# Global Consent Ledger – Distributed Trust Anchoring & Sovereign Federation Registry

Version: 4.1 | Classification: CTO-Mandatory | Language: EN

Scope: Sovereign countermeasure against centralized trust monopolies and unauthorized governance forks

## 0. Purpose & Enforcement Context

This module defines the Global Consent Ledger (GCL), a sovereign anchoring and federation validation layer for MaxOneOpen v4.1. It ensures that no governance authority, trust issuer, or rule enforcer can gain system-wide control without documented cross-consent by sovereign roles, audit authorities, and governance participants. It is designed to neutralize soft takeover vectors and prevent unilateral rule propagation in OSS, public sector, or supranational deployments.

## 1. Consent Capsule Structure & Federation Signature

Each trust-affecting entity (issuer, validator, global enforcer) must register a `Consent Capsule (CC)`:  
`{ entity\_id, role\_scope, trust\_tier\_range, jurisdiction, federation\_signatures[], timestamp }`  
Federation Signatures include:  
- Sovereign Audit Nodes  
- CTO-certified Federation Anchors  
- Role-specific Consent Nodes  
Each Consent Capsule is replay-anchored, ledger-bound (Module 13), and visible to all consent-verifying modules.

## 2. Consent Ledger Chain & Anchor Policy

The GCL is a parallel ledger segment with:  
- independent hash chain of Consent Capsules  
- visibility into fork state and trust spread  
- anchored linkage to Module 13 Ledger Root Capsule  
Consensus policies:  
- Minimum 3-of-N federation signatures  
- Geographic or jurisdictional diversity (configurable)  
- Ledger review quorum logic for high-scope authority capsules

## 3. Unauthorized Authority Detection & Alert Capsule

Any governance or trust entity acting outside GCL scope will trigger:  
- `Consent Violation Capsule (CVC)`  
- system-wide alert with hash conflict reference  
- mandatory certification downgrade (Module 17)  
- auto-lock of offending entity in runtime policy engine  
GCL-integrated audits will automatically expose signature inconsistency or false claims of global authority.

## 4. Federation Registry & Role Scope View

A system-wide registry of participating sovereign actors includes:  
- Federation Entity ID  
- Role Type and Trust Boundaries  
- Consent History  
- Signature Validation State  
Audit tools (Module 14) can render a current and historical scope matrix per entity or federation zone.

## 5. CTO Binding & System Certification Prerequisite

The GCL is a non-optional requirement for any MaxOneOpen v4.1 instance operating across jurisdictional domains, with multiple policy issuers, or in OSS governance roles. Its absence invalidates sovereign certification scope, trust plurality, and fork legitimacy. Module 17 must verify GCL presence, replay depth, and anchor validation before issuance of any certification capsule.