# MaxSuite – AppCapsule Framework

Version: 1.0

Module ID: 01

Document Type: Capsule Structure and Execution Layer

---

## 1. Purpose

This document defines the structural, technical and signing model for MaxSuite AppCapsules. These capsules encapsulate open-source applications with governance-enforced runtime controls, audit trails, and policy-bound execution logic.

## 2. AppCapsule Structure

Each MaxSuite AppCapsule must include the following components:  
- Signed runtime manifest (capsule.yaml)  
- Encrypted or mounted application binaries  
- Policy anchor linking to MaxReg  
- Role binding logic for runtime activation  
- UI isolation metadata (if required)  
- Audit event hooks for capsule execution

## 3. Signature and Validation

Every AppCapsule must be signed with a registered authority key prior to deployment. Signature validation must confirm:  
- Capsule hash integrity  
- Role permission compliance  
- Timestamp freshness and policy version linkage

## 4. Execution Rules and Capsule Boundaries

- Applications must not access host runtime outside declared capsule  
- Network, screen, file access must be explicitly defined in capsule policy  
- Execution must trigger a runtime audit event (linked to capsule ID and role)  
- Emergency overrides must be signed and limited

## 5. Runtime Isolation

Capsules must execute in a virtualized boundary (e.g., sandboxed container, vApp, or sealed environment). They may not retain persistent state outside of policy-bound volume mounts or regulated logs.