Technical Standards Stack

- Standards Overview
- T-01: Identity & Credential Layer
- T-02: Provenance & Quality Layer
- T-03: Policy & Enforcement Layer
- T-04: Discovery & AI Access Layer

Standards Overview

7-Layer Technical Standards Stack

The framework uses a layered architecture where each layer has a specific, non-overlapping responsibility. No single existing standard covers the full pipeline — the stack was assembled to fill real gaps in LATAM climate data governance.

#	Layer	Standards	Purpose	CTH Contribution / Notes
1	**Identity**	W3C DID 1.1 + cth:FPICCredential	Who is acting	CTH-original: FPICCredential as W3C VC
2	**Credential Format**	W3C VC 2.0 (BBS+) + UNTP DTE/DCC + OID4VP	What is asserted	UNTP maps directly to EUDR Article 9
3	**Provenance & Quality**	W3C PROV-O + ISO 8000-220:2025 + cth:FieldDataQuality SHACL	How was it measured	CTH-original: EUDR GPS precision + Andean IoT calibration rules
4	**Governance Ledger**	Append-only Postgres + rolling SHA-256 + KERI anchoring	What decisions were made	5-year persistence; KERI for cross-org verifiability
5	**Policy & Enforcement**	ODRL + W3C DPV 2.0 + OPA (ODRE pattern) + SHACL	What is allowed	ODRE = ODRL policy evaluated by OPA at runtime
6	**Discovery & AI Access**	W3C DCAT v3 + OpenAPI 3.1 + llms.txt + JSON-LD context	How to find and query	llms.txt enables direct agent access without scraping
7	**Compliance Outputs**	EUDR DDS, CSRD ESRS E1/E4, CBAM, ISSB IFRS S2, Art.6	What gets reported	One data pipeline ? five regulatory outputs

CTH-Original Contributions

Two standards were created by CTH because no existing specification covers these requirements for LATAM:

> **cth:FPICCredential**
> Free Prior and Informed Consent as a W3C Verifiable Credential. The community holds the signing key — not CTH, not the coffee buyer. Revocation is handled by the community. No existing VC type covers FPIC for indigenous territorial data in Colombia.

cth:FieldDataQuality SHACL Profile
SHACL validation shapes for EUDR-specific GPS precision (?6 decimal places), IDEAM deforestation data vintage (?24 months), IoT sensor calibration (?180 days), and Andean GPS lock wait time (?90 seconds per polygon vertex). ISO 8000-220 covers data quality generically — none of these field-specific thresholds exist in any standard.

?? The Article 6 / EUDR shared evidence layer is the key commercial innovation: the same UNTP Digital Traceability Event (DTE) that proves deforestation-free status for EUDR serves as the shared evidence layer for an Article 6.4 carbon credit. Two Digital Conformity Credentials (EUDR DDS + carbon credit) against one DTE.

T-01: Identity & Credential Layer

T-01: Identity & Credential Layer

W3C DID 1.1
Decentralized Identifiers. Every participant (human, organisation, AI agent, IoT sensor) has a DID. CTH uses `did:web` for organisations and `did:key` for ephemeral agent sessions.

cth:FPICCredential (CTH-original)
A W3C VC 2.0 credential encoding Free Prior and Informed Consent. Fields: `territoryId` (links to official IGN cadastral ID), `permittedPurposes[]` (e.g. ['eudr','csrd']), `benefitSharingTerms` (hash of signed agreement), `revocable: true`. The community council holds the signing key — stored in their own HSM or managed key service, not CTH infrastructure.

W3C VC 2.0 with BBS+ Selective Disclosure
Verifiable Credentials allow coffee buyers to prove EUDR compliance without revealing GPS coordinates to competitors. BBS+ signatures enable selective disclosure — present only the fields the verifier needs.

OID4VP (OpenID for Verifiable Presentations)
Presentation protocol used by the compliance export API. EU customs systems can request a Verifiable Presentation containing only the EUDR-relevant fields, verified against the issuer DID.

Credential Type	Issued By	Held By	Expires	Revocable
cth:SubmitterCredential	CTH Accreditation Svc	Data Submitter	12 months	Yes — by CTH Steward
cth:ValidatorCredential	CTH Accreditation Committee	Accredited Validator	24 months	Yes — by Governance Board
cth:CommunityCredential	CTH + Community Council	Community Sovereign	Indefinite	Yes — by Community only
cth:StewardCredential	Governance Board	CTH Staff Member	12 months	Yes — by Board vote
cth:AuditorCredential	CTH (on regulatory mandate)	Regulator	Audit scope only	Yes — auto-expires
cth:AgentCredential	Delegating human DID	AI Agent / Script	Human session	Yes — immediate

T-02: Provenance & Quality Layer

T-02: Provenance & Quality Layer

W3C PROV-O
The W3C Provenance Ontology. Every data submission, validation event, and agent action is recorded as a PROV-O graph: `prov:Entity` (the data), `prov:Activity` (what happened), `prov:Agent` (who did it), `prov:wasGeneratedBy`, `prov:wasAttributedTo`.

ISO 8000-220:2025 — Data Quality
International standard for data quality management. Used for metadata quality dimensions: completeness, accuracy, consistency, timeliness. CTH maps these to field-specific thresholds in the SHACL profile.

cth:FieldDataQuality SHACL Profile (CTH-original)
SHACL shapes that enforce EUDR-specific and Andean-specific quality rules at ingestion. Key shapes:

Shape	Rule	Rationale
cth:GpsPrecision	Polygon vertices must have ?6 decimal place precision	EUDR Article 9 requires parcel identification; 5dp = ~1m accuracy; 6dp = ~10cm
cth:DeforestationDataVintage	IDEAM reference raster must be ?24 months old	EUDR requires current deforestation status; stale data invalidates DDS
cth:IotCalibration	IoT soil/weather sensors must have calibration certificate ?180 days old	Sensor drift; CSRD ESRS E4 requires traceable measurement
cth:AndeanGpsLock	GPS receiver must record ?90 second lock wait per polygon vertex	Mountain terrain + tree canopy causes GPS multipath error; 90s reduces error below EUDR threshold

Ledger Integrity

The governance ledger is an append-only Postgres table with rolling SHA-256 hashes. Each entry hashes the previous entry's hash (blockchain-like chain). KERI (Key Event Receipt Infrastructure) anchoring is used for cross-organisational verifiability — validators can independently verify ledger integrity without trusting CTH's infrastructure.

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.

T-04: Discovery & AI Access Layer

T-04: Discovery & AI Access Layer

W3C DCAT v3 (Data Catalog Vocabulary)
Dataset catalogue standard. CTH publishes a DCAT v3 catalogue at `/api/catalogue` listing all available climate datasets, their access conditions, formats, and ODRL usage policies. Registered with Google Dataset Search.

OpenAPI 3.1
Full API specification at `/api/openapi.json`. All endpoints documented with: security schemes (DID-based JWT), request/response schemas (JSON-LD), error codes, policy evaluation requirements. Enables direct agent integration without documentation scraping.

llms.txt
Machine-readable index at `https://wiki.cleantechhub.net/llms.txt` (and `/llms-full.txt`). Lists all framework pages with their purpose, so AI agents can navigate the wiki without embedding the full content. Updated automatically when framework pages change.

JSON-LD Context
Every framework concept (role, rule, credential type, standard) has a JSON-LD term at `https://vocab.cleantechhub.net/climate/`. Enables semantic interoperability with other climate data systems (e.g. UNTP registry, EU Commission linked data).

Agent Access Pattern

Recommended pattern for an AI agent integrating with the framework:

1. Fetch `/llms.txt` to identify relevant framework sections
2. Read specific wiki pages via BookStack API (read-only, no credential required for public pages)
3. Request a delegated `cth:AgentCredential` from the delegating human's session
4. Call `POST /policy/evaluate` with the intended action
5. If `allow: true`, proceed with the action using the policy token
6. PROV-O record is auto-generated by the API gateway (no agent action required)