# Module XX – Federated Consent Anchoring Layer

Version: 4.1 | Classification: CTO Mandatory (Governance Extension)

Scope: Multi-CTO trust coordination, ledger anchoring across domains, parallel federation governance

## 0. Purpose & Sovereign Federation Goal

This module extends the Global Consent Ledger to support multi-CTO and federated operational models, where multiple sovereign actors share governance responsibilities. It defines mechanisms to declare, isolate, synchronize and audit overlapping trust boundaries and ensure shared capsule legitimacy across distributed jurisdictions. It is required in any deployment where two or more independent actors co-govern shared capsule chains or forkable execution environments.

## 1. Federated Consent Capsule & Scope Map

Each federation emits a `Federated Consent Capsule (FCC)`:  
`{ federation\_id, zone\_map[], consent\_participants[], trust\_boundary[], sync\_mode, conflict\_response\_mode, anchor\_hash, timestamp }`  
- `zone\_map[]`: trust zone IDs and scope authority  
- `sync\_mode`: e.g. quorum\_based, parallel\_signoff, delegate\_anchor  
- `conflict\_response\_mode`: ledger\_priority, audit\_dispute, capsule\_split  
All FCCs are embedded in the Consent Ledger and bound to anchor policies.

## 2. Cross-Domain Trust Sync & Fork Isolation

Each capsule entering the shared execution ledger must pass:  
- boundary check against all FCC trust zones  
- capsule re-signature from authorized federation anchors  
- fork split logic based on declared fork anchors and path deviation thresholds  
- ledger duplication validation to avoid audit drift  
Capsules violating multi-CTO enforcement must be routed to `Federation Violation Capsule (FVC)`.

## 3. Parallel Governance & Reconciliation Logic

When capsule policy conflicts occur across federated nodes:  
- replay both chains from last shared FAC (Fork Anchor Capsule)  
- enter Dispute Protocol or Consensus Suspension State (CSS)  
- emit `Federation Reconciliation Capsule (FRC)` documenting all forks, deltas, and rejected chains  
Audit roles are required to review FRCs before any re-certification (Module 17).

## 4. Ledger Anchoring & Cross-Federation Export Capsule

Each federation may export its anchor state into a public ledger overlay:  
- via `Federation Anchor Capsule (FAC)` with confirmed zones and capsule log  
- including capsule hashes, FAC linkage, GCL reference, and trust attestation  
Exported overlays must include machine-verifiable capsule trail and trust transitions.

## 5. Certification Implication & Role Enforcement

Systems using this layer must include:  
- at least 3 certified roles with trust separation per federation  
- runtime governance review checkpoints per capsule stream  
- ledger replication audit window per zone  
- capsule dispute fallback paths  
Absence of this module in federated systems invalidates certification eligibility above Tier 3.