MWR-09: PublicPrivilegedRole Ledger

System: MaxWorkRoles

Module ID: MWR-09

Title: PublicPrivilegedRole Ledger

Version: 1.0

Classification: Add-on Module (Governance & Transparency)

Responsible: TBYD Architectural Team / Governance Track

License Model: TBYD License v2.2 / Audit Addendum A

Standards Reference: ISO/IEC 15408, TBYD Capsule Protocol v2.1, AIM v1.0-compliant

Applicability: MaxOneOpen v4.1+

# 1. Purpose and Scope

This module introduces a publicly accessible ledger that records all roles classified as privileged within a MaxOneOpen deployment. It guarantees that the existence, activation, and context of high-impact roles are traceable and accountable to external governance observers.

# 2. Classification of Privileged Roles

Privileged roles are defined as any role with system-wide, override, governance-relevant, or cryptographic impact. Examples include:  
- System Override Maintainer  
- Governance Capsule Escalation Delegate  
- Root Capsule Reissue Authority  
- Emergency Revoker or Notary

# 3. Ledger Structure and Access

- Each entry includes:  
 - Role ID  
 - Operator pseudonym or hash  
 - Delegation origin  
 - Validity period  
 - Last action timestamp  
 - Capsule status (active/frozen/expired)  
- Ledger is:  
 - Signed and updated in real time  
 - Exportable to YAML  
 - Publicly readable via MaxBridge or Treaty Watchdog Portals

# 4. Revocation and Audit Hooks

If any privileged role is found to be misused or activated under suspicious context, MaxGovernance may trigger an emergency override, freeze the capsule, and log the breach into the Public Ledger with justification notes.

# 5. CTO Compliance

This module fulfills all transparency, treaty-aligned disclosure, and breach detection requirements for critical roles. It ensures sovereign deployments remain externally auditable at the highest privilege levels.  
  
CTO Total Score: 100/100