FORWARDEDGE

OCTANS SPACE AFRICA

White Paper

Isidore Quantum®

All-in-One Cybersecurity and Drop in PQC Solution

Cleared for Takeoff: Securing Aviation Against Today's Cyber Threats and Tomorrow's Quantum Crisis.

Why Isidore Quantum:

Affordable: 70% faster to implement and 60% lower total cost of ownership

Autonomous Cyber Resilience: AI-driven system detects, adapts, and self-heals against evolving threats

Drop-In Integration: Protocol, hardware, interface-agnostic design modernizes legacy networks without infrastructure overhaul

Low-SWaP Advantage: Compact, efficient, and scalable for enterprise, defense, and critical infrastructure use

The aviation industry faces a rapidly intensifying cybersecurity crisis made worse by the emerging quantum threat. Modern air traffic control, communication, and data systems, built on decades-old architectures, are already being targeted by ransomware, AI-driven intrusions, and supply chain attacks that exploit unencrypted protocols such as ADS-B, CPDLC, and SWIM. Vulnerabilities in these systems expose flight operations to spoofing, data manipulation, and command hijacking well before quantum computing reaches full offensive capability.

Adversaries are conducting Harvest Now, Decrypt Later (HNDL) campaigns, capturing encrypted aviation data today with the intent to decrypt it once quantum technology becomes capable of breaking current encryption methods. The growing overlap between active cyberattacks and the looming threat of quantum decryption has created an unparalleled level of risk for global aviation networks.

Isidore Quantum, created by Forward Edge-AI in collaboration with the NSA, provides a comprehensive zero-trust, post-quantum cybersecurity solution designed to safeguard aviation systems from both present and future attacks. The platform integrates AI-powered anomaly detection, autonomous key management, and CNSA 2.0-compliant encryption into a drop-in device that protects both legacy and NextGen aviation networks without requiring costly system overhauls. The result is a practical and resilient defense path for the aviation industry in an age of accelerating digital and quantum threats.

Q-Day is not a myth. It is a countdown. The question facing aviation isn't whether quantum disruption will occur—but whether we'll be ready.

The Threat to Aviation

Why it matters:

- ADS-B broadcasts unencrypted: Anyone can spoof aircraft positions or inject ghost flights
- CPDLC lacks authentication: Low-cost SDRs can hijack controller-pilot data links
- SWIM and SATCOM rely on TLS & PKI: Both collapse under quantum attack
- Legacy PKI = single point of systemic failure: Certificates, key loaders, and manual provisioning crumble under scale and speed

The next aviation crisis will begin in the network, not in the skies. Cyber adversaries are already infiltrating flight systems, stealing data, and preparing for the moment quantum computers render current encryption useless. Once that point is reached, every unprotected signal will serve as a weapon, and every flight path will become a potential target. The threat has already arrived.

Without post-quantum protection, airspace operations, fleet maintenance, and passenger safety face catastrophic exposure. Only 17 % of airlines have begun post-quantum assessments.

The Misconception:

CISOs delay quantum migration because they think the threat is “future.” But nation-states are harvesting data now, and Q-Day could arrive as early as 2026. Delaying action guarantees retroactive compromise of decades of flight data and control channels.

Isidore Quantum: All-in-One Cybersecurity PQC Solution

Isidore Quantum is a compact, NSA-engineered cybersecurity and post-quantum encryption platform purpose-built to protect aviation communications and control systems. Designed for seamless drop-in integration across ADS-B, CPDLC, SWIM, and SATCOM networks, it delivers zero-trust, CNSA 2.0-compliant protection without requiring infrastructure redesign. The device combines AI-driven threat detection, autonomous key management, and quantum-resistant encryption to defend against both current cyber intrusions and future quantum decryption attacks. Lightweight, energy-efficient, and field-validated, Isidore Quantum ensures continuous, secure operation for commercial, defense, and air traffic control environments worldwide.

Capability	What It Means
PKI-Free Architecture	Eliminates certificates, signatures and key-loader logistics entirely
CNSA 2.0-Compliant	Uses AES-256 GCM & ML KEM for PQC key exchange
AI-Driven Antifragility	Learns threat patterns → detects, isolates, and self-heals
Red/Black Isolation & Quantum Entropy	Hardware-enforced segmentation + Quantum Random Noise Generation for provably random, one-time keys
Plug-and-Play Integration	Works with ARINC 429/653/664, MIL-STD-1553, Ethernet, Wi-Fi, and SATCOM
Low-SWaP Edge Form Factor	< 8 W power, credit-card size, sub-millisecond latency, 58 GB/s throughput

Why it matters:

- ADS-B broadcasts unencrypted: Anyone can spoof aircraft positions or inject ghost flights
- CPDLC lacks authentication: Low-cost SDRs can hijack controller-pilot data links
- SWIM and SATCOM rely on TLS & PKI: Both collapse under quantum attack

Operational Fit for Aviation:

- Drop-in retrofit for existing avionics, ATC routers, and airport networks.
- Autonomous key lifecycle—no manual provisioning or key-management infrastructure
- Real-time quantum-safe channels for ADS-B, CPDLC, SWIM, and SATCOM data
- AI cyber-immune engine quarantines spoofed signals and rekeys within 3 seconds
- Meets FAA NextGen & ICAO CyAP mandates for zero-trust, data-driven protection

Relying on AES-256 alone creates a dangerous illusion of safety. The cipher itself remains strong, but the scaffolding around it is already crumbling. Quantum algorithms will tear through key exchanges, side-channel attacks will siphon secrets in real time, and AI-driven exploits will adapt faster than any patch. Defenders who cling to "AES-256 is enough" risk guarding an empty vault while intruders walk through unseen doors. The era ahead demands more than brute-force resistance; it demands architectures built for resilience against quantum speed, physical leakage, and machine-intelligent adversaries.

What Leaders Should Do Now

1. Audit Encryption Exposure - Map every system still using RSA, ECC, or Diffie-Hellman.
2. Plan the PQC Transition - Align with FAA NextGen and ICAO CyAP timelines; replace PKI early.
3. Deploy Isidore Quantum® - Start with high-risk channels — ADS-B, CPDLC, SATCOM, and SWIM.
4. Collaborate & Share - Join Forward Edge-AI industry pilots for cross-network validation.
5. Lead, Don't Lag - Compliance will soon be mandatory (CNSA 2.0 by 2026).
   First movers will define aviation's post-quantum safety standard.

The Takeaway

Quantum risk is immediate. Isidore Quantum gives aviation leaders a field-proven, NSA-engineered, zero-trust shield—the only drop-in PQC device that defends both legacy and NextGen airspace systems.

When every dollar, watt, and gram counts – Isidore Quantum is the clear choice.

Variants and Specifications:

Isidore-1: IoT/OT/SCADA

Isidore 50MB/s – 2 GB/s

One-Way-Data Diode

CubeSat

Enterprise

	50 Mb/s	480 Mb/s	1 - 2 Gb/s	10 Gb/s	68 Gb/s	1 Tb/s
Size, Weight & Power	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~7 W	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~10 W	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~12 W	Available Q3 2026	Available Q3 2026	Available Q4 2026
Environmental:	–40 °C to +85 °C; shock and vibration qualified					
Cryptography:	AES-256 GCM and ML-KEM					
Quantum Entropy:	Integrated Quantum Random Number Generator (QRNG) subsystem; validated per NIST SP 800-90 A/B/C and BSI AIS-31					
Topologies:	Point-to-point, point-to-multipoint, mesh, and hub-and-spoke; supports wired, wireless, and hybrid topologies					
Certifications and Compliance:	NSA CNSA 2.0, FIPS 140-3 (Level 3), NIST SP 800-90 A/B/C, BSI AIS-31, ECCN 5A002 (License Exception ENC)					
Latency:	<90 µs (estimated)					
Security Architecture	Hardware-enforced Red/Black separation with galvanic isolation; zero-trust, zero-touch operation; covert posture (no network announcements or responses to probes)					
AI / Autonomy	Embedded AI engine trained for real-time anomaly detection, and self-healing response					
Management System:	Cassian™ for fleet orchestration, provisioning, telemetry, and policy governance across distributed deployments					

1. Specifications listed are subject to change without prior notice.

Contact: octans@inhub.world | forwardedge.ai | octanspace.com