ENKIDU

— MIOVSKI GROUP —

CONCEPTUAL ARCHITECTURE

Aegis Defence

The quantum-resistant cryptographic layer of the Enkidu stack — hybrid post-quantum key establishment, quantum-resistant signatures, and fleet-wide crypto-agility, enforced by Origi and operated by Helios Grid across the Northwind fabric.

English · Complete edition

Version 0.1 · First Draft

4 July 2026

Prepared by MIOVSKI GROUP

Classification · Unclassified · Draft for Internal Review

Glossary

Terms used throughout this conceptual architecture. Code names are shown in bold. Terms defined in the Northwind, Helios Grid, Tangram, and Trust Assurance documents are carried forward and not redefined except where Aegis extends them.

Aegis Defence

The Enkidu cryptographic framework: the quantum-resistant key-establishment, digital-signature, and crypto-agility layer that secures every link, artifact, and custody record across the Enkidu stack. Aegis defines what cryptography is used and how it changes; Origi enforces it; Helios Grid distributes and operates it.

CRQC (Cryptanalytically Relevant Quantum Computer)

A future quantum computer large and reliable enough to break today's public-key cryptography (RSA, elliptic-curve Diffie-Hellman, ECDSA) using Shor's algorithm. Its arrival date is uncertain; the mandates below assume it must be planned for now.

Harvest Now, Decrypt Later (HNDL)

The attack that makes the quantum threat a present-tense problem: an adversary records encrypted traffic today and decrypts it once a CRQC exists. Any data whose confidentiality must outlive the CRQC horizon must be protected with quantum-resistant key establishment before that horizon.

Post-Quantum Cryptography (PQC)

Public-key cryptography based on mathematical problems that neither classical nor quantum computers are known to solve efficiently. PQC is a software upgrade path deployable on existing hardware — the property that makes it the correct choice for a distributed edge fabric.

Quantum Key Distribution (QKD)

A hardware technique that uses quantum physics to distribute keys over dedicated optical channels. Aegis does not use QKD (Section 9): it requires special-purpose equipment, does not fit mobile or tactical topologies, and is excluded from allied national-security cryptographic guidance.

ML-KEM (FIPS 203)

The Module-Lattice-Based Key-Encapsulation Mechanism (formerly CRYSTALS-Kyber): NIST's primary standard for quantum-resistant key establishment. Aegis's default KEM, deployed in hybrid constructions.

ML-DSA (FIPS 204)

The Module-Lattice-Based Digital Signature Algorithm (formerly CRYSTALS-Dilithium): NIST's primary standard for quantum-resistant digital signatures. Aegis's default signature algorithm.

SLH-DSA (FIPS 205)

The Stateless Hash-Based Digital Signature Algorithm (formerly SPHINCS+): a conservative backup signature scheme whose security rests only on hash functions — deliberately different mathematics from ML-DSA.

HQC

A code-based key-encapsulation mechanism selected by NIST in March 2025 as the backup KEM to ML-KEM, providing algorithm diversity on non-lattice mathematics.

LMS / XMSS

Stateful hash-based signature schemes used for firmware and software signing, preferred in national-security guidance for code-signing roles because their security assumptions are minimal and well understood.

Hybrid key establishment

Deriving a session key from both a classical exchange (e.g., X25519) and a post-quantum KEM (e.g., ML-KEM-768) so the session remains secure if either algorithm is broken. Aegis's default posture during the transition era.

Crypto-agility

The ability to change algorithms, parameters, and protocol bindings without re-engineering the systems that use them. In Aegis, cryptographic policy is a versioned, signed artifact distributed by Helios Grid — agility is an operations function, not a redesign.

CBOM (Cryptographic Bill of Materials)

The authoritative inventory of every cryptographic algorithm, key, certificate, and protocol binding in use across the fleet — assembled in Aegis from Helios node twins, and the prerequisite for any migration.

CNSA 2.0

The NSA's Commercial National Security Algorithm Suite 2.0: the algorithm and timeline mandate for U.S. National Security Systems, specifying ML-KEM-1024 and ML-DSA-87 and excluding QKD.

ITSM.40.001

The Canadian Centre for Cyber Security's Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada: migration plans by April 2026, high-priority systems migrated by end of 2031, all remaining systems by end of 2035.

cuPQC

NVIDIA's CUDA Post-Quantum Cryptography SDK: GPU-accelerated, batched implementations of ML-KEM and ML-DSA plus cryptographic hash primitives, used by Aegis at the GPU-server tiers of the fabric.

Abstract

Every promise the Enkidu stack makes rests, in the end, on cryptography. Origi's chain of custody is signatures; Helios Grid's artifact admission is signatures; every mesh link, reachback spoke, and control channel is a key exchange. Today those primitives — elliptic-curve key agreement and classical signatures — are secure. Against a cryptanalytically relevant quantum computer, they are not: Shor's algorithm breaks them outright, and the harvest now, decrypt later attack means traffic recorded off a reachback link today can be read retroactively the day such a machine exists. For a fabric that carries Protected B data with multi-decade sensitivity, the quantum threat is not a future problem — it is a present recording problem.

Aegis Defence is Enkidu's answer: the quantum-resistant cryptographic framework of the stack, and its fourth foundational framework. Where Tangram gives a fabric its structure, Origi its runtime trust, and Helios Grid its operability, Aegis gives it cryptographic longevity — hybrid post-quantum key establishment on every link, quantum-resistant signatures on every artifact and custody record, and crypto-agility engineered as a fleet operation rather than a re-engineering project.

Aegis is deliberately conservative and deliberately standards-bound. Its algorithm suite is the finalized NIST set — ML-KEM (FIPS 203), ML-DSA (FIPS 204), SLH-DSA (FIPS 205), with HQC as the code-based backup and LMS/XMSS for firmware signing [1][2][4] — deployed in hybrid constructions per IETF practice [13], aligned to CNSA 2.0 for the defence tiers [3][4] and to Canada's ITSM.40.001 timeline for Government of Canada systems [5][6]. It is implementable today on the exact hardware Northwind fields: ARM-optimized embedded PQC libraries on the Jetson node and hub tiers [12][14][15], and NVIDIA's cuPQC SDK for batched, GPU-accelerated verification at the Grace-Blackwell fusion-centre tiers [9][10][11]. And it explicitly rejects quantum key distribution for this fabric, in line with allied national-security guidance [3][8][16].

One sentence carries the design: hybrid by default, agile by construction, and nothing trusted to mathematics that a quantum computer is known to break.

1. Purpose and Scope

1.1 What this document is

This is a conceptual architecture, not an implementation manual or a cryptographic specification. It defines Aegis Defence's structure, algorithm suite, protocol bindings, and contracts with the other Enkidu frameworks — enough to build against, assess for procurement, and accredit — without fixing every parameter to a specific library version. Where a concrete technology is named, it is named because it shapes the architecture or because Aegis deliberately adopts its pattern.

The reference deployment throughout is Northwind — the distributed Fusion-in-a-Box platform — because Northwind presents the hardest version of the problem: contested, bandwidth-poor links; security classification; hosts ranging from a battery-powered Jetson node to a rack-scale Grace-Blackwell data centre; and data whose sensitivity outlives any credible CRQC horizon. The same architecture, with civilian parameter profiles, is the cryptographic layer for Lamassu, Helios Grid, and every other Enkidu deployment.

1.2 Position in the Enkidu stack

The Enkidu stack now has four foundational frameworks, each answering a different question about the same fabric:

- Framework — Question it answers — Plane
- Tangram — Where does work happen, and under what boundary conditions? — Structure
- Origi — May this action happen, and can we prove what happened? — Trust
- Helios Grid — Is the fabric healthy, current, and recoverable? — Operations
- Aegis Defence — Will every key, signature, and link still hold when the adversary has a quantum computer? — Cryptography

Aegis is not a new plane of components on the fabric; it is the cryptographic substance of the planes that exist. Origi's secured-communication regime, its chain of custody, and its artifact admission checks are Aegis algorithms; Helios's enrolment identities, signed desired state, and signed runbooks are Aegis signatures. Aegis defines the suite, the bindings, and the change discipline; Origi enforces them at every boundary; Helios distributes them to every node.

1.3 What Aegis is not

Aegis does not perform key escrow, does not define classification policy (that is the fabric's data-sensitivity framework), and does not attempt to out-engineer the standards bodies: no bespoke primitives, no unstandardized algorithms, no cryptography invented in-house. Its value is in disciplined selection, correct binding, and operable migration — not novelty. In cryptography, novelty is risk.

2. The Quantum Threat and the Mandates

2.1 What breaks, and what does not

A CRQC running Shor's algorithm breaks the public-key cryptography in use today — RSA, elliptic-curve Diffie-Hellman, and ECDSA — completely. Grover's algorithm weakens symmetric cryptography only quadratically, which is answered by key size: AES-256 and the SHA-2/SHA-3 families remain secure [1][17]. The consequence for the Enkidu stack is precise: every key exchange and every signature must migrate; the symmetric encryption and hashing underneath — including the hash-linking of Origi's chain of custody — need parameter discipline, not replacement.

2.2 Harvest now, decrypt later

The urgency is asymmetric between the two functions. A signature forged in the future does not retroactively falsify the past; but a key exchange broken in the future retroactively exposes everything it protected. An adversary recording Northwind reachback traffic today needs no quantum computer now — only patience and storage [17]. This is why every mandate below prioritizes key establishment, and why Aegis's first deployment wave is hybrid KEMs on links, not signatures.

2.3 The standards are final

The transition is no longer speculative. NIST published the finalized standards in August 2024: FIPS 203 (ML-KEM) as the primary general-encryption standard, FIPS 204 (ML-DSA) as the primary signature standard, and FIPS 205 (SLH-DSA) as a signature backup on different mathematics [1]. HQC was selected in March 2025 as a code-based backup KEM for algorithm diversity, and FN-DSA (Falcon) is in development as FIPS 206 [2]. The spread across lattices, hash functions, and codes is deliberate: if one mathematical family falls, the suite does not.

2.4 The mandates Aegis must satisfy

- Authority — Instrument — What it requires
- NSA (U.S. NSS) — CNSA 2.0 — ML-KEM-1024 and ML-DSA-87 for National Security Systems; LMS (SHA-256 preferred) / XMSS for firmware and software signing; QKD explicitly excluded; migration on a product-class schedule running to the early 2030s [3][4].
- CSE / Cyber Centre (Canada) — ITSM.40.001 + TBS SPIN — Applies to all GC systems UNCLASSIFIED through PROTECTED B. Departmental migration plans by April 2026; high-priority systems migrated by end of 2031; all remaining systems by end of 2035. Completion is strict: vulnerable algorithms "disabled, isolated or tunnelled" [5][6].
- NCSC (U.K.) — PQC migration timelines — Discovery and planning now; full migration by 2035, prioritizing systems processing sensitive data and critical communications [7].

A Northwind fielded for the Canadian Armed Forces sits under the strictest reading of all three: defence data with decades-long sensitivity, Protected B handling, and Five Eyes interoperability expectations shaped by CNSA 2.0. Aegis therefore takes CNSA 2.0 parameters as the ceiling profile and ITSM.40.001 as the binding schedule.

The mandate horizon is not the CRQC's arrival date. It is the recording adversary's patience, subtracted from your data's lifetime.

3. Design Premise and Principles

3.1 The core premise

Aegis rests on one sentence: hybrid by default, agile by construction, and nothing trusted to mathematics a quantum computer is known to break. Hybrid, because the post-quantum algorithms are young and the classical ones are quantum-doomed — combining them means a session survives the failure of either. Agile, because the one certainty in a young field is change: algorithms, parameters, and protocol codepoints will move, and a ten-thousand-node fleet must follow them as an operations task, not a rebuild.

3.2 The load-bearing invariants

Six invariants hold everywhere Aegis applies. They are deliberately parallel to the invariants of Northwind and Helios Grid, because the cryptographic layer must be as disciplined as the fabric it protects.

- # — Invariant — What it means in Aegis
- 1 — Standards only — Every algorithm in the suite is a finalized NIST standard or an explicitly designated backup from the NIST process. No bespoke primitives, ever [1][2].
- 2 — Hybrid until mandated otherwise — Key establishment combines a classical exchange with a post-quantum KEM (e.g., X25519 + ML-KEM-768) so that a break of either leaves the session secure. Pure-PQC modes are enabled only where a mandate directs it [13].
- 3 — Algorithm diversity is held in reserve — For every primary algorithm there is a designated backup on different mathematics — HQC behind ML-KEM, SLH-DSA behind ML-DSA — pre-integrated so a cryptanalytic surprise is a policy flip, not a crisis program [2][79].
- 4 — Cryptographic policy is a signed artifact — The active suite, parameters, and bindings per fleet segment are declared in a versioned, signed crypto-policy artifact distributed by Helios Grid and admitted by Origi like any other artifact.
- 5 — The symmetric layer is sized, not replaced — AES-256, SHA-2/SHA-3 (384-bit and above for the highest tiers) are retained; Grover is answered with key and digest size [17].
- 6 — Nothing is removed until it is tunnelled — Classical algorithms are withdrawn only per the mandate discipline — disabled, isolated, or tunnelled inside a quantum-resistant layer — never silently left in a fallback path [5].

3.3 Why not wait

Two arguments end the "wait for the field to mature" position. First, HNDL: the data being recorded today is already lost or safe depending on what protects it today (Section 2.2). Second, the schedule arithmetic: Canada's high-priority deadline is the end of 2031 [5][6], Northwind's Phase 1 fields in the same window, and a cryptographic layer retrofitted after fielding costs a multiple of one designed in. Aegis exists so that Northwind never ships a quantum-vulnerable link in the first place.

4. The Aegis Algorithm Suite

The suite assigns one primary and one reserve algorithm to each cryptographic function, with parameters profiled per deployment tier. The defence ceiling profile follows CNSA 2.0; the standard profile follows NIST Level 3 guidance and Cyber Centre recommendations for Protected B [3][5].

- Function — Primary — Reserve / notes
- Key establishment (links, sessions) — Hybrid X25519 + ML-KEM-768 (standard profile); hybrid with ML-KEM-1024 (defence ceiling / CNSA 2.0) — HQC held as code-based reserve KEM; pure ML-KEM mode available where mandated [2][3][13].
- Signatures — custody records, telemetry, enrolment, verdicts — ML-DSA-65 (standard); ML-DSA-87 (defence ceiling) — SLH-DSA as the hash-based reserve on independent mathematics [1][3].
- Signatures — firmware, boot chain, BSP images — LMS (SHA-256), XMSS — Stateful hash-based schemes per CNSA 2.0 code-signing guidance; verify-only builds on constrained nodes [4][14].
- Signatures — artifact registry (models, containers, policies) — ML-DSA, dual-signed with LMS for base-system artifacts — Dual signature covers both the general and code-signing mandates during transition.
- Symmetric encryption — AES-256 (GCM) — Unchanged; quantum-resistant at this size [17].
- Hashing / custody chain linking — SHA-384 / SHA-512, SHA-3 family — Unchanged in structure; digest sizes set per profile [17].
- Certificates / PKI — ML-DSA certificate chains; hybrid certificates during transition — Classical chains tunnelled inside Aegis-protected channels until withdrawn [5].

Two deliberate omissions. FN-DSA (Falcon) is tracked but not adopted until FIPS 206 finalizes — its compact signatures are attractive for the most bandwidth-starved links, and Section 10 reserves its slot [2]. And no algorithm outside the NIST process appears at all (Invariant 1).

5. The Aegis Layer Architecture

Aegis materializes at four binding points, all of which already exist in the stack — which is the point: Aegis is a substitution of cryptographic substance, not an addition of moving parts.

5.1 Link protection — the Origi secured-communication regime

Every link in the fabric — node-to-node mesh, node-to-hub, hub-to-FOB-IFC, FOB-IFC-to-Central-IFC, and every Helios control channel — is mutually authenticated and encrypted under Origi. Aegis defines what that means concretely: TLS 1.3 with the hybrid X25519+ML-KEM-768 group (the construction now shipped as a default key share in mainstream TLS stacks [12][13]), DTLS 1.3 with the same hybrid groups for datagram-oriented mesh bearers [14], and hybrid ML-KEM key exchange for administrative SSH sessions (mlkem768x25519-sha256; mlkem1024nistp384-sha384 at the ceiling profile) [15]. Session keys derive from both exchanges; the recording adversary of Section 2.2 gains nothing.

5.2 Identity — enrolment and the PKI

Node identities, Warden and Core identities, and operator credentials are certificate-based. Aegis moves the certificate chains to ML-DSA, with hybrid certificates during the transition window so that a fleet mid-migration interoperates without downgrade ambiguity. Hardware-rooted keys on tiers that support them hold the private material; the certificate profile, like everything else, is carried in the crypto-policy artifact.

5.3 Integrity — custody, telemetry, and artifacts

Origi's chain of custody is a signed, hash-linked record; Aegis specifies ML-DSA for the signatures and SHA-384-class digests for the links, with SLH-DSA available by policy for records whose evidentiary weight justifies the conservative scheme's cost. Helios artifacts — models, containers, zone definitions, policy bundles — are ML-DSA-signed in the registry and verified on the node at the moment of admission; base-system artifacts carry the LMS dual signature per code-signing guidance [4]. The verification always runs at the last trust boundary before use, so a compromised cache or relay can deliver nothing a node will accept.

5.4 Boot — the root of the whole argument

A quantum-resistant fabric booted by a quantum-forgeable loader is a contradiction. The boot chain — bootloader, BSP, kernel — is signed with the stateful hash-based schemes (LMS/XMSS), whose security rests on nothing but hash functions and which embedded PQC libraries support in small-footprint, verify-only configurations suited to the node tier [4][14]. This is the deepest layer of the A/B fail-safe update mechanism Helios already mandates: the slot that fails Aegis verification is the slot that never boots.

Aegis adds no new component to the fabric. It changes what every existing handshake, signature, and boot check is made of.

6. Mapping Aegis onto the Fabric

PQC's costs are asymmetric — computation is nearly free, bandwidth is not — and the fabric's tiers are asymmetric in the opposite direction. Aegis exploits both.

- Fabric tier — Aegis implementation posture
- FIB node (Jetson Orin-class) — CPU-side PQC on the ARM cores: embedded libraries with ARM assembly-optimized ML-KEM/ML-DSA and small-footprint LMS/XMSS verify-only builds; hybrid (D)TLS 1.3 on every link. Per-node cryptographic volume is small — a node's handshakes and signatures are milliseconds of CPU per hour [12][14].
- FIB hub (Jetson Thor-class) — Same CPU-side stack, plus hub duties: terminating dozens of node sessions, verifying node telemetry signatures, and re-signing aggregates. Comfortably CPU-bound at cluster scale; the GPU remains dedicated to inference.
- FOB-IFC (DGX Station GB300-class) — cuPQC enters: batched, GPU-accelerated ML-DSA verification for theatre-scale custody and telemetry streams, and batched ML-KEM operations for session management across dozens of hubs [9][10].
- Central IFC (GB200/GB300 NVL72-class) — Full cuPQC deployment through the liboqs integration [11]: registry signing infrastructure, fleet-scale batched verification (millions of operations per second per GPU [9][10]), key-lifecycle services, and the crypto-policy authoring pipeline.

The headline numbers justify the tiering: cuPQC achieves on the order of 13 million ML-KEM-768 key generations and millions of encapsulations and verifications per second on a single H100-class GPU — roughly two orders of magnitude over a CPU core [9][10] — while at the node tier a single hybrid handshake costs tens of microseconds of compute [13]. The fleet's cryptographic burden concentrates exactly where the fabric's compute concentrates. Aegis's design work at the edge is therefore not computational but budgetary — the bandwidth arithmetic of Section 10.

One verification item is recorded for detailed design: cuPQC targets data-centre-class CUDA GPUs; Aegis does not assume its availability on Jetson tiers, where CPU implementations are sufficient by the analysis above, and this assumption must be confirmed against current cuPQC platform support [9].

7. Crypto-Agility — Cryptography as a Managed Artifact

The deepest lesson of the last decade of cryptanalysis — including the abrupt collapse of a fourth-round NIST candidate to a classical attack in 2022 [77] — is that confidence in young mathematics can fail suddenly. Aegis's answer is to make the change of cryptography a routine fleet operation.

7.1 The crypto-policy artifact

The active suite — algorithms, parameter sets, protocol groups, certificate profiles, deprecation flags — is declared per fleet segment in a signed, versioned crypto-policy artifact. It is distributed by Helios Grid exactly like a model or a zone definition: staged rollout waves, health gates (handshake success rates, interoperability with the previous policy), automatic rollback, and full custody recording. Flipping a fleet from ML-KEM-768-hybrid to ML-KEM-1024-hybrid — or, in the surprise scenario, from ML-KEM to HQC — is a rollout, not a program.

7.2 The CBOM from node twins

Every mandate begins with discovery: you cannot migrate what you have not inventoried [5][7]. In the Enkidu stack this is nearly free — the Helios node twin already records every installed artifact and binding per node, so the fleet's Cryptographic Bill of Materials is a query over the twins, not a manual audit. The CBOM is the compliance evidence for ITSM.40.001's planning and reporting milestones and the input to every migration wave [5][6].

7.3 The deprecation discipline

Migration completes only when the vulnerable algorithm is gone from the negotiation, not merely deprioritized — the "disabled, isolated or tunnelled" standard [5]. Aegis enforces this through the same policy artifact: a deprecated algorithm first loses its default status, then is confined to tunnelled legacy interfaces behind Aegis-protected channels, then is removed from the build. Each step is a fleet rollout with a custody trail, so the question every auditor eventually asks — prove RSA is gone — is answered from the record.

8. Sizing and Performance on Contested Links

PQC's real tax on Northwind is bytes, not cycles, and the mesh bearers are the place it bites. Aegis budgets for it explicitly.

- Object — Classical (typical) — Aegis (standard profile) — Notes
- KEM public key / ciphertext — 32 B / 32 B (X25519) — ~1.2 KB / ~1.1 KB (ML-KEM-768) plus classical share — Paid once per handshake; ML-KEM public keys run 800–1568 B and ciphertexts 768–1568 B across levels [17].
- Signature — 64–72 B (ECDSA) — 2.4–4.6 KB (ML-DSA-44/-87) — Paid per signed record; the dominant recurring cost [17].
- Hash-based signature (reserve) — — — ~7.9 KB and up (SLH-DSA) — Reserved for high-evidentiary records and firmware roles; orders of magnitude costlier to sign [17].

Three mitigations keep this inside the fabric's envelopes. Handshake amortization — mesh sessions are long-lived and resumed, so kilobyte-scale handshakes amortize across hours of link life. Signature batching and aggregation at the hub — nodes sign at the record level, hubs verify locally and forward hub-signed aggregates upstream, so per-node ML-DSA signatures do not transit the reachback link individually; this composes exactly with Helios Grid's signal-not-data telemetry reduction. Compact-signature reserve — FN-DSA's slot in the suite (Section 4) exists for the most bandwidth-starved bearers once FIPS 206 finalizes, where its sub-kilobyte combined footprint matters [2][80]. The residual overhead is then a design input to Helios's telemetry-envelope arithmetic rather than a surprise discovered in the field.

9. The Position on Quantum Key Distribution

Aegis takes a definite position: no QKD on this fabric. The reasons are the allied agencies' reasons, and they are architectural, not fashionable. QKD requires special-purpose optical equipment and dedicated channels — a hardware solution where PQC is a software one [8][16]; it is architecturally unsuited to mobile and tactical communications and to any path requiring relays outside organizational control [16]; it provides key distribution but not authentication, so it depends on PQC-grade signatures anyway [16]; and it concentrates denial-of-service risk in a channel an adversary can saturate with light [16]. Accordingly, the NSA does not support QKD for National Security Systems and CNSA 2.0 excludes it, with allied agencies taking materially the same position [3][8][16].

One watch item is recorded for completeness: fixed, strategic point-to-point links between permanent Central IFC sites are the single niche where QKD deployments exist worldwide, and Canada's QEYSSat program is exploring satellite QKD for reach into fibre-impractical regions [16][18]. If policy or alliance direction ever changes, such a link would enter the stack as one more key source underneath Aegis's hybrid derivation — an additional layer, never a replacement, and never on the tactical fabric.

10. Compliance Crosswalk

- Requirement — Source — Aegis mechanism
- ML-KEM-1024 / ML-DSA-87 for NSS-class systems — CNSA 2.0 [3] — Defence ceiling profile in the crypto-policy artifact (Section 4).
- LMS/XMSS for firmware and software signing — CNSA 2.0 [4] — Boot-chain and base-artifact signing roles (Sections 5.3–5.4).
- No QKD for NSS — CNSA 2.0 [3] — Section 9 position; no QKD dependency anywhere in the suite.
- Migration plans and annual reporting from April 2026 — ITSM.40.001 / TBS SPIN [5][6] — CBOM generated from Helios node twins; policy-artifact version history as the progress record (Section 7.2).
- High-priority systems migrated by end of 2031 — ITSM.40.001 [5] — Hybrid KEMs on all links in the first Aegis wave; Northwind fields with no quantum-vulnerable link (Sections 3.3, 11).
- Vulnerable algorithms "disabled, isolated or tunnelled" by completion — ITSM.40.001 [5] — Deprecation discipline enforced through policy rollouts with custody evidence (Section 7.3).
- Full migration by end of 2035 — ITSM.40.001 / NCSC [5][7] — Fleet-wide policy convergence, verified from twins and custody records.

11. Maturity and Forward Path

Aegis delivery aligns with the Northwind and Helios Grid phases and with the mandate clock:

- Phase — Aegis scope
- Phase 1 — Hybrid key establishment (X25519+ML-KEM-768) on every link and Helios control channel; ML-DSA signing for custody, telemetry, and registry artifacts; LMS-signed boot chain on node and hub tiers; first crypto-policy artifact and CBOM baseline. Outcome: no quantum-vulnerable key exchange anywhere in the fielded fabric.
- Phase 2 — Defence ceiling profile (ML-KEM-1024 / ML-DSA-87) for designated segments; cuPQC batched verification at the FOB-IFC; hybrid certificates fleet-wide; SLH-DSA policy option for high-evidentiary records; deprecation of classical-only negotiation.
- Phase 3 — Central-IFC key-lifecycle and registry-signing services on cuPQC/liboqs; FN-DSA adoption for bandwidth-starved bearers upon FIPS 206 finalization; classical algorithms removed from builds per the tunnelling discipline; continuous compliance reporting from the assurance register.

Open questions recorded as commitments for detailed design: FIPS-validated module selection per tier (including the certification status of the chosen embedded and GPU implementations); hardware key custody on tiers without a hardware root; hybrid-certificate profile selection as IETF work settles; and confirmation of cuPQC platform coverage against the fabric's exact GPU inventory [9].

12. Conclusion

Tangram made the Enkidu fabrics legible; Origi made them defensible; Helios Grid made them operable. Aegis Defence makes them durable — able to promise that what the fleet encrypts, signs, and boots today will still be confidential, authentic, and trusted when the adversary's computer is no longer classical.

Its contribution is discipline rather than invention: a finalized-standards-only suite with a reserve algorithm on independent mathematics behind every primary; hybrid key establishment so youth and obsolescence cover each other's weaknesses; signatures assigned to roles the mandates actually distinguish; the whole thing expressed as signed policy that Helios rolls out and Origi enforces, so that changing cryptography is an audited fleet operation; and a flat refusal to spend the fabric's weight and money on quantum hardware the mission cannot use.

Hybrid by default. Agile by construction. Nothing trusted to mathematics a quantum computer is known to break.

References

[1] NIST. NIST Releases First 3 Finalized Post-Quantum Encryption Standards (FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA), August 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standa rds

[2] NIST CSRC. Post-Quantum Cryptography Standardization Process (HQC selected March 11, 2025; FN-DSA / FIPS 206 in development). https://csrc.nist.gov/projects/post-quantum-cryptograp hy/post-quantum-cryptography-standardization

[3] Applied Quantum / PostQuantum. CNSA 2.0: Complete Guide to NSA's PQC Requirements (ML-KEM-1024, ML-DSA-87, QKD exclusion, timelines). https://postquantum.com/cnsa-2-0/complete-guide/

[4] Encryption Consulting. Quantum-Proof with CNSA 2.0 (LMS with SHA-256 preference for code signing; QKD not recommended for NSS). https://www.encryptionconsulting.com/quantum-proof-wit h-cnsa-2-0/

[5] Canadian Centre for Cyber Security. Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada (ITSM.40.001) (plans by April 2026; high-priority by end 2031; all systems by end 2035; "disabled, isolated or tunnelled"). https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

[6] Treasury Board of Canada Secretariat. Migrating the Government of Canada to Post-Quantum Cryptography: Security Policy Implementation Notice. https://www.canada.ca/en/government/system/digital-gov ernment/policies-standards/spin/migrating-government-c anada-post-quantum-cryptography.html

[7] U.K. National Cyber Security Centre. Timelines for Migration to Post-Quantum Cryptography (2035 completion target). https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[8] RAND Corporation. U.S.-Allied Militaries Must Prepare for the Quantum Threat to Cryptography (PQC vs. QKD; NSA position; allied agency choices). https://www.rand.org/pubs/commentary/2025/06/us-allied -militaries-must-prepare-for-the-quantum-threat/

[9] NVIDIA. cuPQC — GPU-Accelerated Post-Quantum Cryptography SDK (ML-KEM/ML-DSA performance; cuHash). https://developer.nvidia.com/cupqc ; https://docs.nvidia.com/cuda/cupqc/introduction.html

[10] NVIDIA. Introducing NVIDIA cuPQC for GPU-Accelerated Post-Quantum Cryptography (ML-KEM-768 throughput on H100; side-channel review). NVIDIA Technical Blog. https://developer.nvidia.com/blog/introducing-nvidia-c upqc-for-gpu-accelerated-post-quantum-cryptography/

[11] Post-Quantum Cryptography Alliance / Linux Foundation. Open Quantum Safe Integrates NVIDIA cuPQC (liboqs GPU backends; batched verification use cases); cuPQC SDK v0.4 (Merkle trees, hash primitives for XMSS/LMS-class schemes). https://www.linuxfoundation.org/press/post-quantum-cry ptography-alliance-brings-accelerated-computing-to-pos t-quantum-cryptography-with-nvidia-cupqc ; https://pqca.org/blog/2025/release-of-cupqc-sdk-v0-4-a ccelerating-quantum-safe-cryptography/

[12] OpenSSL 3.5 post-quantum support (ML-KEM, ML-DSA, SLH-DSA; hybrid X25519MLKEM768 as a default TLS 1.3 key share). https://faisalyahya.com/access-control/openssl-3-5-ent ering-the-post-quantum-era/ ; https://www.cryptomathic.com/blog/quantum-ready-crypto graphy-with-openssl-3.5-on-rhel-9.6

[13] SystemsHardening. Post-Quantum TLS 1.3 in Production: Deploying X25519+ML-KEM-768 (IETF hybrid design; codepoints; microsecond-scale handshake overhead). https://www.systemshardening.com/articles/network/tls- post-quantum-hybrid-deployment/

[14] wolfSSL. wolfCrypt Post-Quantum (CNSA 2.0-compliant ML-KEM/ML-DSA/SLH-DSA/LMS/XMSS; ARM assembly optimization; (D)TLS 1.3 integration; verify-only stateful-signature builds for embedded).

https://www.wolfssl.com/products/wolfcrypt-post-quantum/

[15] wolfSSL. Post-Quantum SSH Hybrid Key Exchange (mlkem768x25519-sha256; mlkem1024nistp384-sha384; draft-ietf-sshm-mlkem-hybrid-kex). https://www.wolfssl.com/category/post-quantum/

[16] Quantum Security Defence. QKD in Government: What Works and What Doesn't (NCSC and NSA positions; architectural limits — tactical/mobile, trusted relays, authentication dependence, DoS; niche fixed-link deployments). https://quantumsecuritydefence.com/quantum-news/quantu m-key-distribution-government-deployments/

[17] arXiv. Securing Cryptography in the Age of Quantum Computing and AI (key/ciphertext/signature size ranges for ML-KEM, ML-DSA, SLH-DSA; Grover and symmetric sizing; HNDL). https://arxiv.org/pdf/2603.06969

[18] Innovation, Science and Economic Development Canada. National Quantum Strategy Roadmap: Quantum Communication and Post-Quantum Cryptography (QEYSSat satellite QKD demonstration). https://ised-isde.canada.ca/site/national-quantum-stra tegy/en/national-quantum-strategy-roadmap-quantum-comm unication-and-post-quantum-cryptography

[19] Enkidu Enterprises (2026). Northwind — Conceptual Architecture for a Distributed Fusion-in-a-Box Edge Platform, v0.14.

[20] Enkidu Enterprises (2026). Helios Grid — The Control Plane for Distributed Intelligence, v0.1.

[21] Enkidu Enterprises (2026). Trust Assurance Overview (Origi), v1.0; Tangram Overview, v1.0.