Librem PQC Encryptor 400

A Data in Transit (DIT) Post Quantum Cryptography (PQC) Encryptor at 100Gbps Line Rate Speeds

- The **Librem PQC Encryptor 400** takes a data link in, encrypts via Post Quantum Cryptography (PQC) toward the target **Librem PQC Encryptor 400**, and sends that PQC encrypted data out.
- PQC encryption can only be decrypted by the destination device, not even a quantum computer can compromise nor decrypt the data.
- The **Librem PQC Encryptor 400** utilizes the latest (published August 2024) NIST Standard FIPS 203 for post-quantum cryptography. ML-KEM key exchange and AES-256 encryption protect the entire data stream.
- Offering Line Rate Speeds with PQC at **400Gbps** line rate with full PQC DIT.
- Purism's implementation of PQC offers a unique approach whereby the secret key never leaves the **Librem PQC Encryptor 400**. Ensuring that keys are not compromised by requiring to share the secret—as is the case with all symmetric key cryptography.
- Purism's unique implementation allows for an administrator to setup devices, manage devices, sign certificates, and revoke device keys, without ever touching the secret key generated on **Librem PQC Encryptor 400**.
- Utilizing an existing **Librem 4U Server**, and adding Purism's PQC solution with the added benefit that the secret keys generated on device never leaves.

Two Librem PQC Encryptor 400 devices offer drop-in PQC into an existing network, one at each end.

A **Librem PQC Admin Server** manages all Encryptors on the visible network.

Purism