PATERO

QUANTUM SECURE COMMUNICATION

CryptoQoR - Quantum Safe Cryptomodule

Your Encryption is Obsolete

Quantum computing will bring unimaginable capabilities to science and business. No question. But they will also be used to crack the classical encryption we all use every day. In fact, the U.S. Government warns that adversaries are already collecting our encrypted data *because it will be decryptable later* with quantum computing.

Quantum Safety from SNDL is Essential

That's why quantum-safe encryption is so important now. The bad guys are storing our encrypted data now for decryption later (SNDL). Take it from Congress, the White House, the NSA, and NIST. The U.S. government is driving a national encryption upgrade. The NSA has already implemented quantum-safe encryption for itself. With NIST's standardization of quantum-safe encryption, small and remote offices can protect their "today" data as it traverses the "vulnerable attack" surface of the Internet from attacks tomorrow.

Patero Future Safes Your Data

Patero's highly efficient CryptoQoR software module protects data-in-motion with hybrid quantum-safe, NIST-standard post-quantum cryptography.

CryptoQoR provides end-to-end, hybrid post-quantum encrypted communication channels leveraging kernel-based multithreaded encryption. This high-performance, low latency, quantum-safe connectivity protects data-in-motion, retaining traditional encryption protection as the efficacy and resilience of quantum-resistant encryption evolve.

Hybrid

Patero hybridizes classic encryption with NIST standardized post-quantum-encryption as advocated by CISA, BSI and NIST.

Cryptoagile

CryptoQoR's modular design enables users to select and switch cryptographic algorithms

Standards-based

CryptoQoR combines today's trusted encryption with NIST candidates for quantum-resilient algorithms.

Ready to deploy

CryptoQoR leverages kernel-based symmetric encryption on a broad range of compute options including EDGE gateways, bare metal, VM's, cloud and mobile devices allowing for unified security architectures that protect critical assets without rip and replace.

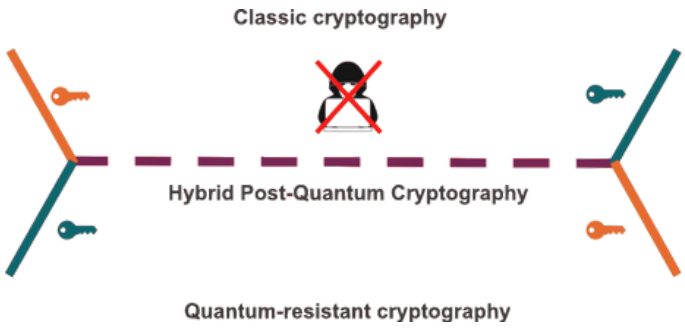
Red Hat Certified Technology · carahsoft · axiom MANUFACTURING SYSTEMS · ORACLE Partner · GIS GLOBAL INFRASTRUCTURE SOLUTIONS

ADVANTECH · ONLOGIC · WHITEHAWK · industry 4.0 Accelerator · PATERO QUANTUM SECURE COMMUNICATION

Deployment Topologies

QoR is software-based cryptography technology that establishes ultra-secure channels between defined endpoints to protect communications and data in transit from today's advanced attacks and tomorrow's quantum-based attacks. QoR is hardware-agnostic, can be deployed in new and existing assets and works in a broad range of compute options. The most common deployment topologies are:

- **Point to Point** - one-to-one channels transmitting sensitive data, including edge-to-anything and cloud-to-cloud topologies.
- **Multipoint to Point (Cloud)** - communication from multiple assets and/or locations to virtual private cloud or private cloud.
- **Multipoint to Point (on-premises)** - communication from multiple assets or locations that are consolidated in a central, on-premises server, datacenter or historian.



Specifications

Supporting Operating Systems

x86 based systems:
- RHEL 9
- Ubuntu 20.04
- Ubuntu 22.04
- Debian 10
- Debian 11
- Oracle Linux 9 UEK
- SELinux

ARM based systems:
- Ubuntu 20.04
- Ubuntu 22.04
- Raspbian 10
- Raspbian 11

Performance (*)

- Latency: < 1 msec
- Bandwidth: 99%
- CPU Load: < 5%

- Typical Performance of QoR encryption observed in Oracle Cloud Infrastructure. Performance may vary in your environment and depends on many factors like throughput, MTU size, CPU performance etc.

Recommended Edge Endpoint Configuration

QoR supports ARM and x86 endpoints:
- 1 GHz CPU
- 1 GB RAM
- 1 network interface

Supported network types are physical ethernet interfaces including WiFi, 4G / 5G.

Recommended Cloud Endpoint Configuration

QoR supports cloud-based virtual machines and containers:
- 2 GHz CPU, 4 cores
- 4 GB RAM
- 2 network interfaces

QoR supports standard VMWare, KVM, and OpenStack virtual interfaces. CPU and memory requirements depend on the desired throughput and latency.

Ships With Slectible Encryption

- CRYSTALS-Kyber 1024
- CRYSTALS-Kyber 768
- Classic McEliece 460896
- Classic McEliece 4668828
- Classic McEliece 8192128

QoR protects communications by cloaking internet-facing network elements and using hybrid post-quantum encryption to improve not replace today's encryption. Please visit www.patero.io

EMEA
Patero GmbH
Feldstraße 15
29386 Hankensbüttel
GERMANY
+49 151-16246830
quantumsafe@patero.de
www.patero.de

North America
Patero Inc.
7757 Baltimore Ave, Suite 1603
College Park, MD 20742
U.S.A
+1 650-641-0678
quantumsafe@patero.io
www.patero.io

PATERO
QUANTUM SECURE COMMUNICATION