Roles & Permissions

Role Taxonomy Overview

Role Taxonomy

Six roles. Each is bounded by a credential. AI agents are first-class participants.

Roles & Permissions · R-00

Every actor in the framework — human, organisation, or AI agent — operates under one of six defined roles. Roles are not just labels: each role is a Verifiable Credential issued by CTH (or by the community for the Sovereign role) that gates API permissions. You cannot perform an action without the credential that authorises it.

Permissions Matrix

Permission	Submitter	Validator	Sovereign	Steward	Auditor	AI Agent
Submit polygon / emissions data	? Own data	—	—	—	—	? If delegated by Submitter
Issue VALIDATED event / DCC	—	?	—	—	—	? If delegated by Validator
Issue / revoke FPIC credential	—	—	?	—	—	—
Read own submitted data	?	?	? (own territory)	?	? Public only	? Delegated scope
Read all non-restricted data	—	?	? Own territory	?	? Public only	? Public scope
Manage schemas / framework	—	—	—	?	—	—
Call POST /policy/evaluate	?	?	?	?	?	? Mandatory before write
Override FPIC consent block	? Never	? Never	N/A	? Never	? Never	? Never

Key principle: An AI agent inherits the permissions of the human role that delegated it — never more. An agent acting for a Submitter can write polygon data but cannot validate it. Agents cannot combine permissions from multiple delegating roles.

Data Submitter

?

Data Submitter

SUBMITTER

Who holds this role: Coffee cooperatives, smallholder farmers, IoT sensor operators, KoboToolbox field agents

? Permitted Actions

- Submit parcel GPS polygons via KoboToolbox or direct API
- Attach evidence documents (photos, invoices, lab certificates)
- View own submission status and validation results
- Request data deletion for own submissions

? Prohibited Actions

- Validate other parties' data
- Access other submitters' raw data
- Modify or delete after ledger entry
- Override FPIC flags

Required Credential: `cth:SubmitterCredential`

Issued after identity verification + GDPR/habeas-data consent; expires 12 months; renewable

Accredited Validator

?

Accredited Validator

VALIDATOR

Who holds this role: IDEAM-certified labs, SGS/Bureau Veritas auditors, satellite data providers (Planet, Mapbiomas), academic partners

? Permitted Actions

- Cryptographically sign validation results as W3C VC 2.0 assertions
- Issue Digital Conformity Credentials (UNTP DCC)
- Access raw submission data for assigned parcels
- Flag data quality issues; trigger R-SUB-03

? Prohibited Actions

- Self-certify own submissions
- Access data outside assigned scope
- Modify ledger entries after signing
- Issue credentials outside accreditation scope

Required Credential: `cth:ValidatorCredential`

Issued by CTH Accreditation Committee; requires ISO 17025 or equivalent; 2-year term; public registry

Community Sovereign

?

Community Sovereign

SOVEREIGN

Who holds this role: Indigenous territorial councils (cabildos), Afro-Colombian community boards (consejos comunitarios), campesino associations with collective land title

? Permitted Actions

- Grant or revoke FPIC for territory-level data collection
- Set purpose limitations on community data (e.g. EUDR only, no carbon market use)
- Require benefit-sharing terms before validator access
- Audit all uses of community data at any time

? Prohibited Actions

- Submit individual parcel data (use Data Submitter role)
- Override individual member consent
- Transfer sovereignty credential to another entity without community resolution

Required Credential: `cth:CommunityCredential`

Issued after verification of legal collective title or territorial recognition; held by council secretary; multi-sig (3-of-5 council members) for revocation. The Community Sovereign's FPIC block is structural — enforced at Postgres row-level security below OPA. No board vote, no emergency patch, no API call can override it. This is non-negotiable.

CTH Data Steward

??

CTH Data Steward

STEWARD

Who holds this role: CleantechHUB staff members with explicit stewardship assignment (not all CTH staff)

? Permitted Actions

- Manage framework configuration and standards versions
- Onboard and offboard validators (with Governance Board approval)
- Execute emergency patches (R-CHG-03) within 48h window
- Run compliance exports (EUDR DDS, CSRD reports)
- Access all data for governance purposes only

? Prohibited Actions

- Use data for CTH commercial purposes
- Override FPIC blocks
- Approve own stewardship actions without peer review
- Modify ledger entries

Required Credential: `cth:StewardCredential`

Issued internally; requires Governance Board nomination; logged access; annual review

Regulator / Auditor

?
Regulator / Auditor

AUDITOR

Who holds this role: EU customs authorities (EUDR), DIAN (Colombia), ANLA, IDEAM, financial supervisors (CVM, CNBV), carbon registry auditors

? Permitted Actions

- Read-only access to compliance packages (EUDR DDS, CBAM declarations, CSRD reports)
- Verify ledger integrity via rolling SHA-256 hashes
- Request data lineage traces for specific parcels
- Receive automated compliance alerts

? Prohibited Actions

- Access raw submissions beyond compliance package scope
- Request personal data beyond what's in compliance outputs
- Modify any data or metadata

Required Credential: `cth:AuditorCredential`

Issued upon presentation of official regulatory mandate; time-limited to audit scope; zero data retention after audit closes

AI Agent

?

AI Agent

AGENT

Who holds this role: Claude instances, automated pipeline scripts, Pipedream workflows, any non-human principal acting on behalf of a credentialed human

? Permitted Actions

- Submit data on behalf of delegating human (inherits human's permissions only)
- Read permitted datasets for analysis
- Call POST /policy/evaluate before any write operation
- Generate PROV-O provenance records for every action

? Prohibited Actions

- Hold independent credentials (credential must be delegated from a human DID)
- Exceed the permission scope of the delegating human
- Bypass POST /policy/evaluate
- Take any action when FPIC block is active — absolute prohibition

Required Credential: `cth:AgentCredential (delegated from human DID)`

Agent inherits the delegating human's DID permissions — never more. Every agent action creates a PROV-O record naming the delegating human DID and the agent ID. FPIC block is enforced at DB row-level security — OPA never even sees the request.