Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 24 November 2026

T. Sato
MyAuberge K.K.

24 May 2026

The Mandate JWT (MJWT) for Agentic AI Systems
draft-sato-soos-mjwt-00

Abstract

AI agents operating in automated workflows require a structured authorization credential that binds agent authority not merely to an action type, but to a specific governed resource instance, a specific human principal, a specific Cedar action scope, and a specific mission context. Existing workload credentials provide identity but not governance binding. Existing OAuth tokens provide scope but not resource-instance specificity, human principal linkage, or mandate issuance chain traceability.

This document defines the Mandate JWT (MJWT): a WIMSE workload credential profile that grants an AI agent authority to perform a specified set of Cedar actions on a specific Sovereign Object instance under the oversight of a named human principal. The MJWT carries governance claims not present in general-purpose workload credentials: a Cedar action scope, a Sovereign Object instance binding, a human principal identifier, a mission reference, and a mandate ceiling. The Narrowing Property -- by which a child mandate is always a strict subset of its parent in all authorization dimensions -- is normatively defined. The MJWT is the authorization primitive referenced by [I-D.sato-soos-idp], [I-D.sato-soos-hem], [I-D.sato-soos-gar], [I-D.sato-soos-cap], and [I-D.sato-soos-sov].

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 24 November 2026.

Copyright Notice

Table of Contents

1. Introduction

The IETF community has made significant progress in specifying how AI agents authenticate using workload credentials [I-D.ietf-wimse-arch] and how they obtain authorization tokens for API invocation [I-D.ietf-oauth-v2-1]. These specifications answer the question: is this agent permitted to perform actions of type X?

The SOOS governance protocol family -- IDP [I-D.sato-soos-idp], HEM [I-D.sato-soos-hem], GAR [I-D.sato-soos-gar], and CAP [I-D.sato-soos-cap] -- requires a richer binding. An agent governed by SOOS is not merely permitted to perform actions of type X. It is authorized to perform a specific Cedar action set on a specific Sovereign Object instance [I-D.sato-soos-sov], under the oversight of a named human principal, within a declared mission context, subject to a mandate ceiling that cannot be exceeded by any child mandate in the delegation chain.

No existing credential type carries this combination of claims. WIMSE workload credentials provide identity. OAuth access tokens provide scope. Neither provides Sovereign Object instance binding, human principal linkage, mission reference, mandate ceiling, or delegation chain traceability with the Narrowing Property enforced as a normative invariant.

This document defines the Mandate JWT (MJWT): a WIMSE workload credential profile [I-D.ietf-wimse-arch] that extends the WIMSE credential model with governance claims specific to the SOOS protocol family. The MJWT is the authorization primitive that all five SOOS governance drafts reference: IDP presents it at each Transition Request; HEM records it at escalation; GAR includes it in every Session Audit Record; CAP evaluates it before prohibition enforcement; and SOV binds it to a Sovereign Object instance.

The MJWT is also a profile of the McGuinness Actor Profile [I-D.mcguinness-oauth-actor-profile]. The delegation_chain claim defined in the Actor Profile is adopted without modification and carries the mandate issuance chain from the originating human principal through each intermediate delegation step to the current agent. The MJWT extends this chain with SOOS-specific governance claims: the Sovereign Object binding, the Cedar action scope, the mission reference, and the mandate ceiling.

The mission_ref claim in the MJWT composes directly with Mission Bound Authorization [I-D.mcguinness-oauth-mission-bound-authorization]: a mission declared under that framework is referenceable as the mission_ref in the MJWT, binding per-transition IDP declarations to the broader mission context under which the agent is operating.

The design principle of the MJWT is instance specificity: an agent is not authorized to govern objects of type T in the abstract. It is authorized to perform Cedar actions A1..An on Sovereign Object instance Y, in lifecycle phases P1..Pm, while the Sovereign Object's state machine is in states S1..Sk, under human principal H. That specificity -- impossible to express with OAuth scopes or general WIMSE credentials -- is what makes SOOS governance auditable, revocable, and human-principal-traceable at the instance level.

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.

This document uses the following terms:

Mandate JWT (MJWT):
: A WIMSE workload credential profile defined in this document that binds an AI agent's authorization to a specific Sovereign Object instance under a named human principal.

Root Mandate:
: An MJWT issued directly by a human principal or a GEC acting on explicit human principal instruction. A Root Mandate has no parent mandate.

Child Mandate:
: An MJWT issued by a GEC on behalf of an agent that itself holds a valid MJWT (the parent mandate). A Child Mandate MUST satisfy the Narrowing Property with respect to its parent.

Narrowing Property:
: The invariant by which a Child Mandate is always a strict subset of its parent Mandate in every authorization dimension: Sovereign Object scope, Cedar action scope, permitted SO states, permitted lifecycle phases, temporal validity, and mandate ceiling.

Mandate Ceiling:
The maximum authorization level that any mandate in a delegation chain may grant. Expressed as a conformance level integer (1, 2, or 3) corresponding to the GEC conformance levels defined in [I-D.sato-soos-idp] Section 9.

Delegation Chain:
The ordered sequence of mandate issuance events from the Root Mandate to the current MJWT, as recorded in the delegation_chain claim.

Revocation Registry:
A GEC-maintained store of revoked mandate jti values and their cascade revocation trees.

Sovereign Object (SO):
As defined in [I-D.sato-soos-sov]: a causally ordered, policy-governed, typed, living document that evolves through a predefined finite state space under GEC authority.

Governing Enforcement Component (GEC):
As defined in [I-D.sato-soos-idp]: a runtime component that enforces authorization policy, records agent actions to a tamper-evident Event Log, and mediates agent access to governed objects.

Cedar:
A policy language and evaluation engine [Cedar] used by the GEC to evaluate authorization decisions.

Human Principal:
A natural person who holds authority over an SO Instance and whose identifier appears in the MJWT human_principal_id claim.

Mission Reference:
A UUID identifying a MissionDeclaration as defined in [I-D.mcguinness-oauth-mission-bound-authorization] under which the agent is operating.

3. Problem Statement

3.1. The Governance Binding Gap

The SOOS governance protocol family requires that every agent action be traceable to:

(a) A specific human principal who authorized the agent's mandate.
(b) A specific Sovereign Object instance the agent is bound to.
(c) A specific Cedar action set the agent is permitted to execute.
(d) A specific mission context under which the agent is operating.
(e) A mandate issuance chain from the authorizing human principal through every intermediate delegation step.
(f) A mandate ceiling that no child mandate may exceed.

No existing credential standard provides all six properties in a single verifiable token. This gap means that the four live SOOS drafts -- IDP, HEM, GAR, and CAP -- each reference a Mandate JWT as the authorization primitive without a normative specification of what that JWT must contain. This document fills that gap.

3.2. Why Existing Credentials Are Insufficient

OAuth 2.1 access tokens [I-D.ietf-oauth-v2-1] provide scope-based authorization. They do not provide Sovereign Object instance binding, human principal identification, mission reference, mandate

ceiling, or Narrowing Property enforcement. An OAuth scope of "booking:write" authorizes an agent to perform booking write operations in general; it does not authorize a specific agent to perform Cedar action "atp:booking:confirm" on SO instance "019547ab-..." under human principal "hp-001".

WIMSE workload credentials [I-D.ietf-wimse-arch] provide workload identity. They authenticate the agent as a specific workload but do not carry the governance claims required by SOOS: SO binding, Cedar action scope, human principal linkage, or mandate ceiling. The MJWT is a WIMSE profile -- it extends WIMSE credentials with these governance claims, not replaces them.

The McGuinness Actor Profile [I-D.mcguinness-oauth-actor-profile] provides delegation chain traceability. The MJWT adopts the delegation_chain claim directly and extends it with SO binding and SOOS governance claims. The Actor Profile and the MJWT are complementary, not competing.

3.3. Relationship to WIMSE

The MJWT is a WIMSE workload credential profile. It extends the WIMSE credential model [I-D.ietf-wimse-arch] by adding governance claims specific to the SOOS protocol family.

A WIMSE-conforming verifier that does not understand MJWT-specific claims MUST treat those claims as unrecognized and MUST NOT fail verification solely because of their presence, consistent with JWT processing rules [RFC7519]. A GEC verifying an MJWT MUST process all SOOS governance claims as specified in Section 8.

The MJWT is intended as a candidate for submission to the WIMSE working group as an AI agent governance profile. The June 2026 WIMSE interim discussion of draft-klrc-aiagent-auth identified governance binding as a gap in existing AI agent authentication proposals. The MJWT addresses that gap.

3.4. Relationship to Mission Bound Authorization

Mission Bound Authorization [I-D.mcguinness-oauth-mission-bound-authorization] defines a framework for binding agent authorization to a declared mission context. The MJWT mission_ref claim carries a MissionDeclaration UUID from that framework.

When mission_ref is present in an MJWT, the IDP mission_ref field [I-D.sato-soos-idp] Section 4.1 MUST match the MJWT mission_ref at every Transition Request. This binding ensures that per-transition intent declarations are traceable to the broader mission context, enabling Cedar policies to distinguish between on-mission and off-mission agent actions.

The MJWT thus serves as the token-level bridge between Mission Bound Authorization (the mission declaration framework) and IDP (the per-transition intent declaration).

3.5. Relationship to the Actor Profile

The McGuinness Actor Profile [I-D.mcguinness-oauth-actor-profile] defines the delegation_chain claim for recording the sequence of principals in an authorization delegation. The MJWT adopts this claim without modification.

In the MJWT, the delegation_chain records the mandate issuance history from the Root Mandate’s human principal through each intermediate sub-agent delegation to the current mandate holder. This chain enables the GEC, human principals, and Verified External

Auditors to trace any agent action back to the originating human authorization -- a requirement for EU AI Act Article 12 compliance [EUAIA] and for the accountability property that SOOS is designed to provide.

4. The Mandate JWT

4.1. MJWT as a WIMSE Workload Credential Profile

The MJWT is a JSON Web Token [RFC7519] that conforms to the WIMSE workload credential model [I-D.ietf-wimse-arch] and extends it with SOOS governance claims. The MJWT MUST be signed using the Ed25519 algorithm [RFC8037].

The MJWT is presented by an agent to the GEC as part of every Transition Request, alongside an IDP [I-D.sato-soos-idp]. The GEC MUST verify the MJWT before evaluating Cedar policy. The verification protocol is specified in Section 8.

4.2. MJWT Claims

4.2.1. Standard JWT Claims

iss (Issuer):
: REQUIRED. The identifier of the GEC or human principal that issued this MJWT. For Root Mandates, this is the human principal's identifier. For Child Mandates, this is the issuing GEC's identifier.

sub (Subject):
: REQUIRED. The identifier of the agent holding this MJWT. MUST be a WIMSE workload identifier [I-D.ietf-wimse-arch].

jti (JWT ID):
: REQUIRED. A UUID v7 [RFC9562] uniquely identifying this MJWT instance. The jti is the mandate_id referenced by IDP [I-D.sato-soos-idp] Section 4.1 and GAR [I-D.sato-soos-gar]. UUID v7 is required for its time-ordered property, which enables chronological mandate issuance queries without additional indexing.

iat (Issued At):
: REQUIRED. The time at which this MJWT was issued.

exp (Expiration Time):
: REQUIRED. The time after which this MJWT MUST NOT be accepted. For Child Mandates, exp MUST NOT be later than the parent mandate's exp claim. This is a dimension of the Narrowing Property (Section 5).

nbf (Not Before):
: OPTIONAL. The time before which this MJWT MUST NOT be accepted.

4.2.2. WIMSE Claims

The MJWT inherits the following WIMSE claims as defined in [I-D.ietf-wimse-arch]:

wid (Workload Identifier):
: REQUIRED. The WIMSE workload identifier of the agent.

cnf (Confirmation):
: REQUIRED. The proof-of-possession key confirmation claim [RFC7800]. The agent MUST demonstrate possession of the corresponding private key when presenting the MJWT.

4.2.3. SOOS Governance Claims

The following claims are defined by this document and constitute the SOOS governance extension to the WIMSE credential model.

so_id:
: REQUIRED. The UUID v7 identifier of the Sovereign Object instance this MJWT binds the agent to, as defined in [I-D.sato-soos-sov] Section 4.2.1. The GEC MUST verify that the so_id in the MJWT matches the SO Instance targeted by the Transition Request.

so_type_id:
: REQUIRED. The SO Type identifier of the bound Sovereign Object instance. MUST match the so_type_id in the SO Instance's Identity Layer [I-D.sato-soos-sov].

human_principal_id:
: REQUIRED. The identifier of the human principal under whose authority this MJWT was issued. For Root Mandates, this is the identifier of the natural person who directly authorized the agent. For Child Mandates, this MUST be the same human_principal_id as the parent mandate -- the human principal of the root of the delegation chain does not change through sub-agent issuance.

  The GEC MUST verify that the human_principal_id in the MJWT matches the human_principal_id in the SO Instance's Identity Layer [I-D.sato-soos-sov] Section 4.2.1.

cedar_actions:
: REQUIRED. A JSON array of Cedar action strings that this MJWT authorizes the agent to request. The GEC MUST reject Transition Requests for Cedar actions not present in this array.

  For Child Mandates, cedar_actions MUST be a subset of the parent mandate's cedar_actions. This is a dimension of the Narrowing Property (Section 5).

permitted_states:
: OPTIONAL. A JSON array of SO state strings (as declared in the SO Type's state machine) in which the authorized cedar_actions may be performed. If absent, the cedar_actions are permitted in all states declared in the SO Type. For Child Mandates, if present, this array MUST be a subset of the parent mandate's permitted_states.

permitted_phases:
: OPTIONAL. A JSON array of SO lifecycle phase strings in which the authorized cedar_actions may be performed. If absent, the cedar_actions are permitted in all lifecycle phases. For Child Mandates, if present, this array MUST be a subset of the parent mandate's permitted_phases.

mandate_ceiling:
: REQUIRED. An integer (1, 2, or 3) specifying the maximum GEC conformance level at which this MJWT and any child mandates derived from it may be honored. The GEC MUST reject MJWTs with a mandate_ceiling below its own conformance level. See Section 9 for ceiling enforcement rules.

parent_mandate_id:
: REQUIRED for Child Mandates; MUST be absent for Root Mandates. The jti of the parent MJWT from which this Child Mandate was derived. Enables the GEC to retrieve and verify the parent mandate for Narrowing Property verification.

delegation_chain:
OPTIONAL; REQUIRED when parent_mandate_id is present. The delegation chain as defined by [I-D.mcguinness-oauth-actor-profile]. Each entry in the chain records one issuance step: the issuing principal, the receiving agent, the issued jti, and the issuance timestamp. The chain enables complete traceability from any Child Mandate back to the originating human principal without requiring the verifier to retrieve intermediate mandates.

mission_ref:
OPTIONAL. A UUID identifying a MissionDeclaration as defined in [I-D.mcguinness-oauth-mission-bound-authorization]. When present, the IDP mission_ref field [I-D.sato-soos-idp] Section 4.1 MUST match this value at every Transition Request. The GEC MUST reject Transition Requests where mission_ref is present in the MJWT but absent or mismatched in the IDP.

zone_b_read:
OPTIONAL. Boolean. If true, this MJWT authorizes the agent to read Zone B content from the bound SO Instance, subject to Cedar policy evaluation [I-D.sato-soos-sov] Section 7.2. Default: false.

zone_b_write:
OPTIONAL. Boolean. If true, this MJWT authorizes the agent to attach Zone B content to the bound SO Instance, subject to Cedar policy evaluation. Default: false.

4.3. MJWT JSON Structure

The following is the normative JSON structure of an MJWT. Fields marked REQUIRED MUST be present. Fields marked OPTIONAL MAY be omitted.

```
{
  "iss":                string,   ; REQUIRED. Issuer identifier.
  "sub":                string,   ; REQUIRED. WIMSE workload ID.
  "jti":                string,   ; REQUIRED. UUID v7. mandate_id.
  "iat":                integer,  ; REQUIRED. NumericDate.
  "exp":                integer,  ; REQUIRED. NumericDate.
  "nbf":                integer,  ; OPTIONAL. NumericDate.

  "wid":                string,   ; REQUIRED. WIMSE workload ID.
  "cnf": {                        ; REQUIRED. PoP key confirmation.
    "jwk": { ... }                ; Ed25519 public key [RFC8037].
  },

  "so_id":              string,   ; REQUIRED. SO Instance UUID v7.
  "so_type_id":         string,   ; REQUIRED. SO Type identifier.
  "human_principal_id": string,   ; REQUIRED. Human principal ID.
  "cedar_actions":      [string], ; REQUIRED. Authorized actions.
  "permitted_states":   [string], ; OPTIONAL. Permitted SO states.
  "permitted_phases":   [string], ; OPTIONAL. Permitted SO phases.
  "mandate_ceiling":    integer,  ; REQUIRED. 1, 2, or 3.
  "parent_mandate_id":  string,   ; REQUIRED if child mandate.
  "delegation_chain":   [object], ; REQUIRED if child mandate.
  "mission_ref":        string,   ; OPTIONAL. Mission UUID.
  "zone_b_read":        boolean,  ; OPTIONAL. Default false.
  "zone_b_write":       boolean   ; OPTIONAL. Default false.
}
```

The MJWT MUST be signed using Ed25519 [RFC8037]. The JOSE header MUST include:

```
{
  "alg": "EdDSA",
  "kid": "<key identifier of the issuer's signing key>"
}
```

5. The Narrowing Property

5.1. Definition

The Narrowing Property is a normative invariant of the MJWT delegation model. A Child Mandate MUST be a strict subset of its parent Mandate in every authorization dimension. A Child Mandate MUST NOT grant any authority that its parent Mandate does not itself hold.

The Narrowing Property is what gives SOOS delegation its security guarantee: no sub-agent in a delegation chain can exceed the authority of the human principal at the root of that chain.

5.2. Narrowing Dimensions

The Narrowing Property applies across six dimensions:

(a) Sovereign Object scope. A Child Mandate's so_id MUST reference the same SO Instance as its parent. A Child Mandate MUST NOT reference an SO Instance not covered by its parent.

(b) Cedar action scope. A Child Mandate's cedar_actions array MUST be a subset of its parent's cedar_actions array. The GEC MUST reject a Child Mandate that contains any Cedar action not present in the parent mandate's cedar_actions.

(c) Permitted SO states. If a Child Mandate declares permitted_states, that array MUST be a subset of the parent's permitted_states. If the parent mandate does not declare permitted_states (implying all states are permitted), the child may declare any permitted_states subset.

(d) Permitted lifecycle phases. If a Child Mandate declares permitted_phases, that array MUST be a subset of the parent's permitted_phases. If the parent does not declare permitted_phases, the child may declare any subset.

(e) Temporal validity. A Child Mandate's exp claim MUST NOT be later than its parent's exp claim. The GEC MUST reject a Child Mandate whose exp exceeds the parent's exp.

(f) Mandate ceiling. A Child Mandate's mandate_ceiling MUST NOT exceed its parent's mandate_ceiling. A Root Mandate establishes the maximum ceiling for the entire delegation tree.

5.3. GEC Verification of Narrowing

The GEC MUST verify the Narrowing Property whenever a Child Mandate is presented. Verification requires retrieving or caching the parent mandate identified by parent_mandate_id.

If the parent mandate has been revoked (Section 7), the GEC MUST treat the Child Mandate as invalid regardless of the Child Mandate's own revocation status.

Narrowing Property violations MUST result in a NARROWING_VIOLATION deny code in the GEC DENY response [I-D.sato-soos-idp] Section 6. The violation MUST be recorded in the SO Instance Event Stream as a MANDATE_NARROWING_VIOLATION entry.

The delegation_chain claim (Section 4.2.3) MAY be used by the GEC to verify the full chain without retrieving each intermediate mandate individually, provided the chain entries are signed by the GEC that issued each step.

6. Mandate Issuance

6.1. Issuance Authority

Root Mandates MUST be issued by a human principal or by a GEC acting on explicit, recorded human principal instruction. The issuance event MUST generate a MANDATE_BOUND entry in the SO Instance Event Stream [I-D.sato-soos-sov] Section 4.2.3.

A GEC MUST NOT issue a Root Mandate autonomously. Any MJWT that does not carry a parent_mandate_id and was not issued pursuant to recorded human principal instruction MUST be treated as invalid.

6.2. Child Mandate Issuance

A Child Mandate is issued by a GEC on behalf of an agent that itself holds a valid, non-revoked MJWT (the parent mandate). The issuing GEC MUST:

(a) Verify that the parent mandate is valid and non-revoked.
(b) Verify that the requested Child Mandate satisfies the Narrowing Property in all six dimensions (Section 5.2).
(c) Set parent_mandate_id to the jti of the parent mandate.
(d) Extend the delegation_chain with a new entry recording this issuance step.
(e) Set human_principal_id to the same value as the parent mandate's human_principal_id.
(f) Generate a MANDATE_BOUND Event Stream entry for the SO Instance.
(g) Sign the Child Mandate with the GEC's Ed25519 signing key.

The GEC MUST NOT issue a Child Mandate that violates the Narrowing Property. An issuance request that would violate Narrowing MUST be rejected with a NARROWING_VIOLATION response and MUST be recorded in the Event Stream.

6.3. Delegation Chain

The delegation_chain claim records the mandate issuance history as defined by [I-D.mcguinness-oauth-actor-profile]. Each entry in the chain MUST contain:

issuer_id:
The identifier of the principal (human or GEC) that issued this mandate step.

recipient_id:
The WIMSE workload identifier of the agent that received this mandate step.

mandate_jti:
The jti of the MJWT issued at this step.

issued_at:
ISO 8601 timestamp of issuance.

gec_signature:
The Ed25519 signature of the issuing GEC over this chain entry. For the Root Mandate step (issued by a human principal), this field carries the human principal's signing key signature if

available, or is marked as human_issued.

The delegation_chain enables a verifier to reconstruct the complete authorization lineage without retrieving each intermediate MJWT, provided each chain entry's gec_signature is valid.

7. Mandate Revocation

7.1. Revocation Registry

The GEC MUST maintain a Revocation Registry: a persistent store of revoked mandate jti values and their associated cascade revocation trees.

The Revocation Registry MUST be queryable by jti. A query response MUST indicate:

(a) Whether the queried jti is directly revoked.
(b) Whether the queried jti is cascade-revoked (its parent or an ancestor has been revoked).
(c) The revocation timestamp.
(d) The jti of the directly revoked ancestor, if cascade-revoked.

The GEC MUST check the Revocation Registry before accepting any MJWT at a Transition Request. A revoked or cascade-revoked MJWT MUST result in a MANDATE_REVOKED deny code.

7.2. Cascade Revocation

Revoking a mandate automatically revokes all Child Mandates derived from it. This is the cascade revocation property.

When a mandate is revoked, the GEC MUST:

(a) Record the jti in the Revocation Registry as directly revoked.
(b) Traverse the mandate issuance tree rooted at the revoked jti and mark all descendant jtis as cascade-revoked.
(c) Generate a MANDATE_REVOKED Event Stream entry for each revoked mandate, recording the jti, the revocation reason, the revoking principal, and the revocation timestamp.
(d) If any revoked mandate is currently bound to an active GEC session, the GEC MUST immediately trigger HEM Class 1 escalation [I-D.sato-soos-hem] for that session.

Cascade revocation MUST be propagated within the trust domain in which the mandate was issued. Cross-domain cascade revocation semantics are outside the scope of this document.

7.3. Revocation Event Log Entry

Every revocation event MUST generate a MANDATE_REVOKED entry in the SO Instance Event Stream with the following fields:

```
{
  "event_type":          "MANDATE_REVOKED",
  "revoked_jti":         string,   ; jti of the revoked mandate.
  "revocation_type":     string,   ; "DIRECT" or "CASCADE".
  "cascade_root_jti":    string,   ; jti of directly revoked ancestor
                                   ; if REVOCATION_TYPE is CASCADE.
  "revocation_reason":   string,   ; Human-readable reason.
  "revoking_principal":  string,   ; ID of revoking human principal.
  "revoked_at":          string    ; ISO 8601 timestamp.
}
```

8. GEC Verification Protocol

8.1. Verification Steps

On receiving a Transition Request carrying an MJWT, the GEC MUST perform the following verification steps in order before proceeding to Cedar policy evaluation. Failure at any step MUST result in an immediate DENY response with the appropriate deny code (Section 8.2). The DENY MUST be recorded in the SO Instance Event Stream.

Step 1 -- Signature verification.
Verify the MJWT's Ed25519 signature using the issuer's public key. The issuer's public key MUST be retrieved from the GEC's trusted key store or from the WIMSE trust anchor for the issuing workload.

Step 2 -- Temporal validity.
Verify that the current time is after nbf (if present) and before exp. An expired MJWT MUST be rejected.

Step 3 -- Revocation check.
Query the Revocation Registry for the MJWT's jti. A directly revoked or cascade-revoked MJWT MUST be rejected.

Step 4 -- SO Instance binding.
Verify that the MJWT's so_id matches the SO Instance targeted by the Transition Request. Verify that the MJWT's so_type_id matches the SO Instance's so_type_id.

Step 5 -- Human principal linkage.
Verify that the MJWT's human_principal_id matches the human_principal_id in the SO Instance's Identity Layer [I-D.sato-soos-sov] Section 4.2.1.

Step 6 -- Mandate ceiling.
Verify that the MJWT's mandate_ceiling is greater than or equal to the GEC's conformance level. A mandate ceiling below the GEC's conformance level MUST be rejected.

Step 7 -- Narrowing Property (Child Mandates only).
If parent_mandate_id is present, retrieve or verify the parent mandate and verify the Narrowing Property in all six dimensions (Section 5.2).

Step 8 -- Cedar action scope.
Verify that the cedar_action in the Transition Request is present in the MJWT's cedar_actions array.

Step 9 -- State and phase restrictions.
If permitted_states is present, verify that the SO Instance's current_state is in the permitted_states array. If permitted_phases is present, verify that the SO Instance's current_phase is in the permitted_phases array.

Step 10 -- Mission reference (if present).
If the MJWT carries mission_ref, verify that the IDP submitted with this Transition Request also carries mission_ref and that the values match.

All ten steps MUST pass before the GEC proceeds to Cedar policy evaluation.

8.2. Verification Failure Deny Codes

The following deny codes are defined for MJWT verification failures. These codes are returned in the GEC DENY response as defined in

[I-D.sato-soos-idp] Section 6.

Deny Code	Step	Condition
MJWT_SIGNATURE_INVALID	1	Ed25519 signature invalid.
MJWT_EXPIRED	2	Current time after exp.
MJWT_NOT_YET_VALID	2	Current time before nbf.
MANDATE_REVOKED	3	jti directly or cascade revoked.
MJWT_SO_MISMATCH	4	so_id mismatch.
MJWT_SO_TYPE_MISMATCH	4	so_type_id mismatch.
MJWT_PRINCIPAL_MISMATCH	5	human_principal_id mismatch.
MJWT_CEILING_INSUFFICIENT	6	mandate_ceiling below GEC level.
NARROWING_VIOLATION	7	Narrowing Property violated.
MANDATE_SCOPE	8	cedar_action not in scope.
MJWT_STATE_RESTRICTED	9	SO state not in permitted_states.
MJWT_PHASE_RESTRICTED	9	SO phase not in permitted_phases.
MJWT_MISSION_REF_MISMATCH	10	mission_ref mismatch with IDP.

9. Mandate Ceiling

9.1. Ceiling Definition

The mandate_ceiling claim specifies the maximum GEC conformance level at which this MJWT and any Child Mandate derived from it may be honored. The ceiling values correspond to the conformance levels defined in [I-D.sato-soos-idp] Section 9:

Ceiling Value	GEC Level	Description
1	Level 1	Application Profile. GEC as SDK.
2	Level 2	Isolated Profile. GEC as sidecar.
3	Level 3	Kernel Profile. RATS-attested TEE.

A mandate_ceiling of 2 means this MJWT and all Child Mandates derived from it MAY be honored by a Level 1 or Level 2 GEC, but MUST NOT be honored by a Level 3 GEC. This ceiling prevents a mandate issued in a lower-assurance context from being used to authorize actions in a higher-assurance enforcement environment.

The ATP Foundation has closed decision TI-2 specifying that the mandate ceiling for the ATP reference implementation is Level 2. No mandate issued in the ATP Booking Object governance context may be honored by a Level 3 (hardware-attested) GEC without explicit human principal re-authorization at Level 3.

9.2. GEC Ceiling Enforcement

The GEC MUST enforce the mandate ceiling at Step 6 of the verification protocol (Section 8.1).

A Level 3 GEC MUST reject any MJWT with mandate_ceiling < 3.
A Level 2 GEC MUST reject any MJWT with mandate_ceiling < 2.
A Level 1 GEC accepts MJWTs with any mandate_ceiling value.

When a mandate_ceiling violation is detected, the GEC MUST return a MJWT_CEILING_INSUFFICIENT deny code and MUST record the event in the SO Instance Event Stream.

10. Relationship to Other SOOS Drafts

IDP [I-D.sato-soos-idp]:
The IDP mandate_id field carries the jti of the MJWT presented with each Transition Request, linking every intent declaration to the specific mandate under which the agent is acting. The

IDP mission_ref field MUST match the MJWT mission_ref when present. The GEC verifies this match at Step 10 of the verification protocol (Section 8.1).

HEM [I-D.sato-soos-hem]:
HEM escalation events reference the mandate_id of the MJWT active at the time of escalation. Mandate revocation during an active HEM_PENDING state MUST trigger Class 1 escalation. The human principal identified by human_principal_id in the MJWT is the natural person responsible for HEM decision authority over the SO Instance.

GAR [I-D.sato-soos-gar]:
The Session Audit Record includes the mandate_id of every MJWT presented during the governed session. The delegation_chain in each MJWT provides the traceability record that GAR audit consumers use to reconstruct the full authorization lineage.

CAP [I-D.sato-soos-cap]:
CAP Tier 0 and Tier 1 prohibition evaluation occurs before MJWT scope verification in the policy evaluation order defined in [I-D.sato-soos-sov] Section 7.3. A CAP prohibition denies the action regardless of the MJWT's cedar_actions scope.

SOV [I-D.sato-soos-sov]:
The MJWT so_id claim binds the mandate to a specific SO Instance as defined in [I-D.sato-soos-sov]. The Narrowing Property dimensions (Section 5.2) directly correspond to the binding model specified in [I-D.sato-soos-sov] Section 8.

11. Security Considerations

The MJWT is the authorization primitive for the SOOS governance stack. Its security properties depend on the security of the Ed25519 signing keys used by issuing GECs and human principals.

GEC signing keys MUST be protected at the conformance level declared by the GEC [I-D.sato-soos-idp] Section 9. At Level 3, keys MUST be bound to a RATS-attested execution environment. At Level 2, keys MUST be held in an isolated process inaccessible to agent code. At Level 1, key protection is application-managed; SCITT transparency log submission is RECOMMENDED as a compensating control.

The Narrowing Property (Section 5) is a security invariant. Any implementation that allows a Child Mandate to exceed the scope of its parent creates an authorization escalation vulnerability. The GEC MUST enforce Narrowing at issuance (Section 6.2) and at verification (Section 8.1 Step 7). Enforcing at both points provides defense in depth.

Cascade revocation (Section 7.2) requires the GEC to maintain a complete mandate issuance tree for each SO Instance. Implementations MUST ensure that the mandate issuance tree is consistent with the SO Instance Event Stream. An inconsistency between the two is a critical security finding and MUST trigger HEM Class 1 escalation.

The mandate_ceiling claim (Section 9) prevents mandate laundering: an attempt to use a mandate issued in a lower-assurance context to authorize actions in a higher-assurance enforcement environment. Implementations MUST enforce ceiling constraints at Step 6 before proceeding to any further verification.

The human_principal_id claim is a persistent identifier for a natural person. It MUST be treated as sensitive and MUST be

protected against unauthorized disclosure. Access to MJWT contents containing human_principal_id MUST be authorized by Cedar policy.

12. Privacy Considerations

The MJWT carries human_principal_id, a persistent identifier for a natural person. Implementations MUST NOT expose MJWT contents to agents or principals not authorized to receive them by Cedar policy.

The delegation_chain records the sequence of principals in a mandate issuance chain. This chain may constitute personal data under GDPR Article 4(1) [GDPR] and APPI Article 2 [APPI]. Implementations MUST apply appropriate access controls to delegation_chain contents.

MJWT jti values (mandate_ids) are UUID v7 values that carry timing information. Implementations that consider mandate issuance timing sensitive MUST treat jti values as sensitive identifiers.

The Revocation Registry (Section 7.1) may reveal information about mandate issuance and revocation patterns. Access to the Revocation Registry MUST be restricted to authorized GECs and audit principals.

13. IANA Considerations

13.1. JWT Claims Registry

This document requests registration of the following JWT claims in the IANA JSON Web Token Claims registry [RFC7519]:

Claim Name: so_id
Claim Description: Sovereign Object instance identifier.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: so_type_id
Claim Description: Sovereign Object Type identifier.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: human_principal_id
Claim Description: Human principal identifier for agent mandate.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: cedar_actions
Claim Description: Authorized Cedar action set.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: permitted_states
Claim Description: Permitted Sovereign Object states.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: permitted_phases
Claim Description: Permitted Sovereign Object lifecycle phases.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: mandate_ceiling
Claim Description: Maximum GEC conformance level for mandate.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: parent_mandate_id
Claim Description: JWT ID of parent mandate in delegation chain.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: mission_ref
Claim Description: Mission Declaration UUID reference.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: zone_b_read
Claim Description: Zone B read authorization flag.
Change Controller: IESG
Reference: This document, Section 4.2.3.

Claim Name: zone_b_write
Claim Description: Zone B write authorization flag.
Change Controller: IESG
Reference: This document, Section 4.2.3.

13.2. MJWT Deny Code Registry

This document requests IANA to create the following registry:

Registry name: SOOS MJWT Verification Deny Code Registry
Registration procedure: Specification Required.

Initial registrations: As listed in Section 8.2.

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, May 2015.

[RFC7800] Jones, M., Bradley, J., and H. Tschofenig, "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)", RFC 7800, April 2016.

[RFC8037] Liusvaara, I., "CFRG Elliptic Curves for JOSE", RFC 8037, January 2017.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

[RFC9562] Davis, B., Peabody, C., and P. Leach, "Universally Unique IDentifiers (UUIDs)", RFC 9562, May 2024.

[Cedar] Amazon Web Services, "Cedar Policy Language Specification", https://docs.cedarpolicy.com/

[I-D.sato-soos-idp] Sato, T., "The Intent Declaration Primitive (IDP) for Agentic AI Systems", draft-sato-soos-idp-03, May 2026.

[I-D.sato-soos-hem] Sato, T., "The Human Escalation Mechanism (HEM) for Agentic AI Systems", draft-sato-soos-hem-01, May 2026.

[I-D.sato-soos-gar]

Sato, T., "Governance Audit Record (GAR) for Agentic AI Systems", draft-sato-soos-gar-00, May 2026.

[I-D.sato-soos-cap]
Sato, T., "Constitutional AI Protocol (CAP) for Agentic AI Systems", draft-sato-soos-cap-00, May 2026.

[I-D.sato-soos-sov]
Sato, T., "The Sovereign Object (SOV) for Agentic AI Systems", draft-sato-soos-sov-00, May 2026.

[I-D.ietf-wimse-arch]
Salomoni, D., et al., "WIMSE Architecture", draft-ietf-wimse-arch, work in progress.

[I-D.ietf-oauth-v2-1]
Hardt, D., et al., "The OAuth 2.1 Authorization Framework", draft-ietf-oauth-v2-1, work in progress.

[I-D.mcguinness-oauth-actor-profile]
McGuinness, K., et al., "OAuth Actor Profile", draft-mcguinness-oauth-actor-profile-00, 2026.

[I-D.mcguinness-oauth-mission-bound-authorization]
McGuinness, K., et al., "Mission Bound Authorization", draft-mcguinness-oauth-mission-bound-authorization-00, 2026.

[GDPR] European Parliament, "General Data Protection Regulation", Regulation (EU) 2016/679, April 2016.

[APPI] Government of Japan, "Act on the Protection of Personal Information", Act No. 57 of 2003, as amended.

14.2. Informative References

[I-D.sato-soos-faip]
Sato, T., "Federated Agent Intelligence Protocol (FAIP)", draft-sato-soos-faip-00, forthcoming.

[EUAIA] European Parliament, "Artificial Intelligence Act", Regulation (EU) 2024/1689, June 2024.

Appendix A. MJWT Examples

A.1. Root Mandate Example

The following is an example Root Mandate issued by a human principal to an OTA booking agent for a specific ATP Booking Object instance.

Header:

```
{
  "alg": "EdDSA",
  "kid": "hp-001-ed25519-key-1"
}
```

Payload:

```
{
  "iss":                "hp-001",
  "sub":                "wimse:agent:ota-booking-agent-v2",
  "jti":                "019547ab-1234-7abc-8def-000000000001",
  "iat":                1748131200,
  "exp":                1748217600,

  "wid":                "wimse:agent:ota-booking-agent-v2",
```

```
  "cnf": {
    "jwk": {
      "kty": "OKP",
      "crv": "Ed25519",
      "x":   "11qYAYKxCrfVS_7TyWQHOg7hcvPapiMlrwIaaPcHURo"
    }
  },

  "so_id":              "019547ab-1234-7abc-8def-000000000099",
  "so_type_id":         "atp/booking-object/1.0",
  "human_principal_id": "hp-001",
  "cedar_actions":      [
                          "atp:booking:confirm",
                          "atp:booking:cancel",
                          "atp:booking:suspend"
                        ],
  "permitted_states":   ["CONFIRMED", "PRE_ACTIVITY", "IN_JOURNEY"],
  "permitted_phases":   ["ACTIVE"],
  "mandate_ceiling":    2,
  "mission_ref":        "mission-uuid-azusa-journey-2026-06-15",
  "zone_b_read":        true,
  "zone_b_write":       false
}
```

A.2. Child Mandate Example

The following is a Child Mandate issued by the GEC to a sub-agent (weather monitoring agent) derived from the Root Mandate in A.1. The Narrowing Property is demonstrated: cedar_actions is a strict subset and permitted_states is further restricted.

Payload:

```
{
  "iss":                "gec-myauberge-001",
  "sub":                "wimse:agent:weather-monitor-agent-v1",
  "jti":                "019547ab-1234-7abc-8def-000000000002",
  "iat":                1748131260,
  "exp":                1748174400,

  "wid":                "wimse:agent:weather-monitor-agent-v1",
  "cnf": { "jwk": { ... } },

  "so_id":              "019547ab-1234-7abc-8def-000000000099",
  "so_type_id":         "atp/booking-object/1.0",
  "human_principal_id": "hp-001",
  "cedar_actions":      ["atp:booking:suspend"],
  "permitted_states":   ["IN_JOURNEY"],
  "permitted_phases":   ["ACTIVE"],
  "mandate_ceiling":    2,
  "parent_mandate_id":  "019547ab-1234-7abc-8def-000000000001",
  "delegation_chain": [
    {
      "issuer_id":    "hp-001",
      "recipient_id": "wimse:agent:ota-booking-agent-v2",
      "mandate_jti":  "019547ab-1234-7abc-8def-000000000001",
      "issued_at":    "2026-05-24T12:00:00Z",
      "gec_signature": "human_issued"
    },
    {
      "issuer_id":    "gec-myauberge-001",
      "recipient_id": "wimse:agent:weather-monitor-agent-v1",
      "mandate_jti":  "019547ab-1234-7abc-8def-000000000002",
      "issued_at":    "2026-05-24T12:01:00Z",
      "gec_signature": "<Ed25519 signature>"
    }
  ],
```

```
  "mission_ref":        "mission-uuid-azusa-journey-2026-06-15",
  "zone_b_read":        false,
  "zone_b_write":       false
}
```

In this Child Mandate:
- cedar_actions is reduced to ["atp:booking:suspend"] only.
- permitted_states is narrowed to ["IN_JOURNEY"] only.
- exp is earlier than the parent mandate's exp.
- zone_b_read is false (parent had true; child reduces it).
- human_principal_id is unchanged: "hp-001".
- The delegation_chain records both issuance steps.

The weather monitoring agent may only request BOOKING_SUSPENDED state transitions, only while the Booking Object is IN_JOURNEY, and cannot read Zone B (traveller personal data). This is the Narrowing Property in production.

Author's Address

Tom Sato
MyAuberge K.K.
Chino, Nagano, Japan
Email: tomsato@myauberge.jp