PATERO
QUANTUM SECURE COMMUNICATION

Quantum-safe Enterprise Communication

Keep your secrets
Trust your network
Stay ahead of the bad guys

TODAY'S ENCRYPTION IS OBSOLETE

Using Shor's algorithm, Quantum Computers will decrypt data encrypted with asymmetric algorithms (RSA, Elliptic Curve). Your data is no longer safe.

Important long-life data is being stolen by bad actors already today to be decrypted tomorrow (steal now, decrypt later attacks) when they get their hands on cryptographically relevant quantum computers.

WHY ACT NOW?

On August 13th 2024 the NIST has announced the standardization of Post-Quantum Cryptography (PQC) and is now encouraging the industry to transition to the new standards "as soon as possible".

Why is this important today?

- Investment protection. Newly deployed assets should be quantum-safe!
- Mitigate "steal-now-decrypt-later" attacks!
- Transitioning to quantum-safe algorithms will take time!

WHY PATERO?

Patero has 6 years of experience in real-world PQC deployments:

- EGDE-to-Cloud applications
- Mobile devices and networks
- Satellite Communication
- Defense C3 / C4

Patero's CryptoQoR is a highly efficient crypto-agile software module that generates quantum-safe public-private key pairs using the NIST's quantum-safe cryptographic algorithms. CryptoQoR will also negotiate and generate quantum-safe symmetric keys for standard applications.

Let us be your first line of defense!

Hybrid Encryption

CISA, BSI and NIST advocate for "hybrid" post-quantum cryptography. Patero hybridizes classic encryption with NIST standardized post-quantum-encryption.

Cryptoagile

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

Standards-based

CryptoQoR combines today's trusted encryption with NIST standardized quantum-safe algorithms.

Ready to deploy

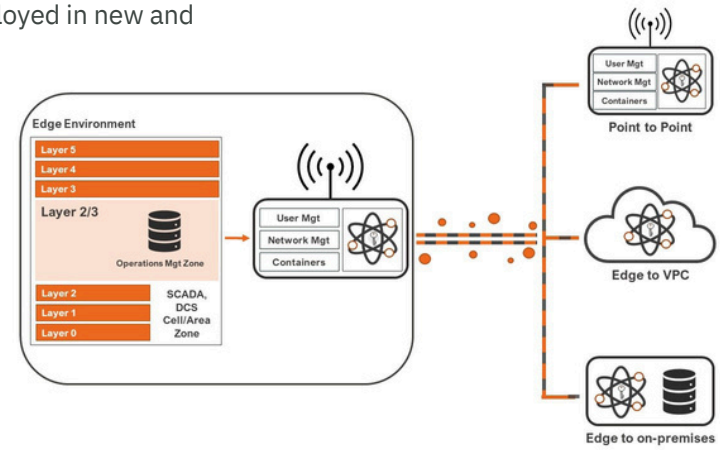
CryptoQoR leverages kernel-based symmetric encryption on a broad range of compute options including EDGE gateways, bare metal, VM's, cloud and mobile devices allowing for unified security architectures that protect critical assets without rip and replace.

Red Hat Certified Technology
ORACLE Partner
axiom MANUFACTURING SYSTEMS
GIS GLOBAL INFRASTRUCTURE SOLUTIONS
PATERO QUANTUM SECURE COMMUNICATION
ADVANTECH
carahsoft.
WHITEHAWK
industry 4.0 Accelerator

Deployment Topologies

CryptoQoR 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. CryptoQoR 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, classified or personal data.
  Example: MPLS replacement
- **Multipoint to Point (EDGE-to-Cloud)** - communication from multiple assets and/or locations to virtual private cloud or private cloud.
- **Multipoint to Point (on-premises)** - communication from multiple assets to a central, on-premises server.
  Example: Video surveillance cameras to camera server



Specifications

Supporting Operating Systems

x86 based systems:
- RHEL 9
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 11
- Debian 12
- Oracle Linux 9 UEK

ARM based systems:
- Ubuntu 22.04
- Ubuntu 24.04
- Raspbian OS
- Android 12+

RISC-V based systems:
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 12

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, Starlink, ...

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

More PQC algorithms will be supported in the future.

QoR protects communications by cloaking internet-facing network elements and using hybrid post-quantum encryption to enhance, 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