MaxDeploy v1.0 – QuickStart Capsule Kit (Developer Edition)

This QuickStart guide provides essential template files and structural examples for immediate use of MaxDeploy in standalone or OSS projects. The files outlined below should be adapted to your deployment context and signed with appropriate operator credentials.

# 1. Included Capsule Files

* - manifest.deploy.yaml
* - meta.audit.json
* - operator.capsule.example.json

# 2. Capsule Directory Structure

/deploy/  
├── manifest.deploy.yaml # Deployment intent + policy.ref  
├── operator.capsule.example.json # Signed role declaration  
└── meta.audit.json # Audit trail linkage & trace hash

# 3. Minimal Signature Chain

Each capsule must include:

* - A signed operator ID or valid delegation link
* - A valid policy.ref linked to MaxReg or self-hosted config
* - A capsule-wide hash chain (audit.trace.sig recommended)

# 4. Use Scenario

This capsule kit enables OSS maintainers to enforce deployment integrity during artifact releases, e.g. for GitHub Actions, Docker image releases, or Helm chart publication.  
  
Just insert your configuration, sign with the operator identity, and trigger MaxDeploy with the prepared folder.

# 5. Export Note

These files are publicly exportable and verifiable. If deployed with treaty relevance, make sure to reference the proper `anchor.exec.ref` and supply export logs to your certifier.