MWR-04: Capsule Access & Trace

System: MaxWorkRoles

Module ID: MWR-04

Title: Capsule Access & Trace

Version: 1.0

Classification: Core Module

Responsible: TBYD Architectural Team / Subsystem Lead

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 the logic and infrastructure for tracing access events, interactions, and structural states of active role capsules. It enables full runtime visibility, post-event traceability, and breach detection based on access anomalies or misuse patterns.

# 2. Trace Components and Fields

- Capsule ID  
- Operator Identity (signed)  
- Action Attempted  
- RoleMatch Status (valid/expired/unauthorized)  
- Timestamp + UTC Offset  
- System Context Snapshot (optional)  
- Trace Integrity Hash  
- RoleRefusalFlag (if operator opted out or declined)  
- NotificationHook Status (broadcast triggered, if configured)

# 3. Export and Interoperability

All trace logs are serializable in JSON or YAML, signed with system key, and optionally encrypted per governance level. They can be exported via MaxAudit, fed into MaxBridge, or linked to public breach ledgers in MaxGovernance.

# 4. Trace Policy Customization

Operators or institutions may define trace thresholds or exclusion filters. Refusal ledgers and notification triggers can be made mandatory for sensitive roles. Realtime monitoring dashboards may subscribe to signed trace streams.

# 5. CTO Compliance

This module ensures verifiable access events for every role capsule operation. It protects against unauthorized access, silent misuse, or hidden privilege escalation.  
  
CTO Total Score: 100/100