Network Working Group
Internet-Draft
Intended status: Experimental
Expires: November 5, 2026

Y. Wang
Independent

May 4, 2026

JEP Profiles and Interoperability
draft-wang-jep-profiles-00

Status of This Memo

Copyright Notice

Table of Contents

JEP Profiles and Interoperability
Trust Profiles and Optional Interoperability Bindings for JEP
draft-wang-jep-profiles-00

Author: Yuqiang Wang
Intended status: Experimental
Companion draft: draft-wang-jep-judgment-event-protocol-06

Abstract

This document defines optional trust profiles and interoperability bindings for the Judgment Event Protocol (JEP). JEP-Core defines the neutral event protocol. This document defines how actor identifiers, keys, credentials, authorization context, attestations, archival systems, and chain systems can be bound to JEP events without changing JEP-Core semantics.

The profiles in this document are optional. A JEP-Core implementation MUST NOT require support for DID, VC, X.509, OAuth, RATS, blockchain anchoring, HJS, JAC, or any specific AI platform or agent framework.

Companion Drafts

This draft depends on draft-wang-jep-judgment-event-protocol-06. Conformance classes, schemas, test vectors, and reference-validator behavior are defined in draft-wang-jep-conformance-00.

1. Introduction

JEP-Core defines signed judgment events. It intentionally does not define a global identity, credential, authorization, attestation, legal, or archival framework.

Operational deployments require profile-specific rules for resolving actors, binding signing keys, checking credentials, applying authorization context, validating attestations, preserving archival evidence, and composing chains. This document provides a structured profile model and optional profiles.

---

2. Profile Principles

Profiles MUST follow these principles:

1. A profile MUST NOT redefine JEP-Core event verbs.
2. A profile MUST NOT redefine JEP-Core signature, event hash, or core validation-level semantics.
3. A profile MAY define actor identifier forms.
4. A profile MAY define key-resolution mechanisms.
5. A profile MAY define credential, attestation, authorization, archival, or chain rules.
6. A profile MUST declare security and privacy considerations.
7. A profile MUST declare whether it affects validation levels.
8. A profile MUST define failure mappings to JEP failure codes or profile-specific codes.
9. A profile SHOULD be independently implementable.
10. A profile SHOULD avoid making global legal, policy, or factual determinations unless it explicitly defines evidence rules.

---

3. Trust Profile Model

A JEP trust profile defines how a verifier resolves and evaluates identity, key, actor-binding, algorithm, revocation, and historical validity.

A trust profile specification MUST define:

- profile identifier;
- supported actor identifier forms;
- supported key identifier forms;
- key discovery mechanism;
- binding rules between who and signing keys;
- accepted algorithms;
- downgrade policy;
- key rotation handling;
- revocation handling;
- historical validation rules;
- credential or attestation dependency, if any;
- privacy considerations;
- failure-code mapping;
- conformance requirements.

A trust profile MAY define profile-specific extensions, but those extensions MUST NOT redefine JEP-Core semantics.

---

4. DID / VC Profile

4.1 Profile Identifier

jep-profile:did-vc:0

4.2 Scope

This optional profile defines how JEP events MAY interoperate with Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs).

DID and VC support is OPTIONAL. JEP-Core implementations MUST NOT require DID or VC support.

4.3 DID Binding

When who is a DID, the profile MUST define:

- supported DID methods;
- DID document resolution process;
- verification method selection;
- key controller rules;
- historical key validation;
- DID document caching;
- DID method failure handling;
- revocation or deactivation handling.

A verifier MUST reject a JEP event under this profile if the signing key cannot be bound to who according to the resolved DID document and profile policy.

4.4 VC Binding

A JEP event MAY reference a VC by:

- digest;
- URI;
- embedded object;
- Verifiable Presentation reference;
- HJS archival reference.

A VC MAY support claims about:

- actor role;
- organizational affiliation;
- authorization scope;
- certification;
- delegation capability;
- compliance status;
- human reviewer qualification;
- tool or model certification.

VC validity MUST be evaluated separately from JEP event validity. A valid VC does not automatically make a JEP event valid. A valid JEP event does not automatically make a VC claim true.

4.5 Validation Impact

A verifier under the DID/VC profile SHOULD map successful DID and credential checks to Level 2 actor-binding or Level 4 policy validation, depending on the credential role.

Credential-expired, credential-revoked, issuer-untrusted, or presentation-invalid conditions MUST be reported as profile failures.

4.6 Security and Privacy

DID resolution may reveal correlation metadata. VC references may reveal sensitive role, employment, certification, or authorization information. Digest references may be vulnerable to confirmation or dictionary attacks.

---

5. X.509 / PKI Profile

5.1 Profile Identifier

jep-profile:x509:0

5.2 Scope

This optional profile defines how X.509 certificates and PKI infrastructure MAY be used to bind who to a signing key.

5.3 Requirements

The profile MUST define:

- certificate chain validation;
- name-to-actor binding;
- key usage and extended key usage requirements;
- revocation checking;
- certificate validity at event time;
- archival validation behavior;
- algorithm policy;
- trust anchors.

5.4 Validation Impact

Successful certificate and actor binding checks MAY support Level 2

actor-binding validation. Domain, regulatory, or organizational checks remain Level 4 policy validation.

---

6. OAuth / OIDC Authorization Context Profile

6.1 Profile Identifier

jep-profile:oauth-oidc:0

6.2 Scope

This optional profile defines how OAuth or OIDC context MAY be referenced by JEP events.

OAuth or OIDC artifacts MAY support claims about:

- authorization context;
- client identity;
- resource server;
- subject;
- consent or grant context;
- token-binding evidence.

6.3 Boundary

A JEP event referencing OAuth context does not by itself prove that the underlying action was authorized. Authorization interpretation is profile-specific and policy-dependent.

---

7. RATS / Attestation Profile

7.1 Profile Identifier

jep-profile:rats:0

7.2 Scope

This optional profile defines how remote attestation evidence MAY be referenced by JEP events.

Attestation evidence MAY support claims about:

- runtime environment;
- device identity;
- model execution environment;
- secure enclave or trusted execution context;
- software measurement;
- tool invocation environment.

7.3 Boundary

RATS evidence supports environment claims. It does not prove the factual correctness of a judgment.

---

8. Local IAM Profile

8.1 Profile Identifier

jep-profile:local-iam:0

8.2 Scope

This optional profile defines how enterprise identity and access management systems MAY bind local actor identifiers to signing keys.

The profile MUST define:

- local actor namespace;
- key registry;
- role mapping;
- group or permission mapping;
- revocation handling;
- historical validation;
- audit export format.

---

9. HJS Archive and Privacy Profile

9.1 Profile Identifier

jep-profile:hjs-archive:0

9.2 Scope

This optional profile defines how HJS-like systems MAY store, receive, archive, redact, disclose, and preserve JEP events and evidence.

HJS manages:

- receipt records;
- archive-time metadata;
- retention policy;
- redaction policy;
- selective disclosure;
- privacy policy;
- evidence lifecycle;
- long-term verification context.

HJS is a companion archive/privacy/evidence profile over JEP-Core, not a replacement protocol for JEP-Core.

HJS MUST NOT redefine JEP-Core event semantics, signature semantics, event hash semantics, validation levels, or failure codes.

9.3 Receipt and Archive Times

HJS MAY add receipt time, archive time, or evidence custody metadata. These times are distinct from JEP when.

9.4 Privacy

HJS deployments SHOULD minimize disclosure and support access-controlled evidence stores, redacted logs, digest references, audience-bound disclosure, or selective-disclosure mechanisms.

---

10. JAC Chain Profile

10.1 Profile Identifier

jep-profile:jac-chain:0

10.2 Scope

This optional profile defines how JAC-like systems MAY compose JEP events into causality chains, responsibility chains, delegation paths, verification paths, and workflow accountability graphs.

JAC is a companion causality/accountability-chain profile over JEP-Core, not a replacement protocol for JEP-Core.

JAC MUST NOT redefine:

- JEP event object;
- JEP signature semantics;
- event hash semantics;
- validation levels;
- failure-code semantics.

10.3 Causal Boundary

A JEP reference does not by itself imply causality. JAC defines causal interpretation over JEP events.

A JAC chain result MUST declare:

- observed-log assumption;
- complete-log assumption, if any;
- chain reconstruction method;
- causal edge types;
- termination interpretation;
- verification-scope interpretation.

10.4 Validation Impact

JAC chain reconstruction MAY support Level 3 chain validation. Legal or organizational responsibility remains Level 4 policy validation.

---

11. Blockchain Anchoring Profile

11.1 Profile Identifier

jep-profile:blockchain-anchor:0

11.2 Scope

This optional profile defines how JEP event hashes MAY be anchored in a distributed ledger or transparency mechanism.

Blockchain anchoring is OPTIONAL and MUST NOT be required for JEP-Core conformance.

11.3 Boundary

Anchoring may support timestamping or non-equivocation evidence. It does not prove the content of a JEP event is true, lawful, complete, or policy-compliant.

---

12. AI Actor Profile

12.1 Profile Identifier

jep-profile:ai-actor:0

12.2 Scope

This optional profile defines actor-identifier conventions for AI-native actors, including:

- model actors;
- agent actors;
- tool actors;
- service actors;
- workflow actors;
- session actors;
- human-agent composites;
- organization-agent composites.

The profile MUST define how a signing key represents, controls, or attests to an AI actor.

12.3 Boundary

An AI actor identifier does not prove internal model state, intent, understanding, sentience, correctness, or factual truth.

---

13. Profile Registration Template

A profile registration SHOULD include:

- profile identifier;
- profile name;
- profile version;
- description;
- supported JEP-Core version;
- actor identifier forms;
- key resolution method;
- credential or attestation dependencies;
- algorithm policy;
- validation-level impact;
- failure-code mapping;
- security considerations;
- privacy considerations;
- change controller;
- reference implementation or test vectors, if available.

---

14. Security Considerations

Profiles can expand the trust surface. A malicious or poorly specified profile can cause actor misbinding, algorithm downgrade, credential overclaim, excessive disclosure, or false policy conclusions.

A profile MUST NOT present profile validity as global truth unless it defines external evidence rules.

---

15. Privacy Considerations

Profiles can introduce sensitive identifiers, credentials, roles, organization relationships, location data, execution measurements, or workflow metadata. Profiles SHOULD support data minimization, digest references, access-controlled evidence, redaction, and selective disclosure.

---

16. IANA / Registry Considerations

This draft requests or anticipates registries for:

- JEP trust profile identifiers;
- JEP optional profile identifiers;
- JEP profile conformance classes;
- profile-specific failure codes;
- profile-specific verification scopes.

---

17. Initial Profile Set

Initial optional profiles:

Profile	Identifier	Status
DID/VC	jep-profile:did-vc:0	Optional
X.509/PKI	jep-profile:x509:0	Optional
OAuth/OIDC	jep-profile:oauth-oidc:0	Optional
RATS	jep-profile:rats:0	Optional
Local IAM	jep-profile:local-iam:0	Optional
HJS Archive	jep-profile:hjs-archive:0	Optional
JAC Chain	jep-profile:jac-chain:0	Optional
Blockchain Anchor	jep-profile:blockchain-anchor:0	Optional
AI Actor	jep-profile:ai-actor:0	Optional

Author’s Address

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

v0.6 Direct Upgrade Note

This document is part of the JEP v0.6 draft set. The v0.6 set directly incorporates standardization structure, interoperability profiles, conformance artifacts, schemas, signed test vectors, invalid cases, and multi-language validator seeds without changing the JEP-Core narrow-waist semantics.