

Cryptographic Center of Excellence (CCoE) Charter

Template

As organizations transition to 47-day certificate lifespans, the need for automation, visibility, and governance in cryptographic operations has become urgent. This charter provides a foundational template to help you establish a Crypto Center of Excellence (CCoE) within your organization. Developed as part of the 47-Day Certificate Readiness Summit Toolkit, this document outlines the mission, roles, governance structure, and success metrics needed to lead a coordinated response to the evolving certificate landscape. Use this charter to align teams, drive automation, and build a repeatable governance model to ensure resilience and compliance in an era of rapid certificate rotation.

Mission Statement

The mission of the Crypto Center of Excellence (CCoE) is to drive consistent, scalable, and secure certificate lifecycle management across the organization in response to the industry shift to 47-day certificate lifespans. The CCoE will enable teams to build cryptographic resilience, ensure governance compliance, and reduce operational risks by offering expertise, tools, automation guidance, and best practices.

Scope and objectives

- ✓ **Accelerate adoption of certificate automation**
across all environments and teams.
- ✓ **Reduce risk of certificate-related outages**
through governance, observability, and education.
- ✓ **Establish standards and tooling**
for certificate issuance, renewal, and revocation.
- ✓ **Ensure inventory accuracy and compliance**
with internal policies and external regulations.
- ✓ **Support cultural and operational change**
as cryptographic agility becomes a core capability.



Scope and objectives

Role	Responsibilities
CCoE Lead / Sponsor	Owns vision, funding, and cross-team coordination.
Security/PKI Architect	Defines cryptographic standards and risk posture.
DevOps Lead	Integrates automation into CI/CD pipelines and runtime environments.
Infrastructure Owner	Ensures secure cert management on systems, networks, and workloads.
Compliance Liaison	Aligns crypto policy with audits and governance requirements.
Application Champion(s)	Advocates for ease-of-use and adoption by dev/product teams.

Governance cadence (suggested)

Kickoff Session

Frequency: Once

FOCUS:

Launch CCoE, confirm goals and responsibilities

Tactical Syncs

Frequency: Weekly

FOCUS:

Triage issues, track automation progress

47-Day Update

Frequency: Monthly

FOCUS:

Review cert health, gaps, and lessons learned to keep track of the monthly cert renewal cadence

Executive Briefing

Frequency: Quarterly

FOCUS:

Share KPIs and strategic needs with leadership as postquantum cryptography evolves



Success metrics (KPIs)

Metric	Target Goal
% of certs renewed on 47-day timeline	≥ 98%
% of certs tracked in inventory	≥ 99%
Mean time to renew (MTTR)	≤ 1 hour from renewal trigger
Certificate-related Sev-1 incidents	0 per cycle
% of applications onboarded to tooling	≥ 90% of in-scope apps
# of teams trained or supported	[Define target based on org size]

CCoE deliverables for your organization

The CCoE should produce, own, and maintain the following toolkit components:

- ☒ Certificate Lifecycle Automation Guide
- ☒ Inventory & monitoring standards
- ☒ Approved PKI tools and integration patterns
- ☒ Crypto Governance Policy
- ☒ Developer onboarding & self-service playbook
- ☒ 47-Day certificate compliance tracker
- ☐

