Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: 18 November 2026

Y. Wang
Independent

17 May 2026

JEP Action Mandate Profile (JEP-AMP)
draft-wang-jep-action-mandate-profile-00

Abstract

This document defines the JEP Action Mandate Profile (JEP-AMP), a profile of the Judgment Event Protocol (JEP). JEP-AMP specifies how a JEP Delegation event can express a verifiable, bounded, revocable, and auditable mandate for an agent, human, organization, workflow, or system to perform an action on behalf of a principal.

JEP-AMP does not redefine JEP-Core event verbs, signature semantics, event hash semantics, validation-level semantics, identity systems, credential systems, legal liability, regulatory sufficiency, or global authorization validity. Instead, it defines the minimum interoperable shape of an Action Mandate Descriptor and the rules by which relying parties, gateways, verifiers, and receipt systems can interpret a JEP Delegation event as a candidate action mandate under a stated trust, policy, and profile context.

The profile is intended to support agentic workflows such as enterprise procurement, supplier payment, contract modification, data export, customer refund, claim handling, and other high-responsibility actions where pre-action authorization, in-action policy validation, and after-action receipt evidence are required.

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 18 November 2026.

Table of Contents

1. Introduction

AI agents, delegated workflows, and autonomous software systems are increasingly able to call tools, access enterprise systems, initiate transactions, modify records, and interact with external parties. A system that can perform actions on behalf of a human or organization requires more than a log. It requires a way to express who authorized which actor to perform which action, under which constraints, for which purpose, and with which evidence obligations.

JEP-Core defines signed judgment-related events and the four core event verbs Judgment, Delegation, Termination, and Verification. A JEP Delegation event records that one actor delegates task, authority, responsibility, capability, or decision context to another actor or system. However, a bare Delegation event does not by itself define the business semantics of an executable authorization, nor does it establish legal effectiveness or policy compliance.

JEP-AMP fills this gap at the profile layer. It defines an Action Mandate Descriptor and validation rules that allow a JEP Delegation event to be interpreted as a verifiable action mandate when, and only when, a specified trust profile, policy context, and relying-party validation support that interpretation.

The central question answered by this profile is:

> Can this actor perform this action on this target, under this mandate, in this context, at this time?

This document deliberately keeps JEP-Core thin. It does not attempt to create a global legal authorization system, a global payment protocol, a global identity system, a global compliance system, or a global action taxonomy. Domain-specific meaning is supplied by industry profiles, enterprise policies, credentials, attestations, contracts, laws, and external evidence systems.

2. Terminology and Conventions

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.

This document uses the following terms:

Action: An operation that a delegatee is expected, permitted, requested, or forbidden to perform on a target. Examples include creating a purchase order, requesting a refund, exporting data, submitting a claim decision, modifying a contract, or initiating a payment request.

Action Mandate: A bounded authorization statement, expressed through a JEP Delegation event and an Action Mandate Descriptor, under which a delegatee may attempt to perform one or more actions on behalf of a principal.

Action Mandate Descriptor: A JSON object defined by this profile that identifies the principal, issuer, delegatee, action, target, scope, constraints, validity interval, policy references, evidence requirements, and termination conditions of an action mandate.

Action-valid: A local conclusion by a relying party, gateway, verifier, or policy engine that a requested action is allowed under a Mandate-valid mandate and the applicable policy, trust, industry, legal, and runtime context. Action-validity is not defined globally by JEP-AMP.

Delegatee: The actor to which a mandate is delegated. A delegatee can be a human, organization, software service, model, agent, tool, workflow, or composite actor, subject to the applicable JEP trust profile.

Issuer: The actor that signs the JEP Delegation event. The issuer is represented by the JEP event's 'who' field and MUST be authorized in the relevant policy context to issue or convey the mandate.

Mandate-valid: A profile-level conclusion that a JEP Delegation event and Action Mandate Descriptor satisfy this profile, are within their stated validity interval, have not been observed as terminated, and have not failed applicable profile-level checks. Mandate-validity does not imply Action-validity.

Principal: The person, organization, account, department, tenant, legal entity, or other subject on whose behalf the action is to be performed.

Relying Party: A system, service, verifier, gateway, human reviewer, or organization that relies on an Action Mandate to decide whether to permit, deny, review, or record an action request.

Target: The object, resource, record, account, case, transaction, workflow, customer, supplier, document, or domain entity on which an action is to be performed.

Verifier: An actor or system that evaluates a JEP event, an Action Mandate Descriptor, an action request, an evidence bundle, a receipt, or a chain under a declared verification scope. A verifier can issue a JEP Verification event.

Work Unit: A business or operational unit of work, such as a purchase request, claim, contract review, refund case, data export, supplier payment, or implementation project, within which one or more mandated actions may occur.

3. Profile Identifier and Applicability

The profile identifier for this version is:

urn:jep:profile:amp:0

Implementations MAY also use the short name ‘JEP-AMP-0‘ in user interfaces, documentation, and non-normative contexts.

A JEP event conforms to this profile only when all of the following hold:

1. The event conforms to the JEP-Core event format and validation rules applicable to the declared JEP version.

2. The event’s ‘verb‘ is ‘D‘ for mandate issuance, ‘T‘ for mandate termination, ‘V‘ for mandate or action validation, or ‘J‘ for a related judgment used by the mandate lifecycle.

3. The event declares this profile in the location defined by the applicable JEP Profiles mechanism. If the JEP version in use does not define a profile declaration field, the declaration MUST appear in an extension field that is covered by the JEP signature.

4. Any critical AMP extension used by the event is declared in the JEP critical extension mechanism, if such a mechanism is available.

JEP-AMP is applicable where a relying party needs to evaluate whether an agent, human, service, or workflow may perform a bounded action on behalf of a principal. It is especially applicable to high-responsibility enterprise, commercial, legal, financial, privacy-sensitive, and audit- requiring actions.

4. Relationship to JEP-Core and Other JEP Profiles

JEP-AMP is a JEP profile. It MUST NOT redefine JEP-Core event verbs, JEP-Core signature semantics, JEP-Core event hash semantics, or JEP-Core validation-level semantics.

JEP-AMP relies on JEP-Core for the following:

* event object syntax; * event canonicalization and event hash computation; * event signature and detached signature processing; * actor declaration in ‘who‘; * timestamp, nonce, audience, and reference semantics; * extension processing; and * the base validation model.

JEP-AMP relies on JEP Profiles for profile declaration, trust profile selection, actor identifier interpretation, key resolution, credential binding, attestation rules, archival rules, and chain rules where those functions are required.

JEP-AMP is complementary to receipt and chain profiles. An Action Mandate can be referenced by an HJS-style receipt profile as the pre-action authorization context for an observed agent behavior. A mandate, its validations, its termination events, and its receipts can be arranged by a JAC-style chain profile into a declared dependency or responsibility chain.

JEP-AMP can also reference, map to, or be referenced by domain-specific mandate systems such as payment-domain mandates. Such mappings are informative unless a domain profile makes them normative.

This document is intended to align with the JEP v0.6 draft set. It does not change the JEP-Core narrow-waist semantics. It defines an optional action-mandate profile over JEP Delegation events and leaves legal, regulatory, organizational, and domain-specific action validity to profiles, policies, trust contexts, and external evidence systems.

5. Design Goals and Non-Goals

JEP-AMP has the following goals:

* define a minimal interoperable descriptor for action mandates;
* preserve the thin-core design of JEP;
* allow a JEP Delegation event to express a bounded action mandate;
* distinguish event validity, mandate validity, and local action validity;
* support pre-action authorization, policy validation, termination, receipt binding, and audit export;
* support cross-domain use without forcing a single identity, credential, policy, payment, or legal system; and
* enable domain-specific profiles to refine action, target, evidence, approval, receipt, and settlement semantics.

JEP-AMP has the following non-goals:

* define global legal authorization validity; * assign legal liability or moral responsibility; * determine global regulatory compliance; * define a global identity system, credential system, or trust framework; * define a global action taxonomy for all industries; * define payment clearing, settlement, or funds movement; * replace domain-specific protocols such as payment mandates; * prove that an external-world action physically occurred; * prove that an AI model understood a user request; or * make a JEP Delegation event automatically executable in every context.

A conforming implementation MUST preserve the distinction between a profile-valid mandate and a locally permitted action.

6. The Action Mandate Descriptor

The Action Mandate Descriptor is the profile-defined semantic object that turns a JEP Delegation event into a candidate action mandate. It is a JSON object carried inline in the JEP event's 'what' field or referenced by digest and URI from the JEP event's 'what' and 'ref' fields.

The descriptor MUST be covered by the JEP event signature. If the full descriptor is not inline, the event MUST include a digest over a canonical representation of the descriptor, and the digest MUST be verified before relying on the mandate.

The descriptor has the following top-level members:

profile: REQUIRED. The profile identifier, 'urn:jep:profile:amp:0'.

mandate_id: REQUIRED. A globally unique identifier for the mandate. A URI or URN is RECOMMENDED. A relying party MAY also use the JEP event hash of the issuance event as the operational mandate identifier.

principal: REQUIRED. The subject on whose behalf the action is to be performed.

issuer: OPTIONAL. The actor issuing the mandate. If omitted, the JEP event's 'who' actor is the issuer. If present, it MUST be consistent with the JEP event's 'who' field under the applicable trust profile.

delegatee: REQUIRED. The actor to which action authority is delegated.

action: REQUIRED. A structured description of the action or class of actions authorized by the mandate.

target: REQUIRED. The resource, record, domain object, workflow, case, transaction, or other target on which the action may be performed.

scope: OPTIONAL. Human-readable and machine-readable boundaries for the purpose, objective, work unit, or business context of the mandate.

constraints: OPTIONAL. Constraints such as amount limits, data boundaries, time windows, geography, resource classes, vendor sets, customer sets, risk classes, approval thresholds, or usage limits.

validity: REQUIRED. A validity interval containing at least ‘not_before‘ or ‘expires_at‘. A mandate without an expiry MUST be treated as high risk and SHOULD be rejected unless a domain profile permits it.

policy_ref: OPTIONAL. References to policies, contracts, terms, enterprise rules, industry profiles, regulatory mappings, or other policy sources used to evaluate the mandate.

evidence_required: OPTIONAL. Evidence types that are expected before, during, or after execution. Examples include quotes, approvals, invoices, external attestations, human reviews, logs, receipts, and evidence bundle references.

approval: OPTIONAL. Rules or references for human or system approval. If an approval has already occurred, the approval SHOULD be referenced by a JEP Judgment or Verification event, credential, or external evidence object.

delegation: OPTIONAL. Subdelegation controls. If omitted, subdelegation MUST be treated as not allowed.

termination_conditions: OPTIONAL. Conditions under which the mandate is revoked, consumed, superseded, expired, completed, or otherwise terminated.

receipt: OPTIONAL. Expected receipt profile, evidence bundle, or post-execution record requirements.

extensions: OPTIONAL. Profile-specific extension object. Critical extensions MUST be declared using the JEP critical extension mechanism when such a mechanism is available.

A minimal descriptor is shown below:

```
{
  "profile": "urn:jep:profile:amp:0",
  "mandate_id": "urn:uuid:0d1c0c28-8a7a-4a69-8d73-0d9c8b3e1a00",
  "principal": { "id": "did:example:acme", "type": "organization" },
  "delegatee": { "id": "did:example:agent:procure-7", "type": "agent" },
  "action": { "type": "urn:example:action:procurement.purchase" },
  "target": { "type": "procurement_request", "id": "req-123" },
  "validity": {
    "not_before": "2026-05-17T00:00:00Z",
    "expires_at": "2026-05-19T00:00:00Z"
  },
  "constraints": { "amount": { "currency": "USD", "max": 5000 } },
  "policy_ref": [ { "uri": "urn:policy:acme:procurement:v3" } ],
  "evidence_required": [ { "type": "quote_set", "min_count": 3 } ],
  "delegation": {
    "subdelegation_allowed": false,
    "max_depth": 0,
    "scope_may_expand": false
  }
}
```

7. Mandate Issuance Using a JEP Delegation Event

A JEP-AMP mandate is issued by a JEP Delegation event.

The issuing event:

* MUST have ‘verb‘ equal to ‘D‘;
* MUST be signed according to JEP-Core;
* MUST declare the JEP-AMP profile;
* MUST carry or reference an Action Mandate Descriptor;
* MUST identify the issuer in ‘who‘;
* SHOULD identify expected relying parties in ‘aud‘ when the mandate is intended for a bounded audience;
* SHOULD reference credentials, policies, approvals, work units, or other supporting context in ‘ref‘; and
* MUST NOT state or imply that JEP-AMP alone establishes global legal authorization validity.

A relying party MUST NOT treat a JEP Delegation event as an Action Mandate unless the event conforms to this profile.

If both a descriptor and summary fields appear in JEP extensions, the descriptor is authoritative. Summary fields in extensions are only routing, indexing, or preflight hints. If an extension summary conflicts with the descriptor, the event MUST be rejected as an invalid AMP event.

8. Mandate Lifecycle

A mandate lifecycle can include issuance, validation, execution, receipt, termination, and audit.

Issuance: A JEP Delegation event creates the mandate by carrying or referencing an Action Mandate Descriptor.

Validation: A relying party, gateway, verifier, or policy engine evaluates whether the mandate is Event-valid, Mandate-valid, and, in the local context, Action-valid. A verifier MAY issue a JEP Verification event recording the scope and result of validation.

Execution: A delegatee or downstream actor attempts to perform an action. JEP-AMP does not define tool-calling or execution semantics; it defines the authorization context under which execution may be attempted.

Receipt: After execution, an HJS-style receipt or other evidence object MAY reference the mandate issuance event, mandate descriptor, relevant validations, judgments, and termination events.

Termination: A JEP Termination event MAY revoke, expire, consume, replace, or terminate the mandate. A mandate MUST NOT be relied upon after a valid termination event has been observed in the relying party’s applicable trust and archival context.

Audit: A verifier, auditor, regulator, insurer, or relying party MAY review the issuance, validation, execution, receipt, and termination chain. Such review MAY be recorded by a JEP Verification event.

9. Mandate Termination

A mandate can be terminated by expiry, explicit revocation, successful consumption, replacement, policy change, credential revocation, completion of the work unit, violation of constraints, or other termination conditions declared by the descriptor or domain profile.

An explicit termination event:

* MUST have ‘verb‘ equal to ‘T‘;
* MUST reference the mandate issuance event or mandate identifier;
* SHOULD identify the termination reason;
* SHOULD identify the actor terminating the mandate in ‘who‘;
* MUST be signed and validated under the applicable JEP trust profile; and
* MUST be interpreted only within the visibility and archival context in which it is observed.

Domain profiles MAY define stronger termination propagation rules. For example, a profile can specify that termination of a parent mandate also terminates all child mandates derived from it, unless the child mandate was independently re-authorized.

10. Mandate Validation and Verification Events

A JEP Verification event can record validation of a mandate, an action request, a policy check, an approval, a receipt, an evidence bundle, or a mandate chain.

A JEP-AMP Verification event:

* MUST have ‘verb‘ equal to ‘V‘;
* MUST reference the mandate issuance event or mandate identifier;
* MUST declare a verification scope;
* MUST distinguish cryptographic validity from actor binding, mandate validity, policy compliance, human review, external evidence review, and action validity;
* SHOULD include a structured validation result; and
* MUST NOT imply validation beyond its declared scope.

Recommended AMP verification scopes include:

amp_descriptor_schema: The descriptor conforms to this profile’s schema.

amp_descriptor_digest: A detached descriptor digest matches the descriptor used for validation.

amp_issuer_authority: The issuer is authorized, under the applicable trust and policy context, to issue the mandate.

amp_delegatee_match: The actor requesting the action matches the delegatee or a valid delegated chain.

amp_time_validity: The action request occurs within the mandate validity interval.

amp_termination_status: No applicable termination event has been observed, or a termination event has been observed and the mandate is no longer valid.

amp_scope_match: The requested action and target fit within the mandate scope and constraints.

amp_policy_compliance: The action request satisfies one or more referenced policies.

amp_human_review: A human review or approval occurred within the stated scope.

amp_receipt_validation: A post-action receipt or evidence bundle was reviewed under the stated scope.

The following result values are RECOMMENDED: ‘pass‘, ‘fail‘, ‘conditional‘, ‘indeterminate‘, and ‘not_applicable‘.

11. Validation Model

JEP-AMP distinguishes three forms of validity.

Event-valid: The JEP event is syntactically, cryptographically, and structurally valid under JEP-Core and the applicable JEP trust profile.

Mandate-valid: The Event-valid JEP Delegation event and its Action Mandate Descriptor conform to this profile, are within their validity interval, have not been observed as terminated in the applicable context, and satisfy profile-level checks.

Action-valid: The requested action is allowed under the Mandate-valid mandate and the local relying-party context, including enterprise policy, industry profile, domain policy, legal requirements, credential status, approval state, evidence state, and runtime risk.

JEP-AMP defines Event-valid and Mandate-valid checks. Action-validity is local and domain-specific.

A conforming validator SHOULD perform the following checks:

1. Validate the JEP event under JEP-Core.

2. Confirm that the event declares ‘urn:jep:profile:amp:0‘.

3. Confirm that the event verb is appropriate for the operation being validated.

4. Parse and validate the Action Mandate Descriptor.

5. If the descriptor is detached, canonicalize and hash the descriptor and verify that the digest matches the signed JEP event.

6. Check that descriptor summary fields, if any, do not conflict with authoritative descriptor fields.

7. Resolve the issuer, principal, delegatee, and relevant credentials under the applicable trust profile.

8. Check that the issuer has authority to issue or convey the mandate, if such policy information is available.

9. Check the mandate validity interval.

10. Check audience restrictions, if any.

11. Check observed termination events relevant to the mandate.

12. Check that the action-requesting actor matches the delegatee or a valid subdelegation chain.

13. Check that the requested action, target, amount, data boundary, purpose, resource, and other requested parameters are within scope.

14. Check subdelegation controls. Subdelegation MUST NOT expand scope unless a domain profile explicitly permits scope expansion.

15. Apply policy, approval, evidence, and risk checks required by the relying party.

16. If the mandate is single-use or consumable, perform a reservation or consumption procedure that prevents concurrent double use.

17. Return a structured result identifying which checks passed, failed, were conditional, or were indeterminate.

A validator MUST NOT report an action as allowed solely because a JEP signature is valid. Cryptographic validity is not policy validity.

12. Subdelegation and Delegation Chains

Subdelegation is not allowed unless the descriptor or a domain profile explicitly permits it.

If subdelegation is allowed, the descriptor SHOULD specify:

* whether subdelegation is permitted; * maximum delegation depth; * whether the child mandate can narrow, but not expand, scope; * whether the child mandate inherits evidence requirements; * whether the child mandate must reference the parent mandate; * whether parent termination terminates the child mandate; and * whether the child delegatee must accept the mandate.

A child mandate MUST NOT grant more authority than the parent mandate unless a domain profile explicitly permits expansion and the relying party accepts that expansion. In the absence of a domain rule, scope may only be preserved or narrowed.

When validating a chain, a verifier SHOULD evaluate each parent mandate, termination status, scope relationship, time interval, issuer authority, and policy context. A JAC-style profile MAY be used to declare and transport the dependency chain, but this document does not require a specific chain format.

13. Receipt and Evidence Binding

JEP-AMP is primarily a pre-action authorization profile. Post-action behavior, evidence, and accountability receipts are expected to be represented by a receipt profile such as HJS or another domain-specific receipt mechanism.

A receipt that relies on a JEP-AMP mandate SHOULD reference:

* the JEP Delegation issuance event; * the Action Mandate Descriptor or its digest; * relevant Verification events; * relevant Judgment events, including approvals or risk determinations; * relevant Termination events; * the action actually performed; * evidence objects or evidence digests; * the acting delegatee; * the execution time or interval; and * the work unit, transaction, case, or workflow context.

A receipt MUST NOT imply that all policy, legal, or factual requirements were satisfied unless it contains or references a Verification event or other evidence supporting that claim within a declared verification scope.

14. Interaction with Domain Mandates and Payment Protocols

JEP-AMP is cross-domain. It can represent action authorization in procurement, contract, refund, claim, data export, payment-adjacent, and other workflows. It does not replace domain protocols.

In a payment or commerce domain, a domain-specific mandate protocol can carry stronger semantics than JEP-AMP, such as cart formation, checkout, payment authorization, charge authorization, settlement, or dispute handling. JEP-AMP can reference such a domain mandate as evidence, policy context, or action target, or can be referenced by it as a broader action authorization context.

A domain profile MAY define a mapping between a JEP-AMP mandate and a domain mandate. Such a mapping MUST state which fields are authoritative for domain execution, which validation scopes are required, and whether receipt evidence must be produced by the domain protocol, JEP/HJS, or both.

15. Privacy Considerations

Action mandates can reveal sensitive relationships, business intent, commercial plans, customer data, transaction details, employee authority, enterprise policy, and risk posture. Implementations SHOULD minimize the amount of sensitive information embedded directly in JEP events.

Where possible, sensitive evidence SHOULD be referenced by digest, capability, encrypted reference, or selective-disclosure credential rather than embedded inline. Audience restrictions SHOULD be used for mandates that are intended only for specific relying parties. Domain profiles SHOULD define retention, redaction, archival, and selective- disclosure rules.

A public or semi-public mandate registry can leak commercial activity, internal authority structures, or business relationships. Implementers SHOULD evaluate whether mandates and receipts are stored in private, consortium, enterprise, encrypted, or public archival systems.

A Verification event that records human review, policy compliance, external evidence review, or factual-claim review SHOULD disclose only the minimum information needed to support its verification scope.

16. Security Considerations

JEP-AMP introduces authorization semantics and therefore requires careful security treatment.

Replay: Attackers can attempt to reuse a valid mandate. Implementations MUST respect nonce, audience, validity interval, termination status, and usage constraints. Single-use mandates require reservation or consumption mechanisms that prevent concurrent double use.

Confused Deputy: A delegatee can be tricked into using a mandate for a different target, action, or relying party. Validators MUST check the requested action, target, audience, scope, and policy context against the descriptor.

Overbroad Mandates: Broad actions or vague targets increase risk. Profiles SHOULD encourage narrow, purpose-bound, time-bound, target-bound mandates.

Descriptor Substitution: If a descriptor is detached, attackers can substitute a different descriptor. Validators MUST verify descriptor digests and MUST reject mismatches.

Extension Mismatch: Extension summary fields can conflict with the authoritative descriptor. Validators MUST reject such conflicts.

Policy Downgrade: Attackers can attempt to present cryptographic validity as policy validity. Validators MUST report verification scope and MUST NOT conflate signature validation with authorization or policy compliance.

Revocation Lag: A relying party might not observe a termination event in time. Profiles SHOULD specify archival, synchronization, freshness, and revocation-check requirements appropriate to the risk level.

Subdelegation Expansion: A child mandate can attempt to expand scope. Validators MUST reject expansion unless a domain profile permits it and the relying party accepts the profile.

Credential Expiry: Issuer, principal, or delegatee credentials may expire or be revoked after issuance. Profiles SHOULD state whether validation uses issuance-time, action-time, or verification-time credential status.

Prompt Injection and Tool Abuse: AI agents can be induced to act outside mandate scope. Gateways SHOULD validate every high-responsibility action request against the mandate and not rely solely on agent self-reporting.

Evidence Poisoning: Evidence referenced by a mandate or receipt can be false, incomplete, or malicious. JEP-AMP does not prove external factual truth. External evidence review requires explicit Verification events and domain-specific evidence policy.

17. IANA Considerations

This document requests no IANA actions.

If a JEP Profile Registry is created by another document, this document requests registration of:

```
Profile name:  JEP-AMP-0
Profile URI:   urn:jep:profile:amp:0
Description:   JEP Action Mandate Profile, version 0
Reference:     This document
```

If a JEP validation-scope registry is created, this document requests registration of the AMP verification scopes listed in Section 10.

If a JEP failure-code registry is created, this document requests registration of the failure codes listed in Appendix D.

18. References

[JEP] Y., W., "Judgment Event Protocol (JEP)", draft-wang-jep-judgment-event-protocol-06, 2026.

[JEP-PROFILES] Y., W., "JEP Profiles and Interoperability", draft-wang-jep-profiles-00, 2026.

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

[RFC8174] B., L., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", RFC 8174, 2017.

[HJS] Y., W., "HJS: Accountability Receipts for AI Agents", draft-wang-hjs-accountability-05, 2026.

[JAC] Y., W., "JAC: Declared Dependency Chains for Agent Receipts", draft-wang-jac-02, 2026.

[AP2-AUTH] contributors, G. A., "Agent Authorization Framework", Agentic Payment Protocol documentation, 2025.

[AP2-SPEC] contributors, G. A., "Agentic Payment Protocol v0.2 Core Specification", Agentic Payment Protocol documentation, 2025.

Appendix A. Enterprise Procurement Mandate

Field names follow the JEP event model assumed by this profile. This example includes the JEP version field and uses a Unix-second event timestamp.

```
{
  "jep": "1",
  "verb": "D",
  "who": "did:example:acme:employee:alice",
  "when": 1779008400,
  "aud": [
    "did:example:acme:procurement-gateway"
  ],
  "nonce": "a3d3b4e0-8902-4d71-a090-3e9e8e850aaa",
  "what": {
    "type": "amp.action_mandate",
    "descriptor": {
      "profile": "urn:jep:profile:amp:0",
      "mandate_id": "urn:uuid:21c7a4ea-37ef-4b0c-9c33-8b2f0a7a1c10",
      "principal": {
        "id": "did:example:acme",
        "type": "organization"
      },
      "issuer": {
        "id": "did:example:acme:employee:alice",
        "role": "requester"
      },
      "delegatee": {
        "id": "did:example:agent:procure-7",
        "type": "agent"
      },
      "action": {
        "type": "urn:example:action:procurement.purchase"
      },
      "target": {
        "type": "category",
        "id": "office.monitor"
      },
      "scope": {
        "work_unit": "purchase_request:PR-2026-0007",
        "purpose": "purchase 20 monitors for marketing team"
      },
      "constraints": {
        "amount": {
          "currency": "USD",
          "max": 30000
        },
        "vendor": {
          "allow_list_ref": "urn:vendor-list:acme:approved:v4"
        },
        "data": {
          "allow_customer_pii": false
        }
```

```
  },
  "validity": {
    "not_before": "2026-05-17T09:00:00Z",
    "expires_at": "2026-05-19T09:00:00Z"
  },
  "policy_ref": [
    {
      "uri": "urn:policy:acme:procurement:v3"
    }
  ],
  "approval": {
    "rules": [
      {
        "if": "amount > 10000",
        "requires": "manager_approval"
      }
    ]
  },
  "evidence_required": [
    {
      "type": "quote_set",
      "min_count": 3
    },
    {
      "type": "approval_record",
      "when": "if_required"
    },
    {
      "type": "invoice",
      "when": "post_action"
    }
  ],
  "delegation": {
    "subdelegation_allowed": false,
    "max_depth": 0,
    "scope_may_expand": false
  },
  "termination_conditions": [
    {
      "type": "expiry"
    },
    {
      "type": "successful_consumption"
    },
    {
      "type": "explicit_revocation"
    }
  ],
```

```
        "receipt": {
          "expected_profile": "urn:jep:profile:hjs:receipt",
          "required": true
        }
      }
    },
    "ref": [
      {
        "type": "policy",
        "uri": "urn:policy:acme:procurement:v3"
      },
      {
        "type": "work_unit",
        "uri": "urn:work-unit:acme:purchase_request:PR-2026-0007"
      }
    ],
    "ext": {
      "profile": [
        "urn:jep:profile:amp:0"
      ]
    },
    "sig": "..."
  }
```

A procurement gateway can then issue a JEP Verification event declaring that it checked ‘amp_descriptor_schema‘, ‘amp_time_validity‘, ‘amp_delegatee_match‘, ‘amp_scope_match‘, and ‘amp_policy_compliance‘. After execution, an HJS-style receipt can reference the mandate event and the evidence objects.

Appendix B. Validation Result Object

The following non-normative validation result can be embedded in a JEP Verification event or returned by a gateway API. The API itself is not specified by this document.

```
{
  "profile": "urn:jep:profile:amp:0",
  "mandate_id": "urn:uuid:21c7a4ea-37ef-4b0c-9c33-8b2f0a7a1c10",
  "result": "conditional",
  "checks": [
    {
      "scope": "syntax",
      "result": "pass"
    },
    {
      "scope": "cryptographic",
      "result": "pass"
```

```
      },
      {
        "scope": "actor_binding",
        "result": "pass"
      },
      {
        "scope": "amp_descriptor_schema",
        "result": "pass"
      },
      {
        "scope": "amp_time_validity",
        "result": "pass"
      },
      {
        "scope": "amp_delegatee_match",
        "result": "pass"
      },
      {
        "scope": "amp_scope_match",
        "result": "pass"
      },
      {
        "scope": "amp_policy_compliance",
        "result": "conditional",
        "reason": "manager_approval_required"
      }
    ],
    "required_next_events": [
      {
        "verb": "J",
        "purpose": "manager_approval"
      },
      {
        "verb": "V",
        "scope": "human_review"
      }
    ]
  }
```

Appendix C. Action Mandate Descriptor JSON Schema

The following schema is non-normative. It is intended to assist implementers. Domain profiles can define stricter schemas.

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "$id": "urn:jep:profile:amp:0:schema:mandate-descriptor",
  "title": "JEP-AMP Action Mandate Descriptor",
  "type": "object",
  "required": [
    "profile",
    "mandate_id",
    "principal",
    "delegatee",
    "action",
    "target",
    "validity"
  ],
  "additionalProperties": false,
  "properties": {
    "profile": {
      "const": "urn:jep:profile:amp:0"
    },
    "mandate_id": {
      "type": "string",
      "minLength": 1
    },
    "principal": {
      "$ref": "#/$defs/actor"
    },
    "issuer": {
      "$ref": "#/$defs/actor"
    },
    "delegatee": {
      "$ref": "#/$defs/actor"
    },
    "action": {
      "$ref": "#/$defs/action"
    },
    "target": {
      "$ref": "#/$defs/target"
    },
    "scope": {
      "type": "object",
      "additionalProperties": true
    },
    "constraints": {
      "type": "object",
      "additionalProperties": true
    },
    "validity": {
      "$ref": "#/$defs/validity"
```

```
      },
      "policy_ref": {
        "type": "array",
        "items": {
          "$ref": "#/$defs/ref"
        }
      },
      "evidence_required": {
        "type": "array",
        "items": {
          "type": "object",
          "additionalProperties": true
        }
      },
      "approval": {
        "type": "object",
        "additionalProperties": true
      },
      "delegation": {
        "$ref": "#/$defs/delegation"
      },
      "termination_conditions": {
        "type": "array",
        "items": {
          "type": "object",
          "additionalProperties": true
        }
      },
      "receipt": {
        "type": "object",
        "additionalProperties": true
      },
      "extensions": {
        "type": "object",
        "additionalProperties": true
      }
    },
    "$defs": {
      "actor": {
        "type": "object",
        "required": [
          "id"
        ],
        "additionalProperties": true,
        "properties": {
          "id": {
            "type": "string",
            "minLength": 1
```

```
        },
        "type": {
          "type": "string"
        },
        "role": {
          "type": "string"
        }
      }
    },
    "action": {
      "type": "object",
      "required": [
        "type"
      ],
      "additionalProperties": true,
      "properties": {
        "type": {
          "type": "string",
          "minLength": 1
        },
        "profile": {
          "type": "string"
        },
        "version": {
          "type": "string"
        }
      }
    },
    "target": {
      "type": "object",
      "required": [
        "type"
      ],
      "additionalProperties": true,
      "properties": {
        "type": {
          "type": "string",
          "minLength": 1
        },
        "id": {
          "type": "string"
        },
        "uri": {
          "type": "string"
        }
      }
    },
    "validity": {
```

```
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "not_before": {
          "type": "string",
          "format": "date-time"
        },
        "expires_at": {
          "type": "string",
          "format": "date-time"
        }
      },
      "anyOf": [
        {
          "required": [
            "not_before"
          ]
        },
        {
          "required": [
            "expires_at"
          ]
        }
      ]
    },
    "ref": {
      "type": "object",
      "required": [
        "uri"
      ],
      "additionalProperties": true,
      "properties": {
        "uri": {
          "type": "string"
        },
        "digest": {
          "type": "string"
        },
        "type": {
          "type": "string"
        }
      }
    },
    "delegation": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "subdelegation_allowed": {
```

```
            "type": "boolean",
            "default": false
          },
          "max_depth": {
            "type": "integer",
            "minimum": 0,
            "default": 0
          },
          "scope_may_expand": {
            "type": "boolean",
            "default": false
          }
        }
      }
    }
  }
```

Appendix D. Recommended Failure Codes

The following failure codes are non-normative unless registered by a future JEP registry or required by a domain profile:

amp_profile_missing: The event does not declare the JEP-AMP profile.

amp_wrong_verb: The event verb is not appropriate for the AMP operation.

amp_descriptor_missing: No descriptor or descriptor reference is found.

amp_descriptor_schema_invalid: The descriptor fails schema validation.

amp_descriptor_digest_mismatch: A detached descriptor digest does not match.

amp_extension_conflict: A summary extension conflicts with the descriptor.

amp_issuer_not_authorized: The issuer is not authorized under the applicable trust or policy context.

amp_delegatee_mismatch: The actor requesting the action does not match the delegatee or a valid delegation chain.

amp_not_yet_valid: The mandate is not yet valid.

amp_expired: The mandate has expired.

amp_terminated: A relevant termination event has been observed.

amp_audience_mismatch: The relying party is outside the mandate audience.

amp_action_out_of_scope: The requested action is outside mandate scope.

amp_target_out_of_scope: The requested target is outside mandate scope.

amp_constraints_failed: One or more constraints are not satisfied.

amp_policy_failed: Policy validation failed.

amp_policy_indeterminate: The relying party cannot determine policy compliance.

amp_approval_required: Human or system approval is required.

amp_evidence_missing: Required evidence is missing.

amp_subdelegation_not_allowed: The mandate chain includes an unauthorized subdelegation.

amp_subdelegation_scope_expanded: A child mandate expands scope without permission.

amp_single_use_already_consumed: A consumable mandate has already been used.

amp_validation_scope_downgrade: A validation result attempts to report a broader conclusion than its declared scope supports.

Appendix E. Open Issues for -00

This -00 draft intentionally leaves several issues open for implementer feedback:

1. Whether ‘mandate_id‘ should be mandatory when the JEP event hash can serve as the stable identifier.

2. Whether a compact inline form should be defined for very small mandates.

3. Whether AMP should define a registry for action type namespaces or leave all action taxonomies to domain profiles.

4. Whether single-use consumption should require a dedicated reservation event, or whether a Termination event is sufficient for low-risk domains.

5. Whether child mandates should be represented only as independent JEP Delegation events or whether a special child-mandate extension is needed.

6. Whether receipt binding should be purely informative or mandatory for high-risk profiles.

7. Whether a machine-readable policy language should be profiled or whether AMP should continue to reference external policy systems.

Appendix F. Acknowledgements

This document is part of the JEP profile family and is intended as a companion profile to JEP-Core, JEP Profiles, HJS, and JAC.

The profile design reflects the layered approach of JEP-Core, JEP Profiles, HJS, and JAC: thin event core, profile-defined semantics, receipt-layer evidence, and chain-layer dependency declarations.

Author’s Address

Yuqiang Wang
Independent
Email: signal@humanjudgment.org
URI: https://github.com/hjs-spec