ETSI The Standards People

IQC Institute for Quantum Computing

ETSI/IQC Quantum Safe Cryptography Conference 2026

Securing the AI supercycle through Innovation in Symmetric Key Cryptography and Quantum Key Distribution

Presented by:

NOKIA

18/06/2026

Agenda

1. **PQC for all networks**
2. MACsec Enhanced Update
3. Key distribution challenge
4. Final words

Agenda

1. **PQC for all networks**
2. MACsec Enhanced Update
3. Key distribution challenge
4. Final words

Networks in need of strong security

Let's protect our digital economy, starting today

Multi-tenant (services)
Segment Routing (SR-MPLS, SRv6)

MPLS transport
Redundancy and Resiliency (LFA, FRR)
Legacy services (EPIPE, CPIPE, APIPE)

Large FAT pipes (400, 800 GE)
EVPN for IP transport

End-to-end encryption for any OSI layer with existing hardware and respecting existing SLA

Ease of enabling security on existing services or transport

Simplified and Quantum Safe Key Distribution

Agenda

1. PQC for all networks
2. **MACsec Enhanced Update**
3. Key distribution challenge
4. Final words

IEEE 802.1AE MACsec Enhanced

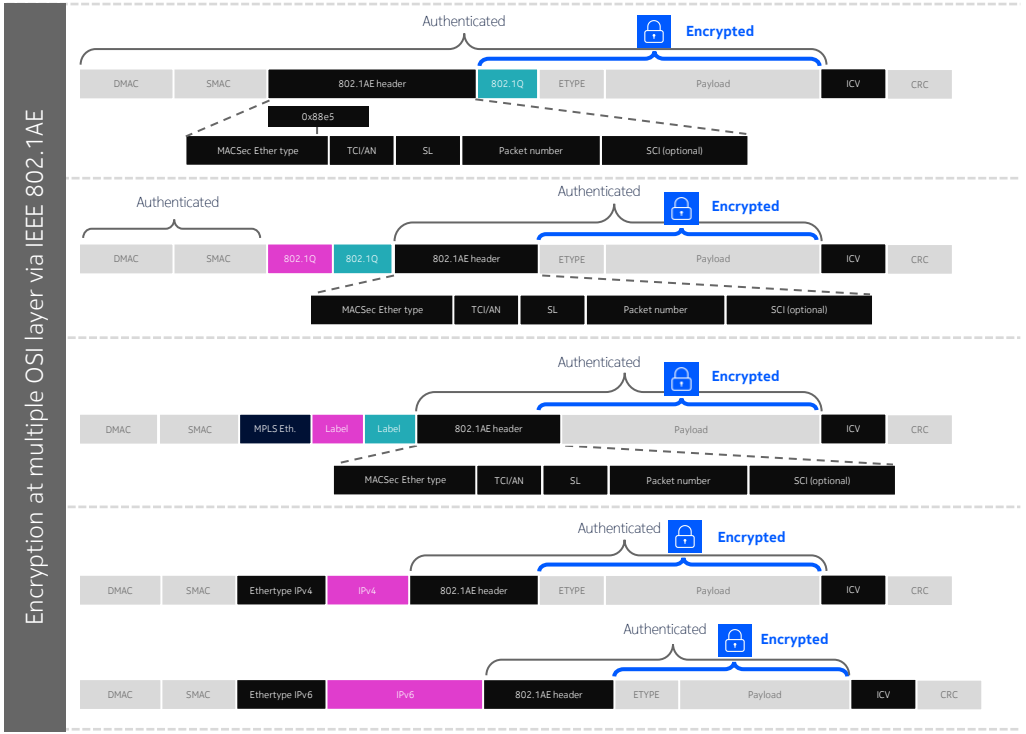
Most Current Encryption Engined can support MACsec Enhanced

Off the shelf ASICs and Encryption Engines can currently support MACsec Enhanced

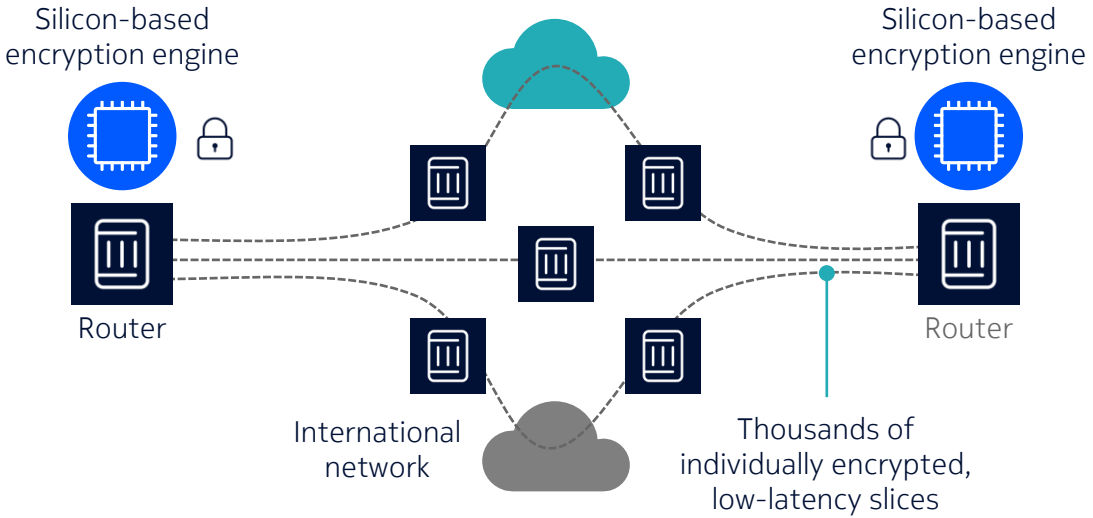
MACsec Enhanced is capable of:

- IEEE802.1AE MACSec standard encryption
- WAN-MODE MACSec encryption, VLAN tags in clear
- MPLS and services encryption, by leaving the MAC header, VLAN tags and MPLS label in clear
- IPv4/IPv6 encryption, providing an alternative to IPSec. Leaving MAC, VLAN Tags and the IP header in clear

Working to Standardize MACsec Enhanced in IEEE, first drafts are already posted and ongoing conversations in the security WG.



Easy to Implement, Quantum Safe, Line Rate, Low Latency Encryption



Quantum Safe Encryption

- GCM-AES 256, IP/MPLS encryption
- Managed end-to-end encrypted services
- Reuses IEEE802.1AE and IEEE802.1x (MKA)

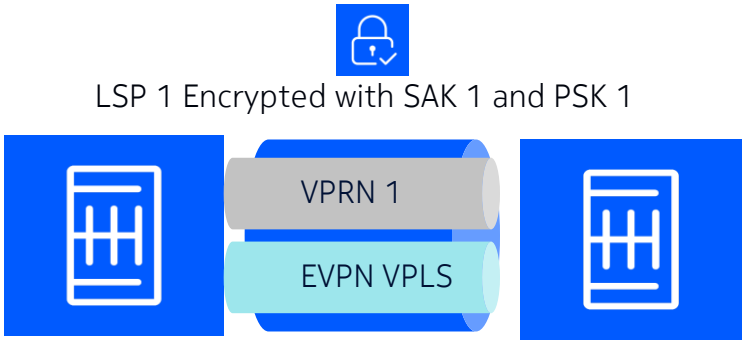
Encrypt existing services

- No need to re-engineer your network or services
- MACsec Enhanced encrypts existing tunnels with a flip of a switch
- Transparent to transit/LSR router

Encryption suited for any type of network

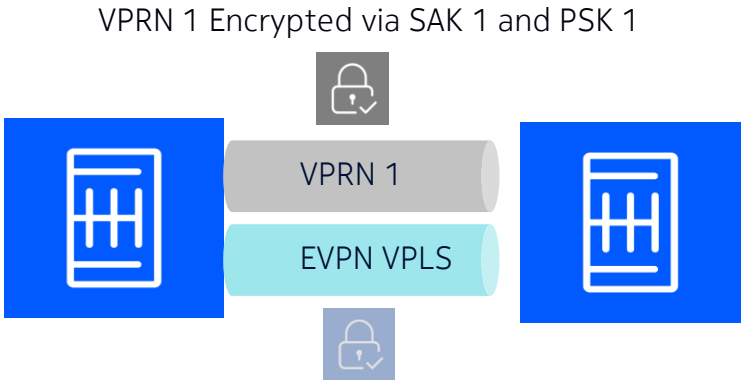
- Latency prune or low latency
- Encrypt at any network speed

Flexible Quantum Safe Encryption



Bulk encryption

All services transported by the LSP 1 are encrypted via the same SAK



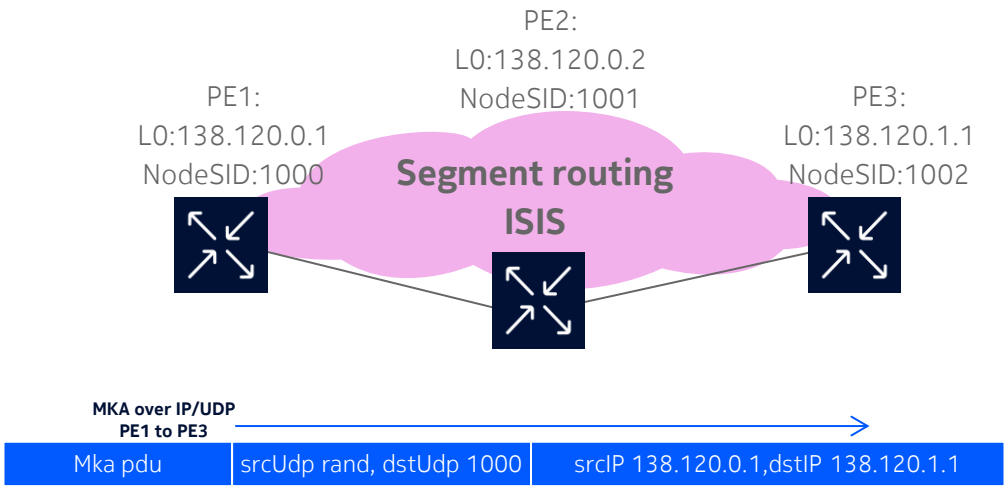
Per service encryption

Each Service is encrypted via its own SAK

Agenda

1. PQC for all networks
2. MACsec Enhanced Update
3. **Key distribution challenge**
4. Final words

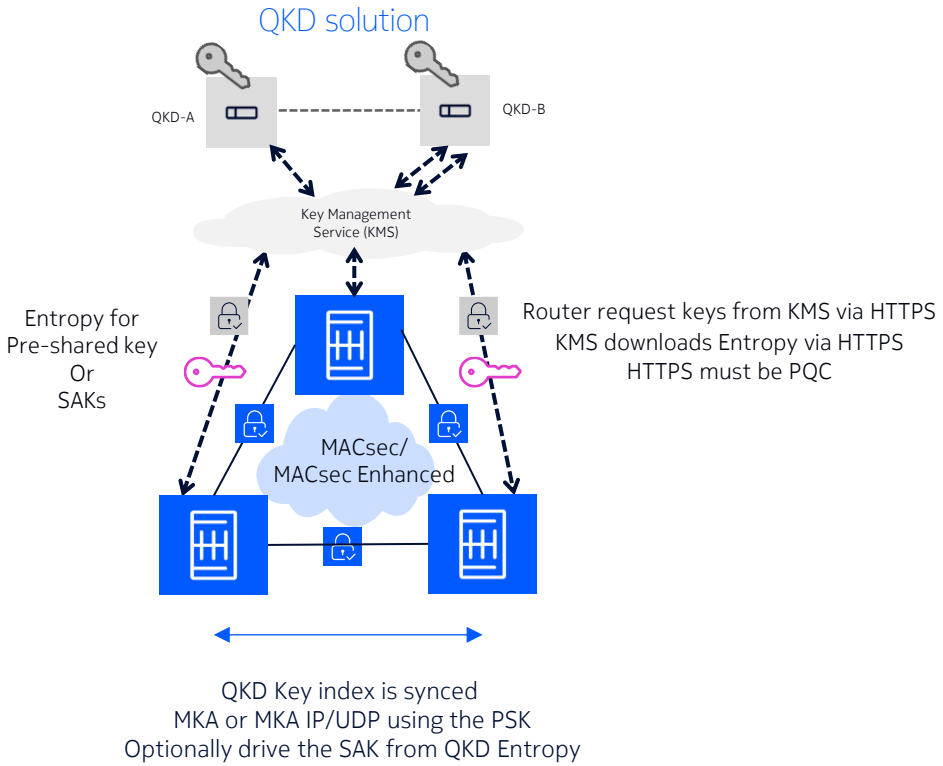
Symmetric Key Distribution, MKA over UDP/IP



Ease of Symmetric Key Distribution

- MACsec Key Agreement (MKA) is the leading solution for SKD
  - Can be used for Layer 3 or Layer 2 SKD
- On going work in IEEE 802.1 security WG to use MKA over UDP/IP for Layer 3 encryption solutions
- Symmetric Key Distribution (SKD) is preferred in some TIER one operators
  - Simplicity of the deployment
  - Ease of integration with current QKD solutions or other Key Distribution Solutions
  - Less complex than setting up PKI

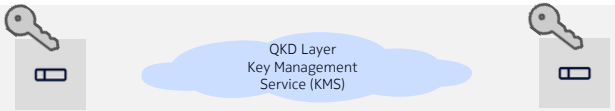
QKD Entropy Distribution for PSK



QKD Entropy Distribution for PSK

Automation is the key

1. At first the Pre-Shared Keys (PSKs) are derived from QKD and KMS layer



2. Establish MKA or MKAoIP(UDP) with PSK derived from QKD Entropy. Distribute SAKs in a QS method via MKA

QKD Failure detected via BFD, Heartbeat methods lie BFD

Key Chains

- Key chains contain multiple key entries that become active at certain date and time
- The PSK must be configured manually
- PSK must be generated via Quantum Safe Entropy and preferably from a certified entropy source

Dynamic CAK

- PSKs are auto generated and rotated via a Radius Server
- 802.1X/EAP-TLS authentication
- Usually is used for host to switch type of deployments (NIC to Switch)
- Can be used for switch to switch as well
- EAP-TLS signatures MUST be PQC
- Radius entropy must be Quantum Safe and certified

PSK Auto Generate Auto Distribute

- Uses IEEE 802.1AE Distribute CAK parameter set
- PSKs are Auto Generated and Auto distributed to the peer by the Key Server
- The Router entropy must be Quantum safe and certified

Importance of NIST and Common Criteria Certification

More demand for Regional Certification for Entropy and Ciphers

- Entropy Source Verification Certified by NIST
- Usually Open-Source Entropy
- Open-Source means more secure
- High Entropy (2^256) = Quantum Safe

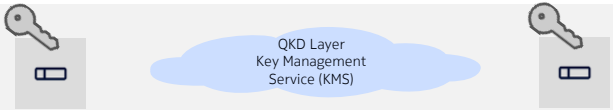
- FIPS-140-3
- Different FIPS Levels
- Certifies the Algorithms and Start up procedures including PQC

- Common Criteria certification
- Different Regions have different certifications
- Certifies the general nodes security features and security protocols in addition to the entropy

Fully Automated PSK Management via QKD

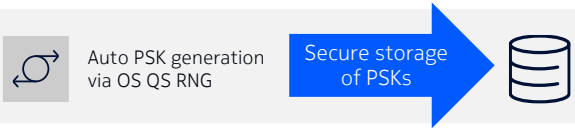
Simplicity, Local PSK Generation via Local ESV Certified RNG

1. At first the Pre-Shared Keys (PSKs) are derived from QKD and KMS layer

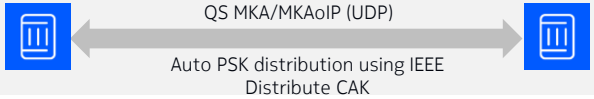


2. Establish MKA or MKAoIP(UDP) with PSK derived from QKD Entropy. Distribute SAKs in a QS method via MKA

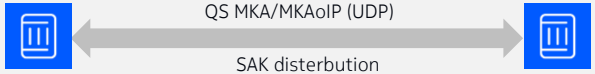
3. PSK generation is possible locally via **OS ESV/FIPS Certified/QS** Random Number Generator (RNG)



4. PSK distribution via the existing QS MKA/MKAoIP(UDP)



5. SAK distribution via the existing QS MKA/MKAoIP(UDP)



Agenda

1. PQC for all networks
2. MACsec Enhanced Update
3. Key distribution challenge
4. **Final words**

Conclusion

Simplified Quantum Safe Networks are Recipe for Success!

For ANY network

Operators should be able to engineer their networks based on their SLA and enable QSN as requirements arrive

Going forward any network should support the tools to enable QSN as needed

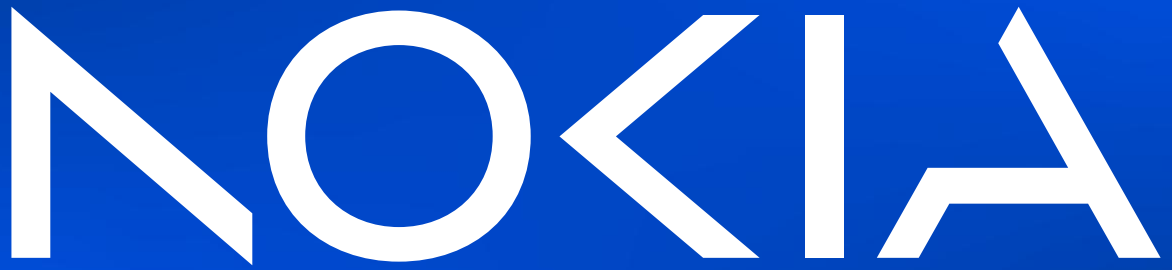
For ANY SLA

Deploying quantum safe networks should not change operator's network or the customer's network SLAs including throughput and latency

Simplified Key Distribution

Key distribution is typically the nightmare, like any application or protocol key distribution MUST have resiliency.

Symmetric key distribution is usually preferred, combined with QKD would provide a powerful simplified solution.


NOKIA