LIBREM PQC ENCRYPTOR

INFORMATION SHEET

for

Librem PQC Encryptor 10

Librem PQC Encryptor 100

Librem PQC Encryptor 400

Purism

Table of Contents

1. Overview

1.1. The Librem PQC Encryptor [10|100|400] takes a data link in, encrypts via Post Quantum Cryptography (PQC) toward the target Encryptor, and sends that PQC data link out. This PQC encryption can only be decrypted by the destination device, not even a quantum computer can compromise nor decrypt the data.

1.2. Post Quantum Cryptography (PQC) is the current and promoted NIST approved standard FIPS 203 of cryptographically guaranteeing data is the most secure possible.

1.3. The Librem PQC Encryptor [10|100|400] is targeted for Data In Transit (DIT). If the installation or ecosystem requires Data At Rest (DAR) on device, Purism has a complete PQC Ecosystem from User Equipment (UEs) to self-hosted on-premise PQC server as well as administrative tools for the entire ecosystem.

1.4. The Librem PQC Encryptor 10 leverages the pre-certified 3926 route/switch from Ciena: https://www.ciena.com/products/3926 utilizing its Field Replaceable Unit (FRU) to add Purism's unique implementation of PQC, where **the secret keys never leave the Librem PQC Encryptor 10**.

1.5. The Librem PQC Encryptor 100 and 400 leverage Librem Servers with PureBoot and Purism's unique implementation of PQC, where **the secret keys never leave the Librem PQC Encryptor [100|400].**

2. Librem PQC Encryptors Contents

2.1. Librem PQC Encryptor 10 Contents

2.1.1. PQC Encryptor 10 (on a Ciena 3926)

2.1.2. 4x 10Gbps Ports

2.1.3. Cabling

2.2. Librem PQC Encryptor 100 Contents

2.2.1. Librem PQC Encryptor 100

2.2.2. 2x 100Gbps Ports

2.2.3. Cabling

2.3. Librem PQC Encryptor 400 Contents

2.3.1. Librem PQC Encryptor 400

2.3.2. 8x 100Gbps Ports

2.3.3. Cabling

3. Librem PQC Encryptor Specifications

3.1. Librem PQC Encryptor 10 Specifications

Form Factor	1U Rackmount
Specs Page	https://www.ciena.com/products/3926

3.2. Librem PQC Encryptor 100/400 Specifications

Form Factor	4U Rackmount
Dimensions	W 16.93″ (430mm) H 6.93″ (176mm) D 20.57″ (522.4mm)
On-board Network Controllers	1Gb and 10Gb
PQC Data Network Controllers	2x100Gb QSFP28
Power Supply	500 W redundant power supplies
USB I/O	2x USB 2.0 (front) 2x USB 3.2 Gen 1 (rear)
Fans	1x 120mm PWM (front) 2x 80mm (rear)

4. PQC Implementation

4.1. Purism's Librem PQC Encryptor [10|100|400] utilizes the latest (published August 2024) NIST Standard FIPS 203 for pots-quantum cryptography. ML-KEM key exchange and AES-256 encryption protect the entire data stream.

4.2. Purism's implementation offers a unique approach whereby the secret key never leaves the Librem PQC Encryptor [10|100|400]. This ensures that security is not compromised by requiring to share the secret—as is the case with all symmetric key cryptography.

4.3. Purism's unique implementation allows for an administrator to setup devices (via the Librem PQC Admin Server), manage devices, sign certificates, and revoke device keys, without ever touching the secret key generated on device.

5. Librem PQC Admin Server

5.1. The Librem PQC Admin Server is a self-hosted on-premise (or in-domain) administrative server.

5.2. To set up a new Librem PQC Encryptor [10|100|400], an administrator creates a name for the PQC Encryptor, then authorizes it by generating a secret key and public certificate. After setup: one PQC Encryptor delivers quantum-safe data to a separate targeted PQC Encryptor.

6. Minimum Setup Requirements

6.1. Quantity 2: Librem PQC Encryptor [10|100|400]

It is required to have a Librem PQC Encryptor of identical specifications at both ends of the networking, during administrative setup one is married to the other for direct-link-encryption via that administrative interface (it can also allow group destinations if required).

6.2. Appropriate Cabling

Cabling from a Librem PQC Encryptor [10|100|400] to/from a Route/Switch is recommended.

6.3. Quantity 1: Librem PQC Admin Server

It is required to have a Librem Admin Server within network to administer the Librem PQC Encryptor [10|100|400] devices, public certs, revocation list, and any monitoring.

7. Conclusion

7.1. The Librem PQC Encryptor [10|100|400] offers full data encryption using the latest NIST standard for Post Quantum Cryptography (PQC) from one location to another, ensuring all Data in Transit (DIT) is cryptographically safe—even future-safe from a quantum computer attack.

7.2. The Librem PQC Encryptor [10|100|400] has added security by the unique implementation by Purism to generate secret keys on the Librem PQC Encryptor 10 itself and never having them leave.

7.3. The Librem PQC Encryptor 10 uses Ciena's certified hardware. The Librem PQC Encryptor [100|400] use Purism servers.

7.4. One Librem PQC Admin Server can manage all Librem PQC Encryptors on a given visible network.