# CRYPTO AGILITY READINESS FRAMEWORK

Reference Architecture — Lab + System Design

Version 1.0 · November 2026
Status: Reference — open for comment
Author: Ajay Salunkhe · Classification: Public

*Lab view. The label is not the measurement.*

---

## 1. Document control

| Version | Date | Author | Description |
|---|---|---|---|
| 0.1 | Nov 2026 | Ajay Salunkhe | Structure |
| 1.0 | Nov 2026 | Ajay Salunkhe | First complete reference + measurement emphasis |

## 2. Executive summary

Public-key algorithms in wide use today (RSA, ECC, Diffie–Hellman) are vulnerable to a sufficiently large quantum computer. Sensitive data that must remain confidential for years is already exposed to harvest-now-decrypt-later risk.

Most programmes still treat “PQC readiness” as a flag: hybrid enabled, library upgraded, dashboard green. That is not readiness. Readiness is inventory, measurement on the wire, and a clear path to change algorithms without an outage or a silent classical fallback.

This document is a reference architecture for assessing crypto agility and PQC migration readiness. It is written for system architects and security engineers who must answer:

- What cryptography is actually in use (and what was not scanned)?
- Where is quantum-relevant risk concentrated?
- How hard is it to change algorithms on each path?
- What should be measured so that “PQC on” is not only a label?

### Design stance

- Inventory first.
- Risk and agility are separate dimensions.
- Key-agreement (KEM / hybrid TLS) and signatures / PKI are different tracks with different clocks.
- Hybrid is a controlled transition, not a destination.
- Outputs must be explainable to both engineers and leadership.

This is a design reference and assessment model. It is not a product specification and not a compliance certificate.

## 3. Scope

### In scope

- Cryptographic inventory and CBOM structure
- Quantum-oriented risk view
- Crypto-agility scoring
- Readiness maturity (0–4)
- Prioritised actions
- Measurement requirements (what to log and test)

### Out of scope (v1.0)

- Full automated source-code AST scanning of every repository
- Deep HSM internal firmware analysis
- Real-time enforcement or automated algorithm replacement
- Legal or regulatory certification

### Assumptions

- The organisation can supply or allow collection of cryptographic metadata
- Some form of asset list exists
- The framework is used for assessment and planning, not live blocking

## 4. Goals and non-goals

### Goals

- Give a clear, implementable reference for readiness assessment
- Force inventory before scoring
- Separate risk from agility
- Make hybrid and pure-PQC states explicit
- Tie readiness to measurable wire and system facts, not only configuration flags

### Non-goals

- Shipping a commercial product in v1.0
- Replacing existing vulnerability or certificate lifecycle tools
- Claiming coverage of every legacy library in the first revision

## 5. Architecture principles

1. Inventory first — no reliable CBOM, no reliable score.
2. Separation of risk and agility — high risk + high agility is a different problem from high risk + rigid stack.
3. Two tracks — key agreement (ML-KEM / hybrid groups) vs signatures and certificates (ML-DSA / SLH-DSA / PKI).
4. Measurement over labels — handshake success is not the same as negotiated PQ group; “ticket issued” is not the same as resume success.
5. Hybrid is transitional — enablement must include exercised exit paths (classical-only and PQ-leaning), not only “both on”.
6. Explainable scoring — weights and inputs must be visible.
7. Human + machine readable outputs.

## 6. High-level architecture

Logical components: Discovery & inventory engine; CBOM store; Risk assessment engine; Crypto agility scoring engine; Configuration & policy layer; Reporting & visualisation layer; Extension / plugin interface.

Flow: Scope → discover → normalise into CBOM → score risk → score agility → combine into maturity + priority list → report. What the architecture deliberately does not do in v1.0: pretend that a green “hybrid TLS” tile equals migration complete.

## 7. Component responsibilities

### 7.1 Discovery & inventory engine

Collects cryptographic observations from reachable surfaces: endpoints, configs, certificate stores, known libraries, protocol settings. Outputs raw observations with confidence and coverage notes (including where the scan did not run).

### 7.2 CBOM store

Structured inventory. Minimum fields (v1.0):

- Asset / path identifier
- Owner
- Algorithm name and OID (if known)
- Key size / parameter set
- Protocol and usage context (TLS, VPN, code-signing, etc.)
- Library / implementation and version
- Certificate chain role (if any)
- Data sensitivity and retention (business input)
- Discovery timestamp and confidence
- Coverage flag: observed | inferred | not scanned

“Not scanned” rows are first-class. A CBOM with no unknown rows is usually incomplete, not complete.

### 7.3 Risk assessment engine

Quantum-oriented exposure per asset, using algorithm class, parameter strength, data sensitivity, retention / lifetime of ciphertext or signatures, and exposure path. Output: risk score and category. Long-lived, externally exposed classical public-key material ranks higher than short-lived internal sessions.

### 7.4 Crypto agility scoring engine

How hard is change on this path? Illustrative weights for v1.0:

- Configuration flexibility vs hardcoding — 40%
- Key management and issuance path — 25%
- Protocol negotiation / hybrid support — 20%
- Abstraction and modularity — 15%

Output: agility score 0–100. Rigid, hardcoded, single-vendor paths score low even if risk is currently “only medium”.

### 7.5–7.7 Reporting, policy, extension

Reporting: executive summary, maturity, priority list, measurement checklist. Policy: org-specific weights and mandatory measurements. Extension: new algorithms, connectors, and rules without redesigning the core.

## 8. Measurement requirements (non-negotiable for “ready”)

These are the difference between a label and a measurement.

### Key-agreement track

- Log negotiated group after Finished (e.g. X25519MLKEM768 / 0x11EC), not only “TLS 1.3 success”.
- Confirm hybrid enablement does not silently accept classical-only when policy forbids it.
- On upgrades, re-test group intersection (draft codepoints vs final codepoints are not interchangeable).

### Resumption / performance track

- Measure session ticket (or session-id) issue and resume rates.
- Note ticket size growth under hybrid; edge buffers and header limits can drop tickets and force full handshakes.
- First-flight size vs typical TCP initial window (~10 segments / ~14.6 KB on many stacks): full ML-DSA chains can force an extra RTT on untuned paths.

### Signature / PKI track

- Separate clock from KEM enablement.
- Roots, issuance policy, client trust stores, and HSM/module capability often lag hybrid key exchange by years.
- Do not score “PQC %” as a single number that hides a red certificate track behind a green KEM tile.

### Inventory track

- Every assessment records where discovery did not run.
- Owners and retention are part of the row, not a footnote.

## 9. Readiness maturity model (0–4)

**Level 0 — Unknown** — No usable crypto inventory; no systematic quantum risk view.

**Level 1 — Inventory started** — Partial CBOM; major internet-facing paths identified; large “not scanned” set.

**Level 2 — Risk and agility visible** — Risk and agility scored on known assets; prioritisation possible; measurements defined but not yet routine.

**Level 3 — Hybrid-capable and measured** — Hybrid key agreement on priority paths with negotiated-group logging; resume and flight-size checks in place; signature track planned with owners.

**Level 4 — Crypto-agile** — Algorithm change is an exercised operational path; inventory coverage is high; KEM and signature tracks both have exit and upgrade drills; labels match wire measurements.

Maturity is not a marketing badge. Moving from 2 → 3 requires evidence on the wire, not only a library version.

## 10. Prioritisation

Order work by: (1) High risk + low agility (2) High risk + medium agility (3) Medium risk + low agility (4) Everything else.

Within high risk, prefer: long retention + external exposure (HNDL-relevant); paths with no owner or no change process; classical-only termination still sitting behind a “PQ-ready” edge.

## 11. Sample CBOM row (illustrative)

- Asset: Internet-banking TLS termination · Owner: Platform / payments
- Algorithms: ECDHE + RSA-2048 (certificates); session classical · Protocol: TLS 1.2 / 1.3
- Library: OpenSSL 1.1.1x · Retention: session + archival logs (years)
- Risk: High · Agility: 35 (hardcoded curves, old library, no hybrid group)
- Coverage: Observed at edge; origin and HSM not scanned
- Next measurement: negotiated group after Finished if hybrid enabled; ticket resume rate

## 12. Security of the assessment itself

CBOM data is sensitive. Protect it with role-based access, encryption in transit and at rest, and audit logs. The assessment store must not become a high-value map of the estate's weak points for an adversary.

## 13. Implementation notes (v1.0)

- Reference stack: Python; JSON / SQLite / PostgreSQL; CLI first; PDF/HTML reports
- Scale target: hundreds to a few thousand assets per assessment run
- Discovery may be manual or semi-automated; full agents are a later increment
- Scoring weights are baselines — tune per organisation and document the change
- Known limits: limited automation; manual enrichment expected; no claim of complete library coverage

## 14. How this differs from a dashboard tile

| Label-only view | This framework |
|---|---|
| "Hybrid enabled" | Negotiated group logged and tested |
| "Handshake success" | Success + selected group + resume rate |
| "CBOM complete" | CBOM + explicit not-scanned rows |
| Single "PQC %" | KEM track and signature track separate |
| Library version upgrade | Agility of the path + owner + exit |

## 15. References (indicative)

- NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA)
- NIST IR 8547 and related migration guidance
- CBOM / cryptographic inventory practice
- IETF hybrid key-exchange work for TLS
- Operational notes on handshake size, resumption, and middlebox behaviour

## 16. Glossary

- **CBOM** — Cryptographic Bill of Materials
- **Crypto agility** — ability to change algorithms with minimal disruption
- **Hybrid** — classical + PQ mechanisms used together for transition
- **PQC** — post-quantum cryptography
- **Selected group** — the key-agreement group actually negotiated on the wire

---

Inventory what you use. Measure what you negotiate. Separate the KEM clock from the certificate clock. Treat hybrid as a transition with an exit, not a sticker.

*Lab view. The label is not the measurement.*

— End of document —

Ajay Salunkhe · Crypto Agility Readiness Framework v1.0 (Reference)