PKI Migration Checklist (Enterprise)

Use this checklist to plan and execute a migration from legacy AD CS or other CA platforms to a modern, compliant, and resilient PKI (on-prem, cloud, or hybrid). Tailored for regulated/complex environments.

Version: 25 Oct 2025

0) Governance & Scope

- ■ Executive sponsor identified and migration success criteria agreed
- ■ In-scope business units, environments (Prod/Non-Prod), and geos defined
- ■ Compliance regimes mapped (e.g., ISO 27001, NIST SP 800-53/-57, eIDAS, SOX, PCI context)
- ■ Risk register created with owner and review cadence
- ■ Change window and rollback authority documented

1) Discovery & Inventory

- ■ Certificate discovery run (servers, devices, apps, containers, IoT/OT)
- ■ Issuance points & enrollment flows mapped (AD autoenrollment, SCEP/EST, ACME, MDM/EMM, API)
- ■ Application dependencies listed (TLS, mTLS, code signing, VPN, DB/TDE, MQ, email, device auth)
- ■ Existing PKI topology diagrammed (roots, sub-CAs, RA, HSMs, CRL/OCSP, AIA/CDP)
- ■ Crypto posture baseline captured (algorithms, key sizes, validity periods, EKUs)
- ■ Expiring certs/backlogs identified and prioritised
- ■ External trust anchors catalogued (public CAs, partner CAs)

2) Policy & Documentation

- ■ Draft Certificate Policy (CP) aligned to business/regulatory needs
- ■ Draft Certificate Practice Statement (CPS) aligned to target platform
- ■ Naming standards, profiles/templates, and issuance/renewal SLAs defined
- ■ Key ceremony SOPs, M-of-N, roles & segregation of duties defined
- ■ Audit & logging requirements defined (events, retention, immutable storage)
- ■ PQC roadmap statement (crypto-agility stance; hybrid cert approach) documented

3) Target Architecture & Platform Selection

- ■ Deployment model chosen: On-prem, Cloud HSM, Managed HSM (e.g., Azure), or Hybrid
- ■ Root & Sub-CA hierarchy design approved (offline/online roles, cross-certs if needed)
- ■ Key protection boundary selected (on-prem HSM vs. Cloud/Managed HSM) with rationale
- ■ Resilience: HA/DR design, multi-region, backup/restore, escrow strategies
- ■ Directory/identity integration defined (AD/Entra ID, LDAP, SCIM/RBAC)
- ■ Interfaces chosen: SCEP/EST/ACME/REST, MDM/EMM, device gateways
- ■ Publishing: AIA/CDP/OCSP endpoints, caching/CDN strategy

4) Security Controls

- ■ HSM policy set: FIPS level, partitions, M-of-N, operator roles
- ■ Root key ceremony plan approved (witnesses, scripts, recording, evidence artefacts)
- ■ Access model: RBAC, least privilege, break-glass, PAM
- ■ Network controls: segmentation, firewall rules, private endpoints, bastions
- ■ Logging: SIEM integration, alert thresholds, test use-cases
- ■ Secrets handling: admin creds, API tokens, bootstrap secrets in vault

5) Migration Plan

- ■ Coexistence strategy defined (parallel issuance, trust bridging, or cutover)
- ■ Trust propagation plan (GPO, MDM, MAM, container images, golden AMIs)
- ■ Certificate profile parity/changes mapped (SANs, EKU, policies)
- ■ App validation plan per use-case (TLS/mTLS, code signing, DB/TDE, mail, device)
- ■ Renewal/rotation sequencing (by BU, risk, expiry)
- ■ Communications plan to app owners & stakeholders
- ■ Back-out/rollback plan written and tested

6) Build & Test

- ■ Non-prod hierarchy built; keys generated in target HSM boundary
- ■ AIA/CDP/OCSP published; availability & latency tested
- ■ Enrollment paths validated (Autoenroll, SCEP/EST, ACME, API)
- ■ Interop tests: legacy clients, embedded/OT devices, load & perf
- ■ Monitoring dashboards created (issuance rate, failures, OCSP/CRL health)
- ■ Disaster recovery drill completed (restore keys/CA; RTO/RPO evidenced)

7) Cutover

- ■ Freeze window agreed; pager & command channel established
- ■ Pre-cutover checklist passed (health, backups, sign-offs)
- ■ Stepwise execution: revoke/retire legacy, enable new issuance, repoint AIA/CDP/OCSP if needed
- ■ Validation: sample certs, app smoke tests, customer-facing checks
- ■ Incident log maintained; deviations recorded

8) Post-Migration

- ■ Decommission plan executed: archive, revoke, destroy keys (where allowed), wipe hardware
- ■ CP/CPS finalised and published; evidence pack for audit completed
- ■ Ops runbooks delivered (renewals, revocation, incident response, ceremonies)
- ■ Training delivered to PKI operators and helpdesk
- ■ Continuous discovery turned on; auto-renew policies enforced
- ■ PQC pilot scheduled (hybrid certs, constrained devices, vendor readiness)

Quick Worksheet (fill in)

- ■ Executive sponsor: _____
- ■ In-scope platforms: _____
- ■ Regulatory drivers: _____

- ■ Target HSM boundary: On-prem / Cloud HSM / Managed HSM
- ■ Root ceremony date: _____ M-of-N: ___/___
- ■ Primary issuance: Autoenroll / SCEP / EST / ACME / API
- ■ Cutover window: _____ Rollback authority: _____
- ■ Monitoring owner: _____ SIEM use-cases: _____
- ■ PQC stance (2025–2027): Hybrid / Observe / Pilot / Defer

Contact: https://safecipher.co.uk/book-a-call/ — Quotes in USD or GBP