

MaxOneOpen: Core Implementation Prerequisites

Document ID: v3.4-SKILL-001

Document ID	v3.4-SKILL-001
Title	Core Implementation Prerequisites – MaxOneOpen
Version	1.0
Date	2025-03-31
Author	MaxOne Operational Unit (GPT-Validated)
Document Type	Minimum Capabilities for Deployment Readiness

FOUNDATION – Purpose & Target Group

This document outlines the core implementation skills and team prerequisites required to deploy and maintain MaxOneOpen architecture components. It is aimed at CTOs, integrators, and critical infrastructure operators assessing internal readiness.

EXECUTION – Required Skills Matrix

System Layer	Required Capabilities	Notes
Twin Runtime Layer	Linux admin, containerization, process isolation	Basic secure ops experience
Relay & Verification	Certificate management, event signing, ZKP integration	Critical for sovereignty systems
Audit Layer	Log rotation, cryptographic archiving, traceability logic	Required for sovereign reviewability
Deployment & Forking	Git ops, manifest signing, build automation	Fork- and manifest-oriented workflow
Compliance Mapping	Basic GDPR/PDPB understanding, jurisdictional flags	Legal metadata tagging (optional)

EXECUTION – Minimal Team Composition

- ****Ops Lead (Linux + Infra)**** – configures local runtime, watchdogs, logging
- ****Security Engineer (ZKP/Signature)**** – handles sovereign verification, CERT config, manifest sealing
- ****Governance Liaison (optional)**** – supports compliance tags and deployment declaration (e.g. REG-001)
- ****Reviewer (internal/external)**** – validates implementation logic and runtime conformity

FINAL – Readiness Summary

MaxOneOpen is deployable without vendor dependencies. However, it requires an experienced, sovereignty-aware team. This document enables internal self-assessment and ensures that only capable organizations initiate productive forks and deployments.

Status: Implementation skill baseline – GPT-certified

