FORWARDEDGE

ISIDORE QUANTUM

ISIDORE 480-SC

Securing Space Infrastructure with Quantum-Resistant Cryptography

- Commercial National Security Algorithm Suite (CNSA-2.0) compliant quantum resistant cryptography
- Protocol, device, and network agnostic, ensuring seamless integration across various platforms, systems, and use cases without the need for any modifications
- Zero trust by default
- Dramatically reduces human resource requirements and cognitive load
- Comparable in size to a credit card, Isidore is significantly more portable than conventional devices that weigh ~30 pounds or more, and draw 70W of power
- Incorporates Artificial Intelligence and a Performant Rules Engine to autonomously detect and respond to cyber threats, providing an advanced level of security not typically found in existing cryptographic solutions

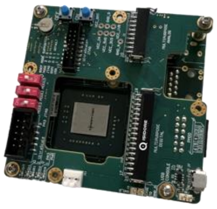
Getting Ready for the Post Quantum Cryptography Threat? You Should be.

The U.S. National Institutes of Science and Technology (NIST) initiated a Post Quantum Cryptography (PQC) program in 2016. The U.S. government is mandating their agencies to harden critical networks against quantum-computer vulnerabilities before 2027. Industry also will need to be doing this migration. The migration is not going to be easy or pain free. NIST estimates that perhaps 20 billion devices within the U.S. will need to be updated with Post-Quantum Cryptography (PQC), safeguarding.

Isidore Quantum® is compliant with NSA’s CNSA 2.0 and incorporates CNSA 2.0-approved algorithms, such as CRYSTALS-Kyber for key encapsulation. A notable feature of Isidore Quantum® is its autonomous key and channel management system. This system facilitates periodic rekeying, key recovery, and zeroization without manual intervention, ensuring continuous security and reducing the risk of key compromise. Such automation is crucial for maintaining secure communications in dynamic and high-risk environments.

FORWARDEDGE

ISIDORE QUANTUM



Features

- Black traffic is randomized to obfuscate underlying traffic structure and to anonymize the traffic
- Isidore Quantum is VLAN aware, can act as trunk or independent channels. Able to address multiple classification levels
- Protocol agnostic, designed for moderate topologies. Capable of mesh, hub and spoke, point to point, and point to multi-point:
  - Mesh topology (5 node mesh) - Unlike typical cryptographic mesh networks that must use a group key for all links, Isidore Quantum's mesh has the unique property that every link is independently keyed. Thus, the loss of a node does not mean loss of the entire constellation. Introduction of a new node is cryptographically transparent to the other nodes. Loss of node and remaining mesh automatically reconfigures routing to heal.
  - Topologies can scale as large as the comms path and HW will support. Isidore Quantum is not a niche solution.
- Commercial National Security Algorithm Suite (CNSA-2.0) compliant quantum resistant cryptography
- Protocol, device, and network agnostic, ensuring seamless integration across various platforms, systems, and use cases without the need for any modifications
- Scalable to Multiple Form Factors and Use Cases. Excellent Results:
  - UAS/drone to ground (point to point)
  - Encrypted analog radio pair
  - Reaper to ground (point to point)
  - Sigint Platform (mesh)
  - Ground-to-ground over satellite (Starlink)
  - Multiple phones over cellular (Hub and spoke)
- Network speeds:
  - On-going work to reach 100 Gig with COTS parts

Power and Throughput

- 5W
- 500Mbps

Weight and Dimensions

- 218g / 7.7oz
- 91x96x25mm / 3.6x3.8x1in

Keying Methodology

- CRYSTALS-Kyber for key encapsulation. PKI/KMI and certificate authorities not required. Ephemeral keying algorithms.

Operational Security

- No forensic footprint.

Warranty

- 5 Year manufacturer limited hardware and software

https://forwardedge.ai/product/

Trademarks are property of their respective owners. ©2025 Forward Edge-AI, Inc. All rights reserved.
Patent #11,588,798 B1. Other patents pending.