DMSC
Internet-Draft
Intended status: Informational
Expires: 8 November 2026

L. Zhang
W. Qiao
W. Zhang
H. Yang
Y. Li
AsiaInfo Technologies (China) Inc.

7 May 2026

Verifiable Usage Accounting for Internet of Agents
draft-zhang-ioa-usage-accounting-00

Abstract

This document describes a usage accounting and evidence framework for the Internet of Agents (IoA). In cross-domain agent collaboration, agents may attach to gateways, discover capabilities, delegate subtasks, invoke tools, consume model or compute resources, and produce auditable outcomes. Existing application logs or platform-specific billing interfaces are insufficient for interoperable accounting across agents, gateways, and administrative domains.

This document defines requirements and a common object model for verifiable usage accounting, including Accounting Contexts, Metering Profiles, Measurement Dimensions, Usage Event Records, and Accounting Evidence References. These objects are intended to support interoperable recording, correlation, export, verification, correction, and dispute handling for agent collaboration events.

This document does not define pricing, charging policy, token issuance, financial settlement, revenue-sharing rules, invoices, or business support system interfaces. It focuses on protocol-visible accounting records and evidence objects that may be used by other systems.

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/.

Copyright Notice

Table of Contents

1. Introduction

The Internet of Agents (IoA) envisions large-scale collaboration among autonomous or semi-autonomous agents across domains, vendors, networks, and execution environments. Agents may act on behalf of users, services, organizations, or other agents. They may also interact through Agent Gateways, agent-to-agent session protocols, capability directories, task protocols, tool invocation interfaces, and model services.

Once agents collaborate across administrative domains, a system needs a common way to record what occurred during the collaboration. A task may be decomposed into subtasks, delegated to several agents, routed through gateways, and completed by invoking models, tools, data services, or network functions. The resulting usage information is useful for resource accounting, cost allocation, audit, operational analysis, quota control, accountability, and dispute handling.

Existing application logs, local billing records, or platform-specific usage APIs do not provide a common cross-domain accounting view. They often lack stable task correlation, gateway provenance, signed evidence references, usage-category semantics, measurement-dimension declarations, privacy-controlled export, and correction semantics. In addition, coarse-grained records such as "API request count" or "total input/output tokens" do not distinguish between orchestration, execution, tool invocation, delegated subtasks, reasoning or inference cost, gateway mediation, and result verification.

This document defines a protocol-visible object model for verifiable usage accounting in IoA. It is inspired by existing Internet accounting and measurement work, including accounting management concepts [RFC2975], network access accounting [RFC2866], and flow information export [RFC7011]. However, the objects defined here are intended for agent collaboration rather than packet flows or network access sessions.

The key design principle is separation between accounting facts and business charging. This document defines usage accounting contexts, metering profiles, measurement dimensions, event records, and evidence references. It does not define prices, tariffs, token economics, revenue sharing, invoices, or financial settlement.

2. Conventions and Terminology

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 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Agent
: An autonomous or semi-autonomous software entity that can perform tasks, invoke tools, interact with other agents, or act on behalf of a user, service, or organization.

Agent Gateway
: A gateway that mediates agent attachment, registration, discovery handoff, policy enforcement, routing, accounting, or interconnection between agents or domains.

Accounting Context
: A scoped object that binds accounting-relevant identifiers, policies, metering profiles, and evidence requirements for a task, invocation, session, or gateway-mediated collaboration.

Metering Profile
: A description of supported usage categories, measurement dimensions, aggregation behavior, privacy constraints, and evidence requirements for a capability, agent, gateway, or accounting domain.

Measurement Dimension
: A declaration of what is measured, which unit is used, the applicable usage category or modality, and how the value is obtained and aggregated.

Usage Event Record
: A structured record describing an observed accounting-relevant event, such as task start, delegation, tool invocation, model inference, workflow step completion, or task result verification.

Accounting Evidence Reference
: A reference to integrity-protected evidence that supports a Usage Event Record, such as a signature, receipt, hash, authorization reference, execution trace, result attestation, or human confirmation record.

Usage Unit
: A unit used by a Measurement Dimension to express measured values. Examples include token, byte, millisecond, second, frame, pixel, request, operation, step, and standard-compute-unit.

Standard Compute Unit (SCU)
: A normalized Usage Unit used by a Measurement Dimension to express compute resource consumption across heterogeneous models, tools, or execution environments. This document treats SCU as a profile-defined unit and does not define its calibration, exchange rate, or pricing model.

Verified Result Event
: A record indicating that a task outcome has been verified according to a declared policy, such as successful ticket closure, approved transaction completion, or confirmed network fault localization.

Accounting Domain
: An administrative domain responsible for generating, validating, exporting, or retaining accounting records.

Exporter
: An entity that exports Usage Event Records or accounting summaries to another entity.

Collector
: An entity that receives Usage Event Records or accounting summaries from an Exporter.

3. Scope and Non-Goals

This document specifies:

* a common object model for verifiable usage accounting in IoA deployments;

* requirements for Accounting Contexts, Metering Profiles, Measurement Dimensions, Usage Event Records, and Accounting Evidence References;

* usage event categories suitable for task, invocation, delegation, model, tool, gateway, workflow, and result events;

* requirements for event correlation, evidence binding, cross-domain export, correction, and dispute handling; and

* privacy and security considerations for accounting records.

This document does not specify:

* pricing, tariffs, rating algorithms, charging policy, invoices, revenue sharing, token issuance, token exchange, or financial settlement;

* a general-purpose business support system, online charging system, payment protocol, or financial ledger;

* a discovery query protocol, routing algorithm, task orchestration protocol, or agent-to-agent message exchange protocol;

* a complete identity, credential issuance, or trust framework;

* a mandatory serialization format or transport protocol in this version; or

* a normative definition of SCU calibration, VPT calculation, model pricing, or business-result valuation.

4. Architectural Context

An IoA deployment may contain Requesting Agents, Serving Agents, Agent Gateways, Accounting Exporters, Accounting Collectors, and Evidence Verifiers. The accounting model can be used with gateway-mediated interaction, direct agent-to-agent interaction, or a combination of both. A gateway is a common observation and enforcement point, but the object model does not require every event to be observed by the same gateway.

The core relationship among the accounting objects is shown in Figure 1. An Accounting Context defines the scope of accounting for a task, session, invocation, or collaboration. A Metering Profile defines how usage is measured and what evidence is required. Usage Event Records describe individual accounting-relevant events within that context. Accounting Evidence References bind records to signatures, hashes, receipts, authorization references, trace evidence, result attestations, or human confirmations.

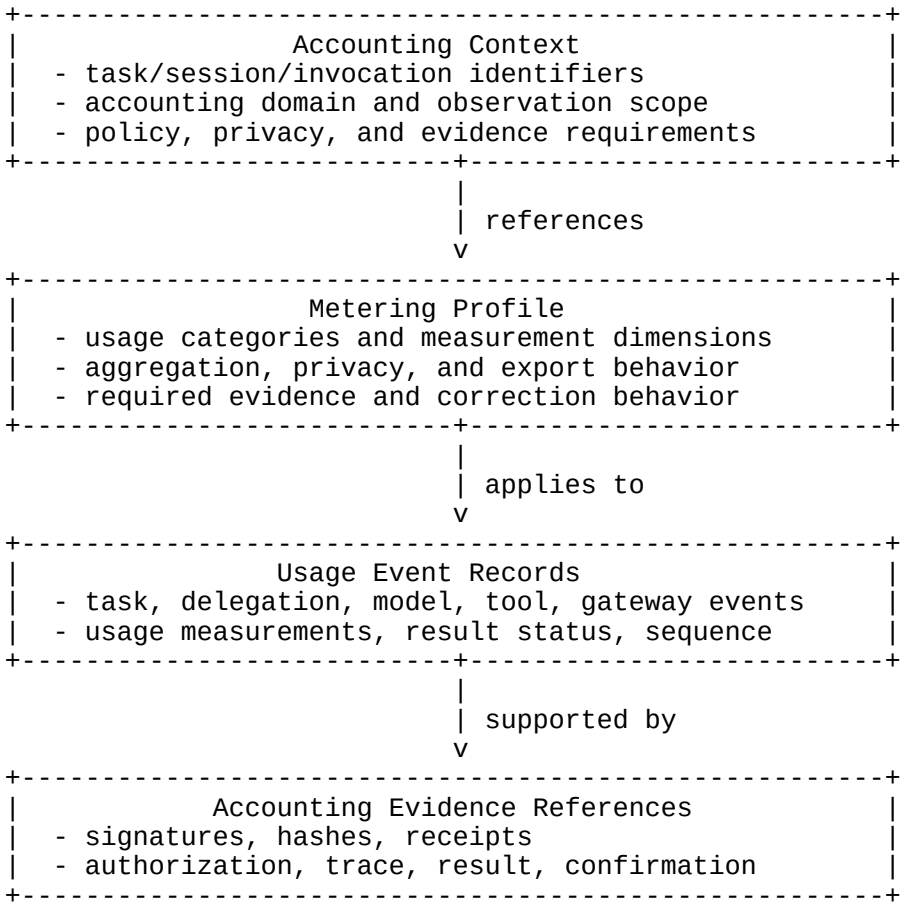

Figure 1: Core Accounting Object Relationships

Figure 2 illustrates how these objects are used during a cross-domain collaboration. The accounting context is normally established before or during task/session setup. Usage event records are generated as the collaboration proceeds. Evidence references are attached when records require later verification. Exporters can then send records or summaries to collectors according to the Metering Profile and privacy policy.

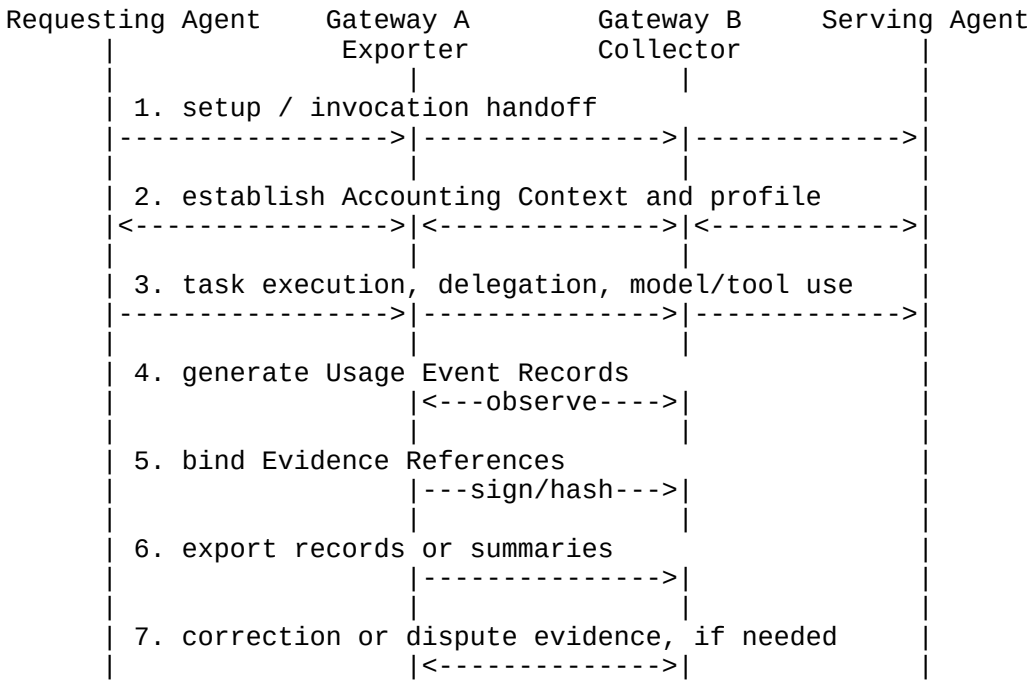

Figure 2: Accounting Flow in Cross-Domain Agent Collaboration

The accounting model is not required to expose agent internals or raw prompt content. A gateway or platform may generate summary records, privacy-preserving digests, or evidence references according to local policy. For example, an exported record can indicate that a result was verified and signed by a gateway without disclosing the raw ticket, prompt, tool output, or business data used to make that determination.

5. Accounting Object Model

5.1. Accounting Context

An Accounting Context defines the scope within which Usage Event Records are correlated and interpreted. An Accounting Context MAY be established during agent attachment, capability registration, discovery handoff, task creation, session establishment, or invocation setup.

An Accounting Context SHOULD contain the following fields:

* accounting-context-id: a stable identifier for the accounting context;

* accounting-domain-id: the domain that asserts or manages the context;

* gateway-id: the gateway that created or accepted the context, when applicable;

* agent-id or agent-did: the agent identifier associated with the context, when available;

* task-id, session-id, invocation-id, or trace-id: identifiers used for correlation;

* subject-ref: a reference to the user, organization, service, or agent on whose behalf the task is performed, when policy permits;

* policy-ref: a reference to applicable policy, quota, authorization, or consent information;

* metering-profile-ref: a reference to the Metering Profile that applies to the context;

* evidence-policy: requirements for signatures, receipts, retention, redaction, or result verification;

* validity: start time, expiration time, and freshness constraints; and

* privacy-scope: constraints on disclosure, aggregation, and export.

An Accounting Context MUST be unambiguous within the accounting domain that asserts it. If a context is propagated across domains, each receiving entity MUST be able to determine the asserting entity, the validity of the context, and the applicable disclosure constraints.

5.2. Metering Profile

A Metering Profile describes the accounting behavior supported or required by an agent, capability, gateway, service, or accounting domain.

A Metering Profile MAY be referenced by a gateway capability directory entry, capability advertisement, task object, handoff reference, session setup message, or policy object. If multiple profiles apply, the effective profile MUST be determined according to local policy and MUST be auditable.

5.2.1. Profile Structure

A Metering Profile SHOULD specify:

* profile-id and version;
* supported usage categories;
* supported measurement dimensions, such as token usage, multimodal generation or processing parameters, latency, gateway routing attributes, and quota state;
* required measurement methods;
* required evidence types;
* aggregation behavior, such as per-event, per-task, per-session, per-window, or summary-only;
* correction behavior, such as whether corrected records can be emitted and how they reference original records;
* privacy behavior, including redaction, pseudonymization, minimization, and selective disclosure; and
* export behavior, including push, pull, batch, streaming, or local-only retention.

5.2.2. Measurement Dimensions

A Metering Profile MAY declare one or more measurement dimensions. A measurement dimension identifies what is measured, the unit used for the measurement, the applicable modality or usage category, and how the value is obtained and aggregated. Measurement dimensions provide a common way to describe text-token usage, model inference usage, multimodal processing usage, gateway usage, quota state, workflow usage, and verified-result usage.

A measurement dimension SHOULD contain:

* dimension-id: a stable identifier for the dimension;
* dimension-name: a human-readable name;
* usage-category: the usage category to which the dimension applies;
* modality: text, image, video, audio, speech, multimodal, or another modality when applicable;

* unit: the unit of measurement, such as token, byte, millisecond, second, frame, pixel, request, operation, step, or standard-compute-unit;

* value-type: integer, decimal, boolean, string, enumeration, or structured value;

* measurement-method: observed, provider-reported, estimated, sampled, aggregated, normalized, corrected, or verified;

* aggregation-scope: per-request, per-output, per-inference, per-tool-call, per-task, per-session, per-time-window, or summary-only;

* normalization-reference: a reference to a normalization profile when the dimension uses a normalized unit such as SCU; and

* privacy-class: an indication of whether the dimension is usage-only metadata, pseudonymous metadata, sensitive metadata, content-derived metadata, or subject to stricter disclosure policy.

Examples of measurement dimensions include input-token-count, output-token-count, total-token-count, cached-token-count, reasoning-token-count, processing-time-ms, request-count, transferred-bytes, quota-used, quota-limit, image-count, image-pixel-count, image-quality-level, video-duration-seconds, frame-rate, audio-duration-seconds, sample-rate, channel-count, tool-call-count, workflow-step-count, delegation-count, verified-result-count, and standard-compute-usage.

The usage-category of each Measurement Dimension SHOULD be one of the supported usage categories declared by the Metering Profile, unless the dimension is explicitly marked as extension-specific.

Reasoning or chain-of-thought resource consumption can be represented as a measurement dimension, such as reasoning-token-count or reasoning-compute-duration. This document only accounts for the resource usage of such reasoning processes; it does not require or encourage disclosure of chain-of-thought content.

Measurement dimensions are accounting metadata. They do not define a pricing model, charging rule, tariff, or business valuation method.

5.2.3. Content Recording and Export Behavior

A Metering Profile SHOULD specify content recording behavior. Supported behavior can include disabled, digest-only, metadata-only, excerpt-only, or full-content recording under explicit policy. Full-content recording MUST NOT be the default behavior for cross-domain export.

A Metering Profile SHOULD also specify export behavior, including whether records are retained locally, exported as per-event records, exported as summaries, exported in batches, streamed to a collector, or exported only through evidence references. Export behavior MUST be evaluated together with the privacy behavior and evidence requirements of the profile.

5.3. Usage Event Record

A Usage Event Record describes an observed accounting-relevant event. It is not required to contain all raw operational data. It SHOULD contain enough information to support correlation, aggregation, verification, correction, and dispute handling.

A Usage Event Record SHOULD contain the following fields:

* record-id: a unique identifier for the record;

* accounting-context-id: the Accounting Context to which the record belongs;

* event-type: the event type, such as task-start, tool-call, or task-complete;

* event-time: the time at which the event occurred or was observed;

* observation-point: the gateway, agent, tool adapter, or platform component that observed the event;

* request-metadata: request identifier, start time, completion time, client address or pseudonymous client reference, path, method, consumer reference, API key reference, or equivalent metadata, subject to privacy policy;

* route-service-info: route name, backend cluster, model identifier, provider identifier, modality, or service binding reference;

* actor-ref: the agent, gateway, user, or service that performed or initiated the event, subject to privacy policy;

* target-ref: the agent, model, tool, service, resource, or task object affected by the event, subject to privacy policy;

* usage-category: a category such as orchestration, execution, tool-invocation, model-inference, gateway-forwarding, workflow, or result-verification;

* usage-measurements: one or more measured values keyed by measurement dimension identifiers declared in the applicable Metering Profile;

* quota-state: rate-limit decision, rate-limit status code, throttling state, or rejection reason when the event is affected by quota or rate-limit policy;

* content-ref: a reference, digest, redacted excerpt, or policy-controlled pointer to request or response content when content recording is enabled;

* result-status: started, in-progress, completed, failed, cancelled, degraded, corrected, disputed, or verified;

* sequence-info: ordering or deduplication information;

* evidence-ref: one or more Accounting Evidence References; and

* signature or integrity-ref: a signature, MAC, hash, or reference to integrity protection.

A Usage Event Record that is exported across administrative domains MUST include enough provenance information for the receiver to identify the asserting gateway, platform, or accounting domain. The receiver MUST NOT treat a record as verified solely because it is syntactically valid.

5.4. Accounting Evidence Reference

An Accounting Evidence Reference links a Usage Event Record to evidence that supports the record. This document does not require a particular evidence format. Implementations may use existing mechanisms such as JOSE [RFC7515], COSE [RFC9052], JWT [RFC7519], CWT [RFC8392], or selective disclosure mechanisms where appropriate.

An Accounting Evidence Reference SHOULD contain:

* evidence-id;

* evidence-type: signature, receipt, trace-hash, authorization-ref, consent-ref, result-attestation, human-confirmation, policy-decision, downgrade-decision, correction, or dispute-reference;

* evidence-location: embedded, local, URI, digest-only, or unavailable due to policy;

* digest and digest-algorithm, when evidence is not embedded;

* asserting-entity;

* verification-method;

* validity or retention period; and

* disclosure-policy.

Evidence references MUST NOT require disclosure of raw prompts, tool results, personal data, or sensitive operational data unless such disclosure is allowed by policy and necessary for the accounting purpose.

6. Usage Event Categories

The following initial usage event categories are defined for interoperability. Future specifications may extend this list.

orchestration
: Usage associated with intent interpretation, planning, task decomposition, routing decisions, state management, or coordination prompts.

execution
: Usage associated with an agent or sub-agent performing a concrete task step.

tool-invocation
: Usage associated with invoking an external tool, function, API, database, network function, or resource server.

model-inference
: Usage associated with model invocation, including input units, output units, reasoning units, compute duration, or normalized compute units.

multimodal-processing
: Usage associated with image, video, audio, speech, or other non-text modality generation or processing.

quota-control
: Usage or decision events associated with quota consumption, rate-limit checks, throttling, or rejection.

gateway-forwarding
: Usage associated with gateway mediation, forwarding, policy checks, protocol translation, or cross-domain handoff.

workflow
: Usage associated with workflow steps, task-state changes, retries, cancellation, fallback, pause, resume, or escalation.

result-verification
: Usage associated with verification of task results, human confirmation, external validation, or business-outcome confirmation.

correction
: A record that corrects or supersedes a previous record.

dispute
: A record that indicates an accounting dispute, dispute evidence submission, or dispute resolution status.

These categories describe accounting semantics and do not imply any particular pricing or charging rule.

7. Procedures

7.1. Accounting Context Establishment

An Accounting Context MAY be established when an agent attaches to a gateway, a gateway accepts or creates a capability directory entry, a task is created or accepted, an invocation handoff is returned, a session or collaboration group is established, or a policy decision requires accounting or audit.

The entity establishing the context MUST determine the applicable Metering Profile and evidence policy before usage events are exported across administrative domains. If no compatible profile exists, the gateway or platform MAY reject the interaction, fall back to local-only accounting, or export only a minimal summary according to policy.

Accounting Context establishment SHOULD be bound to authentication and authorization decisions where available. An accounting context MUST NOT be used as proof of authorization unless it explicitly references verifiable authorization evidence.

7.2. Usage Event Generation

A gateway or platform component SHOULD generate a Usage Event Record when an accounting-relevant event is observed. The granularity of event generation depends on the Metering Profile.

Implementations SHOULD support at least task-start and task-complete or task-failed records, delegation records, tool-invocation records, model-inference or compute-usage records, and correction records.

A Usage Event Record MUST include ordering or deduplication information if it can be retransmitted, corrected, or exported through multiple gateways or platforms.

7.3. Evidence Binding

A Usage Event Record SHOULD be bound to evidence according to the applicable evidence policy. Evidence binding MAY be achieved by embedding evidence, including a digest, including a URI, or referencing a protected evidence store.

Evidence binding SHOULD support integrity verification of the record, provenance verification of the asserting gateway or domain, correlation with authorization, consent, policy, or task context, result verification when a record asserts a verified outcome, and later dispute handling without exposing more data than necessary.

If evidence is unavailable due to privacy, retention, or policy constraints, the record MUST indicate that evidence is unavailable and SHOULD include the reason class.

7.4. Cross-Domain Export

Gateways or platforms MAY export Usage Event Records or summaries to other gateways, platforms, or collectors. Export behavior MUST follow the Metering Profile and privacy-scope constraints associated with the Accounting Context.

Cross-domain export SHOULD support record authentication and integrity protection, replay protection, duplicate detection, batch and streaming export models, summary export when raw event export is not allowed, correction records, and receiver-side validation of provenance and freshness.

A receiving entity MUST apply local policy before accepting exported accounting data for operational decisions. A receiving entity SHOULD retain the source identifier, received time, verification status, and any transformation performed on the record.

7.5. Correction and Dispute Handling

Accounting records may require correction because of delayed events, clock skew, aggregation errors, task cancellation, gateway failures, or later result verification.

A correction record MUST reference the original record or record set that it corrects. It MUST indicate whether it replaces, amends, reverses, or annotates the original record.

A dispute record SHOULD reference the disputed records, the accounting context, the asserting entity, the dispute reason, evidence references submitted by the disputing entity, and the dispute status.

This document defines only protocol-visible dispute references and evidence objects. It does not define arbitration rules, legal process, liability, compensation, or financial settlement.

8. Illustrative JSON Objects

The following examples are illustrative and are not a normative serialization profile.

8.1. Accounting Context Example

```
{
  "accounting_context_id": "acctx-20260507-001",
  "accounting_domain_id": "example.net",
  "gateway_id": "agw-east-1",
  "task_id": "task-5gc-fault-1192",
  "session_id": "sess-71d1",
  "trace_id": "trace-88b7",
  "policy_ref": "policy://example.net/ioa/accounting/basic",
  "metering_profile_ref": "profile://example.net/scu-v1",
  "evidence_policy": {
    "signature_required": true,
    "result_evidence_required": true,
    "raw_prompt_export": false
  },
  "validity": {
    "not_before": "2026-05-07T06:00:00Z",
    "not_after": "2026-05-07T12:00:00Z"
  }
}
```

Figure 3

8.2. Metering Profile Example


```
{
  "profile_id": "profile://example.net/scu-v1",
  "version": "1.0",
  "supported_usage_categories": [
    "tool-invocation",
    "model-inference",
    "multimodal-processing"
  ],
  "measurement_dimensions": [
    {
      "dimension_id": "input-token-count",
      "usage_category": "model-inference",
      "modality": "text",
      "unit": "token",
      "value_type": "integer",
      "measurement_method": "provider-reported",
      "aggregation_scope": "per-inference",
      "privacy_class": "usage-only"
    },
    {
      "dimension_id": "output-token-count",
      "usage_category": "model-inference",
      "modality": "text",
      "unit": "token",
      "value_type": "integer",
      "measurement_method": "provider-reported",
      "aggregation_scope": "per-inference",
      "privacy_class": "usage-only"
    },
    {
      "dimension_id": "standard-compute-usage",
      "usage_category": "tool-invocation",
      "unit": "standard-compute-unit",
      "value_type": "decimal",
      "measurement_method": "observed",
      "aggregation_scope": "per-tool-call",
      "privacy_class": "usage-only"
    },
    {
      "dimension_id": "reasoning-token-count",
      "usage_category": "model-inference",
      "modality": "text",
      "unit": "token",
      "value_type": "integer",
      "measurement_method": "provider-reported",
      "aggregation_scope": "per-inference",
```

```
        "privacy_class": "usage-only"
      },
      {
        "dimension_id": "total-token-count",
        "usage_category": "model-inference",
        "modality": "text",
        "unit": "token",
        "value_type": "integer",
        "measurement_method": "derived",
        "aggregation_scope": "per-inference",
        "privacy_class": "usage-only"
      },
      {
        "dimension_id": "processing-time-ms",
        "usage_category": "tool-invocation",
        "unit": "millisecond",
        "value_type": "integer",
        "measurement_method": "observed",
        "aggregation_scope": "per-tool-call",
        "privacy_class": "usage-only"
      }
        ]
  }
```

Figure 4

8.3. Model Inference Usage Event Record Example

```
{
  "record_id": "uer-20260507-0038",
  "accounting_context_id": "acctx-20260507-001",
  "event_type": "model-inference",
  "event_time": "2026-05-07T06:12:45Z",
  "observation_point": "agw-east-1",
  "actor_ref": "agent:core-network-diagnosis",
  "target_ref": "model:diagnosis-llm-v1",
  "usage_category": "model-inference",
  "usage_measurements": {
    "input-token-count": 1832,
    "output-token-count": 412,
    "reasoning-token-count": 960,
    "total-token-count": 3204
  },
  "result_status": "completed",
  "sequence_info": {
    "sequence": 38,
    "previous_record_hash": "sha256-..."
  },
  "evidence_ref": [
    {
      "evidence_id": "ev-0038",
      "evidence_type": "receipt",
      "digest_algorithm": "sha-256",
      "digest": "..."
    }
  ]
}
```


Figure 5

8.4. Usage Event Record Example

```
{
  "record_id": "uer-20260507-0037",
  "accounting_context_id": "acctx-20260507-001",
  "event_type": "tool-call",
  "event_time": "2026-05-07T06:12:43Z",
  "observation_point": "agw-east-1",
  "actor_ref": "agent:core-network-diagnosis",
  "target_ref": "tool:amf-log-analysis",
  "usage_category": "tool-invocation",
  "usage_measurements": {
    "standard-compute-usage": 1200,
    "processing-time-ms": 1840
  },
  "result_status": "completed",
  "sequence_info": {
    "sequence": 37,
    "previous_record_hash": "sha256-..."
  },
  "evidence_ref": [
    {
      "evidence_id": "ev-0037",
      "evidence_type": "trace-hash",
      "digest_algorithm": "sha-256",
      "digest": "..."
    }
  ]
}
```


Figure 6

9. Privacy Considerations

Usage accounting records can reveal sensitive information about users, organizations, agents, tasks, capabilities, tools, business workflows, network operations, and resource consumption. Implementations MUST minimize disclosure according to the accounting purpose.

Accounting records exported across domains SHOULD avoid raw prompts, raw tool outputs, personal data, confidential business data, and detailed operational logs unless explicitly authorized and necessary. Privacy-preserving summaries, pseudonymous identifiers, redaction, selective disclosure, and digest-only evidence references SHOULD be used where possible.

A Metering Profile SHOULD state whether records are event-level, aggregated, sampled, or summary-only. It SHOULD also state retention expectations and disclosure constraints.

The ability to correlate records across gateways or sessions can improve audit and dispute handling, but it can also enable tracking. Accounting Context identifiers and trace identifiers SHOULD be scoped, rotated, or pseudonymized according to policy.

10. Security Considerations

Accounting records may influence quota decisions, audit findings, operational analysis, and downstream business systems. Attackers may attempt to forge, modify, replay, suppress, duplicate, delay, or selectively disclose records.

Implementations SHOULD provide integrity protection, source authentication, replay protection, freshness validation, and duplicate detection for exported records. Existing mechanisms such as TLS [RFC8446], JOSE [RFC7515], COSE [RFC9052], JWT [RFC7519], and CWT [RFC8392] may be used as appropriate.

A receiving entity MUST NOT treat a Usage Event Record as trustworthy only because it is syntactically valid. The receiving entity SHOULD validate the asserting domain, signature status, freshness, evidence references, and applicable policy.

Records that contain usage values may be manipulated to inflate, suppress, or shift apparent usage. Implementations SHOULD support correction records, evidence references, and audit trails for changes to accounting state.

Result-verification records are especially sensitive because they may assert that a task outcome occurred. Such records SHOULD be bound to evidence, policy, and verification method. If human confirmation is used, the record SHOULD indicate the confirmation reference without exposing unnecessary personal data.

Accounting data loss can affect auditability. Implementations SHOULD consider reliable export, local buffering, non-volatile storage, acknowledgements, or retransmission where archival accounting is required by deployment policy.

11. IANA Considerations

This document requests no IANA actions in this version.

Future versions may request creation of registries for IoA Usage Event Types, IoA Usage Categories, IoA Measurement Dimensions, IoA Usage Units, IoA Measurement Methods, IoA Accounting Evidence Types, and IoA Accounting Result Status Values.

12. 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, <https://www.rfc-editor.org/info/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/info/rfc8174>.

13. Informative References

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, DOI 10.17487/RFC2866, June 2000, <https://www.rfc-editor.org/info/rfc2866>.

[RFC2975] Aboba, B., Arkko, J., and D. Harrington, "Introduction to Accounting Management", RFC 2975, DOI 10.17487/RFC2975, October 2000, <https://www.rfc-editor.org/info/rfc2975>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[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/info/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/info/rfc7519>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[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/info/rfc9052>.

Authors' Addresses

Lianhua Zhang
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: zhanglh2@asiainfo.com

Wen Qiao
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: qiaowen@asiainfo.com

Wei Zhang
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: zhangwei41@asiainfo.com

Huiling Yang
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: yanghl10@asiainfo.com

Yun Li
AsiaInfo Technologies (China) Inc.
Beijing
100000
China
Email: liyun9@asiainfo.com