shape of the composite trust query response (Section 3).
* The reference to the canonicalisation rule applicable to the response (Section 4 -- normative reference to draft-hopley-x402-canonicalisation-jcs, not redefined inline).
* The audit chain composition pattern under which CTQ responses compose with the four AlgoVoi-authored receipt formats and may themselves participate in higher-level audit chains (Section 5).
* The year-N auditability properties the format pins (Section 6).
* Worked examples covering all four trust_outcome outcomes (Appendix A).

This document does NOT specify:

* The query format. The query is identified by query_ref (content-addressed); the query encoding is opaque to this response format. Callers MAY use JSON-LD, JSON Schema, SQL-like predicates, or any other structured-question encoding. The query's canonical bytes are addressed by SHA-256 and referenced via sha256:<hex>.
* The verifier's risk model or finality semantics. The verifier applies whatever evidence-evaluation discipline its risk model requires; the response records the categorical conclusion, not the evaluation discipline.
* The transport protocol for delivering CTQ responses. The format is shape-only; transport (HTTPS, agent-to-agent messaging, on-chain anchoring, file artifact) is out of scope.

1.3. Relationship to other Internet-Drafts

This document normatively references:

* draft-hopley-x402-canonicalisation-jcs -- the JCS canonicalisation discipline pinned in Section 4.

This document is complementary to:

* draft-hopley-x402-compliance-receipt -- admission-time compliance screening receipts. A CTQ response's chain_ref MAY anchor a chain that includes a compliance receipt at its root.
* draft-hopley-x402-settlement-attestation -- per-execution settlement attestations.
* draft-hopley-x402-cancellation-receipt -- mandate-termination receipts.
* draft-hopley-x402-refund-receipt -- post-settlement refund receipts.

A CTQ response sits above all four receipt classes. The verifier reads the chain composed of them and emits a single categorical response. The chain remains independently verifiable at the chain_ref content-address.

2. Conventions and Definitions

2.1. 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.

2.2. Definitions

composite trust query response (CTQ response): a JSON object of the shape specified in Section 3, canonicalised under the discipline of draft-hopley-x402-canonicalisation-jcs, emitted by a verifier recording a categorical conclusion over an audit chain in response to a stated query.

content_hash: SHA-256, lowercase hex, of the JCS-canonical bytes of the CTQ response object.

chain_ref: a string of the form sha256:<lowercase-hex-64> identifying the root of the audit chain the verifier walked, by content hash of the chain’s root record (typically a chain row record per draft-hopley-x402-compliance-receipt Section 5.1, or an equivalent root-anchor record under the operator’s audit-chain format).

query_ref: a string of the form sha256:<lowercase-hex-64> identifying the canonical bytes of the query that was answered. The query encoding is out of scope for this document; the reference is opaque.

verifier_did: a string-valued DID URI identifying the verifier that emitted the response.

trust_outcome: a string-valued field carrying one of four closed enumeration values. See Section 3.1.

canon_version: an in-band string identifying the canonicalisation discipline. Fixed value jcs-rfc8785-v1 for this version.

3. Response Format Specification

A CTQ response is a JSON object with the following seven fields. All fields are REQUIRED. The response is canonicalised under draft-hopley-x402-canonicalisation-jcs per Section 4. Field names are sorted lexicographically by JCS during canonicalisation; the object itself uses arbitrary authoring order.

3.1. trust_outcome

A string-valued field. The value MUST be one of:

* TRUSTED -- the verified chain answers the query affirmatively. All anchored receipts are valid, present, and consistent. No revocation, reversal, or compliance-forced termination on the chain.
* PROVISIONAL -- the chain is partially complete; some receipts are in PENDING_FINALITY or analogous non-terminal state. The verifier can affirm partial state but not full settlement.
* INSUFFICIENT_EVIDENCE -- the chain does not contain enough evidence to answer the query. Chain segments are missing, the query references state outside the chain, or content-addressed pointers cannot be dereferenced.
* UNTRUSTED -- the chain contains evidence that negates the query. Compliance-forced termination, settled-then-reversed transaction, REJECTED refund, expired-without-renewal mandate.

The four-element enumeration is closed. Implementations MUST reject any other value at validation time before canonicalisation. Free-form "reason" strings, score-based representations, or operator-internal classification labels are not acceptable substitutes for the categorical outcome.

The four-value enumeration captures a genuinely four-state decision space: proceed (TRUSTED), proceed-with-caution (PROVISIONAL), hold-pending-more-data (INSUFFICIENT_EVIDENCE), and halt (UNTRUSTED). Collapsing to three values loses the operationally-distinct INSUFFICIENT_EVIDENCE state. This matters because INSUFFICIENT_EVIDENCE drives a different operator action (gather more evidence) than UNTRUSTED (halt the framed action).

3.2. chain_ref

A string-valued field of the form sha256:<lowercase-hex-64>. The hex digest is SHA-256 of the JCS-canonical bytes of the audit chain root the verifier walked.

The "audit chain root" is the operator-defined anchor record at the top of the chain (typically the row 1 record of a hash-chained audit-row sequence per draft-hopley-x402-compliance-receipt Section 5.1). The CTQ response references the root, not individual chain rows or receipts within the chain; resolution of the chain itself is out-of-band (chain-by-content-address dereference, operator-side audit-log fetch, etc.).

Implementations MUST NOT strip the sha256: prefix during canonicalisation or verification.

3.3. query_ref

A string-valued field of the form sha256:<lowercase-hex-64>. The hex digest is SHA-256 of the canonical bytes of the query that was answered.

The query encoding is opaque to this response format. Callers MAY use any structured-question encoding (JSON-LD, JSON Schema, SQL-like predicate, operator-internal DSL, etc.). The canonical bytes of the query are addressed by SHA-256 and referenced here; resolving the query bytes is out-of-band.

Implementations MUST NOT strip the sha256: prefix during canonicalisation or verification.

3.4. ctq_timestamp_ms

An integer-valued field carrying the epoch-millisecond timestamp at which the verifier emitted the response, in UTC.

This field MUST be an integer. RFC 3339 string forms (e.g. "2026-05-30T12:00:00Z") MUST be rejected at the validation layer before canonicalisation. This is Substrate Rule 2, normatively specified in draft-hopley-x402-canonicalisation-jcs Section 4.1.

3.5. jurisdiction_flags

An ordered array of string-valued ISO-3166-1 alpha-2 country codes or alpha-3 region codes identifying the applicable regulatory frameworks under which the response was reached.

Authoring convention: primary jurisdiction first (where the verifier is licensed or operates), secondary jurisdictions in order of regulatory precedence.

Array element ORDER is SIGNIFICANT and load-bearing per draft-hopley-x402-canonicalisation-jcs Section 4.3.

3.6. verifier_did

A string-valued DID URI identifying the verifier emitting the response. Whether the verifier's DID is registered in any particular DID method registry is out of scope; the field is treated as opaque identifier-bytes under JCS canonicalisation.

3.7. canon_version

A string-valued in-band canonicalisation rule pin. For this version of the response format the value MUST be jcs-rfc8785-v1.

4. Canonicalisation

The CTQ response MUST be canonicalised under the discipline pinned by draft-hopley-x402-canonicalisation-jcs and identified by the URN:

urn:x402:canonicalisation:jcs-rfc8785-v1

The full normative specification of the discipline (JCS RFC 8785 plus the schema-normalisation requirements including Substrate Rule 2) is in that document. This document does not redefine the discipline inline.

5. Audit Chain Composition

5.1. CTQ Response as Chain Consumer

A CTQ response is typically emitted in response to a query over an existing audit chain. The chain is composed of records under the four AlgoVoi-authored receipt formats. The CTQ response's chain_ref is the SHA-256 of the row 1 record's JCS-canonical bytes. A consumer reading the CTQ response trusts the verifier's categorical conclusion and may optionally walk the underlying chain themselves at the same content-address to verify.

5.2. CTQ Response as Chain Row

A CTQ response MAY ALSO be embedded as a row in a higher-level audit chain. The chain row shape is identical to that specified in draft-hopley-x402-compliance-receipt Section 5.1:

```
{
  "row_number": 1,
  "content_hash": "<hex64>",
  "prev_hash": "<hex64>",
  "row_content_hash": "<hex64>"
}
```

The CTQ response's content_hash populates the row's content_hash field. A verifier-of-verifier reading the higher chain can walk sequences of CTQ responses (a chain of verifier conclusions over chains of receipts) and emit a meta-CTQ response over the composite.

This recursive pattern enables multi-party audit-chain composition: a regulator verifying an operator's audit chain may emit a CTQ response. A higher regulator (e.g. cross-border supervisor) verifying multiple national regulators' CTQ responses may emit a meta-CTQ response over those. Each level retains independent byte-deterministic verifiability.

5.3. Linkage Verification

Per draft-hopley-x402-compliance-receipt Section 5.2: a verifier reading a chain segment recomputes each row's row_content_hash from its first three fields and confirms forward linkage via prev_hash. Any mismatch indicates tampering or chain integrity loss.

6. Year-N Auditability Properties

The same six properties pinned by draft-hopley-x402-canonicalisation-jcs Section 5 apply to the CTQ response:

1. Self-describing canonicalisation pin via canon_version.
2. No external rule registry required.
3. Cross-implementation verifiability (8-implementation matrix per the discipline I-D).
4. Tamper detection via per-row content_hash and chain prev_hash linkage.
5. Regulatory distinction preserved via closed enumeration.

Plus one CTQ-specific property:

6. *Verifier-decision evidence chain.* A consumer reading a retained CTQ response years after emission can determine (a) which chain was queried (via chain_ref), (b) which question was asked (via query_ref), (c) who emitted the response (via verifier_did), (d) when the response was emitted (ctq_timestamp_ms), and (e) the categorical answer (trust_outcome), without dependence on the verifier's continued operation. Both the queried chain and the query bytes are independently re-fetchable at their content-addresses.

7. Composition with Other x402 Substrate

7.1. Receipt Format Composition

A CTQ response composes above the four AlgoVoi-authored receipt formats. The chain identified by chain_ref is typically composed of records under these formats:

* draft-hopley-x402-compliance-receipt -- admission events
* draft-hopley-x402-settlement-attestation -- per-execution settlements
* draft-hopley-x402-cancellation-receipt -- mandate terminations
* draft-hopley-x402-refund-receipt -- refunds

A verifier walking the chain applies its evaluation discipline to each receipt's closed enumeration value, considers the linkage via prev_hash, and emits a single categorical response.

7.2. Cryptographic Settlement Proofs

Cryptographically-strong settlement proofs (post-quantum proofs of payment conditions, validator signatures, STARK proofs of inclusion, etc.) are orthogonal to this response format. A verifier MAY consult such proofs as part of its evaluation discipline; the response records only the categorical conclusion, not the evidence consulted.

7.3. Non-Goals

This document does not encode:

* The query bytes themselves. The query is identified by query_ref (content-addressed); the query encoding is out of scope.
* The verifier's evaluation discipline. The verifier applies whatever evidence-evaluation logic its risk model requires; the response records the categorical conclusion, not the discipline.
* The transport protocol. CTQ responses are emitted as byte payloads; transport is out of scope.

8. IANA Considerations

8.1. URN Namespace Registration

This document references the URN urn:x402:canonicalisation:jcs-rfc8785-v1 registered by draft-hopley-x402-canonicalisation-jcs Section 10.1. No additional URN namespace registration is required by this document.

8.2. Response Format Identifier

This document defines the response format identifier:

urn:x402:response:composite-trust-query-v1

This identifier MAY be used by composite-trust-query implementations to refer to CTQ responses as a class. Registration with IANA is requested under the x402 URN namespace.

9. Security Considerations

9.1. Response Tampering

A CTQ response's content_hash is the SHA-256 of its JCS-canonical bytes. Tampering with any field produces a different hash; the tampered response fails verification against any chain row referencing the original content_hash.

9.2. Verifier Compromise

A CTQ response is only as trustworthy as the verifier that emitted it. The format does not specify verifier-identity verification; consumers MUST establish trust in the verifier through out-of-band means (DID method, certificate authority, regulator licensing, mutual-trust agreement). The verifier_did field supports accountability but does not by itself establish trust.

A malicious verifier could emit TRUSTED responses over chains that do not satisfy the query. Detection is consumer-side: consumers SHOULD periodically sample CTQ responses by re-walking the referenced chain themselves, especially for high-value decisions.

9.3. Chain Reference Spoofing

The chain_ref field is operator-asserted at emission time. A verifier could emit a CTQ response with a chain_ref pointing to a chain that does not exist or is no longer retrievable. Mitigation: consumers SHOULD dereference chain_ref against an independent content-addressed store before relying on a TRUSTED response, at least at first encounter with a new verifier.

9.4. Query Reference Spoofing

The query_ref field is similarly operator-asserted. A verifier could emit a CTQ response claiming to answer query A while actually having evaluated query B. Mitigation: consumers MUST resolve query_ref against an independent content-addressed store and confirm the canonical bytes match the query they intended to issue, before accepting the response.

9.5. Stale Responses

A CTQ response records the verifier’s conclusion at ctq_timestamp_ms. Subsequent events on the underlying chain (reversal, cancellation, refund) MAY invalidate the conclusion. Consumers SHOULD re-query at intervals appropriate to the decision being made; high-value decisions over chains that may evolve SHOULD NOT rely on CTQ responses older than the consumer’s risk model tolerates.

9.6. Operator Continuity Loss

If the verifier becomes unavailable, the CTQ response remains independently verifiable from retained bytes plus the reference implementations cited in draft-hopley-x402-canonicalisation-jcs Section 7. The conclusion the verifier reached at emission time is fixed in the response bytes; whether to continue relying on that conclusion is a consumer-side decision.

Appendix A. References

A.1. Normative References

* [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.
* [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017.
* [RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017.
* [RFC8785] Rundgren, A., Jordan, B., and S. Erdtman, "JSON Canonicalization Scheme (JCS)", RFC 8785, DOI 10.17487/RFC8785, June 2020.

A.2. Informative References

* draft-hopley-x402-canonicalisation-jcs-v1, Hopley, C., "JCS Canonicalisation Discipline for Agentic-Payment Receipts", May 2026.

* draft-hopley-x402-compliance-receipt-00, Hopley, C., "Categorical Compliance Screening Receipt Format for Agentic-Payment Flows", May 2026.
* draft-hopley-x402-settlement-attestation-00, Hopley, C., "Categorical Settlement Attestation Format for Agentic-Payment Flows", May 2026.
* draft-hopley-x402-cancellation-receipt-00, Hopley, C., "Categorical Mandate Cancellation Receipt Format for Agentic-Payment Flows", May 2026.
* draft-hopley-x402-refund-receipt-00, Hopley, C., "Categorical Refund Receipt Format for Agentic-Payment Flows", May 2026.
* AlgoVoi, "Substrate Authorship and Provenance", target="https://docs.algovoi.co.uk/substrate-authorship-provenance" (https://docs.algovoi.co.uk/substrate-authorship-provenance)
* EU Markets in Crypto-Assets Regulation (MiCA, Regulation (EU) 2023/1114), Article 80.
* EU Anti-Money Laundering Regulation (AMLR, Regulation (EU) 2024/1624), Article 56.
* EU Payment Services Directive 2 (PSD2, Directive 2015/2366), Articles 64, 72, 89.
* EU Anti-Money Laundering Directive 5 (Directive (EU) 2018/843).
* EU Anti-Money Laundering Directive 6 (Directive (EU) 2018/1673).

Appendix B. Appendix A. Examples (Informative)

B.1. A.1. TRUSTED over a settled-and-uncancelled chain


```
{
  "canon_version": "jcs-rfc8785-v1",
  "chain_ref": "sha256:0dd5d0b76c9b9281fdeb2509ad38ab132b16a17385ca01d976ff9e6e12563a0
f",
  "ctq_timestamp_ms": 1716494400000,
  "jurisdiction_flags": ["UK", "EU"],
  "query_ref": "sha256:8b7df143d91c716ecfa5fc1730022f6b421b05cedee8fd52b1fc65a96030ad5
2",
  "trust_outcome": "TRUSTED",
  "verifier_did": "did:web:api.algovoi.co.uk"
}
```


Records the verifier's TRUSTED conclusion over the chain at chain_ref in response to the query at query_ref, under joint UK + EU jurisdiction. The consumer reading this response trusts that the chain satisfies the query (e.g. "is this payment cleared for settlement?") and may proceed with the action the query was framed to authorise.

B.2. A.2. PROVISIONAL over a settled-but-not-yet-final chain

```
   {
     "canon_version": "jcs-rfc8785-v1",
     "chain_ref": "sha256:0dd5d0b76c9b9281fdeb2509ad38ab132b16a17385ca01d976ff9e6e12563a0
f",
     "ctq_timestamp_ms": 1716494400000,
     "jurisdiction_flags": ["UK", "EU"],
     "query_ref": "sha256:8b7df143d91c716ecfa5fc1730022f6b421b05cedee8fd52b1fc65a96030ad5
2",
     "trust_outcome": "PROVISIONAL",
     "verifier_did": "did:web:api.algovoi.co.uk"
   }
```


Records that the verifier could affirm settlement-inclusion but not yet operator-required finality on the chain. The consumer should proceed cautiously and re-query after the pending settlement attestation reaches the SETTLED state.

B.3. A.3. INSUFFICIENT_EVIDENCE over an incomplete chain


```
   {
     "canon_version": "jcs-rfc8785-v1",
     "chain_ref": "sha256:0dd5d0b76c9b9281fdeb2509ad38ab132b16a17385ca01d976ff9e6e12563a0
f",
     "ctq_timestamp_ms": 1716494400000,
     "jurisdiction_flags": ["UK", "EU"],
     "query_ref": "sha256:8b7df143d91c716ecfa5fc1730022f6b421b05cedee8fd52b1fc65a96030ad5
2",
     "trust_outcome": "INSUFFICIENT_EVIDENCE",
     "verifier_did": "did:web:api.algovoi.co.uk"
   }
```


Records that the verifier could not reach a conclusion: chain segments were missing, the query referenced state outside the chain, or content-addressed pointers could not be dereferenced. The consumer should gather more evidence rather than proceed under a defaulted-trusted posture.

B.4. A.4. UNTRUSTED over a settled-then-reversed chain


```
   {
     "canon_version": "jcs-rfc8785-v1",
     "chain_ref": "sha256:0dd5d0b76c9b9281fdeb2509ad38ab132b16a17385ca01d976ff9e6e12563a0
f",
     "ctq_timestamp_ms": 1716494400000,
     "jurisdiction_flags": ["UK", "EU"],
     "query_ref": "sha256:8b7df143d91c716ecfa5fc1730022f6b421b05cedee8fd52b1fc65a96030ad5
2",
     "trust_outcome": "UNTRUSTED",
     "verifier_did": "did:web:api.algovoi.co.uk"
   }
```

Records that the chain contains evidence negating the query (a REVERSED settlement attestation, a COMPLIANCE_TERMINATED cancellation receipt, a REJECTED refund receipt). The consumer should halt the action the query was framed to authorise.

Appendix C. Appendix B. Reference Implementations (Informative)

The following open-source implementations conform to this format:

* algovoi-composite-trust-query (Python) on PyPI: target="https://pypi.org/project/algovoi-composite-trust-query/" (https://pypi.org/project/algovoi-composite-trust-query/) Provides build_ctq_response(). Depends on algovoi-substrate for the JCS canonicalisation primitive. Apache 2.0 licensed.

* @algovoi/composite-trust-query (TypeScript) on npm: target="https://www.npmjs.com/package/@algovoi/composite-trust-query" (https://www.npmjs.com/package/@algovoi/composite-trust-query) Byte-for-byte parity with the Python sibling. Depends on @algovoi/substrate for the JCS canonicalisation primitive. Apache 2.0 licensed.

Conformance vectors:

https://github.com/chopmob-cloud/algovoi-jcs-conformance-vectors/tree/main/vectors/composite_trust_query_v1

8 byte-level reference vectors + 7 pair invariants + 3 chain invariants pinning the closed four-element enumeration, jurisdiction-array-order, canon_version pin, and audit-chain linkage properties.

Appendix D. Known Adopters (Informative)

The following downstream parties have published artefacts that anchor to the composite trust query response format specified by this document, or to the canonicalisation discipline shared with this format. Inclusion in this list is informational and reflects public adoption only; it does not imply endorsement or normative authority from the listed party.

Adopter	Surface	Anchor
AlgoVoi (api.algovoi.co.uk)	Production trust-query verifier	All AlgoVoi-emitted CTQ responses under canon_version: jcs-rfc8785-v1

Table 1

Adopters publishing vector sets or response-format extensions that anchor to this format are encouraged to publish them in adopter-controlled repositories with canon_version recorded in-band, so each adopter’s authorship is unambiguous and their artefact is independently citable.

This appendix is maintained as a record of observed adoption at the time of revision; absence from this list is not normative.

Appendix E. Acknowledgments

This document, the response format it specifies, and the conformance vectors derived from it are AlgoVoi work under AlgoVoi authorship. Substrate authorship history is catalogued at target="https://docs.algovoi.co.uk/substrate-authorship-provenance" (https://docs.algovoi.co.uk/substrate-authorship-provenance).

The canonicalisation discipline pinned by Section 4 is normatively specified in draft-hopley-x402-canonicalisation-jcs under the same authorship.

This document closes the lifecycle gap at the top of the agentic-payment receipt stack. Below it sit four AlgoVoi-authored receipt formats: compliance, settlement, cancellation, and refund. The CTQ response sits above all four and provides the verifier-emitted consumer interface for the audit chains they compose. The five formats share the same canonicalisation pin, audit-chain row shape, and integer-millisecond timestamp encoding, so that a consumer of the full agentic-payment stack requires only one implementation of the canonicalisation discipline.

The author acknowledges Anders Rundgren as the editor of RFC 8785, the JSON Canonicalization Scheme on which the discipline builds.

Author’s Address

Christopher Hopley
AlgoVoi
Email: chopmob@gmail.com