ENKIDU

— MIOVSKI GROUP —

ARCHITECTURE CONCEPTUELLE

Aegis Defence

La couche cryptographique résistante au quantique de la pile Enkidu — établissement de clés post-quantique hybride, signatures résistantes au quantique et crypto-agilité à l'échelle de la flotte, appliquée par Origi et exploitée par Helios Grid sur le tissu Northwind.

Français · Édition condensée

D'après la version 0.1 · 4 juillet 2026

Préparé par MIOVSKI GROUP

Classification · Non classifié · Ébauche pour examen interne

L'édition anglaise complète fait foi

À propos de cette édition

Ce document est une édition condensée, en français, de « Aegis Defence — Conceptual Architecture », version 0.1 (4 juillet 2026), préparée par Miovski Group. Chaque section de l’original y est représentée sous forme abrégée. En cas de divergence, l’édition anglaise complète fait foi. Classification : non classifié — ébauche pour examen interne.

Résumé

Chaque promesse de la pile Enkidu repose, en dernier ressort, sur la cryptographie. La chaîne de possession d'Origi, ce sont des signatures ; l'admission d'artefacts d'Helios Grid, ce sont des signatures ; chaque liaison du maillage, chaque rayon de liaison arrière et chaque canal de contrôle est un échange de clés. Aujourd'hui, ces primitives — accord de clés à courbes elliptiques et signatures classiques — sont sûres. Face à un ordinateur quantique cryptanalytiquement pertinent, elles ne le sont pas : l'algorithme de Shor les brise entièrement, et l'attaque « récolter maintenant, déchiffrer plus tard » signifie que le trafic enregistré aujourd'hui sur une liaison arrière pourra être lu rétroactivement le jour où une telle machine existera. Pour un tissu qui porte des données Protégé B à la sensibilité pluri-décennale, la menace quantique n'est pas un problème futur — c'est un problème d'enregistrement présent.

Aegis Defence est la réponse d'Enkidu : le cadre cryptographique résistant au quantique de la pile, et son quatrième cadre fondamental. Là où Tangram donne au tissu sa structure, Origi sa confiance à l'exécution et Helios Grid son exploitabilité, Aegis lui donne sa longévité cryptographique — établissement de clés post-quantique hybride sur chaque liaison, signatures résistantes au quantique sur chaque artefact et enregistrement de possession, et une crypto-agilité conçue comme une opération de flotte plutôt qu'un projet de réingénierie.

Aegis est délibérément conservateur et délibérément lié aux normes. Sa suite d'algorithmes est l'ensemble NIST finalisé — ML-KEM (FIPS 203), ML-DSA (FIPS 204), SLH-DSA (FIPS 205), avec HQC comme réserve à base de codes et LMS/XMSS pour la signature de micrologiciels — déployé en constructions hybrides selon la pratique IETF, aligné sur CNSA 2.0 pour les paliers de défense et sur le calendrier ITSM.40.001 du Canada pour les systèmes du gouvernement. Il est réalisable aujourd'hui sur le matériel exact que Northwind déploie : bibliothèques PQC embarquées optimisées ARM aux niveaux nœud et concentrateur Jetson, et le SDK cuPQC de NVIDIA pour la vérification par lots, accélérée par GPU, aux niveaux des centres de fusion Grace-Blackwell. Et il rejette explicitement la distribution quantique de clés (QKD) pour ce tissu, conformément aux orientations alliées de sécurité nationale.

Une phrase porte le dessein : hybride par défaut, agile par construction, et rien de confié à des mathématiques qu'un ordinateur quantique sait briser.

1. Objet et portée

Ceci est une architecture conceptuelle, non un manuel d'implémentation ni une spécification cryptographique : elle définit la structure d'Aegis, sa suite d'algorithmes, ses liaisons de protocole et ses contrats avec les autres cadres Enkidu. Le déploiement de référence est Northwind — la version la plus difficile du problème : liaisons contestées et pauvres en bande passante, classification de sécurité, hôtes allant d'un nœud Jetson sur batterie à un centre de données Grace-Blackwell, et des données dont la sensibilité dépasse tout horizon crédible d'ordinateur quantique. La même architecture, avec des profils de paramètres civils, est la couche cryptographique de Lamassu, d'Helios Grid et de tout autre déploiement Enkidu.

Aegis n'est pas un nouveau plan de composants sur le tissu ; il est la substance cryptographique des plans existants. Le régime de communications sécurisées d'Origi, sa chaîne de possession et ses contrôles d'admission sont des algorithmes Aegis ; les identités d'enrôlement d'Helios, son état désiré signé et ses runbooks signés sont des signatures Aegis. Aegis définit la suite, les liaisons et la discipline de changement ; Origi les applique à chaque frontière ; Helios les distribue à chaque nœud. Ce qu'Aegis n'est pas : pas de séquestre de clés, pas de primitives maison, pas d'algorithmes non normalisés — en cryptographie, la nouveauté est un risque.

2. La menace quantique et les mandats

Ce qui casse, et ce qui ne casse pas : un ordinateur quantique exécutant Shor brise complètement la cryptographie à clé publique actuelle — RSA, Diffie-Hellman à courbes elliptiques, ECDSA. Grover n'affaiblit la cryptographie symétrique que de façon quadratique, ce à quoi répond la taille des clés : AES-256 et les familles SHA-2/SHA-3 restent sûres. Conséquence précise pour la pile : chaque échange de clés et chaque signature doivent migrer ; le chiffrement symétrique et le hachage exigent une discipline de paramètres, pas un remplacement.

L'urgence est asymétrique : une signature contrefaite dans le futur ne falsifie pas rétroactivement le passé ; mais un échange de clés brisé dans le futur expose rétroactivement tout ce qu'il protégeait. Un adversaire qui enregistre aujourd'hui le trafic de liaison arrière de Northwind n'a besoin d'aucun ordinateur quantique — seulement de patience et de stockage. C'est pourquoi la première vague d'Aegis porte sur les KEM hybrides des liaisons, non sur les signatures. Et la transition n'est plus spéculative : le NIST a publié les normes finalisées en août 2024, HQC a été retenu en mars 2025 comme KEM de réserve à base de codes, et FN-DSA (FIPS 206) est en préparation — une diversité délibérée entre treillis, fonctions de hachage et codes.

- NSA (systèmes de sécurité nationale des É.-U.) — CNSA 2.0 — ML-KEM-1024 et ML-DSA-87 ; LMS/XMSS pour la signature de code ; QKD explicitement exclue ; migration par classes de produits jusqu'au début des années 2030.
- CSE / Centre canadien pour la cybersécurité — ITSM.40.001 + SPIN du SCT — plans ministériels d'ici avril 2026 ; systèmes hautement prioritaires migrés d'ici fin 2031 ; tous les systèmes d'ici fin 2035 ; les algorithmes vulnérables « désactivés, isolés ou tunnellisés ».
- NCSC (R.-U.) — calendriers de migration PQC — découverte et planification maintenant ; migration complète d'ici 2035.

Un Northwind déployé pour les Forces armées canadiennes relève de la lecture la plus stricte des trois : Aegis prend donc les paramètres CNSA 2.0 comme profil plafond et ITSM.40.001 comme calendrier contraignant. L'horizon du mandat n'est pas la date d'arrivée de l'ordinateur quantique : c'est la patience de l'adversaire qui enregistre, soustraite de la durée de vie de vos données.

3. Prémisse de conception et invariants

Aegis repose sur une phrase : hybride par défaut, agile par construction, et rien de confié à des mathématiques qu'un ordinateur quantique sait briser. Hybride, parce que les algorithmes post-quantiques sont jeunes et que les classiques sont condamnés par le quantique — les combiner fait survivre la session à la défaillance de l'un ou de l'autre. Agile, parce que la seule certitude d'un domaine jeune est le changement : algorithmes, paramètres et points de code bougeront, et une flotte de dix mille nœuds doit suivre comme une tâche d'exploitation, pas une reconstruction.

- 01 · Normes seulement — chaque algorithme de la suite est une norme NIST finalisée ou une réserve explicitement désignée du processus NIST. Aucune primitive maison, jamais.
- 02 · Hybride jusqu'à mandat contraire — l'établissement de clés combine un échange classique et un KEM post-quantique (p. ex. X25519 + ML-KEM-768) ; les modes purement PQC ne sont activés que là où un mandat le prescrit.
- 03 · La diversité d'algorithmes est tenue en réserve — derrière chaque primaire, une réserve sur des mathématiques différentes — HQC derrière ML-KEM, SLH-DSA derrière ML-DSA — pré-intégrée, pour qu'une surprise cryptanalytique soit un basculement de politique, pas un programme de crise.
- 04 · La politique cryptographique est un artefact signé — la suite active, les paramètres et les liaisons par segment de flotte sont déclarés dans un artefact de crypto-politique versionné et signé, distribué par Helios Grid et admis par Origi comme tout artefact.
- 05 · La couche symétrique est dimensionnée, pas remplacée — AES-256, SHA-2/SHA-3 (384 bits et plus aux paliers les plus élevés) sont conservés ; Grover reçoit pour réponse la taille des clés et des empreintes.
- 06 · Rien n'est retiré avant d'être tunnellisé — les algorithmes classiques ne sont retirés que selon la discipline du mandat — désactivés, isolés ou tunnellisés dans une couche résistante au quantique — jamais laissés en silence dans un chemin de repli.

Pourquoi ne pas attendre ? Deux arguments closent la question : l'attaque « récolter maintenant, déchiffrer plus tard » — les données enregistrées aujourd'hui sont déjà perdues ou sauves selon ce qui les protège aujourd'hui — et l'arithmétique du calendrier : l'échéance canadienne haute priorité est fin 2031, la phase 1 de Northwind se déploie dans la même fenêtre, et une couche cryptographique rattrapée après déploiement coûte un multiple de celle conçue d'emblée. Aegis existe pour que Northwind ne livre jamais une liaison vulnérable au quantique.

4. La suite d’algorithmes Aegis

La suite affecte à chaque fonction cryptographique un algorithme primaire et une réserve, avec des paramètres profilés par palier de déploiement — profil plafond de défense selon CNSA 2.0, profil standard selon le niveau 3 du NIST et les recommandations du Centre pour la cybersécurité pour le Protégé B.

- Établissement de clés (liaisons, sessions) — hybride X25519 + ML-KEM-768 (standard) ; hybride avec ML-KEM-1024 (plafond défense) — HQC en réserve à base de codes ; mode ML-KEM pur disponible là où mandaté.
- Signatures — possession, télémétrie, enrôlement, verdicts — ML-DSA-65 (standard) ; ML-DSA-87 (plafond défense) — SLH-DSA en réserve à base de hachage, sur des mathématiques indépendantes.
- Signatures — micrologiciel, chaîne d’amorçage, images BSP — LMS (SHA-256), XMSS — schémas à état, par la doctrine de signature de code CNSA 2.0 ; versions de vérification seule sur les nœuds contraints.
- Signatures — registre d’artefacts (modèles, conteneurs, politiques) — ML-DSA, double signature LMS pour les artefacts de base système.
- Chiffrement symétrique — AES-256 (GCM) — inchangé ; résistant au quantique à cette taille.
- Hachage / chaînage de possession — SHA-384 / SHA-512, famille SHA-3 — structure inchangée ; tailles d’empreinte fixées par profil.
- Certificats / ICP — chaînes ML-DSA ; certificats hybrides pendant la transition — chaînes classiques tunnellisées dans des canaux protégés par Aegis jusqu’au retrait.

Deux omissions délibérées : FN-DSA (Falcon) est suivi mais non adopté avant la finalisation de FIPS 206 — ses signatures compactes intéressent les liaisons les plus affamées en bande passante, et sa place est réservée — et aucun algorithme hors du processus NIST n’apparaît, nulle part.

5. L’architecture en couches

Aegis se matérialise en quatre points de liaison qui existent déjà tous dans la pile — c’est le point : Aegis est une substitution de substance cryptographique, non un ajout de pièces mobiles. Protection des liaisons : chaque liaison du tissu et chaque canal de contrôle Helios passe en TLS 1.3 avec le groupe hybride X25519+ML-KEM-768, DTLS 1.3 pour les supports maillés orientés datagrammes, et SSH hybride pour l’administration — l’adversaire qui enregistre n’y gagne rien. Identité : les chaînes de certificats des nœuds, Wardens, Cores et opérateurs passent à ML-DSA, avec des certificats hybrides pendant la fenêtre de transition ; les clés privées résident dans du matériel là où le palier le permet.

Intégrité : la chaîne de possession d’Origi est signée en ML-DSA avec des empreintes de classe SHA-384, SLH-DSA disponible par politique pour les enregistrements à fort poids probatoire ; les artefacts Helios sont signés ML-DSA au registre et vérifiés au nœud au moment de l’admission — la vérification court toujours à la dernière frontière de confiance avant l’usage. Amorçage : un tissu résistant au quantique amorcé par un chargeur falsifiable au quantique est une contradiction — la chaîne d’amorçage est signée avec les schémas à base de hachage à état (LMS/XMSS) ; l’emplacement qui échoue à la vérification Aegis est l’emplacement qui ne démarre jamais. Aegis n’ajoute aucun composant au tissu : il change ce dont chaque poignée de main, signature et contrôle d’amorçage est fait.

6. Projection sur le tissu

Les coûts de la PQC sont asymétriques — le calcul est presque gratuit, la bande passante non — et les paliers du tissu sont asymétriques en sens inverse. Aegis exploite les deux.

- Nœud FIB (classe Jetson Orin) — PQC côté CPU sur les cœurs ARM : bibliothèques embarquées ML-KEM/ML-DSA optimisées en assembleur ARM, LMS/XMSS en vérification seule ; (D)TLS 1.3 hybride sur chaque liaison. Les poignées de main d'un nœud coûtent des millisecondes de CPU par heure.
- Concentrateur FIB (classe Thor) — même pile CPU, plus les devoirs de concentrateur : terminaison de dizaines de sessions, vérification des signatures de télémétrie des nœuds, re-signature des agrégats — confortablement dans le budget CPU ; le GPU reste dédié à l'inférence.
- FOB-IFC (classe GB300) — entrée de cuPQC : vérification ML-DSA par lots, accélérée GPU, pour les flux de possession et de télémétrie à l'échelle du théâtre, et opérations ML-KEM par lots pour la gestion de sessions sur des dizaines de concentrateurs.
- Central IFC (classe NVL72) — déploiement cuPQC complet via l'intégration liboqs : infrastructure de signature du registre, vérification par lots à l'échelle de la flotte (des millions d'opérations par seconde et par GPU), services de cycle de vie des clés, chaîne d'édition de la crypto-politique.

7. Crypto-agilité — la cryptographie comme artefact géré

La leçon la plus profonde de la dernière décennie de cryptanalyse — dont l'effondrement soudain, en 2022, d'un candidat NIST de quatrième tour face à une attaque classique — est que la confiance en de jeunes mathématiques peut céder brutalement. La réponse d'Aegis : faire du changement de cryptographie une opération de flotte de routine. La suite active est déclarée par segment dans un artefact de crypto-politique signé et versionné, distribué par Helios exactement comme un modèle : vagues échelonnées, barrières de santé (taux de réussite des poignées de main, interopérabilité avec la politique précédente), retour arrière automatique, possession intégrale. Basculer une flotte de ML-KEM-768 à ML-KEM-1024 — ou, dans le scénario surprise, de ML-KEM à HQC — est un déploiement, pas un programme.

Tout mandat commence par la découverte : on ne migre pas ce qu'on n'a pas inventorié. Dans la pile Enkidu, c'est presque gratuit — le jumeau de nœud d'Helios enregistre déjà chaque artefact et liaison installés, si bien que l'inventaire cryptographique de la flotte (CBOM) est une requête sur les jumeaux, pas un audit manuel. Et la migration ne s'achève que lorsque l'algorithme vulnérable a disparu de la négociation : d'abord retiré du statut par défaut, puis confiné à des interfaces héritées tunnellisées derrière des canaux protégés par Aegis, puis retiré de la compilation — chaque étape étant un déploiement de flotte avec trace de possession, de sorte que « prouvez que RSA a disparu » se répond depuis le registre.

8. Dimensionnement et performance sur liaisons contestées

Le véritable impôt de la PQC sur Northwind, ce sont les octets, pas les cycles — et ce sont les supports maillés qu'il mord. Une clé publique/un chiffré ML-KEM-768 pèsent ~1,2/1,1 Ko (contre 32 octets en X25519), payés une fois par poignée de main ; une signature ML-DSA pèse 2,4 à 4,6 Ko (contre 64-72 octets en ECDSA), payée par enregistrement signé — le coût récurrent dominant ; SLH-DSA, à ~7,9 Ko et plus, est réservé aux enregistrements à fort poids probatoire et aux rôles de micrologiciel.

Trois atténuations tiennent le tout dans les enveloppes du tissu : l'amortissement des poignées de main — les sessions maillées sont longues et reprises, les poignées de main s'amortissent sur des heures de liaison ; le regroupement des signatures au concentrateur — les nœuds signent au niveau de l'enregistrement, les concentrateurs vérifient localement et font suivre des agrégats signés par eux, si bien que les signatures individuelles ne transitent pas la liaison arrière — ce qui se compose exactement avec la réduction « signal, pas données » d'Helios ; et la réserve à signatures compactes — la place de FN-DSA existe pour les supports les plus contraints dès la finalisation de FIPS 206. Le surcoût résiduel devient une donnée d'entrée de l'arithmétique d'enveloppe de télémétrie d'Helios, plutôt qu'une surprise découverte sur le terrain.

9. La position sur la distribution quantique de clés

Aegis prend une position nette : pas de QKD sur ce tissu. Les raisons sont celles des agences alliées, et elles sont architecturales : la QKD exige des équipements optiques dédiés — une solution matérielle là où la PQC est logicielle ; elle est inadaptée aux communications mobiles et tactiques et à tout chemin traversant des relais hors du contrôle de l'organisation ; elle distribue des clés mais n'authentifie pas, dépendant donc de toute façon de signatures de niveau PQC ; et elle concentre un risque de déni de service dans un canal saturable. La NSA ne soutient pas la QKD pour les systèmes de sécurité nationale et CNSA 2.0 l'exclut. Un point de veille est consigné : les liaisons fixes stratégiques point à point entre sites permanents du Central IFC sont l'unique niche où des déploiements QKD existent (le programme canadien QEYSSat explore la QKD satellitaire) ; si la politique changeait, une telle liaison entrerait comme une source de clés supplémentaire sous la dérivation hybride d'Aegis — une couche de plus, jamais un remplacement, et jamais sur le tissu tactique.

10. Correspondance de conformité

Chaque exigence des mandats est tracée vers son mécanisme : ML-KEM-1024/ML-DSA-87 pour les systèmes de classe NSS via le profil plafond de la crypto-politique ; LMS/XMSS pour la signature de code via les rôles d’amorçage ; l’exclusion de la QKD par la position de la section 9 ; les plans de migration et rapports annuels dès avril 2026 via le CBOM issu des jumeaux et l’historique de versions de la politique ; l’échéance 2031 par la première vague hybride sur toutes les liaisons ; « désactivé, isolé ou tunnellisé » par la discipline de retrait ; et la migration complète 2035 par la convergence de politique à l’échelle de la flotte, vérifiée depuis les jumeaux et les traces de possession.

11. Maturité et chemin à venir

La livraison s’aligne sur les phases de Northwind et d’Helios Grid et sur l’horloge des mandats. Phase 1 : établissement de clés hybride sur chaque liaison et canal de contrôle ; signature ML-DSA pour la possession, la télémétrie et les artefacts ; chaîne d’amorçage signée LMS ; premier artefact de crypto-politique et CBOM de référence — résultat : aucun échange de clés vulnérable au quantique nulle part dans le tissu déployé. Phase 2 : profil plafond de défense pour les segments désignés ; vérification par lots cuPQC au FOB-IFC ; certificats hybrides à l’échelle de la flotte ; option SLH-DSA ; retrait de la négociation purement classique. Phase 3 : services centraux de cycle de vie des clés et de signature de registre sur cuPQC/liboqs ; adoption de FN-DSA pour les supports contraints à la finalisation de FIPS 206 ; algorithmes classiques retirés des compilations ; rapport de conformité continu. Les questions ouvertes — sélection de modules validés FIPS par palier, garde matérielle des clés, profils de certificats hybrides, couverture plateforme de cuPQC — sont consignées comme engagements pour la conception détaillée.

Conclusion

Tangram a rendu les tissus Enkidu lisibles ; Origi les a rendus défendables ; Helios Grid les a rendus exploitables. Aegis Defence les rend durables — capables de promettre que ce que la flotte chiffre, signe et amorce aujourd'hui sera encore confidentiel, authentique et digne de confiance quand l'ordinateur de l'adversaire ne sera plus classique.

Sa contribution est la discipline plutôt que l'invention : une suite composée exclusivement de normes finalisées, avec derrière chaque primaire une réserve sur des mathématiques indépendantes ; un établissement de clés hybride où la jeunesse et l'obsolescence couvrent mutuellement leurs faiblesses ; des signatures affectées aux rôles que les mandats distinguent réellement ; le tout exprimé en politique signée qu'Helios déploie et qu'Origi applique, de sorte que changer de cryptographie soit une opération de flotte auditée ; et un refus net de dépenser le poids et l'argent du tissu en matériel quantique que la mission ne peut utiliser.

Hybride par défaut. Agile par construction. Rien de confié à des mathématiques qu'un ordinateur quantique sait briser.