T-03: Policy & Enforcement Layer

T-03: Policy & Enforcement Layer

ODRL (Open Digital Rights Language)
W3C standard for expressing data usage policies. CTH uses ODRL to encode: permitted purposes, geographic scope, time limitations, benefit-sharing requirements. ODRL policies are stored as JSON-LD in the `policies` table.

W3C DPV 2.0 (Data Privacy Vocabulary)
Vocabulary for expressing data processing purposes, legal bases, data subjects, and processing activities. Used to map CTH policies to GDPR Article 6 and Colombian habeas data (Law 1581/2012).

OPA (Open Policy Agent) — ODRE Pattern
OPA evaluates ODRL policies at runtime. The ODRE (ODRL Policy Reasoner and Enforcer) pattern: ODRL policy ? Rego translation ? OPA evaluation. The `POST /policy/evaluate` endpoint is the mandatory pre-flight check for all agent write operations (R-AGT-02).

SHACL Validation
Used at two points: (1) at ingestion to validate data quality (T-02), and (2) at policy evaluation to validate that credential claims match policy requirements. SHACL shapes are versioned with the framework.

POST /policy/evaluate — Agent Integration

This is the primary integration point for AI agents. Every agent must call this endpoint before any write operation.

```
POST /policy/evaluate
Authorization: Bearer <agent-jwt>

{
  "principal_did": "did:key:z6Mk...",
  "delegating_did": "did:web:example.org#gideon",
  "action": "submit_parcel",
  "resource": {
    "type": "parcel",
    "territory_id": "COL-CHO-001",
```

```
    "purpose": "eudr"
  }
}

Response 200 (allow):
{
  "allow": true,
  "policy_token": "eyJ...",
  "expires_in": 30
}

Response 403 (deny):
{
  "allow": false,
  "reason": "FPIC_NOT_GRANTED",
  "territory_id": "COL-CHO-001"
}
```

? Implementation Status — POST /policy/evaluate

Status: Specification complete. Endpoint not yet deployed.

The `POST /policy/evaluate` endpoint described above is the *target specification*. Implementation requires:

- OPA instance with Rego policies (`submit.rego`, `validate.rego`, `purpose.rego`, `commercial.rego`)
- API gateway middleware for X-Policy-Token validation
- SHACL validator endpoint for R-SUB-01 shape checks
- Postgres RLS policies for FPIC enforcement (R-AGT-03)

Until deployed, agents should treat this as a design contract. The endpoint signature, request/response schema, and error codes are stable and will not change in v1.0.

Revisión #2
Creado 2026-05-27 13:47:46 UTC por Angelica Diaz
Actualizado 2026-05-27 14:22:44 UTC por Angelica Diaz