ENKIDU

— MIOVSKI GROUP —

KONZEPTARCHITEKTUR

Aegis Defence

Die quantenresistente kryptografische Schicht des Enkidu-Stacks — hybride Post-Quanten-Schlüsselaushandlung, quantenresistente Signaturen und flottenweite Krypto-Agilität, durchgesetzt von Origi und betrieben von Helios Grid über das Northwind-Gewebe.

Deutsch · Kompaktausgabe

Nach Version 0.1 · 4. Juli 2026

Erstellt von MIOVSKI GROUP

Einstufung · Nicht klassifiziert · Entwurf zur internen Prüfung

Die vollständige englische Ausgabe ist maßgeblich

Zu dieser Ausgabe

Dieses Dokument ist eine deutsche Kompaktausgabe von « Aegis Defence — Conceptual Architecture », Version 0.1 (4. Juli 2026), erstellt von der Miovski Group. Jeder Abschnitt des Originals ist in gekürzter Form vertreten. Bei Abweichungen ist die vollständige englische Ausgabe maßgeblich. Einstufung: nicht klassifiziert — Entwurf zur internen Prüfung.

Zusammenfassung

Jedes Versprechen des Enkidu-Stacks ruht am Ende auf Kryptografie. Origis Beweiskette sind Signaturen; Helios Grids Artefaktzulassung sind Signaturen; jede Mesh-Verbindung, jede Rückverbindungsspeiche und jeder Steuerkanal ist ein Schlüsselaustausch. Heute sind diese Primitiven — Schlüsselvereinbarung über elliptische Kurven und klassische Signaturen — sicher. Gegen einen kryptanalytisch relevanten Quantencomputer sind sie es nicht: Shors Algorithmus bricht sie vollständig, und der Angriff jetzt ernten, später entschlüsseln" bedeutet, dass heute an einer Rückverbindung mitgeschnittener Verkehr rückwirkend lesbar wird, sobald eine solche Maschine existiert. Für ein Gewebe, das Protected-B-Daten mit jahrzehntelanger Sensitivität trägt, ist die Quantenbedrohung kein Zukunftsproblem — sie ist ein gegenwärtiges Aufzeichnungsproblem.

Aegis Defence ist Enkidus Antwort: das quantenresistente kryptografische Framework des Stacks und sein viertes Grundframework. Wo Tangram einem Gewebe seine Struktur gibt, Origi sein Laufzeitvertrauen und Helios Grid seine Betreibbarkeit, gibt Aegis ihm kryptografische Langlebigkeit — hybride Post-Quanten-Schlüsselaushandlung auf jeder Verbindung, quantenresistente Signaturen auf jedem Artefakt und Beweisketteneintrag, und Krypto-Agilität als Flottenoperation statt als Reengineering-Projekt.

Aegis ist bewusst konservativ und bewusst normgebunden. Seine Algorithmen-Suite ist der finalisierte NIST-Satz — ML-KEM (FIPS 203), ML-DSA (FIPS 204), SLH-DSA (FIPS 205), mit HQC als codebasierter Reserve und LMS/XMSS für die Firmware-Signierung — eingesetzt in hybriden Konstruktionen nach IETF-Praxis, ausgerichtet an CNSA 2.0 für die Verteidigungsebenen und an Kanadas ITSM.40.001-Zeitplan für Regierungssysteme. Es ist heute auf genau der Hardware umsetzbar, die Northwind einsetzt: ARM-optimierte eingebettete PQC-Bibliotheken auf den Jetson-Knoten- und Hub-Ebenen und NVIDIAs cuPQC-SDK für gebündelte, GPU-beschleunigte Verifikation an den Grace-Blackwell-Fusionszentren. Und es lehnt Quantenschlüsselverteilung (QKD) für dieses Gewebe ausdrücklich ab, im Einklang mit alliierten Vorgaben der nationalen Sicherheit.

Ein Satz trägt den Entwurf: hybrid als Standard, agil durch Konstruktion, und nichts Mathematik anvertraut, die ein Quantencomputer nachweislich bricht.

1. Zweck und Geltungsbereich

Dies ist eine Konzeptarchitektur, kein Implementierungshandbuch und keine kryptografische Spezifikation: Sie definiert Aegis' Struktur, seine Algorithmen-Suite, seine Protokollbindungen und seine Verträge mit den anderen Enkidu-Frameworks. Die Referenzimplementierung ist Northwind — die härteste Version des Problems: umkämpfte, bandbreitenarme Verbindungen, Sicherheitseinstufung, Wirte vom batteriebetriebenen Jetson-Knoten bis zum Grace-Blackwell-Rechenzentrum, und Daten, deren Sensitivität jeden glaubwürdigen Quantenhorizont überdauert. Dieselbe Architektur, mit zivilen Parameterprofilen, ist die kryptografische Schicht für Lamassu, Helios Grid und jede weitere Enkidu-Installation.

Aegis ist keine neue Komponentenebene auf dem Gewebe; es ist die kryptografische Substanz der bestehenden Ebenen. Origis Regime gesicherter Kommunikation, seine Beweiskette und seine Zulassungsprüfungen sind Aegis-Algorithmen; Helios' Enrollment-Identitäten, sein signierter Sollzustand und seine signierten Runbooks sind Aegis-Signaturen. Aegis definiert die Suite, die Bindungen und die Änderungsdisziplin; Origi setzt sie an jeder Grenze durch; Helios verteilt sie an jeden Knoten. Was Aegis nicht ist: keine Schlüsselhinterlegung, keine hausgemachten Primitiven, keine unstandardisierten Algorithmen — in der Kryptografie ist Neuheit Risiko.

2. Die Quantenbedrohung und die Mandate

Was bricht und was nicht: Ein Quantencomputer mit Shors Algorithmus bricht die heutige Public-Key-Kryptografie — RSA, Elliptische-Kurven-Diffie-Hellman, ECDSA — vollständig. Grover schwächt symmetrische Kryptografie nur quadratisch, was mit Schlüsselgröße beantwortet wird: AES-256 und die SHA-2/SHA-3-Familien bleiben sicher. Die präzise Konsequenz für den Stack: Jeder Schlüsselaustausch und jede Signatur müssen migrieren; symmetrische Verschlüsselung und Hashing brauchen Parameterdisziplin, keinen Ersatz.

Die Dringlichkeit ist asymmetrisch: Eine in der Zukunft gefälschte Signatur verfälscht nicht rückwirkend die Vergangenheit; ein in der Zukunft gebrochener Schlüsselaustausch legt aber rückwirkend alles offen, was er schützte. Ein Gegner, der heute Northwinds Rückverbindungsverkehr aufzeichnet, braucht keinen Quantencomputer — nur Geduld und Speicher. Deshalb ist Aegis' erste Welle hybride KEMs auf den Verbindungen, nicht Signaturen. Und der Übergang ist nicht mehr spekulativ: Das NIST veröffentlichte die finalisierten Normen im August 2024, HQC wurde im März 2025 als codebasierte Reserve gewählt, und FN-DSA (FIPS 206) ist in Arbeit — eine bewusste Streuung über Gitter, Hashfunktionen und Codes.

- NSA (US-Systeme der nationalen Sicherheit) — CNSA 2.0 — ML-KEM-1024 und ML-DSA-87; LMS/XMSS für Code-Signierung; QKD ausdrücklich ausgeschlossen; Migration nach Produktklassen bis in die frühen 2030er.
- CSE / Kanadisches Zentrum für Cybersicherheit — ITSM.40.001 + TBS-SPIN — Ressortpläne bis April 2026; hochprioritäre Systeme bis Ende 2031 migriert; alle Systeme bis Ende 2035; verwundbare Algorithmen deaktiviert, isoliert oder getunnelt".
- NCSC (Vereinigtes Königreich) — PQC-Migrationszeitpläne — Erfassung und Planung jetzt; vollständige Migration bis 2035.

Ein für die kanadischen Streitkräfte ausgebrachtes Northwind fällt unter die strengste Lesart aller drei: Aegis nimmt daher die CNSA-2.0-Parameter als Obergrenzenprofil und ITSM.40.001 als bindenden Zeitplan. Der Mandatshorizont ist nicht das Ankunftsdatum des Quantencomputers: Er ist die Geduld des aufzeichnenden Gegners, abgezogen von der Lebensdauer Ihrer Daten.

3. Entwurfsprämisse und Invarianten

Aegis ruht auf einem Satz: hybrid als Standard, agil durch Konstruktion, und nichts Mathematik anvertraut, die ein Quantencomputer nachweislich bricht. Hybrid, weil die Post-Quanten-Algorithmen jung sind und die klassischen quantenverloren — ihre Kombination lässt eine Sitzung den Ausfall eines der beiden überleben. Agil, weil die einzige Gewissheit eines jungen Feldes der Wandel ist: Algorithmen, Parameter und Codepunkte werden sich bewegen, und eine Flotte von zehntausend Knoten muss als Betriebsaufgabe folgen, nicht als Neubau.

- 01 · Nur Normen — jeder Algorithmus der Suite ist eine finalisierte NIST-Norm oder eine ausdrücklich benannte Reserve aus dem NIST-Prozess. Keine hausgemachten Primitiven, niemals.
- 02 · Hybrid bis zum gegenteiligen Mandat — die Schlüsselaushandlung kombiniert einen klassischen Austausch mit einem Post-Quanten-KEM (z. B. X25519 + ML-KEM-768); reine PQC-Modi nur dort, wo ein Mandat es vorschreibt.
- 03 · Algorithmenvielfalt wird in Reserve gehalten — hinter jedem Primären eine Reserve auf anderer Mathematik — HQC hinter ML-KEM, SLH-DSA hinter ML-DSA — vorintegriert, damit eine kryptanalytische Überraschung ein Richtlinienwechsel ist, kein Krisenprogramm.
- 04 · Kryptografische Richtlinie ist ein signiertes Artefakt — die aktive Suite, Parameter und Bindungen je Flottensegment stehen in einem versionierten, signierten Kryptorichtlinien-Artefakt, verteilt von Helios Grid und zugelassen von Origi wie jedes Artefakt.
- 05 · Die symmetrische Schicht wird dimensioniert, nicht ersetzt — AES-256, SHA-2/SHA-3 (384 Bit und mehr auf den höchsten Ebenen) bleiben; Grover wird mit Schlüssel- und Digestgröße beantwortet.
- 06 · Nichts wird entfernt, bevor es getunnelt ist — klassische Algorithmen werden nur nach der Mandatsdisziplin zurückgezogen — deaktiviert, isoliert oder in eine quantenresistente Schicht getunnelt — niemals stillschweigend in einem Rückfallpfad belassen.

Warum nicht warten? Zwei Argumente beenden die Frage: Jetzt ernten, später entschlüsseln" — die heute aufgezeichneten Daten sind bereits verloren oder sicher, je nachdem, was sie heute schützt — und die Kalenderarithmetik: Kanadas Hochprioritätsfrist ist Ende 2031, Northwinds Phase 1 wird im selben Fenster ausgebracht, und eine nachgerüstete Kryptoschicht kostet ein Mehrfaches einer von Anfang an entworfenen. Aegis existiert, damit Northwind niemals eine quantenverwundbare Verbindung ausliefert.

4. Die Aegis-Algorithmen-Suite

Die Suite weist jeder kryptografischen Funktion einen primären und einen Reserve-Algorithmus zu, mit Parametern je Einsatzebene — Verteidigungs-Obergrenzenprofil nach CNSA 2.0, Standardprofil nach NIST Level 3 und den Empfehlungen des Cyberzentrums für Protected B.

- Schlüsselaushandlung (Verbindungen, Sitzungen) — hybrid X25519 + ML-KEM-768 (Standard); hybrid mit ML-KEM-1024 (Verteidigungsobergrenze) — HQC als codebasierte Reserve; reiner ML-KEM-Modus, wo mandatiert.
- Signaturen — Beweiskette, Telemetrie, Enrollment, Urteile — ML-DSA-65 (Standard); ML-DSA-87 (Verteidigungsobergrenze) — SLH-DSA als hashbasierte Reserve auf unabhängiger Mathematik.
- Signaturen — Firmware, Bootkette, BSP-Images — LMS (SHA-256), XMSS — zustandsbehaftete Verfahren nach CNSA-2.0-Code-Signierungsdoktrin; Verify-only-Builds auf beschränkten Knoten.
- Signaturen — Artefaktregister (Modelle, Container, Richtlinien) — ML-DSA, doppelt signiert mit LMS für Basissystem-Artefakte.
- Symmetrische Verschlüsselung — AES-256 (GCM) — unverändert; in dieser Größe quantenresistent.
- Hashing / Beweisketten-Verkettung — SHA-384 / SHA-512, SHA-3-Familie — Struktur unverändert; Digestgrößen je Profil.
- Zertifikate / PKI — ML-DSA-Ketten; hybride Zertifikate während der Übergangszeit — klassische Ketten getunnelt in Aegis-geschützten Kanälen bis zum Rückzug.

Zwei bewusste Auslassungen: FN-DSA (Falcon) wird beobachtet, aber nicht übernommen, bis FIPS 206 finalisiert ist — seine kompakten Signaturen sind für die bandbreitenärmsten Verbindungen attraktiv, sein Platz ist reserviert — und kein Algorithmus außerhalb des NIST-Prozesses erscheint irgendwo.

5. Die Schichtarchitektur

Aegis materialisiert sich an vier Bindungspunkten, die alle bereits im Stack existieren — das ist der Punkt: Aegis ist eine Substitution kryptografischer Substanz, keine Hinzufügung beweglicher Teile. Verbindungsschutz: Jede Verbindung des Gewebes und jeder Helios-Steuerkanal läuft auf TLS 1.3 mit der hybriden Gruppe X25519+ML-KEM-768, DTLS 1.3 für datagrammorientierte Mesh-Träger und hybrides SSH für die Administration — der aufzeichnende Gegner gewinnt nichts. Identität: Die Zertifikatsketten von Knoten, Wardens, Cores und Bedienern wechseln zu ML-DSA, mit hybriden Zertifikaten während des Übergangsfensters; private Schlüssel liegen in Hardware, wo die Ebene es erlaubt.

Integrität: Origis Beweiskette wird mit ML-DSA signiert und mit Digests der SHA-384-Klasse verkettet, SLH-DSA per Richtlinie für Einträge mit hohem Beweisgewicht verfügbar; Helios-Artefakte werden im Register ML-DSA-signiert und am Knoten im Moment der Zulassung verifiziert — die Prüfung läuft stets an der letzten Vertrauensgrenze vor der Nutzung. Boot: Ein quantenresistentes Gewebe, das von einem quantenfälschbaren Loader gestartet wird, ist ein Widerspruch — die Bootkette wird mit den zustandsbehafteten hashbasierten Verfahren (LMS/XMSS) signiert; der Slot, der die Aegis-Prüfung nicht besteht, ist der Slot, der niemals bootet. Aegis fügt dem Gewebe keine Komponente hinzu: Es ändert, woraus jeder Handshake, jede Signatur und jede Bootprüfung besteht.

6. Abbildung auf das Gewebe

Die Kosten der PQC sind asymmetrisch — Rechenleistung ist fast gratis, Bandbreite nicht — und die Ebenen des Gewebes sind in der Gegenrichtung asymmetrisch. Aegis nutzt beides.

- FIB-Knoten (Jetson-Orin-Klasse) — PQC auf den ARM-Kernen: eingebettete, ARM-Assembler-optimierte ML-KEM/ML-DSA-Bibliotheken, LMS/XMSS verify-only; hybrides (D)TLS 1.3 auf jeder Verbindung. Die Handshakes eines Knotens kosten Millisekunden CPU pro Stunde.
- FIB-Hub (Thor-Klasse) — derselbe CPU-Stack, plus Hub-Pflichten: Terminierung Dutzender Sitzungen, Verifikation der Telemetriesignaturen der Knoten, Neusignierung von Aggregaten — bequem im CPU-Budget; die GPU bleibt der Inferenz gewidmet.
- FOB-IFC (GB300-Klasse) — hier beginnt cuPQC: gebündelte, GPU-beschleunigte ML-DSA-Verifikation für Beweisketten- und Telemetrieströme im Theatermaßstab und gebündelte ML-KEM-Operationen für das Sitzungsmanagement über Dutzende Hubs.
- Central IFC (NVL72-Klasse) — voller cuPQC-Einsatz über die liboqs-Integration: Register-Signaturinfrastruktur, flottenweite Bündelverifikation (Millionen Operationen pro Sekunde und GPU), Schlüssellebenszyklus-Dienste, Autorenkette der Kryptorichtlinie.

7. Krypto-Agilität — Kryptografie als verwaltetes Artefakt

Die tiefste Lehre des letzten Jahrzehnts der Kryptanalyse — einschließlich des abrupten Zusammenbruchs eines NIST-Viertrundenkandidaten 2022 gegen einen klassischen Angriff — lautet: Vertrauen in junge Mathematik kann plötzlich versagen. Aegis' Antwort: den Wechsel der Kryptografie zur routinemäßigen Flottenoperation machen. Die aktive Suite wird je Segment in einem signierten, versionierten Kryptorichtlinien-Artefakt deklariert und von Helios genau wie ein Modell verteilt: gestaffelte Wellen, Gesundheitsschranken (Handshake-Erfolgsraten, Interoperabilität mit der Vorgängerrichtlinie), automatisches Rollback, volle Beweiskette. Eine Flotte von ML-KEM-768 auf ML-KEM-1024 umzustellen — oder im Überraschungsszenario von ML-KEM auf HQC — ist ein Rollout, kein Programm.

Jedes Mandat beginnt mit der Erfassung: Man migriert nicht, was man nicht inventarisiert hat. Im Enkidu-Stack ist das fast gratis — der Helios-Knotenzwilling verzeichnet bereits jedes installierte Artefakt und jede Bindung, sodass das kryptografische Inventar der Flotte (CBOM) eine Abfrage über die Zwillinge ist, kein manuelles Audit. Und die Migration ist erst abgeschlossen, wenn der verwundbare Algorithmus aus der Aushandlung verschwunden ist: erst den Standardstatus verlieren, dann auf getunnelte Altschnittstellen hinter Aegis-geschützten Kanälen beschränkt, dann aus dem Build entfernt — jeder Schritt ein Flottenrollout mit Beweisspur, sodass beweisen Sie, dass RSA weg ist" aus dem Register beantwortet wird.

8. Dimensionierung und Leistung auf umkämpften Verbindungen

Die wahre Steuer der PQC auf Northwind sind Bytes, nicht Zyklen — und sie beißt auf den Mesh-Trägern. Ein öffentlicher Schlüssel/ein Chiffrat von ML-KEM-768 wiegt ~1,2/1,1 KB (gegenüber 32 Bytes bei X25519), einmal pro Handshake bezahlt; eine ML-DSA-Signatur wiegt 2,4 bis 4,6 KB (gegenüber 64-72 Bytes bei ECDSA), pro signiertem Eintrag bezahlt — der dominierende wiederkehrende Posten; SLH-DSA, ab ~7,9 KB, bleibt Einträgen mit hohem Beweisgewicht und Firmware-Rollen vorbehalten.

Drei Milderungen halten das in den Hüllen des Gewebes: Handshake-Amortisation — Mesh-Sitzungen sind langlebig und werden wiederaufgenommen, Handshakes amortisieren sich über Stunden; Signaturaggregation am Hub — Knoten signieren auf Eintragsebene, Hubs verifizieren lokal und leiten hubsignierte Aggregate weiter, sodass Einzelsignaturen die Rückverbindung nicht einzeln durchqueren — was sich exakt mit Helios' Signal statt Daten"-Reduktion zusammenfügt; und die Kompaktsignatur-Reserve — FN-DSAs Platz existiert für die knappsten Träger, sobald FIPS 206 finalisiert ist. Der Restaufwand wird zur Eingangsgröße von Helios' Telemetriehüllen-Arithmetik statt zur Überraschung im Feld.

9. Die Position zur Quantenschlüsselverteilung

Aegis bezieht eine klare Position: keine QKD auf diesem Gewebe. Die Gründe sind die der alliierten Behörden, und sie sind architektonisch: QKD verlangt optische Spezialausrüstung — eine Hardwarelösung, wo PQC eine Softwarelösung ist; sie passt nicht zu mobiler und taktischer Kommunikation und zu Pfaden über Relais außerhalb der eigenen Kontrolle; sie verteilt Schlüssel, authentifiziert aber nicht und hängt damit ohnehin an Signaturen auf PQC-Niveau; und sie konzentriert Denial-of-Service-Risiko in einem mit Licht sättigbaren Kanal. Die NSA unterstützt QKD für nationale Sicherheitssysteme nicht, und CNSA 2.0 schließt sie aus. Ein Beobachtungspunkt ist festgehalten: Feste strategische Punkt-zu-Punkt-Verbindungen zwischen permanenten Central-IFC-Standorten sind die einzige Nische mit existierenden QKD-Installationen (Kanadas QEYSSat-Programm erprobt Satelliten-QKD); sollte die Politik sich ändern, träte eine solche Verbindung als weitere Schlüsselquelle unter Aegis' hybride Ableitung — eine zusätzliche Schicht, niemals ein Ersatz, und niemals auf dem taktischen Gewebe.

10. Konformitätsübersicht

Jede Mandatsanforderung ist auf ihren Mechanismus abgebildet: ML-KEM-1024/ML-DSA-87 für Systeme der NSS-Klasse über das Obergrenzenprofil der Kryptorichtlinie; LMS/XMSS für Code-Signierung über die Boot-Rollen; der QKD-Ausschluss durch die Position von Abschnitt 9; Migrationspläne und Jahresberichte ab April 2026 über das aus den Zwillingen erzeugte CBOM und die Versionshistorie der Richtlinie; die Frist Ende 2031 über die erste hybride Welle auf allen Verbindungen; deaktiviert, isoliert oder getunnelt" über die Rückzugsdisziplin; und die vollständige Migration 2035 über flottenweite Richtlinienkonvergenz, verifiziert aus Zwillingen und Beweisspuren.

11. Reifegrad und weiterer Weg

Die Lieferung richtet sich an den Phasen von Northwind und Helios Grid und an der Mandatsuhr aus. Phase 1: hybride Schlüsselaushandlung auf jeder Verbindung und jedem Steuerkanal; ML-DSA-Signierung für Beweiskette, Telemetrie und Registerartefakte; LMS-signierte Bootkette; erstes Kryptorichtlinien-Artefakt und CBOM-Basislinie — Ergebnis: kein quantenverwundbarer Schlüsselaustausch irgendwo im ausgebrachten Gewebe. Phase 2: Verteidigungs-Obergrenzenprofil für benannte Segmente; cuPQC-Bündelverifikation am FOB-IFC; hybride Zertifikate flottenweit; SLH-DSA-Richtlinienoption; Rückzug der rein klassischen Aushandlung. Phase 3: zentrale Schlüssellebenszyklus- und Registersignaturdienste auf cuPQC/liboqs; FN-DSA-Übernahme für knappe Träger nach Finalisierung von FIPS 206; klassische Algorithmen aus den Builds entfernt; kontinuierliche Konformitätsberichte. Offene Fragen — FIPS-validierte Modulauswahl je Ebene, Hardware-Schlüsselverwahrung, hybride Zertifikatsprofile, cuPQC-Plattformabdeckung — sind als Verpflichtungen für den Detailentwurf festgehalten.

Schlussfolgerung

Tangram machte die Enkidu-Gewebe lesbar; Origi machte sie verteidigbar; Helios Grid machte sie betreibbar. Aegis Defence macht sie dauerhaft — fähig zu versprechen, dass das, was die Flotte heute verschlüsselt, signiert und bootet, noch vertraulich, authentisch und vertrauenswürdig sein wird, wenn der Computer des Gegners nicht mehr klassisch ist.

Sein Beitrag ist Disziplin statt Erfindung: eine Suite ausschließlich finalisierter Normen, mit einer Reserve auf unabhängiger Mathematik hinter jedem Primären; hybride Schlüsselaushandlung, damit Jugend und Veralterung einander die Schwächen decken; Signaturen, die den Rollen zugewiesen sind, die die Mandate tatsächlich unterscheiden; das Ganze als signierte Richtlinie ausgedrückt, die Helios ausrollt und Origi durchsetzt, sodass der Wechsel der Kryptografie eine auditierte Flottenoperation ist; und die klare Weigerung, Gewicht und Geld des Gewebes für Quantenhardware auszugeben, die die Mission nicht nutzen kann.

Hybrid als Standard. Agil durch Konstruktion. Nichts Mathematik anvertraut, die ein Quantencomputer nachweislich bricht.