Network Working Group
Internet-Draft
Intended status: Experimental
Expires: December 3, 2026

Y. Wang
Independent

June 1, 2026

Semantic Interoperability for the Judgment Event Protocol
draft-wang-jep-semantic-interoperability-00

Abstract

This document defines semantic interoperability requirements for the Judgment Event Protocol (JEP).

JEP-Core defines the event syntax, event classes, signatures, hashes, references, extension processing, and validation levels for signed judgment-related events. This document does not modify those mechanisms. Where this document restates JEP-Core semantics, JEP-Core remains authoritative. Instead, this document defines the minimum shared semantic invariants required for independent systems to interpret JEP events consistently across implementations, profiles, organizations, and jurisdictions.

The document specifies core semantic roles, core semantic relations, event-class interpretation rules for Judgment, Delegation, Termination, and Verification events, verification-scope semantics, semantic identifiers, profile-extension constraints, semantic validation results, non-inference rules, semantic conformance requirements, initial semantic registry requirements, and cross-jurisdictional boundaries. It defines semantic registry contents and constraints, but does not define operational registry governance beyond the requirements stated here.

This document does not define legal effect, moral responsibility, regulatory compliance, runtime enforcement, access-control decisions, domain-specific workflows, or external truth. A JEP event is a protocol-semantic record. Whether that record is sufficient to support an external target claim is outside the scope of this document and must be determined by an applicable profile, evidence policy, domain rule, or target-support analysis.

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 3 December 2026.

Copyright Notice

Table of Contents

1. Introduction
1.1. Purpose
1.2. Relationship to JEP-Core
1.3. Relationship to JEP Profiles and JEP Conformance
1.4. Non-Goals
1.5. Boundary Summary
1.6. Normative and Informative Content
1.7. Terminology
2. Semantic Model
2.1. JEP Events as Protocol-Semantic Records
2.2. Minimum Semantic Invariant
2.3. Profile-Bounded Interpretation
2.4. Open-World Default
2.5. Semantic Validity Is Not Target Sufficiency
2.6. Runtime and Enforcement Boundary
3. Core Semantic Roles
4. Core Semantic Relations
5. Event-Class Semantics
5.1. Judgment
5.2. Delegation
5.3. Termination
5.4. Verification
6. Verification Scope Semantics
6.1. Scope Declaration and Semantic Interpretation
7. Semantic Identifiers
8. Profile Extension Rules
9. Semantic Ambiguity
9.1. Ambiguous Local Actions
9.2. Ambiguity Reporting
9.3. Information Loss in Mapping
10. Semantic Validation
10.1. Separation from JEP-Core Validation
10.2. Semantic Validation Status
10.3. Semantic Validation Result Object
10.4. Failure Conditions
10.5. Semantic Validation and External Targets
11. Non-Inference Rules
12. Semantic Conformance
12.1. Conformance Classes
13. Cross-Jurisdictional Considerations
14. Security Considerations
15. Privacy Considerations
16. IANA Considerations
16.1. JEP Semantic Role Registry
16.2. JEP Semantic Relation Registry
16.3. JEP Verification Scope Registry
16.4. JEP Semantic Validation Status Registry
16.5. JEP Non-Inference Rule Registry
16.6. JEP Profile Semantic Extension Registry
17. Registry Governance Boundary
18. Compatibility with Other JEP Documents
19. Examples
19.1. Approval as Judgment
19.2. Approval as Delegation
19.3. Verification Scope Mismatch
19.4. Termination and Future Reliance
19.5. Reference Without Dependency
20. Invalid Inference Examples

References
Author’s Address
A. Initial Semantic Identifier Registry
A.1. Roles
A.2. Relations
A.3. Verification Scopes
A.4. Semantic Validation Statuses
A.5. Non-Inference Rules
B. Minimal Semantic Validation Result Example
C. Summary

1. Introduction

1.1. Purpose

JEP-Core defines a compact event layer for judgment-related acts. Its four event classes are:

J - Judgment
D - Delegation
T - Termination
V - Verification

JEP-Core defines how these events are represented, signed, hashed, referenced, extended, and validated.

However, syntactic and cryptographic interoperability do not guarantee semantic interoperability. Two systems can both produce valid JEP events while interpreting their meaning differently.

For example:

approved = true
verified = true
revoked = true
reviewed = true

can mean different things in different systems. One system can treat approved as a Judgment. Another can treat it as a Delegation. A third can treat it as Verification. Similarly, verified can mean syntax validation, signature validation, actor binding, chain integrity, human review, policy compliance, external evidence review, factual-claim checking, or target-support checking.

This document defines the common semantic layer needed to prevent such divergence.

It answers the following question:

When independent systems receive the same JEP event,
what must they agree that the event means,
and what must they not infer from it?

1.2. Relationship to JEP-Core

This document is a companion semantic layer for JEP-Core.

It does not modify:

* JEP-Core event syntax
* JEP-Core event classes
* JEP-Core signature semantics
* JEP-Core event-hash semantics
* JEP-Core reference semantics
* JEP-Core validation levels
* JEP-Core anti-replay fields
* JEP-Core critical-extension processing

Where this document appears to restate JEP-Core event semantics, JEP-Core remains authoritative. This document constrains cross-system and cross-profile interpretation of JEP-Core events.

A conforming implementation of this document MUST interpret JEP-Core events in a way that is consistent with JEP-Core.

1.3. Relationship to JEP Profiles and JEP Conformance

JEP Profiles define profile-specific trust, identity, credential, deployment, archival, domain, and interoperability bindings. JEP Conformance defines implementation conformance classes, test vectors, reference-validator behavior, and validation-result expectations. This document does not replace either one.

The relationship is:

JEP-Core
: event syntax, event classes, signatures, hashes, references, validation levels.

JEP Semantic Interoperability
: shared semantic invariants, event-class interpretation, verification-scope semantics, non-inference rules, semantic roles, semantic relations, semantic validation statuses.

JEP Profiles
: trust profiles, identity bindings, domain bindings, deployment-specific semantics.

JEP Conformance
: implementation conformance, validation behavior, schemas, test vectors.

Profiles MAY refine the semantics defined here, but they MUST NOT redefine the core meaning of Judgment, Delegation, Termination, or Verification.

This document defines semantic registry requirements and initial registry contents for the semantic identifiers it introduces. Operational registry maintenance procedures, registry operator selection, appeals, deprecation workflows, ecosystem policy, and namespace delegation MAY be specified by a separate JEP registry-governance document. Such a document MUST preserve the semantic invariants and non-inference rules defined here.

1.4. Non-Goals

This document does not define:

* legal liability
* moral responsibility
* regulatory compliance
* contractual validity
* runtime authorization enforcement
* access-control decisions
* complete governance workflows
* domain-specific approval processes
* truth of external factual claims
* sufficiency of evidence for external targets

A JEP event MAY be used as evidence in such contexts, but it does not by itself settle them.

1.5. Boundary Summary

This document defines semantic interoperability constraints only. It does not assign operational authority, legal effect, governance status, runtime permission, evidentiary sufficiency, or factual truth.

The following boundaries are normative:

JEP-Core boundary
: JEP-Core remains authoritative for event syntax, event classes, signatures, hashes, references, validation levels, and extension processing.

Profile boundary
: Profiles MAY define stronger or domain-specific interpretations, but those interpretations apply only within the declaring profile and MUST NOT be generalized to all JEP events.

Governance boundary
: This document supports governance interoperability by defining semantic invariants, but it does not define governance outcomes, institutional authority, legal liability, or regulatory compliance.

Runtime boundary
: This document does not authorize, deny, execute, block, revoke, or enforce runtime actions. Runtime behavior is profile- or deployment-specific.

Evidence boundary
: This document defines how evidence references and support relations may be interpreted semantically. It does not determine whether referenced evidence is sufficient for an external target.

Registry boundary
: This document defines initial semantic registries and identifier stability rules. Operational registry governance MAY be specified separately and MUST preserve the semantic invariants defined here.

1.6. Normative and Informative Content

The following sections are normative: , , , , , , , , , , , and .

The following sections are informative unless otherwise stated: , , , , , , and appendices.

1.7. Terminology

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 when, and only when, they appear in all capitals, as shown here.

Event class
: One of Judgment, Delegation, Termination, or Verification.

Semantic role
: A function played by an entity in the interpretation of a JEP event.

Semantic relation
: A declared relationship between an event, actor, subject, evidence item, prior event, claim, state object, receipt, or profile.

Verification scope
: The declared boundary of what a Verification event checks.

Semantic validation
: The process of determining whether a JEP event is semantically interpretable under this document and any applicable profiles.

Non-inference rule
: A rule prohibiting implementations or relying parties from deriving claims that are not licensed by the event semantics.

2. Semantic Model

2.1. JEP Events as Protocol-Semantic Records

A JEP event is a signed protocol record declaring that an actor, under a stated event class and applicable profile context, performed or asserted a judgment-related act.

A JEP event is not, by itself:

* a proof of external truth
* a proof of legal authority

* a proof of moral responsibility
* a proof of regulatory compliance
* a proof of target sufficiency
* a proof of complete causal history

2.2. Minimum Semantic Invariant

For any JEP event, a conforming implementation MUST preserve the following invariant:

The event class, actor, subject, declared scope, declared references, and declared semantic relations MUST NOT be interpreted beyond their declared meaning without an applicable profile.

At minimum:

* Judgment records a judgment-related act.
* Delegation records a bounded grant, transfer, assignment, or delegation
* context.
* Termination records closure, revocation, expiry, replacement, or end of
* future reliance.
* Verification records a check under a declared verification scope.

2.3. Profile-Bounded Interpretation

A profile MAY refine event interpretation.

A profile MAY say:

In this profile, a D event creates a mandate-validity claim.

A profile MUST NOT say:

A D event always proves legal authorization in all domains.

2.4. Open-World Default

Unless an applicable profile declares otherwise, JEP interpretation is open-world.

In particular:

* Absence of a JEP event in an observed log does not prove that the
* corresponding real-world event did not occur.
* A reference to an object does not prove that all relevant objects have been
* referenced.
* A structurally valid chain does not prove that the chain is complete.

A closed-world or complete-log interpretation MUST be explicitly declared by profile.

2.5. Semantic Validity Is Not Target Sufficiency

A semantically valid event is one that can be interpreted under JEP semantic rules and any applicable profile.

Semantic validity does not imply that the event, chain, receipt, or evidence bundle is sufficient to support an external target claim.

A target-support analysis MAY be performed by a separate profile or method. Such analysis MAY include target-determinability analysis, evidence-sufficiency analysis, risk-bound analysis, domain-specific evidentiary review, human expert review, or another registered target-support method. This document does not require any particular target-support method.

2.6. Runtime and Enforcement Boundary

This document is record-semantic, not execution-semantic. A semantic validation result under this document MUST NOT be interpreted as an authorization decision, access-control decision, tool-call permission, execution approval, revocation command, rollback instruction, or enforcement action unless an applicable runtime or enforcement profile explicitly defines that behavior.

Implementations that use JEP events in runtime decision-making MUST identify the applicable runtime profile, policy engine, mandate profile, or access-control mechanism. This document alone does not provide such a mechanism.

3. Core Semantic Roles

A semantic role is a function played by an entity in the interpretation of a JEP event. Each role identifier SHOULD be registered in the JEP Semantic Role Registry.

jep:role:actor
  The entity represented as performing or asserting the event. Actor identity does not by itself prove authority, correctness, legal capacity, or competence.
jep:role:issuer
  The entity or system that issued, serialized, or signed the event record. The issuer MAY be the actor, but need not be. Implementations MUST distinguish actor identity from issuer identity when both are present.
jep:role:subject
  The claim, action, mandate, evidence item, workflow, prior event, state object, receipt, or target to which the event applies.
jep:role:principal
  The entity on whose behalf authority, task scope, or responsibility context is granted. A principal identifier does not by itself prove legal authority.
jep:role:delegatee
  The entity receiving delegated authority, task scope, capability, action mandate, or responsibility context.
jep:role:verifier
  The entity or system performing a declared Verification event. The verifier role does not imply competence for every possible verification scope.
jep:role:relying_party
  An entity that consumes, interprets, or acts upon a JEP event. A relying party MUST NOT infer semantics beyond the event class, declared fields, declared verification scope, applicable profiles, and registered semantic identifiers.
jep:role:evidence_holder
  An entity or system that stores, controls, or can disclose evidence referenced by a JEP event. A referenced evidence holder does not imply that evidence has been disclosed, verified, or is sufficient.
jep:role:profile_authority
  An entity that defines or maintains a profile used to interpret JEP events in a particular deployment, trust framework, domain, organization, or jurisdictional context.

4. Core Semantic Relations

A semantic relation is a declared relationship between an event, actor, subject, evidence item, prior event, claim, state object, receipt, or profile. Each relation identifier SHOULD be registered in the JEP Semantic Relation Registry.

jep:relation:references
  An event references another object, event, claim, state, mandate, receipt, or evidence item. A reference alone MUST NOT be interpreted as causality, endorsement, approval, dependency, support, completeness, truth, or authorization unless an applicable profile declares such meaning.
jep:relation:judges
  A Judgment event records a decision-related position about its subject. The

relation does not imply that the judged subject is true, correct, safe, legally valid, or sufficiently evidenced.

jep:relation:delegates_to
: A Delegation event grants, transfers, assigns, or delegates a bounded authority, task, capability, mandate, or responsibility context from a principal or delegating actor to a delegatee. The relation does not imply legal validity unless an applicable profile establishes that effect.

jep:relation:terminates
: A Termination event closes, revokes, expires, replaces, cancels, suspends, or ends future reliance on its declared subject. The relation does not delete historical events.

jep:relation:verifies
: A Verification event records that a declared verification procedure was applied to a declared subject under a declared verification scope. The relation does not imply verification beyond that declared scope.

jep:relation:depends_on
: An event, claim, receipt, or state object declares dependency on another event, evidence item, state, receipt, or claim. A dependency relation MUST be explicit. A reference alone is not dependency.

jep:relation:supports
: An event or evidence item is declared by the emitting system or applicable profile to support a claim, target, judgment, receipt, or state object. This relation records a declared support relationship only. It does not imply evidentiary sufficiency, truth, endorsement, causality, target support, or legal effect unless an applicable profile, evidence policy, domain rule, or target-support analysis establishes those additional conclusions.

jep:relation:supersedes
: An event or record declares that it replaces or supersedes a prior event, record, mandate, state, or claim. Supersession does not imply deletion of the prior record.

jep:relation:bounds
: An event declares a scope, time interval, usage limit, capability limit, policy limit, resource limit, or audience boundary.

jep:relation:challenges
: An event or record declares that a prior claim, event, verification, mandate, judgment, receipt, or state claim is disputed, incomplete, invalid under a profile, or requires further evidence. This relation does not by itself settle the challenge.

5. Event-Class Semantics

5.1. Judgment

A Judgment event records that an actor made, accepted, rejected, classified, selected, approved, disapproved, committed to, or otherwise recorded a decision-related position concerning a declared subject.

A Judgment event establishes only that the judgment-related act was recorded under JEP.

A Judgment event MUST NOT be interpreted as proof that the judged claim is true, that the decision is legally valid, that the decision is morally correct, that the decision is supported by sufficient evidence, or that the decision is target-sufficient unless an applicable profile, evidence policy, domain rule, or target-support analysis establishes those additional conclusions.

Minimum semantic fields for a Judgment interpretation SHOULD include actor, subject, judgment relation, event time or event timestamp, and profile context if any.

5.2. Delegation

A Delegation event records a bounded grant, transfer, assignment, or authorization context from a principal or delegating actor to a delegatee.

A Delegation event establishes only that a delegation-related act was recorded under JEP.

A Delegation event SHOULD declare, directly or through an applicable profile, principal, delegatee, scope, validity interval, constraints, termination conditions, permitted uses, relying parties, and profile context.

A Delegation event MUST NOT be interpreted as proof of legal authorization, organizational legitimacy, correct action by the delegatee, downstream action validity, or unlimited authority unless an applicable profile establishes those effects.

5.3. Termination

A Termination event records closure, revocation, expiry, cancellation, suspension, replacement, or end of future reliance concerning a declared subject.

A Termination event SHOULD declare, directly or through an applicable profile, terminated subject, termination mode, termination time, scope of termination, future reliance effect, replacement reference if any, and downstream revalidation requirement if any.

A Termination event MUST NOT be interpreted as deletion of historical records, proof that all downstream reliance has ended, proof that legal, social, or organizational obligations are resolved, proof that prior actions were invalid, or proof that all child delegations are terminated unless an applicable profile explicitly provides such semantics.

5.4. Verification

A Verification event records that a declared check was applied to a declared subject under a declared verification scope.

A Verification event MUST declare a verification scope, either directly or through an applicable profile.

A Verification event establishes only that the declared verification procedure was recorded under the declared scope. A Verification event MUST NOT be interpreted as verification beyond its declared scope.

Minimum semantic fields for a Verification interpretation SHOULD include verifier, subject, verification scope, verification method or profile reference, and event time or event timestamp.

6. Verification Scope Semantics

Verification scopes MUST be registered or profile-defined. A Verification event with an unknown non-critical scope MAY be treated as semantically uninterpretable. A Verification event with an unknown critical scope MUST fail semantic validation.

The scopes listed in this section are initial registered identifiers. Implementations are REQUIRED to preserve their meanings when used, but are not REQUIRED to support every scope unless required by a declared profile.

6.1. Scope Declaration and Semantic Interpretation

JEP-Core remains authoritative for how verification scopes are represented, carried, and processed as part of JEP events. This document defines the semantic interpretation of registered scopes when those scopes are used. If a future version of JEP-Core or an applicable profile defines event-processing requirements for a scope, those event-processing requirements remain outside this document unless explicitly incorporated here.

A scope identifier registered here does not require every implementation to

perform the corresponding verification procedure. It only requires that implementations preserve the registered meaning when they emit, translate, validate, display, or rely on that scope.

jep:scope:syntax
  Establishes that the checked object conforms to a declared syntax or schema. Does not establish cryptographic validity, actor binding, truth, legal validity, or target sufficiency.
jep:scope:cryptographic_signature
  Establishes that a declared signature verification procedure succeeded. Does not establish truth of the signed claim.
jep:scope:actor_binding
  Establishes that a declared actor-binding procedure succeeded under an applicable identity or trust profile. Does not establish that the actor had authority to act.
jep:scope:credential_status
  Establishes that a declared credential-status check was performed. Does not establish legal authority beyond the credential profile.
jep:scope:chain_integrity
  Establishes that a declared event, receipt, or dependency chain is structurally intact under the declared chain profile. Does not establish that every external event occurred or that the chain proves an external target.
jep:scope:policy_compliance
  Establishes that a declared policy-compliance check was applied. Does not establish legal liability, moral correctness, factual truth, or regulatory compliance unless an applicable profile establishes those conclusions.
jep:scope:mandate_validity
  Establishes that a declared action mandate satisfies an applicable mandate-validity profile. Does not establish that the resulting action is factually correct, safe, lawful, or externally sufficient.
jep:scope:human_review
  Establishes that a human-review process was recorded under the declared profile. Does not establish review quality, expertise, independence, completeness, correctness, or legal sufficiency unless a profile defines those properties.
jep:scope:external_evidence
  Establishes that external evidence was checked or referenced under the declared evidence policy. Does not establish that the evidence is sufficient for the target unless a target-support, evidence, or domain profile establishes such sufficiency.
jep:scope:source_provenance
  Establishes that a provenance check was applied to the declared source. Does not establish source truthfulness.
jep:scope:factual_claim
  Establishes that a factual-claim verification procedure was applied. The level of support, evidence policy, uncertainty, and domain validity MUST be declared by profile.
jep:scope:target_support
  Establishes that a target-support analysis, evidence-sufficiency analysis, target-determinability analysis, risk-bound analysis, or another registered target-support procedure was referenced or checked. Does not establish that the analysis is correct unless its profile, model assumptions, evidence policy, and required verification procedure are also validated.
jep:scope:archival_integrity
  Establishes that an archival-integrity check was applied. Does not establish target truth.
jep:scope:redaction_integrity
  Establishes that a redacted view is linked to a declared source object under a declared redaction proof or policy. Does not establish that the redacted view is sufficient for all relying-party purposes.

7. Semantic Identifiers

Semantic identifiers SHOULD use stable namespaced identifiers. Examples include jep:role:actor, jep:relation:delegates_to, jep:scope:chain_integrity,

and jep:status:semantic_valid.

Profiles MAY define additional identifiers, but they MUST NOT redefine identifiers registered by this document.

Once registered, a semantic identifier MUST NOT be repurposed to mean a different semantic role, relation, scope, status, or rule. If a semantic meaning changes, a new identifier MUST be registered. Deprecated identifiers MUST remain resolvable.

A profile defining a new semantic identifier SHOULD use a namespaced identifier controlled by the profile authority. A profile MUST NOT define an identifier that is visually or semantically confusable with a registered JEP identifier unless it is explicitly declared as a subtype or constrained interpretation of that registered identifier.

8. Profile Extension Rules

A JEP profile MAY extend the semantic model by defining additional roles, relations, verification scopes, domain-specific subject types, domain-specific evidence descriptors, domain-specific conformance requirements, or domain-specific semantic validation results.

A profile MUST NOT redefine Judgment, Delegation, Termination, or Verification; reinterpret a Verification event beyond its declared scope; erase non-inference rules defined by this document; treat references as causality without declaring a relation; treat references as dependency without declaring dependency; or treat absence of an event as proof of absence without a complete-log assumption.

A profile that refines a core semantic identifier MUST declare whether it is a subtype, constraint, domain binding, profile-specific interpretation, or jurisdiction-specific interpretation.

Profiles SHOULD declare whether their semantics are closed-world or open-world, complete-log dependent or partial-log tolerant, jurisdiction-neutral or jurisdiction-specific, record-only or runtime-enforcing, and legal-effect claiming or non-legal-effect.

A profile defining stronger semantics than this document MUST state that those stronger semantics apply only within that profile and MUST NOT be generalized to JEP events outside that profile.

A profile MUST clearly distinguish profile-local effects from JEP-global semantics. Statements such as legal validity, regulatory sufficiency, contractual effect, runtime authorization, organizational approval, or domain-specific evidentiary sufficiency MUST be explicitly scoped to the declaring profile.

A profile MUST NOT register or use a semantic identifier in a way that conflicts with the registered meaning of an identifier defined by this document. If a profile needs a stronger, narrower, or domain-specific meaning, it MUST define a new identifier or an explicit subtype relation.

9. Semantic Ambiguity

9.1. Ambiguous Local Actions

A local action may not map unambiguously to one JEP event class. For example, approve may map to Judgment if it records acceptance of a claim, Delegation if it grants action authority, or Verification if it validates a record or evidence chain.

A bridge processor MUST mark a mapping as semantic_ambiguous unless an applicable profile disambiguates it.

9.2. Ambiguity Reporting

When semantic ambiguity is detected, a processor SHOULD report the source local action, candidate JEP event classes, missing disambiguating fields, required profile if known, information loss if any, and recommended mapping if profile-defined.

9.3. Information Loss in Mapping

A bridge processor translating from an external system into JEP events MUST declare known semantic information loss when the source event contains semantics that cannot be represented using the target JEP event class and declared profiles.

Examples of information loss include loss of authority scope, verification method, evidence provenance, termination effect, human-review context, or target-support status.

10. Semantic Validation

10.1. Separation from JEP-Core Validation

Semantic validation is distinct from JEP-Core syntactic, cryptographic, hash, reference, and validation-level checks.

Failure of semantic validation under this document does not necessarily imply failure of JEP-Core syntactic or cryptographic validation.

An event may be cryptographically valid but semantically uninterpretable, syntactically valid but semantically ambiguous, semantically valid under one profile but not another, or semantically valid but insufficient for an external target.

10.2. Semantic Validation Status

A semantic validator SHOULD output one of:

```
semantic_valid
semantic_valid_with_profile
semantic_ambiguous
profile_required
unsupported_scope
unsupported_relation
unsupported_role
nonconformant
out_of_scope
```

10.3. Semantic Validation Result Object

A semantic validation result SHOULD include fields such as semantic status, event class, declared profiles, roles detected, relations detected, verification scopes, non-inference warnings, required profiles, and semantic failures.

```
{
  "semantic_status": "semantic_valid_with_profile",
  "event_class": "D",
  "declared_profiles": ["jep-profile:amp"],
  "roles_detected": [
    "jep:role:principal",
    "jep:role:delegatee"
  ],
  "relations_detected": [
    "jep:relation:delegates_to",
    "jep:relation:bounds"
  ],
```

```
  "verification_scopes": [],
  "non_inference_warnings": [
    "jep:non_inference:no_legal_authority_from_delegation"
  ],
  "required_profiles": [],
  "semantic_failures": []
}
```

10.4. Failure Conditions

A semantic validator MUST return nonconformant if an event claims a core JEP class but contradicts its core semantics; a Verification event lacks a required scope; an unknown critical semantic identifier is present; a profile attempts to redefine a core event class; or a profile attempts to override a non-inference rule.

10.5. Semantic Validation and External Targets

A semantic validator MAY report that an event is semantically valid while also reporting that the event is insufficient for an external target. Such insufficiency MUST NOT be treated as semantic nonconformance unless the applicable profile requires target sufficiency as part of semantic validation.

11. Non-Inference Rules

This section is normative.

Judgment does not imply truth
: A JEP Judgment event MUST NOT be interpreted as proof of the truth, correctness, legality, or sufficiency of the judged subject.

Delegation does not imply legal authority
: A JEP Delegation event MUST NOT be interpreted as proof of legal, regulatory, contractual, or organizational authority unless an applicable profile explicitly establishes such effect.

Termination does not delete history
: A JEP Termination event MUST NOT be interpreted as deletion, erasure, or invalidation of historical records unless a profile explicitly defines that effect.

Termination does not automatically end all downstream reliance
: A JEP Termination event MUST NOT be interpreted as ending all downstream reliance unless the applicable profile defines the scope and propagation of such termination.

Verification does not exceed scope
: A JEP Verification event MUST NOT be interpreted as verification beyond its declared verification scope.

Reference does not imply causality
: A reference from one event to another MUST NOT be interpreted as causality, endorsement, dependency, support, or completeness unless an explicit semantic relation or profile declares that meaning.

Absence does not imply non-occurrence
: The absence of a JEP event in an observed log MUST NOT be interpreted as proof that the corresponding real-world event did not occur unless a complete-log profile is in force.

Chain integrity does not imply target sufficiency
: A structurally valid event chain MUST NOT be interpreted as sufficient evidence for an external target unless an applicable target-support, evidence, or domain profile establishes such sufficiency.

Support does not imply sufficiency
: A supports relation MUST NOT be interpreted as sufficient support for an external target unless an applicable profile, evidence policy, domain rule, or target-support analysis establishes sufficiency.

Human review does not imply review quality
: A human-review Verification event MUST NOT be interpreted as proof that the review was correct, independent, expert, complete, unbiased, or legally sufficient unless an applicable profile establishes those properties.

Policy compliance does not imply lawfulness

A policy-compliance Verification event MUST NOT be interpreted as legal compliance unless the applicable legal or regulatory profile explicitly defines that mapping.

Target support does not imply universal truth
: A target-support Verification event MUST NOT be interpreted as proof of universal truth, complete evidence, or applicability outside the declared target, evidence policy, model assumptions, and profile.

Profile semantics do not generalize globally
: A stronger interpretation defined by a profile MUST NOT be generalized to JEP events outside that profile unless another applicable profile explicitly adopts that interpretation.

12. Semantic Conformance

12.1. Conformance Classes

This document defines three semantic conformance classes:

S1: Core Semantic Processor
: Identifies event-class semantics, registered roles, registered relations, declared verification scopes, applies non-inference rules, produces semantic validation results, and rejects core semantic redefinition.

S2: Profile-Aware Semantic Processor
: Additionally supports profile resolution, profile-specific semantic identifiers, profile-specific validation rules, profile-specific failure mapping, and profile-specific non-inference constraints.

S3: Bridge Semantic Processor
: Additionally supports mapping external events into JEP semantic roles and relations, declaring information loss, declaring unsupported semantic features, declaring required profiles, and declaring semantic ambiguity where mapping is not unique.

13. Cross-Jurisdictional Considerations

JEP semantic interoperability is jurisdiction-neutral. This document does not assign legal effect to JEP events.

A jurisdiction, regulator, court, organization, contract, or governance domain MAY define how JEP events are used as evidence, but such use is outside this document.

Profiles that define jurisdiction-specific effects MUST identify the jurisdiction, identify the authority of the profile, identify the semantic changes from JEP-Core, state whether legal effect is claimed, state whether relying parties may infer legal consequence, state whether event semantics are evidentiary or dispositive, and state conflict-handling rules.

A JEP event that is semantically valid under this document may still have no legal effect in a given jurisdiction.

Semantic interoperability is therefore evidentiary and interpretive, not dispositive. A jurisdiction-specific profile MAY state how JEP events are used as evidence, but this document does not decide whether such evidence is sufficient, admissible, binding, or legally conclusive.

14. Security Considerations

Implementations MUST consider at least the following risks.

Semantic downgrade
: An attacker may cause a system to treat a high-assurance event as a lower-assurance event, or a lower-assurance event as sufficient for a higher-assurance claim. Mitigations include explicit verification scopes, profile identifiers, semantic validation results, and non-inference warnings.

Verification scope inflation
: An attacker or careless system may present V(scope=cryptographic_signature)

as if it were V(scope=factual_claim). Implementations MUST prevent scope inflation.

Role confusion
: An attacker may confuse issuer, actor, principal, delegatee, verifier, and relying-party roles. Implementations SHOULD display and validate semantic roles separately.

Reference laundering
: An attacker may use references to imply causality, endorsement, dependency, support, or completeness. Implementations MUST enforce explicit semantic relations. Even when a supports relation is explicit, systems MUST NOT treat it as sufficient support without an applicable profile, evidence policy, domain rule, or target-support analysis.

Profile confusion
: An attacker may cause an event valid under one profile to be interpreted under another profile with stronger semantics. Implementations SHOULD bind semantic validation to declared profiles.

Termination ambiguity
: Ambiguous Termination semantics may cause systems to rely on expired or revoked mandates. Profiles SHOULD define future-reliance effects explicitly.

False complete-log assumption
: A system may treat an observed partial log as complete and infer non-occurrence from absence. Implementations MUST NOT assume log completeness without an applicable complete-log profile.

Registry poisoning
: A malicious or careless registration may introduce confusing semantic identifiers. Registries SHOULD require expert review, collision checks, security review, and change-control procedures.

Evidence reference substitution
: An attacker may substitute an evidence reference while preserving the surrounding semantic event structure. Profiles SHOULD bind evidence references cryptographically when evidence integrity is required.

Ambiguous local-action mapping
: An attacker may exploit ambiguity in local actions such as approve, review, or verify to cause a bridge processor to map an event into a stronger JEP semantic class. Bridge processors MUST report ambiguity unless disambiguated by profile.

15. Privacy Considerations

Semantic metadata can reveal sensitive organizational, legal, medical, financial, operational, or personal relationships even when evidence payloads are not disclosed.

Sensitive semantic relationships may include who judged a claim, who delegated authority, who received delegated authority, who verified evidence, which mandate was terminated, which evidence holder controls evidence, which workflow depends on which prior event, and which state claim was challenged.

Implementations SHOULD support data minimization, role minimization, pseudonymous actor references, digest references, selective disclosure, audience-bound semantic views, redaction integrity, encrypted evidence references, and unlinkability where appropriate.

A semantic validator SHOULD NOT require disclosure of sensitive evidence unless the applicable profile requires it.

16. IANA Considerations

This document requests IANA to create the initial semantic registries listed in this section upon publication as an RFC. The registration policy for each registry is Specification Required with Expert Review, as described in .

Each registry entry SHOULD include identifier, name, description, defining document, status, security considerations, privacy considerations, profile dependencies, and change controller.

Registered identifiers MUST NOT be repurposed. Deprecated identifiers MUST remain resolvable. New semantics require new identifiers.

16.1. JEP Semantic Role Registry

This registry records semantic role identifiers used to interpret entities participating in JEP events. Initial entries are listed in .

16.2. JEP Semantic Relation Registry

This registry records semantic relation identifiers used to interpret relationships among events, actors, subjects, evidence items, receipts, state objects, and profiles. Initial entries are listed in .

16.3. JEP Verification Scope Registry

This registry records verification scope identifiers. Implementations are REQUIRED to preserve the registered meaning of a scope when that scope is used, but are not REQUIRED to support every registered scope unless required by a declared profile. Initial entries are listed in .

16.4. JEP Semantic Validation Status Registry

This registry records machine-readable semantic validation status identifiers. Initial entries are listed in .

16.5. JEP Non-Inference Rule Registry

This registry records non-inference rule identifiers. Non-inference rules registered by this document MUST NOT be overridden by profiles. Initial entries are listed in .

16.6. JEP Profile Semantic Extension Registry

This registry records profile-defined semantic extensions, including additional roles, relations, scopes, validation statuses, and profile-specific constraints.

17. Registry Governance Boundary

This document defines semantic registries and initial contents for the identifiers introduced here. It does not define all operational procedures for long-term registry maintenance, registry operator selection, appeals, deprecation workflow, ecosystem policy, or namespace delegation.

A future registry-governance specification MAY define those operational procedures. Such a specification MUST NOT repurpose identifiers registered by this document, weaken the non-inference rules or boundary constraints defined here, or authorize profiles to redefine the core semantics of Judgment, Delegation, Termination, or Verification.

18. Compatibility with Other JEP Documents

This document is compatible with JEP-Core, JEP Profiles, JEP Conformance, JEP-AMP, HJS, JAC, COE, CEP, and CTP. It does not replace their profile-specific semantics. It defines cross-profile semantic invariants and non-inference constraints. JEP-Core remains authoritative for event syntax, event classes, signatures, hashes, references, validation levels, and extension processing. This document is authoritative only for the semantic interoperability constraints defined herein.

If a profile defines a stronger interpretation, that interpretation is valid only within that profile and MUST NOT be generalized to JEP events outside that profile.

JEP-Core defines event syntax, event classes, signatures, hashes, references,

validation levels, and extension rules. This document defines semantic interoperability rules for interpreting JEP-Core events.

JEP Profiles define trust profiles, identity bindings, credential bindings, deployment profiles, and domain-specific interpretations. Profiles MUST conform to this document when extending JEP event semantics.

JEP Conformance defines implementation conformance and test behavior. Semantic conformance tests SHOULD be added for this document.

JEP-AMP defines action mandates using JEP Delegation events. JEP-AMP MUST conform to the Delegation semantics and non-inference rules defined here.

HJS and JAC define receipt and dependency-chain infrastructure over JEP events. They MUST NOT infer semantics beyond registered JEP relations, profiles, and verification scopes.

COE , CEP , and CTP may reference JEP events to bind observations, state claims, evolution records, or temporal claims. Such references MUST NOT imply truth, causality, authority, or completeness unless declared by profile.

19. Examples

19.1. Approval as Judgment

A system records approved = true. If this means a reviewer accepted a report, it SHOULD be represented as a Judgment event. The event MUST NOT be interpreted as proof that the report is true.

19.2. Approval as Delegation

A system records approved tool access. If this grants tool-use authority to an agent, it SHOULD be represented as a Delegation event, preferably under an action-mandate profile. The event SHOULD declare or reference principal, delegatee, scope, validity interval, constraints, and termination conditions.

19.3. Verification Scope Mismatch

A system records verified = true. If the system verified only the signature, the JEP event MUST use V(scope=cryptographic_signature). It MUST NOT be interpreted as V(scope=factual_claim).

19.4. Termination and Future Reliance

A Termination event closes an action mandate. Unless a profile specifies cascade behavior, the event MUST NOT be interpreted as automatically terminating every downstream child mandate.

19.5. Reference Without Dependency

A Judgment event references a prior report. That reference alone does not imply that the Judgment depends on the report. A dependency MUST be declared using jep:relation:depends_on or an applicable profile.

20. Invalid Inference Examples

Signature verification to factual truth
  Input: V(scope=cryptographic_signature). Invalid inference: the signed factual claim is true. Reason: cryptographic signature verification does not imply factual correctness.
Delegation to legal authority
  Input: a D event granting an agent tool access. Invalid inference: the delegatee has legal authority in all contexts. Reason: legal authority requires an applicable profile or external rule.
Parent termination to child termination
  Input: a T event terminating a parent mandate. Invalid inference: all child

mandates are automatically terminated. Reason: cascade termination requires an applicable profile.

Judgment to truth
: Input: a J event approving a report. Invalid inference: the report is true and fully evidenced. Reason: Judgment records a decision-related position; it does not prove truth or evidential sufficiency.

Support to sufficiency
: Input: Event A declares jep:relation:supports for Claim B. Invalid inference: Claim B is sufficiently supported for all targets. Reason: support does not imply sufficiency without an applicable profile, evidence policy, domain rule, or target-support analysis.

Reference to causality
: Input: Event A references Event B. Invalid inference: Event B caused Event A. Reason: reference does not imply causality unless an explicit relation or profile declares it.

References

Normative References

[RFC2119] Scott Bradner. "Key words for use in RFCs to Indicate Requirement Levels." March 1997.
https://www.rfc-editor.org/info/rfc2119

[RFC8174] Barry Leiba. "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words." May 2017.
https://www.rfc-editor.org/info/rfc8174

[RFC8126] Michelle Cotton, Barry Leiba, Thomas Narten. "Guidelines for Writing an IANA Considerations Section in RFCs." June 2017.
https://www.rfc-editor.org/info/rfc8126

[I-D.wang-jep-judgment-event-protocol] Yuqiang Wang. "Judgment Event Protocol." May 2026.
https://datatracker.ietf.org/doc/draft-wang-jep-judgment-event-protocol/

[I-D.wang-jep-profiles] Yuqiang Wang. "Profiles for the Judgment Event Protocol." 2026.
https://datatracker.ietf.org/doc/draft-wang-jep-profiles/

[I-D.wang-jep-conformance] Yuqiang Wang. "Conformance for the Judgment Event Protocol." 2026.
https://datatracker.ietf.org/doc/draft-wang-jep-conformance/

Informative References

[I-D.wang-jep-action-mandate-profile] Yuqiang Wang. "Action Mandate Profile for the Judgment Event Protocol." 2026.
https://datatracker.ietf.org/doc/draft-wang-jep-action-mandate-profile/

[I-D.wang-hjs-accountability] Yuqiang Wang. "Human-Judgment Structured Accountability Receipts." 2026.
https://datatracker.ietf.org/doc/draft-wang-hjs-accountability/

[I-D.wang-jac] Yuqiang Wang. "Judgment Accountability Chains." 2026.
https://datatracker.ietf.org/doc/draft-wang-jac/

[I-D.wang-coe] Yuqiang Wang. "Claim Observation Evidence for JEP-Based Systems." 2026.
https://datatracker.ietf.org/doc/draft-wang-coe/

[I-D.wang-cep] Yuqiang Wang. "Change Evidence Profile for JEP-Based Systems." 2026.
https://datatracker.ietf.org/doc/draft-wang-cep/

[I-D.wang-ctp-definition] Yuqiang Wang. "Cognitive Time Protocol Definition." 2026. https://datatracker.ietf.org/doc/draft-wang-ctp-definition/

Appendix A. Initial Semantic Identifier Registry

A.1. Roles

jep:role:actor
jep:role:issuer
jep:role:subject
jep:role:principal
jep:role:delegatee
jep:role:verifier
jep:role:relying_party
jep:role:evidence_holder
jep:role:profile_authority

A.2. Relations

jep:relation:references
jep:relation:judges
jep:relation:delegates_to
jep:relation:terminates
jep:relation:verifies
jep:relation:depends_on
jep:relation:supports
jep:relation:supersedes
jep:relation:bounds
jep:relation:challenges

A.3. Verification Scopes

jep:scope:syntax
jep:scope:cryptographic_signature
jep:scope:actor_binding
jep:scope:credential_status
jep:scope:chain_integrity
jep:scope:policy_compliance
jep:scope:mandate_validity
jep:scope:human_review
jep:scope:external_evidence
jep:scope:source_provenance
jep:scope:factual_claim
jep:scope:target_support
jep:scope:archival_integrity
jep:scope:redaction_integrity

A.4. Semantic Validation Statuses

jep:status:semantic_valid
jep:status:semantic_valid_with_profile
jep:status:semantic_ambiguous
jep:status:profile_required
jep:status:unsupported_scope
jep:status:unsupported_relation
jep:status:unsupported_role
jep:status:nonconformant
jep:status:out_of_scope

A.5. Non-Inference Rules

jep:non_inference:no_truth_from_judgment
jep:non_inference:no_legal_authority_from_delegation
jep:non_inference:no_history_deletion_from_termination

```
jep:non_inference:no_global_downstream_termination_without_profile
jep:non_inference:no_verification_beyond_scope
jep:non_inference:no_causality_from_reference
jep:non_inference:no_absence_from_missing_event
jep:non_inference:no_target_sufficiency_from_chain_integrity
jep:non_inference:no_sufficiency_from_support
jep:non_inference:no_review_quality_from_human_review
jep:non_inference:no_lawfulness_from_policy_compliance
jep:non_inference:no_universal_truth_from_target_support
jep:non_inference:no_globalization_of_profile_semantics
```

Appendix B. Minimal Semantic Validation Result Example

```
{
  "event_id": "jep-event-123",
  "event_class": "V",
  "semantic_status": "semantic_valid",
  "declared_scope": "jep:scope:cryptographic_signature",
  "roles_detected": [
    "jep:role:actor",
    "jep:role:verifier",
    "jep:role:subject"
  ],
  "relations_detected": [
    "jep:relation:verifies",
    "jep:relation:references"
  ],
  "non_inference_warnings": [
    "jep:non_inference:no_verification_beyond_scope"
  ],
  "semantic_failures": []
}
```

Appendix C. Summary

This document defines semantic interoperability requirements for JEP. It ensures that independent systems can interpret JEP events consistently while avoiding over-inference.

The core principle is:

A JEP event records a declared protocol-semantic act.
It does not prove external truth, legal authority, factual correctness, target sufficiency, or complete causal history unless an applicable profile, evidence policy, domain rule, or target-support analysis establishes that result.

This document provides the minimum semantic foundation required for JEP to serve as a public accountability event layer across agent systems, audit systems, governance systems, workflow systems, and future profiles.

Author’s Address

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