# Module 03 – Identity, Role & Scope Control

Module ID: CORE-ID-003

Version: 4.1 (Revised CTO Edition)

Layer: Core Architecture Layer

Status: RELEASE

Dependencies: Module 00, Module 01

## 0. Purpose & Enforcement Point

This module defines the trusted identity structure, operator roles, and runtime scope enforcement used across MaxOneOpen v4.1. It ensures that all actors (human or machine) are identity-bound, role-constrained, and manifest-declared before any operation can be executed. No action can proceed without scope validation, identity resolution, and runtime capsule tracing.

## 1. Identity Structure, Role Map & Invocation Token

Each actor is assigned a Trusted Identity Token (TIT), containing:  
- `identity\_id` (unique, cryptographically signed);  
- `role\_id` (bound to scope map);  
- `trust\_tier` (0–5, from Module 12);  
- `expiration\_timestamp`.  
Invocation format: `EXEC\_CALL(identity\_token, operation\_type, manifest\_id)`  
The Role Map defines allowed operations, boundaries, escalation paths, and override conditions per role.

## 2. Runtime Behavior & Scope Enforcement

During execution, the following checks apply:  
- `ROLE\_MATCH`: Does identity's role permit this operation?  
- `TRUST\_COMPLIANCE`: Is trust tier sufficient for action context?  
- `SCOPE\_BOUNDS`: Does operation stay within assigned boundaries?  
- `SESSION\_TIME`: Has the token expired or been revoked?  
Failure in any dimension blocks execution and logs a Role Violation Capsule (RVC).

## 3. Isolation, Expiry Logic & Escalation Controls

Identity controls include:  
- hard session expiry enforced via TTL anchor in TIT;  
- role escalation only via declared `Escalation Capsule (EC)` approved by Admin Twin (Module 16);  
- automatic identity invalidation on trust drop or role conflict.  
No inline reassignment, override, or substitution is permitted without capsule logic.

## 4. Capsule Format, Ledger Hooks & Audit Fields

The following capsule formats apply:  
- `Identity Registration Capsule (IRC)` → identity\_id, role\_id, trust\_tier, origin\_hash  
- `Role Execution Capsule (REC)` → session\_id, actor\_id, op\_code, result, violation\_flag  
- `Scope Validation Record (SVR)` → role\_bounds, manifest\_link, evaluation\_result  
All capsules are stored via Module 13 and traceable by Module 14 forensic logic.

## 5. Intermodular Bindings & Control Anchors

This module connects with:  
- Module 01 (Execution Gate) for identity-token evaluation  
- Module 04 (Rule Binding) to evaluate role-bound restrictions  
- Module 12 (Trust Enforcement) to verify tier alignment  
- Module 14 (Audit Capsule) to track all actor actions  
- Module 16 (Admin Twin) to authorize escalations and token revocations

## CTO Validation Matrix

Module 03 (CTO Edition) guarantees the following verifiable conditions:  
- No operation can execute without verified identity & scoped role: YES  
- All roles are bound to static scope and trust rules: YES  
- Escalation or override requires formal capsule logic: YES  
- Every actor’s action is logged and capsule-traceable: YES  
- No dynamic or implicit privilege changes are possible: YES