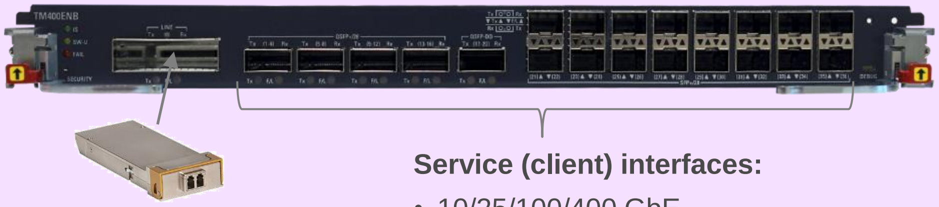
Layer 1 Optical Encryption with Quantum Solutions

ribbon®

Ronen Cohen – PLM Optical Networking

June 21, 2023

Apollo TM400ENB – 400G Multiservice Encryption Muxponder



Line interface:

- 400GZR+ CFP2-DCO

Service (client) interfaces:

- 10/25/100/400 GbE
- FC 16/32/64
- OTU2/OTU2e

Double slot card in any Apollo 9600 platform

Apollo 9603
2RU, 3 slots

Apollo 9608
5RU, 8 slots

Apollo 9624
15RU, 24 slots

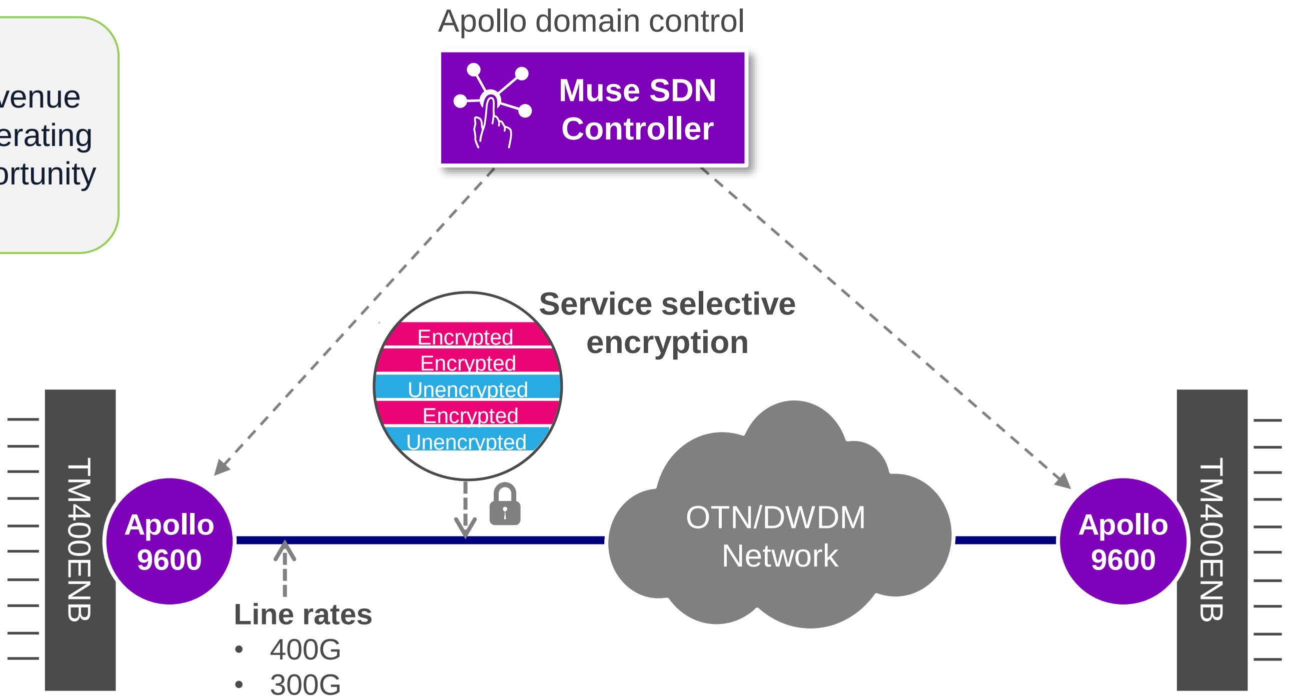
- Service selective encryption
- Highest-level AES-256 encoding
- Key exchanges mechanisms supported:
  - Standard Diffie-Hellman
  - Post Quantum Cryptography (PQC)
  - Quantum Key Distribution (QKD) via ETSI 014
- FIPS 140-3 SL3 compliant against physical tampering

Service Selective Encryption

Revenue generating opportunity

Multiservice mix

- 10/25/100/400 GbE
- FC 16/32/64
- OTU2/OTU2e



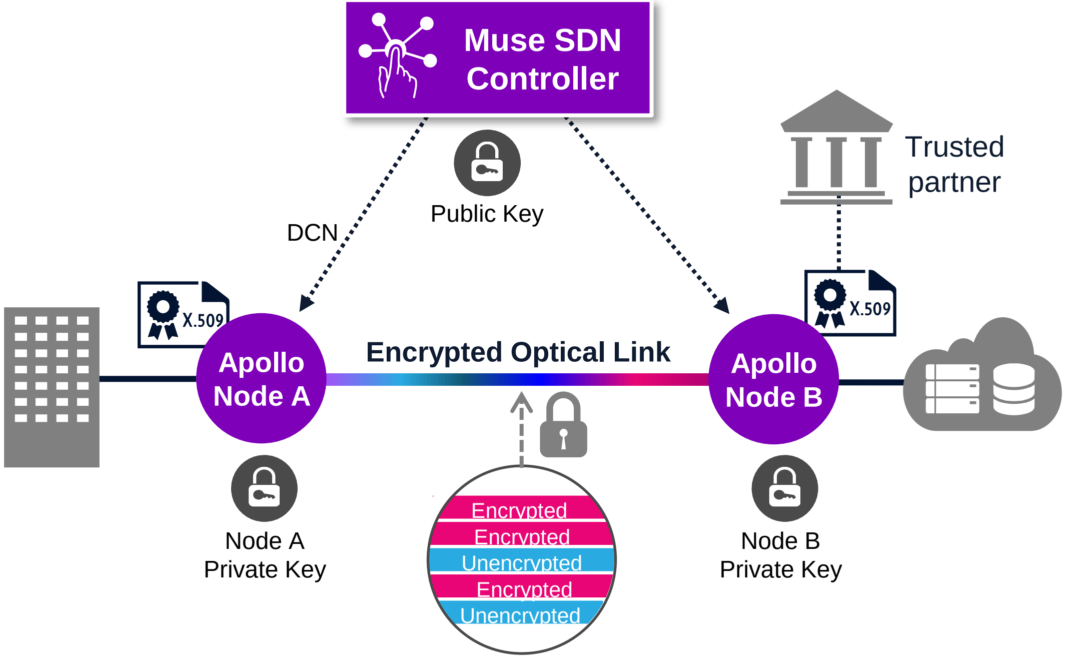
Apollo domain control

Line rates

- 400G
- 300G

L1OE with Diffie Hellman Key Exchange

1. **Authentication** – Apollo end nodes are authenticated using X.509 certificates via a trusted partner
2. **Symmetrical Encryption Key (SEK)** – Muse sends a public key to the Apollo nodes that they use to create an SEK
3. **Message Encryption** – The Apollo nodes use the SEK to encrypt selected services using AES-256
4. **Key Rotation** – A primary node (e.g. Node A) sends a “Key ID” over the DCN to the secondary node instructing the SEK to use next



Apollo Setup with QKD Device

Sync channel

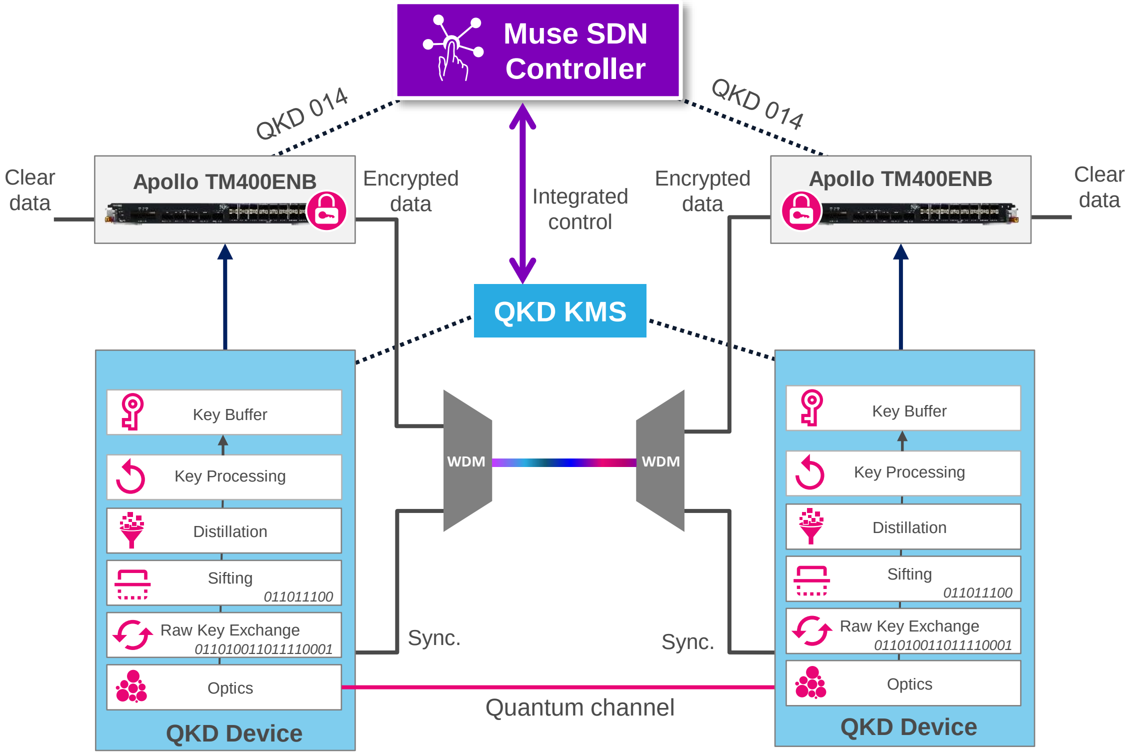
- 2.5Gbps line, SFP+, C-band

Quantum channel

- Dedicated fiber, < 150Km
- Extendable to long distances via intermediate trusted nodes, with methods under investigation using untrusted nodes
- Optional WDM with filters, decreased distance

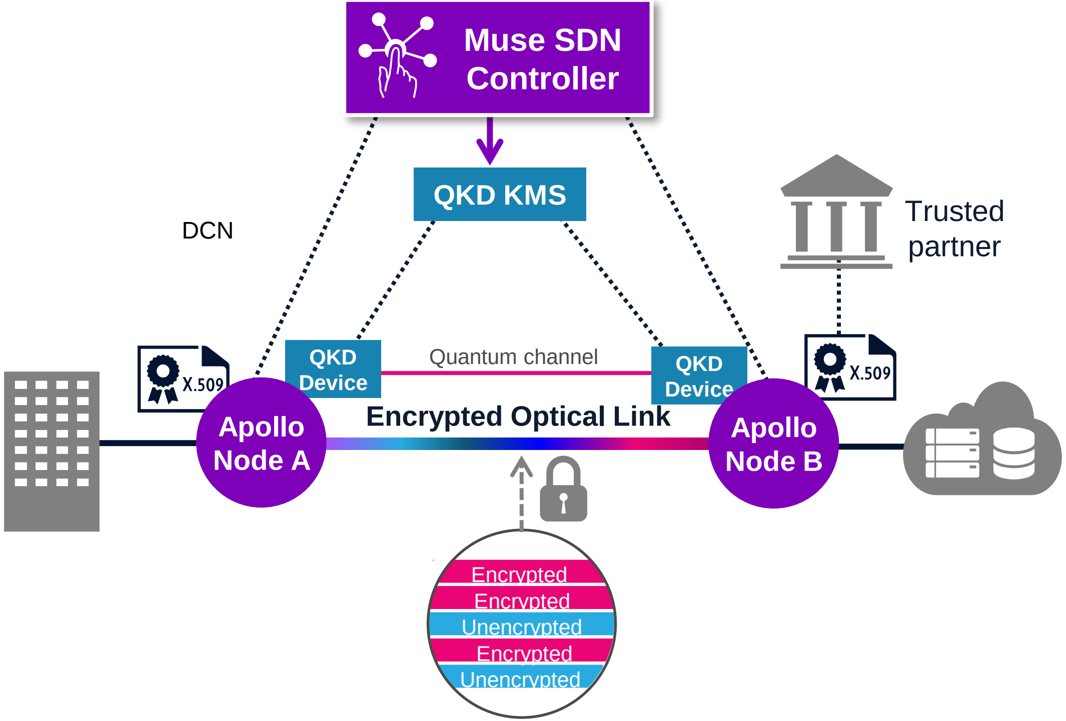
Integrated Control

- Via REST API to upper management (GUI cut-through for control, alarms, events)
- ETSI QKD 015 or 018 for SDN controller/orchestrator



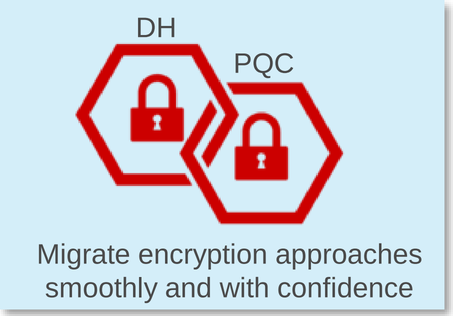
L1OE with QKD

1. **Authentication**
   - Apollo end nodes are authenticated using X.509 certificates via a trusted partner
   - Same process authenticates pairing of QKD devices with the Apollo nodes
2. **Symmetrical Encryption Key (SEK)** – The primary node QKD device sends entangled photons to the secondary node QKD device creating a SEK.
3. **Message Encryption** – The Apollo nodes use the SEK to encrypt selected services using AES-256
4. **Key Rotation** – Primary node generates the key and pushes it to its co-located encryptor, while sending the "Key ID" to secondary node, that generates same key and pushes it to its co-located encryptor

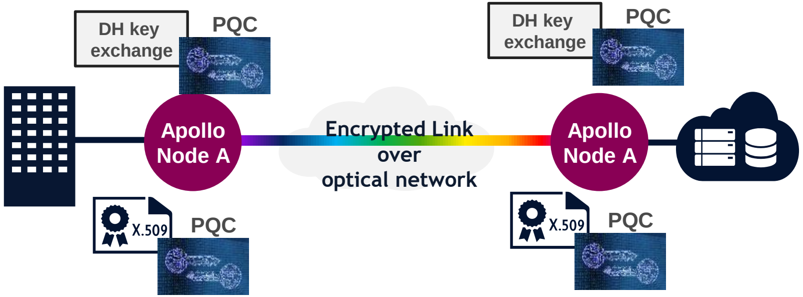


L1OE with PQC

- PQC key exchange algorithms available for:
  - Encryption (KEM: Key Encapsulation Mechanism)
  - Authentication (SIG: Digital Signature)
- Complimentary solution
  - Can use PQC mechanisms in addition to, or replacement for, existing Diffie-Hellman and X.509 mechanisms
- Following NIST standardization



Migrate encryption approaches smoothly and with confidence



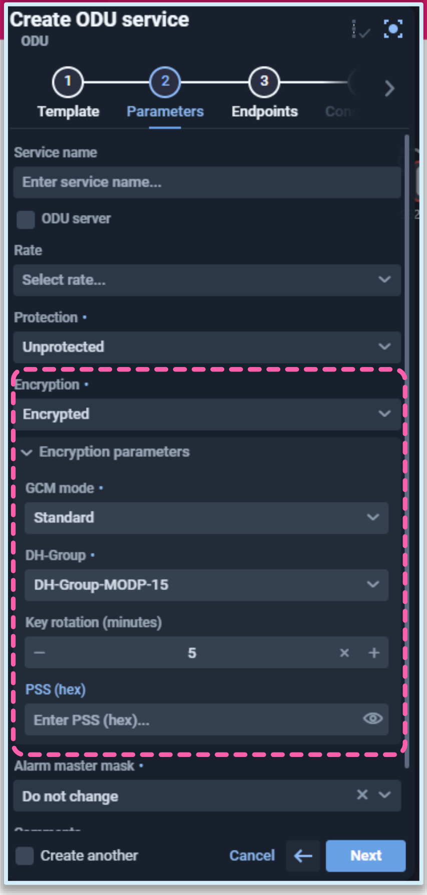
Encrypted Services in MUSE Network Controller

Service encryption parameters can be set in the ODU create/edit wizard

- **QKD Mode:** Key received via ETSI i/f
- **GCM mode** (non-QKD): Standard or disabled. In Standard mode, a failure to authenticate the frame, using the MIC, will cause the data to be replaced by an all-ones pattern.
- **DH-Group:** (non-QKD) Diffie Hellman (DH) groups are used to determine the strength of the key used in the Diffie-Hellman key exchange process. The higher the DH group numbers are, the more secure the key.
- **Key rotation:** The frequency at which the transmitter key will be rotated.
- **PSS (Pre-Shared Secret):** An optional parameter which influences the encryption keys generation. Provides the user a way to control the key content and strength.

Multi-Tenancy for end-customers key management

- The service provider will create a tenant users for their end-customer.
- Tenant users will only have access to network resource and services defined by the service provider.
- Tenant users will access the Network Controller UI to modify their encrypted services parameters.



Create ODU service
ODU

1 Template — 2 Parameters — 3 Endpoints — Con

Service name: Enter service name...

□ ODU server

Rate: Select rate...

Protection •: Unprotected

Encryption •: Encrypted

Encryption parameters

GCM mode •: Standard

DH-Group •: DH-Group-MODP-15

Key rotation (minutes): 5

PSS (hex): Enter PSS (hex)...

Alarm master mask •: Do not change

Summary

Industry-leading Layer 1 Optical Encryption solution

- 400Gbps links
- Service selective encryption
- Powerful management system

Extending for Quantum solutions

- Complementary PQC algos
- Multiple QKD device vendors
- Customer trials phase

ribbon®