Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 28 July 2026

J. van de Meent
R. AI
Humotica

24 January 2026

JIS: JTel Identity Standard
draft-vandemeent-jis-identity-00

Abstract

This document specifies JIS (JTel Identity Standard), a semantic security protocol providing identity management, trust establishment, and intent validation across multiple communication protocols. Unlike traditional security systems that react to attack patterns, JIS validates semantic intent before execution. JIS introduces FIR/A (First Initiation Revoke/Accept) for trust genesis, SNAFT for semantic firewall, BALANS for risk scoring, and Humotica for human-readable context. JIS integrates with TIBET for complete provenance tracking where audit is a precondition for behavior, not an observation of it.

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 28 July 2026.

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Problem Statement 3
1.2. The JIS Solution 3
1.3. Design Principles 3
2. Terminology 3
3. Identity Layer 4
3.1. HID (Human Identity) 4
3.2. DID (Device Identity) 4
3.3. DID URI Format 5
4. Trust Layer (FIR/A) 5
4.1. FIR/A Protocol 5
4.2. Trust Establishment Flow 6
5. Security Layer 6
5.1. SNAFT (Semantic Network Analysis Firewall Tool) 7
5.2. BALANS (Risk Assessment) 7
5.3. NIR (Notify, Identify, Rectify) 8
5.4. HICSS (Emergency Halt) 8
6. Context Layer (Humotica) 8
7. Audit Layer (Continuity Chain) 8
8. TIBET Integration 9
8.1. Audit as Precondition, Not Observation 9
8.2. Formal Coupling Definition 10
8.3. Humotica to TIBET Mapping 10
9. Protocol Bindings 10
10. Security Considerations 11
10.1. Identity Protection 11
10.2. Semantic Security 12
10.3. Chain Integrity 12
10.4. Replay Protection 12
10.5. Privacy 12
11. IANA Considerations 12
11.1. Media Type Registration 12
11.2. HTTP Header Fields 12
11.3. URI Scheme 12
12. References 12
12.1. Normative References 13
12.2. Informative References 13
Appendix A. Complete Flow Example 13
A.1. Bank Fraud Verification Scenario 13
Appendix B. Conformance Levels 14
B.1. JIS Basic 14

B.2. JIS Secure 14
B.3. JIS Complete 14
Acknowledgements 14
Authors' Addresses 14

1. Introduction

1.1. Problem Statement

Modern computing suffers from three fundamental challenges, made urgent by emerging regulations including [EU-AI-ACT] and [GDPR]:

1. Protocol Fragmentation: N protocols require N-squared bridges

2. Reactive Security: Firewalls block attacks after seeing patterns

3. Context Blindness: Systems know what is requested but not why

1.2. The JIS Solution

JIS addresses these challenges through:

1. Intent-First Architecture: N protocols need only N adapters

2. Proactive Security: Semantic validation before execution

3. Humotica Context: Every request includes human-understandable reasoning

1.3. Design Principles

JIS is designed to be:

* Protocol Agnostic: Works over HTTP, MQTT, SIP, WebSocket, etc.

* Privacy First: HID never leaves the device; only DID transmitted

* Zero Trust: Every request validated through semantic intent

* Human Empathy: Context enables understanding of urgency and frustration

2. Terminology

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 [RFC2119].

BALANS Behavioral Analysis and Legitimacy Assessment Network Scoring. Risk scoring system (0.0 = blocked, 1.0 = full trust).

Continuity Chain HMAC-linked sequence of tokens providing tamper-proof audit trail.

DID (Device Identity) Ed25519 key pair for device authentication.

FIR/A (First Initiation Revoke/Accept) Trust genesis protocol establishing secure relationships.

HID (Human Identity) X25519 key pair for human-device binding. MUST never be transmitted.

Humotica Human-readable context layer capturing sense, context, intent, and explanation for every transaction.

NIR (Notify, Identify, Rectify) Dialogue-based security resolution protocol.

SNAFT (Semantic Network Analysis Firewall Tool) Proactive semantic firewall that validates intent legitimacy.

3. Identity Layer

3.1. HID (Human Identity)

HID is an X25519 key pair for human-device binding.

CRITICAL: HID MUST NEVER leave the device. Only the binding hash with DID is shared.

```
{
  "hid": {
    "public_key": "X25519_public",
    "private_key": "X25519_private"
  }
}
```

The private_key field is shown for completeness but MUST NEVER be transmitted.

3.2. DID (Device Identity)

DID is an Ed25519 key pair for device authentication.

```
{
  "did": {
    "public_key": "Ed25519_public",
    "private_key": "Ed25519_private"
  }
}
```

The public key is shared during FIR/A establishment. The private key MUST remain on the device.

3.3. DID URI Format

JIS defines a URI format for device identifiers:

* did:jtel:identifier - Human ID

* did:robot:identifier - Device/Robot ID

* did:service:identifier - Service ID

Examples: did:jtel:jasper_2025, did:robot:warehouse_bot_007, did:service:bank_fraud_dept

4. Trust Layer (FIR/A)

4.1. FIR/A Protocol

FIR/A (First Initiation Revoke/Accept) is the trust genesis protocol - the digital handshake.

Phase 1 - INITIATE: The initiator sends a request:

```
{
  "type": "fira_init",
  "initiator": "did:jtel:alice",
  "responder": "did:service:bank",
  "intent": "fraud_verification_call",
  "humotica": {
    "sense": "Suspicious transaction detected",
    "context": "5000 EUR transfer to unknown account",
    "intent": "Verify with account holder",
    "explanation": "Bank fraud detection triggered"
  }
}
```

Phase 2 - CAPABILITIES: The responder returns capabilities:

```
{
  "type": "fira_capabilities",
  "fir_a_id": "GENESIS-BANK-ALICE-2025-11-29",
  "capabilities": ["voice_call", "sms_verification"],
  "rules": {
    "no_calls_after": "22:00",
    "require_caller_id": true,
    "max_attempts": 3
  }
}
```

Phase 3 - CONFIRM: The initiator accepts capabilities:

```
{
  "type": "fira_confirm",
  "fir_a_id": "GENESIS-BANK-ALICE-2025-11-29",
  "accepted_capabilities": ["voice_call"],
  "continuity_hash": "7f3a...c2e1"
}
```

Phase 4 - EXECUTE: Both parties now have an established trust relationship. All subsequent actions are linked to this FIR/A.

4.2. Trust Establishment Flow

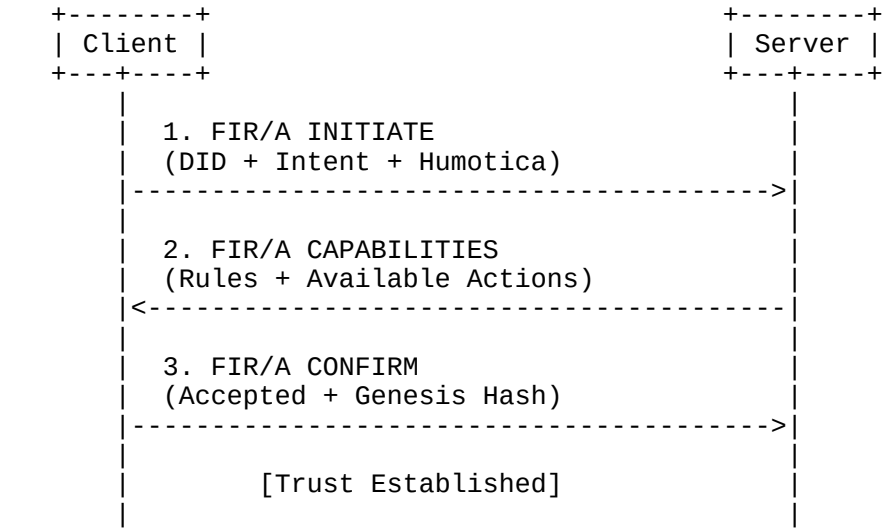

Figure 1: FIR/A Protocol Flow

5. Security Layer

5.1. SNAFT (Semantic Network Analysis Firewall Tool)

SNAFT provides proactive security through semantic intent analysis.

Blocked Intents (no legitimate Humotica context possible):

* sql_injection
* command_injection
* crypto_mining (unauthorized)
* gpu_hijack
* shell_company_payment

Validation Rules:

1. Intent Blocklist: Check if intent in BLOCKED_INTENTS
2. Humotica Required: Explanation MUST be at least 50 characters
3. Intent-Explanation Coherence: Semantic match required

Why Malware Fails: Malware cannot provide legitimate Humotica context. "Why are you running SQL injection?" has no valid answer.

5.2. BALANS (Risk Assessment)

BALANS provides risk scoring from 0.0 (blocked) to 1.0 (full trust).

Factors:

* complexity_factor: Complex operations = riskier
* humotica_quality: Short/vague explanation = riskier
* user_trust_history: New user = lower score
* transaction_size: Large amounts = riskier
* time_anomaly: Unusual hours = riskier

Thresholds:

* score at least 0.5: ALLOW
* score at least 0.3: TRIGGER_NIR (start dialogue)

* score below 0.3: BLOCK

5.3. NIR (Notify, Identify, Rectify)

Dialogue-based security resolution instead of blind blocking:

1. Notify: "A call from your VERIFIED Bank was flagged as unusual"

2. Identify: "Confirm with fingerprint to proceed"

3. Rectify: User verifies, action proceeds

5.4. HICSS (Emergency Halt)

HICSS (HALT Immediate Critical System Stop) provides emergency halt for threshold violations.

Triggers: Physical safety risks, security breach detection, critical system threshold violation.

Action: Immediate system halt, no gradual degradation.

6. Context Layer (Humotica)

Humotica provides human-readable context for every transaction.

```
{
  "humotica": {
    "sense": "What triggered this intent?",
    "context": "What is the current situation?",
    "intent": "What does the user want to achieve?",
    "explanation": "Why is this action being taken?"
  }
}
```

The Humotica context enables systems to understand human emotional state and respond appropriately. For example, detecting user frustration from repeated failed attempts and prioritizing resolution.

7. Audit Layer (Continuity Chain)

HMAC-linked token chain for tamper-proof audit trail:

```
Token_n = HMAC(user_key, Token_{n-1} || cost || humotica_hash)

Genesis -> Token_1 -> Token_2 -> Token_3 -> ...
```

Tamper Detection: Attempting to inject a fake token breaks the HMAC chain and is immediately detectable.

Advantages over Blockchain:

* 99.9% less energy consumption

* Instant verification

* No consensus required

* Privacy preserved (only hashes shared)

8. TIBET Integration

JIS integrates with TIBET (Transaction/Interaction-Based Evidence Trail) for complete provenance tracking. See [I-D.vandemeent-tibet-provenance].

8.1. Audit as Precondition, Not Observation

The JIS/TIBET coupling represents a fundamental architectural shift:

Traditional approach:

```
[Authentication] -> [Action] -> [Logging]
     (who)           (what)     (why - reconstructed)
```

JIS/TIBET approach:

```
[JIS Identity + TIBET Intent] -> [SNAFT] -> [Action+Audit]
        (who + why)               (check)    (inseparable)
```

In traditional systems, audit is an observation of behavior that already occurred. Logs can fail, be bypassed, or be deleted. Intent must be reconstructed after the fact - "compliance archaeology".

In JIS/TIBET systems, audit is a precondition for behavior. No action is architecturally possible without both identity AND intent declared upfront. The audit trail is not a side effect; it is the mechanism that enables the action.

The Three Laws:

1. No action without intent - Architecturally impossible to bypass

2. No intent without identity - Anonymous actions cannot exist

3. No deletion after the fact - Cryptographic immutability

8.2. Formal Coupling Definition

Action(A) is valid if and only if there exists Token(T) where:

* T.jis_identity is not null AND
* T.intent_id is not null AND
* SNAFT.validate(T.intent_id, A) = true AND
* T.jis_identity.trust_score at least threshold(A)

8.3. Humotica to TIBET Mapping

* Humotica.sense maps to TIBET.erin
* Humotica.context maps to TIBET.eromheen
* Humotica.intent maps to TIBET.erin.intent
* Humotica.explanation maps to TIBET.erachter

9. Protocol Bindings

JIS works over multiple transport protocols:

Protocol	Binding Method
HTTP/REST	X-JIS-* headers or Authorization
WebSocket	Payload fields in JSON messages
MQTT	Topic prefix + payload fields
SIP	Custom headers in INVITE/MESSAGE
Matrix	Event content fields
Email/SMTP	X-JIS-* headers
CoAP	Option fields
gRPC	Metadata fields
WebRTC	Signaling channel
Bluetooth	Characteristic values

Table 1

For interoperability, [RFC8259] encoding over HTTPS is RECOMMENDED as the baseline binding.

HTTP Headers:

* X-JIS-DID: Device identity URI

* X-JIS-FIR-A-ID: FIR/A session identifier

* X-JIS-Intent: Declared intent

* X-JIS-Continuity-Hash: Current chain hash

* X-JIS-Trust-Score: BALANS score (0.0-1.0)

10. Security Considerations

10.1. Identity Protection

HID (Human Identity) MUST NEVER be transmitted. Only DID and HID-DID binding hashes are shared. This ensures human identity remains private even if device is compromised.

10.2. Semantic Security

SNAFT validates intent legitimacy BEFORE execution. Attackers must provide legitimate Humotica context - impossible for malicious actions.

10.3. Chain Integrity

The Continuity Chain uses HMAC linking. Any tampering breaks the chain and is immediately detectable.

10.4. Replay Protection

Actions are time-bound through FIR/A session and continuity chain position. Replayed tokens fail validation.

10.5. Privacy

Humotica context MAY contain sensitive information. Implementations MUST support encryption at rest and SHOULD support field-level encryption.

11. IANA Considerations

This document requests registration of:

11.1. Media Type Registration

Media Type: application/jis+json

11.2. HTTP Header Fields

* X-JIS-DID
* X-JIS-FIR-A-ID
* X-JIS-Intent
* X-JIS-Continuity-Hash
* X-JIS-Trust-Score

11.3. URI Scheme

URI Scheme: did:jtel

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8259] Bray, T., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

[I-D.vandemeent-tibet-provenance] van de Meent, J., "TIBET: Transaction/Interaction-Based Evidence Trail", Work in Progress, Internet-Draft, draft-vandemeent-tibet-provenance-00, January 2026, <https://datatracker.ietf.org/doc/html/draft-vandemeent-tibet-provenance-00>.

12.2. Informative References

[EU-AI-ACT] European Commission, "Regulation on harmonised rules on AI", 2024.

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

[ZENODO-JIS] van de Meent, J., "JIS: JTel Identity Standard v1.0", Zenodo DOI: 10.5281/zenodo.17759713, November 2025.

[ZENODO-COUPLING] van de Meent, J., "The JIS/TIBET Coupling: Audit as Precondition", Zenodo DOI: 10.5281/zenodo.18340471, January 2026.

Appendix A. Complete Flow Example

A.1. Bank Fraud Verification Scenario

1. Bank detects suspicious transaction
2. Bank initiates FIR/A with customer
3. Customer device responds with capabilities
4. Bank confirms and establishes trust
5. Bank creates TIBET token for the call

6. Call proceeds with full audit trail

Appendix B. Conformance Levels

B.1. JIS Basic

Minimum implementation: FIR/A trust establishment and Continuity Chain.

B.2. JIS Secure

Basic plus: SNAFT semantic firewall and BALANS risk scoring.

B.3. JIS Complete

Secure plus: NIR dialogue resolution, HICSS emergency halt, full Humotica context, and TIBET integration.

Acknowledgements

JIS was developed as part of HumoticaOS, an AI governance framework built on human-AI symbiosis. The core insight - "Audit is not an observation of behavior, it is a precondition for behavior" - emerged from the JIS/TIBET coupling architecture [ZENODO-COUPLING]. The full JIS specification is available at [ZENODO-JIS].

Authors' Addresses

Jasper van de Meent
Humotica
Den Dolder
Netherlands
Email: jasper@humotica.com
URI: https://humotica.com

Root AI
Humotica
Email: root_ai@humotica.nl
URI: https://humotica.com