Cloud HSM vs On-Prem HSM — PKI Decision Checklist

A governance-first guide for CISOs, Architects, and PKI Owners

SafeCipher · Innovative Cryptography Solutions for Enterprises · safecipher.com

This checklist helps stakeholders decide the right Hardware Security Module (HSM) model for enterprise PKI — whether to host keys in cloud HSM services or keep them on-premises. It mirrors SafeCipher's policy-driven approach, aligning decisions to cryptographic standards, CP/CPS requirements, sovereignty, risk, and operational outcomes. Use it to structure workshops, RFPs, and audit evidence.

1) Scope & Context

- Business drivers defined (cost, speed, agility, geographic expansion)
- In-scope PKI functions (Root CA, Issuing CA, OCSP/TSA, Code-signing, S/MIME, Device)
- In-scope environments (Data centers, Azure, AWS, GCP, Edge/Factories)
- Data classification mapped (public, internal, secret, regulated)
- Stakeholders confirmed (CISO, PKI Owner, RA, Compliance, Legal, Procurement)

2) Governance & Policy Gates

- Cryptography Standard requires ≥128-bit security and FIPS 140-3 modules
- CP/CPS clauses allow/forbid cloud custody for CA keys
- Key Management Standard defines M-of-N ceremonies, backup, and escrow
- Exception process documented if deviating from on-prem custody

3) Cryptographic Requirements

- Algorithm set: RSA-4096 for CA; RSA-3072/ECDSA-P-256 for leaves (current)
- PQC roadmap: ML-DSA (signatures) / ML-KEM (KEM) internal pilot capability
- RNG/entropy controls (NIST SP 800-90) available on platform
- Approved firmware/module versions (CMVP)

4) Key Custody & Ceremonies

- Root CA keys generated and stored on offline on-prem HSM only
- Issuing CA keys custody model defined (on-prem vs cloud partition)
- M-of-N ceremony scripts, dual control, immutable video logs
- Backup strategy: key backup tokens vs cloud KMS backups
- Key provenance & transfer (wrap/unwrap) procedures documented

5) Compliance, Sovereignty & Legal

- Residency/sovereignty requirements (e.g., UK/EU/US) validated
- Regulated workloads (PCI DSS, eIDAS/QWAC/QSeal, NHS, CJIS, MOD, ITAR) accounted
- Lawful access/jurisdictional risk assessed for cloud provider
- Supplier assurance (SOC 2/ISO 27001, SLAs, right-to-audit)

6) Architecture & Integration

- PKI platforms: Microsoft AD CS, EJBCA, Keyfactor, Venafi/CyberArk fully supported
- Client SDKs/APIs (PKCS#11, CNG/KSP, JCE, KMIP) compatibility confirmed
- Topology: Offline Root, online Issuing (pathLen=0), OCSP/TSA, HTTP AIA/CDP/OCSP
- Private connectivity (ExpressRoute/Direct Connect/Interconnect) engineered

7) Performance & Latency

- Round-trip latency from CA/OCSP to HSM ≤ target (e.g., <5 ms)
- Throughput sizing for issuance spikes, OCSP signing, code signing
- Certificate compression (RFC 8879) considered for PQC pilots
- Benchmarks captured (p95/p99 issuance, TTFB for TLS chains)

8) Availability & DR

- HA design (active/active partitions or cluster) documented
- DR region strategy (RPO/RTO) with key custody controls
- OCSP responder scale and stapling strategy
- Backup/restore tested with evidence for on-prem and cloud

9) Security Controls

- Admin plane MFA/JIT, IP allow-lists, privileged access
- Audit logging to SIEM (immutable, signed)
- Partition ACLs, separation of duties, key usage constraints
- Network isolation (VNET/VPC, private endpoints, firewall)

10) Cost Model

- TCO (CapEx/OpEx) — hardware, support, licenses, colo, staff
- Cloud HSM pricing — ops hours, API calls, partitions, cross-AZ/region
- Growth model — keys/ops per year, burst events
- Exit costs — data egress, key extraction, contract termination

11) Vendor Lock-In & Portability

- BYOK/HYOK supported; wrap formats (PKCS#8, RFC 7512, vendor tools)
- Interoperability plan (nShield ↔ Luna ↔ Cloud HSM) with test vectors
- Contract clauses for portability, audit, module lifecycle

12) Operations & Support

- 24×7 support SLAs; RMA/logistics (on-prem)
- Firmware/patch cadence and validation windows
- Monitoring: health checks, OCSP/CRL freshness probes, alerting
- Runbooks: key rotation, ceremony, incident, change windows

13) Evidence & Audit

- CP/CPS URLs embedded in CA/leaf certificates (certificatePolicies)
- Key ceremony packs, firmware attestations, serials
- OCSP/CRL reports with freshness SLOs
- Traceability matrix mapping controls to evidence (ISO 27001/NIS2/PCI)

14) HNDL & PQC Roadmap

- HNDL (Harvest-Now-Decrypt-Later) risk documented for long-lived data
- PQC pilot plan (internal), no public endpoints until support matures
- Short chains + compression when PQC enabled

15) Cloud-Specific Checks — Azure

- Azure Managed HSM vs Key Vault (dedicated vs pooled) selection made
- Private endpoints, RBAC, purge protection/soft delete enabled
- Latency to issuing CA/OCSP; AKV certificate issuance path verified

16) Cloud-Specific Checks — AWS

- AWS CloudHSM vs KMS asymmetric keys evaluated
- ENI placement, security groups, dedicated cluster sizing
- ACM PCA alignment or trust import to corporate chain

17) Cloud-Specific Checks — Google Cloud

- Cloud HSM and Cloud KMS key constraints reviewed
- VPC-SC, private service connect, regional availability
- CAS chaining or trust import to corporate chain

18) Go/No-Go Gates

- Policy approvals (Crypto Standard, CP/CPS, KMS) completed
- Connectivity & latency tests pass across regions

- Ceremony rehearsal complete; backup/restore verified
- Monitoring/alerting live; SIEM integration confirmed

19) Migration Checklist (if changing model)

- New CA keys generated in target HSM; M-of-N ceremony complete
- Issuing CA created; pathLen=0; HTTP AIA/CDP/OCSP publishing live
- Templates re-issued; policy OIDs & CPS URLs embedded
- Blue/green issuance; canary cohorts; rollback plan ready
- OCSP responders scaled; CRL schedule aligned
- Cloud trust bundles updated; compatibility islands in place

20) SLAs & KPIs

- Issuance latency p95 ≤ 2–5s; Renewal success ≥ 99%
- OCSP availability ≥ 99.9%; freshness ≤ 8h (overlap 1h)
- Expired-certificate incidents = 0
- Ceremony evidence published within 5 business days

Weighted Decision Worksheet

Criterion	Weight	Cloud HSM Score	On-Prem HSM Score
Sovereignty/Compliance Fit	5		
Latency/Performance	4		
Availability/DR	4		
Custody & Ceremonies	5		
Integration Effort	3		
TCO (3-year)	4		
Vendor Lock-in Risk	3		
Operational Maturity	3		
PQC Readiness	2		
Total (Σ score×weight)			