Product Brief

CRYPTO4A

Quantum Preparedness for the Connected World

QxEDGE™
Hybrid Security Platform

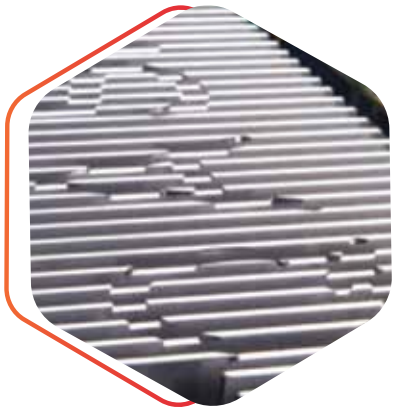
QxEDGE™ Hybrid Security Platform (HSP) is the next evolution of the Hardware Security Module (HSM) that brings together a Quantum Ready HSM, Confidential Compute, Quorum Authorization, Trusted Communications Matrix (TCMx), and the tools and level of integration required by development, security, and operations teams to develop, deploy, and manage their security applications at scale.

The QxEDGE™ is a flexible, programmable, and extensible cyber security platform that has been designed from the start to be Quantum Ready and Crypto Agile while also addressing issues around complexity, usability, and scaling of cyber security solutions. The QxEDGE™ ensures the security of both classic and post-quantum cryptographic key material and the applications that need to access it. It has the flexibility to support numerous applications that run in an environment that is familiar to DevOps teams by supporting the tools and technologies they use every day.

Quantum Preparedness

Digital transformation marks a radical rethinking of how organizations use technology, people, and processes to fundamentally change business practices. Due to advancements in Quantum Computing and the threat to our existing roots of trust, Edge Computing, 5G networks, AI, and the deployment of many billions of IoT devices, organizations need to rethink their approach to cyber security while facing a growing skills shortage.

www.CRYPTO4A.com
INFO@CRYPTO4A.COM



QASM™- New Quantum Ready Root of Trust

At the core of the QxEDGE™ is Crypto4A's next generation HSM, the Quantum Assured Security Module (QASM™), which encapsulates sensitive information within a cryptographic boundary protected by an always-on anti-tamper design providing support for both Classic and Post-Quantum Cryptographic algorithms with FPGA based Crypto Agility. This ensure quantum preparedness now and in the future giving organizations the ability to transition to new and evolving cryptographic algorithms in their applications, products, systems, and protocols.

The QASM™ leverages Quantum-safe hash-based signature (HBS) algorithms and key encapsulation mechanisms (KEMs) to ensure Quantum-safe boot-up procedures, code life-cycle management, and inter-QxEDGE™ communications for secure auto scaling, High Availability (HA) and Disaster Recovery (DR).

Confidential Compute

The QxEDGE provides a software defined, hardware enforced confidential compute environment that has the capability to run any x86 virtual machine, container, application, or algorithm without modification by leveraging the patented Trusted Communication Matrix (TCMx) to provide a trusted and secure full stack runtime environment with secure network zoning and processing engine isolation. By leveraging multiple onboard isolated compute engines complex solutions and workloads can be executed in an environment that prevents unauthorized access or modification of applications, data, keys, and algorithms while in use, in addition to ensuring the secure transfer of information to and from secure storage thereby increasing the security assurances for organizations that manage sensitive and regulated data.

Remote Management & Monitoring

The QxEDGE™ has been designed to allow for fully unattended Remote Management and Monitoring. To achieve this a flexible Quorum Authorization Process is provided to allow multiple users to control access to cryptographic material as well as its usage as members of a policy-based quorum. A second process known as Business Continuity of Operation (BCOOP) provides separate multi-person control that enables the secure archiving and restoration of highly critical keying material.

QxEDGE™ at a glance

- Quantum Assured Security Module (QASM™) containing multiple isolated HSMs instances with dedicated secure storage and processing
- Quantum-safe boot-up procedure(s), code life-cycle management, and inter-QxEDGE™ communications
- Trusted Communications Matrix (TCMx™) enabling Secure Network Zoning & Isolation using Secure One-Way Channels and Data Diodes
- 24/7 Active Anti-Tamper with dedicated backup power source
- FIPS validated random number generator using high-quality entropy generated from multiple independent hardware sources, including quantum random number generators (QRNG)
- QASM™ enforced Quorum Authorization Policy Engine to enable advanced policy-based separation of roles and functions
- Up to 6 Processing Engines (PE), each with Intel Quad Core Xeon CPU, 16GB of RAM, and 256GB of Solid-State Drive (SSD) storage running a Hardened Linux operating system with Docker and Kubernetes support
- Each QxEDGE™ PE can be configured with software defined, hardware enforced network access to one of 6 external 1Gbps Ethernet ports or isolated from external networks
- High Availability (HA), Disaster Recovery (DR) and Secure Auto Scaling features for managing multiple QxEDGE™ machines
- Cryptography: ITSP 40.111 compliant algorithms,full United States Commercial National Security Algorithm suite (CNSA), and support for NIST standards candidate PQC algorithms
- Unlimited client software licenses and unlimited key storage partition licenses included
- Standards: FIPS 140-2 Level 3(Pending - In Coordination), NIST SP 800-90B, NIST Entropy as a Service (EaaS) specification
- 19” 1U rackmount appliance with included mounting hardware
- Dual redundant power supplies

Applications

Quantum Safe HSM

Code Signing

Public Key Infrastructure (PKI)

Confidential compute

Secrets Vault

Domain Name System Security (DNSSEC)

Unified Key Management

Secure CI/CD Pipeline

Crypto Currency Multi Party Authorization

CRYPTO4A

About Crypto4A

Crypto4A is a Canadian cybersecurity technology company whose four founders developed the current market leading HSM over 25 years ago. After five years of research and leveraging 100 combined years of senior leadership experience in cryptography, key management and product development for government, military, and financial deployments, they designed a next generation HSM combining new processing capabilities for Quantum-safe cryptographic outcomes.

INFO@CRYPTO4A.COM

OTTAWA, ONTARIO, K1Z 7T2, CANADA

www.CRYPTO4A.com

linkedin.com/company/crypto4a