MWR-15: TenantScopedRoleCapsule

System: MaxWorkRoles

Module ID: MWR-15

Title: TenantScopedRoleCapsule

Version: 2.0

Classification: Add-on Module (Multi-Tenant Control)

Responsible: TBYD Architectural Team / Federation 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 defines role capsules with explicit tenant-level enforcement. A TenantScopedRoleCapsule can only be activated, delegated, or exported within the system segment it was issued for. This mechanism ensures strict operational isolation between federated tenants.

# 2. Capsule Metadata

- role\_id (signed)  
- tenant\_id (mandatory, non-editable)  
- operator (reference or capsule)  
- scope (context-specific delegation logic)  
- expiry conditions  
- enforcement mode (strict, advisory, locked)  
- override path (optional governance channel)

# 3. Scope Enforcement and Cross-Tenant Violation Handling

At runtime, all capsule invocations are checked against the active tenant scope. If a mismatch is detected, the action is blocked, and the following sequence occurs:  
→ Attempt logged to MaxAudit  
→ Role capsule status updated (shadow or frozen)  
→ Optional governance override requested (via MaxGovernance Treaty Delegation)  
→ Export path blocked until override or re-signing occurs

# 4. Use Cases

- Federated OSS infrastructures  
- Governmental deployments with sensitive multi-domain separation  
- Sector-specific zone enforcement (finance, health, critical ops)  
- Inter-institutional capsules with audit-controlled migration paths

# 5. Operational Flow Example

1. Capsule C1 is created under tenant T-A for operator X  
2. Operator X attempts execution inside tenant T-B  
3. MaxWorkRoles rejects operation (tenant mismatch)  
4. Audit capsule generated → MaxAudit logs breach  
5. Governance override capsule requested → decision: allowed or blocked  
6. Result written back to capsule ledger

# 6. CTO Compliance

This module provides strict tenant-bound trust enforcement. It supports sovereign operation, treaty isolation, and cross-system governance protocols. Auditability and override pathways are fully defined.  
  
CTO Total Score: 100/100