Independent
Internet-Draft
Intended status: Experimental
Expires: 19 November 2026

Y. Wang
Independent

18 May 2026

JEP Action Mandate Profile (JEP-AMP)
draft-wang-jep-action-mandate-profile-01

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, payment clearing, or global authorization validity. JEP-AMP defines the minimum interoperable shape of an Action Mandate Descriptor and profile-level 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, profile, and relying-party context.

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 19 November 2026.

Copyright Notice

Table of Contents

1. Introduction

AI agents, delegated workflows, and autonomous software systems are 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 target, during which validity interval, 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 profile semantics of an executable authorization, nor does it establish legal effectiveness, policy compliance, or local action permission.

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, domain profile, 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 create a global legal authorization system, a global payment protocol, a global identity system, a global compliance system, a global policy language, 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.

Action

An operation that a delegatee is expected, permitted, requested, or forbidden to perform on a target. JEP-AMP does not define a global action taxonomy.

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, termination conditions, and optional operational context 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, runtime, and relying-party 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.

Event-valid
: A conclusion that a JEP event is syntactically, cryptographically, and structurally valid under JEP-Core and 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, have not been consumed beyond permitted usage, 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, reserve, consume, 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
: An optional 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. JEP-AMP treats work units as contextual references, not as globally defined business objects.

3. Profile Identifier and Applicability

The profile identifier for this version is:

urn:jep:profile:amp:1

Implementations MAY also use the short name ‘JEP-AMP-1‘ in user interfaces, documentation, and non-normative contexts.

The profile identifier is a semantic profile identifier, not merely an Internet-Draft revision number. Future revisions of this document that do not change on-wire semantics, descriptor requirements, validation requirements, failure semantics, or critical extension processing SHOULD retain this profile identifier. A future revision that changes those requirements in a non-compatible way SHOULD allocate a new profile identifier.

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

1. The event conforms to 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 a signed extension field.

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 cross-domain and does not replace domain-specific mandate, payment, legal, workflow, identity, or compliance protocols.

4. Interoperability Posture and Profile Capability Declaration

JEP-AMP is intended to minimize cross-system interpretation cost for bounded delegated actions. It does this by standardizing the shape of an Action Mandate Descriptor while leaving transport, identity, credential, policy, receipt, chain, payment, and domain execution semantics to JEP profiles, domain profiles, and local relying-party policy.

A system that supports JEP-AMP SHOULD be able to declare its AMP-related capabilities. Such a declaration can be used during integration, conformance testing, gateway configuration, or profile negotiation. This document does not mandate a discovery protocol, but the following fields are RECOMMENDED for a capability declaration:

```
{
  "jep_versions": ["0.6"],
  "profiles_supported": ["urn:jep:profile:amp:1"],
  "roles_supported": [
    "mandate_producer",
    "mandate_verifier",
    "gateway_validator"
  ],
  "validation_modes": ["acceptance", "archival"],
  "max_validation_level": 4,
  "receipt_profiles_supported": ["urn:jep:profile:hjs:*"],
  "chain_profiles_supported": ["urn:jep:profile:jac:*"],
  "external_mappings_supported": [
    "payment-domain-mandate",
    "general-event-envelope",
    "credential-reference",
    "trace-context"
  ]
}
```

A capability declaration is descriptive. It does not by itself prove that a system is conformant, authorized, certified, regulated, or legally competent to rely on an AMP mandate. Conformance claims SHOULD be backed by test vectors, validator output, or a domain profile’s conformance requirements.

JEP-AMP implementations SHOULD fail safely when a required profile, critical extension, trust profile, receipt profile, or domain mapping is not supported. An implementation MAY degrade to a lower validation level only when the relying party explicitly permits such degradation and the validation result states the reduced scope.

5. 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 event object syntax, canonicalization, event hash computation, signature processing, actor declaration in ‘who‘, timestamp, nonce, audience, 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 or another domain-specific receipt mechanism as pre-action authorization context for an observed behavior. A mandate, its validations, its termination events, and its receipts can be arranged by a JAC-style chain profile or another dependency-chain mechanism into a declared dependency or responsibility chain.

JEP-AMP can 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.

6. External Mapping Principles

JEP-AMP is not a transport protocol, event-delivery protocol, identity protocol, credential protocol, tracing protocol, payment protocol, or receipt protocol. Instead, it defines the action-mandate semantics that can be carried, referenced, mapped, or verified by such systems.

A domain or deployment profile MAY define mappings between AMP mandates and external systems. A mapping profile SHOULD state:

* which external object is being mapped, such as a payment-domain mandate, enterprise approval record, capability token, credential, trace span, general event envelope, receipt, or audit record;

* which fields are authoritative for the external domain;

* which AMP fields provide cross-domain accountability context;

* which validation scopes are required;

* whether the mapping is lossless, lossy, advisory, or evidentiary;

* whether receipts are generated by JEP/HJS, the external domain system, another receipt profile, or more than one mechanism; and

* which system controls execution, settlement, funds movement, access enforcement, or domain-specific authority.

External mappings MUST NOT imply that JEP-AMP has replaced the external domain protocol. For example, a payment-domain mandate MAY be referenced by an AMP mandate, or an AMP mandate MAY be referenced by a payment-domain mandate, but JEP-AMP does not define payment clearing, settlement, charge authorization, or funds movement. Similarly, a general event envelope can carry a JEP event, but the envelope does not by itself provide AMP mandate semantics.

A mapping profile SHOULD also state how errors and validation failures in one system are represented in the other. A relying party MUST NOT treat successful validation of an external envelope, credential, or trace object as Mandate-validity unless the mapping profile explicitly defines that relationship and the AMP validation checks are satisfied.

7. 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, reservation, consumption, termination, receipt binding, and audit export;
* support cross-domain use without forcing a single identity, credential, policy, payment, legal, or runtime system; and
* enable domain-specific profiles to refine action, target, evidence, approval, receipt, settlement, and work-unit 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 policy language;
* 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.

8. 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.

8.1. Descriptor Fields

The descriptor has the following top-level members:

profile
: REQUIRED. The profile identifier, 'urn:jep:profile:amp:1'.

mandate_id
: OPTIONAL. A profile-level application identifier for the mandate. If present, it MUST be covered by the JEP signature. Every AMP mandate is also canonically referable by the JEP event hash of its issuance event. If 'mandate_id' is absent, the operational mandate identifier MUST be derived from the issuance event hash. If 'mandate_id' is present, relying parties SHOULD retain both the explicit identifier and the issuance-event hash, and SHOULD use the issuance-event hash for cross-system termination, reservation, consumption, receipt binding, and chain references unless a domain profile defines a stronger binding rule.

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. The 'action.type' field MUST be a URI, URN, or profile-qualified identifier. Bare action labels such as 'purchase', 'refund', or 'approve_claim' MUST NOT be used as globally interpretable action identifiers. If an action identifier is profile-qualified rather than globally URI/URN scoped, the action object SHOULD include 'action.profile' and, where useful, 'action.version' or 'action.semantics_ref'. JEP-AMP does not define global action semantics.

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 operational 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. JEP-AMP does not define a universal policy language.

evidence_required
OPTIONAL. Evidence types that are expected before, during, or after execution.

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.

work_unit_ref, case_ref, workflow_ref, transaction_ref
: OPTIONAL. Contextual references that identify business or operational units related to the mandate. JEP-AMP does not define the global semantics of these references.

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

8.2. Minimal Descriptor Example

```
{
  "profile": "urn:jep:profile:amp:1",
  "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:procurement:action:purchase",
    "profile": "urn:example:profile:procurement:0"
  },
  "target": { "type": "procurement_request", "id": "req-123" },
  "validity": {
    "not_before": "2026-05-18T00:00:00Z",
    "expires_at": "2026-05-20T00:00:00Z"
  },
  "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,
    "constraints_may_relax": false
  },
  "work_unit_ref": { "type": "purchase_request", "id": "req-123" }
}
```

The use of DID identifiers in this example is illustrative only. Other trust profiles, including X.509, OAuth/OIDC, local IAM, or other actor identifier systems, can be used.

9. 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, domain mandates, 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. A validator MUST NOT make an allow/deny decision from extension summary fields alone. A validator MUST also verify that any external mapping or profile capability claim required for local Action-validity is supported by the relying party or has been explicitly delegated to a trusted verifier.

10. Mandate Lifecycle

A mandate lifecycle can include issuance, validation, reservation, execution, receipt, consumption, 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.

Reservation: A relying party MAY reserve a single-use or consumable mandate before execution. High-risk profiles SHOULD define a reservation mechanism that prevents concurrent double use.

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 domain-specific receipt or evidence object MAY reference the mandate issuance event, mandate descriptor, relevant validations, judgments, and termination events.

Consumption: A mandate can be marked consumed when a permitted use has completed. Consumption SHOULD be recorded by a JEP Termination event or by a domain profile-defined consumption record covered by a JEP event.

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, reservation, execution, receipt, consumption, and termination chain. Such review MAY be recorded by a JEP Verification event.

11. Mandate Termination and Consumption

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, mandate identifier, or derived event-hash 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.

For low-risk mandates, a JEP Termination event MAY be sufficient to record successful consumption. For high-risk single-use or consumable mandates, a domain profile SHOULD define reservation and consumption rules that prevent concurrent double use. A Termination event alone MAY be insufficient to prevent concurrent consumption when multiple gateways can observe and act on the same mandate simultaneously.

A reservation record SHOULD identify the mandate issuance-event hash, the reserving actor, the requested action, the target, an action request digest, a reservation time, an optional reservation expiry, and the reservation result. A reservation result MAY be recorded by a JEP Verification event with scope ‘amp_reservation_status‘ or by a domain profile-defined record that is covered by, or referenced from, a JEP event.

A consumption record SHOULD identify the mandate issuance-event hash, the receipt reference or evidence reference that supports consumption, the consuming actor, the consumption time, and the consumed use count or terminal reason. Consumption MAY be represented by a JEP Termination event with a reason such as ‘consumed‘, or by a domain profile-defined record that is later referenced by a Termination or Verification event.

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.

12. 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, mandate identifier, or derived event-hash identifier;
* MUST declare a verification scope;
* MUST distinguish cryptographic validity from actor binding, mandate validity, policy compliance, human review, external evidence review, receipt validation, 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‘
* ‘amp_descriptor_digest‘

* ‘amp_issuer_authority‘

* ‘amp_delegatee_match‘

* ‘amp_time_validity‘

* ‘amp_termination_status‘

* ‘amp_scope_match‘

* ‘amp_policy_compliance‘

* ‘amp_human_review‘

* ‘amp_reservation_status‘

* ‘amp_consumption_status‘

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

13. 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, have not exceeded their permitted use, 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, runtime risk, and relying-party rules.

JEP-AMP defines Event-valid and Mandate-valid checks. Action-validity is local, domain-specific, and relying-party-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:1‘.

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 reservation and consumption state where applicable.

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

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

15. Check subdelegation controls.

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

17. Return a structured result identifying which checks passed, failed, were conditional, were indeterminate, or were not applicable.

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

14. Subdelegation and Delegation Chains

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

If subdelegation is omitted, the following defaults apply:

```
subdelegation_allowed = false
max_depth = 0
scope_may_expand = false
constraints_may_relax = false
parent_termination_terminates_child = true
credential_revocation_propagates = domain-profile-defined
policy_change_propagates = domain-profile-defined
```

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 can relax constraints;
* 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 and constraints may only be preserved or strengthened. Domain profiles SHOULD state whether parent mandate termination, issuer credential revocation, delegatee credential revocation, or policy change invalidates child mandates. If no such rule is available, relying parties SHOULD treat child mandates as invalid when the parent mandate has been terminated or the parent issuer’s authority is no longer acceptable under the applicable trust profile.

When validating a chain, a verifier SHOULD evaluate each parent mandate, termination status, scope relationship, constraint 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.

15. 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 an HJS-style receipt profile or another domain-specific receipt mechanism.

For low-risk mandates, receipt binding is RECOMMENDED. For high-risk mandates, domain profiles SHOULD require receipt binding. For regulated, high-value, safety-sensitive, payment-adjacent, privacy-sensitive, or externally auditable mandates, domain profiles MAY require HJS or a domain-specific receipt profile.

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 reservation, consumption, or 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, if applicable.

A receipt reference object SHOULD, where practical, identify the mandate issuance-event hash, the descriptor digest, the action request digest, the delegatee, the action type, the target reference, the execution time or interval, evidence references, validation references, and any termination or consumption references. This document does not require a specific receipt profile, but a receipt profile that claims AMP binding SHOULD make these bindings explicit.

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.

16. Interaction with Domain Mandates and Payment Protocols

JEP-AMP is cross-domain. 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 intent capture, 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 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 fields are only cross-domain accountability context;
* which validation scopes are required;
* whether receipt evidence must be produced by the domain protocol, JEP/HJS, another receipt profile, or more than one mechanism; and
* whether the domain protocol or JEP-AMP controls funds movement, settlement, or domain-specific execution.

JEP-AMP MUST NOT define payment clearing, payment settlement, charge authorization, or funds movement semantics.

17. Gateway Validation Interface (Non-Normative)

A gateway implementation can expose the following non-normative operations:

```
validateMandate(mandate, action_request, context) -> validation_result
reserveMandate(mandate_id, action_request, context) -> reservation_result
consumeMandate(mandate_id, receipt_ref, context) -> termination_event
bindReceipt(mandate_id, receipt_ref, context) -> verification_event
terminateMandate(mandate_id, reason, context) -> termination_event
```

These operations are illustrative. JEP-AMP defines profile semantics, not a mandatory API surface.

18. 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 intended for bounded relying parties.

Receipt binding can reveal execution details. Domain profiles SHOULD specify whether receipt evidence is public, private, encrypted, selectively disclosable, redacted, or available only to designated verifiers.

19. Security Considerations

Implementations MUST validate signatures, descriptor digests, critical extensions, issuer authority, validity intervals, audience restrictions, termination status, subdelegation controls, and profile declarations before relying on a mandate.

Implementations MUST NOT confuse Event-validity, Mandate-validity, and Action-validity. A signature-valid event is not necessarily a valid mandate, and a valid mandate is not necessarily locally authorized for a requested action.

Single-use and consumable mandates require care. Where multiple gateways or relying parties can observe the same active mandate, implementations SHOULD use a reservation, locking, transparency-backed log, or domain profile-defined consumption mechanism to prevent concurrent double use.

Extension summaries MUST NOT be treated as authoritative when they conflict with the Action Mandate Descriptor. Validators MUST reject an AMP event when authoritative descriptor fields and signed summary fields conflict.

Subdelegation can amplify risk. Unless explicitly permitted by the descriptor or a domain profile, subdelegation MUST be rejected.

20. IANA Considerations

This document requests registration of the profile identifier:

urn:jep:profile:amp:1

If a JEP profile registry is established, this profile should be registered with that registry. Until such a registry exists, this identifier is a provisional profile identifier.

This document does not request registration of a global action taxonomy. Domain profiles can define action identifiers and action registries.

21. Conformance Considerations

A conforming AMP-1 Mandate Producer MUST produce JEP Delegation events that carry or reference a signed Action Mandate Descriptor conforming to this profile.

A conforming AMP-1 Mandate Verifier MUST validate JEP-Core event validity, profile declaration, descriptor schema, descriptor digest, issuer and delegatee interpretation under the applicable trust profile, validity interval, observed termination status, subdelegation controls, and required critical extensions.

A conforming AMP-1 Gateway Validator MUST additionally evaluate local Action-validity under relying-party policy before allowing an action to proceed.

A conforming implementation SHOULD emit structured validation results and MAY issue JEP Verification events for mandate validation, action validation, receipt validation, reservation, or consumption.

A conforming implementation that claims support for external mappings, receipt binding, chain profiles, or gateway validation SHOULD declare those capabilities separately from baseline AMP support. Baseline AMP support does not imply support for any particular event envelope, identity system, credential system, payment-domain mandate, receipt profile, tracing system, work-unit profile, or domain action taxonomy.

22. Implementation Neutrality and Reference Tools

JEP-AMP defines profile semantics and validation requirements. It does not define, require, endorse, or privilege any official implementation, gateway, validator, SDK, hosted service, registry operator, conformance provider, policy engine, receipt store, or audit service.

A reference implementation, validator, test suite, example gateway, example registry, or SDK, if published, is non-normative unless a separate standards-track, registry, or community-governance document states otherwise. Conformance to JEP-AMP is determined by the requirements in this document, the applicable JEP-Core rules, declared profiles, domain profiles, and applicable test vectors; it is not determined by behavioral compatibility with any single implementation.

Implementations MAY use different programming languages, deployment models, gateway architectures, policy engines, identity systems, credential systems, receipt profiles, chain profiles, archival systems, and audit systems, provided that they satisfy the conformance requirements for the AMP roles they claim.

No implementation, including one maintained by the author, a project, a foundation, a vendor, a registry operator, or a hosted service provider, is considered exclusive, canonical, mandatory, or officially privileged solely by virtue of being published alongside this document or by a party associated with this document.

Example JSON objects, interface sketches, validation examples, and test vector manifests in this document or accompanying material are non-normative unless explicitly stated otherwise. They are intended to help independent implementations converge on interoperable behavior, not to create an exclusive implementation path.

23. Failure Codes and Test Vector Guidance

AMP failure reporting SHOULD identify the layer at which validation failed. A structured failure record SHOULD include ‘code‘, ‘class‘, ‘validity_layer‘, ‘scope‘, and ‘severity‘ fields. Implementations MAY include human-readable diagnostics, but relying parties SHOULD NOT depend on free-form text for authorization decisions.

Recommended failure classes are:

* structural failures, such as missing profile declaration, unsupported critical extension, descriptor schema failure, descriptor digest mismatch, or event/descriptor conflict;

* mandate failures, such as issuer authority failure, delegatee mismatch, expired mandate, observed termination, audience mismatch, scope mismatch, subdelegation failure, reservation conflict, or consumed mandate;

* action failures, such as local policy failure, approval required, evidence missing, risk threshold exceeded, or Action-validity indeterminate;

* mapping failures, such as unsupported external mandate mapping, external envelope mismatch, credential mapping failure, or trace-context mismatch; and

* receipt failures, such as receipt missing, receipt digest mismatch, receipt profile unsupported, or receipt validation scope downgrade.

Failure codes that affect Event-validity or Mandate-validity SHOULD be stable within the AMP profile version. Failure codes that affect only Action-validity MAY be refined by domain profiles, because Action-validity is local and relying-party-specific.

AMP test vectors SHOULD include at least the following cases:

* a valid minimal inline descriptor;

* a valid detached descriptor with digest binding;

* an invalid descriptor digest mismatch;

* an unsupported critical extension;

* a signature-valid event with invalid mandate descriptor;

* an expired mandate;
* a mandate terminated by a JEP Termination event;
* a delegatee mismatch;
* a child mandate that expands parent scope without permission;
* a single-use mandate already consumed;
* a reservation conflict;
* a receipt that references the mandate correctly;
* a receipt that omits required mandate binding; and
* a validation result that attempts to overclaim beyond its declared verification scope.

24. Open Issues

This draft intentionally leaves several areas to domain profiles or later revisions. These items are not required for baseline AMP-1 semantics:

* common machine-readable policy languages;
* domain-specific action taxonomies;
* normative reservation-event formats for high-risk single-use mandates;
* complete payment-domain and other domain-mandate mapping profiles;
* canonical receipt-binding profiles for regulated domains;
* complete profile registry and conformance-class definitions.

25. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

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

[JEP] Wang, Y., "Judgment Event Protocol (JEP)", Work in Progress, Internet-Draft, draft-wang-jep-judgment-event-protocol-06, 2026, <https://datatracker.ietf.org/doc/draft-wang-jep-judgment-event-protocol/>.

[JEP-PROFILES] Wang, Y., "JEP Profiles and Interoperability", Work in Progress, Internet-Draft, draft-wang-jep-profiles-00, 2026, <https://datatracker.ietf.org/doc/draft-wang-jep-profiles/>.

26. Informative References

[HJS] Wang, Y., "HJS: Accountability Receipts for AI Agents", Work in Progress, Internet-Draft, draft-wang-hjs-accountability-05, 2026, <https://datatracker.ietf.org/doc/draft-wang-hjs-accountability/>.

[JAC] Wang, Y., "JAC: Declared Dependency Chains for Agent Receipts", Work in Progress, Internet-Draft, draft-wang-jac-02, 2026, <https://datatracker.ietf.org/doc/draft-wang-jac/>.

[AP2-AUTH] Contributors, G., "Agent Authorization Framework", 2025, <https://ap2-protocol.org/ap2/agent_authorization/>.

[AP2-SPEC] Contributors, G., "Agentic Payment Protocol v0.2 Core Specification", 2025, <https://ap2-protocol.org/ap2/specification/>.

Appendix A. Non-Normative Procurement Example

A procurement profile can define a work unit named ‘purchase_request‘, an action type ‘urn:example:procurement:action:purchase‘, and evidence requirements for quote sets, approvals, purchase orders, invoices, and receipt records. The JEP-AMP mandate authorizes the procurement agent to perform the purchase action within an amount cap and validity interval. The actual purchase, payment, settlement, and dispute rules are defined by the procurement domain profile and local enterprise policy, not by JEP-AMP.

Appendix B. Non-Normative Lifecycle Sketch

```
D: principal delegates bounded action mandate to agent
V: gateway validates mandate descriptor and policy context
J: human or system records approval, recommendation, or risk judgment
V: relying party validates action request as locally Action-valid
J: agent records operational judgment or selection
HJS/domain receipt: execution evidence is recorded
V: receipt or evidence bundle is reviewed
T: mandate is consumed, revoked, expired, or completed
JAC/domain chain: events and receipts are declared as dependencies
```

Appendix C. Changes from -00

This revision tightens JEP-AMP as a thin profile and makes the following notable changes:

* changes the profile identifier to ‘urn:jep:profile:amp:1‘;
* weakens domain-specific examples in the Abstract and moves them toward non-normative examples;
* makes ‘mandate_id‘ optional but requires a deterministic operational ID derived from the issuance event hash when absent;
* requires ‘action.type‘ to be URI/URN/profile-qualified and explicitly avoids a global action taxonomy;
* adds ‘work_unit_ref‘, ‘case_ref‘, ‘workflow_ref‘, and ‘transaction_ref‘ as optional contextual references;
* strengthens the Event-valid / Mandate-valid / Action-valid separation;
* adds reservation and consumption guidance for single-use or consumable mandates;
* strengthens subdelegation defaults;
* makes receipt binding risk-based rather than universally mandatory;
* clarifies that JEP-AMP maps to domain mandates such as payment mandates rather than replacing them;
* adds a non-normative Gateway validation interface;
* adds an interoperability posture and profile capability declaration section;

* adds external mapping principles for event envelopes, credentials, traces, payment-domain mandates, receipts, and audit records;

* clarifies profile semantic versioning and deterministic mandate identity;

* tightens action namespace requirements;

* adds structured reservation and consumption record guidance;

* strengthens child-mandate propagation guidance;

* adds minimum receipt-binding guidance; and

* adds failure-code and test-vector guidance; and

* adds implementation-neutrality language clarifying that validators, gateways, SDKs, registries, test tools, and example implementations are non-normative and non-exclusive unless a separate governance document states otherwise.

Author’s Address

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