

NDN 2026

Lightning Talks

Quantum Safe Networking in IP and
DWDM networks

September 2026

mikhail.lenko@nokia.com

The Nokia logo is displayed in white, consisting of the word "NOKIA" in a sans-serif font. It is positioned within a large, stylized graphic on the right side of the slide. This graphic consists of two concentric circles: an outer white ring and an inner dark blue circle. The background of the slide features a blue-to-green gradient.

Why is trusted nodes not the best solution for long distances?

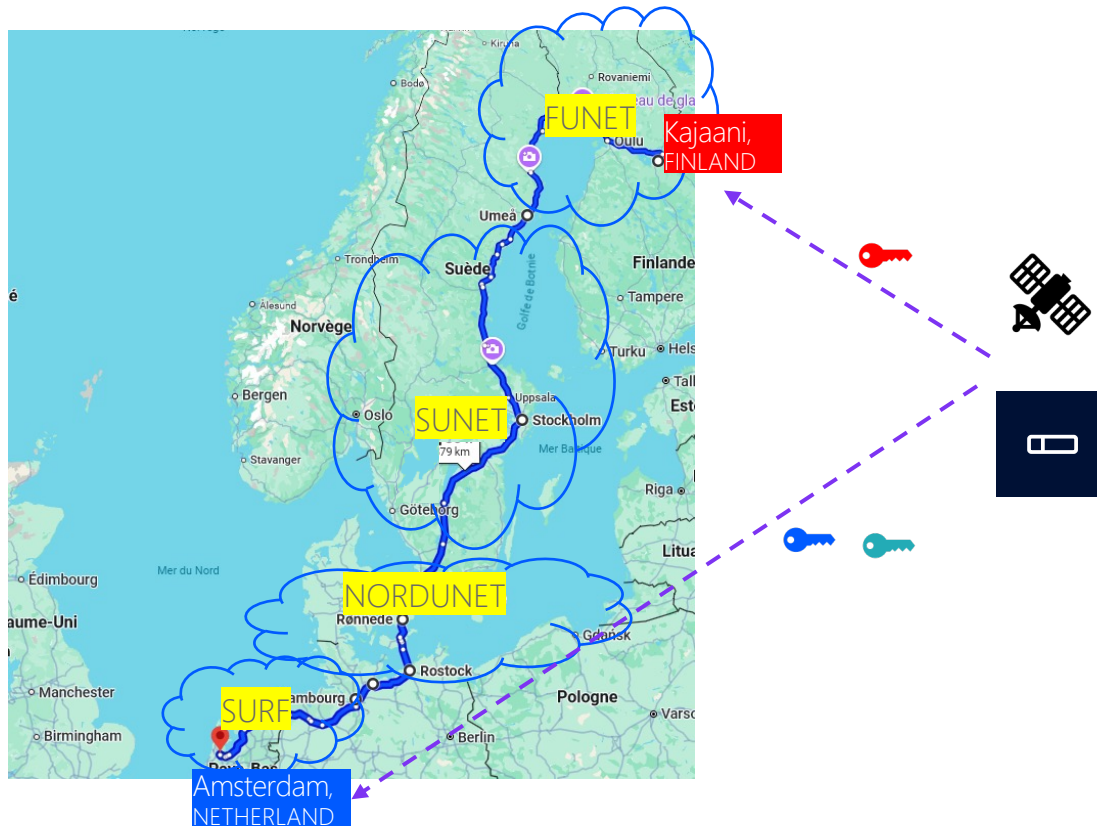
From Kajaani to Amsterdam, there is about 3500 km. fiber distance (short route).

Considering about 80 km as maximum distance for QKD* link, you need at least **44 trusted nodes**

Trusted Nodes have the following disadvantages:

1. Key is decrypted – encrypted, so special security control is needed
2. They are hosting QKD appliances, so they are costly.
3. The existing OLS infrastructure can't be reused 100%
4. Dedicated dark fiber is required for QKD connectivity.

No possibility to arrange trusted-node in long-haul submarine networks.



$$\text{Red Key} = \text{Blue Key} \oplus \text{Green Key}$$

*QKD – Quantum Key Distribution

Seems QKD is not preferred technology choice in the USA...

- US security guidance favors Post-Quantum Cryptography (PQC), not QKD
NSA states that quantum-resistant algorithms are more cost-effective, easier to maintain, and better suited for securing National Security Systems than Quantum Key Distribution.
- Google's choice reflects hyperscale practicality
Google prefers PQC because it can be deployed in existing software and infrastructure, whereas QKD would require major hardware replacement across global networks.

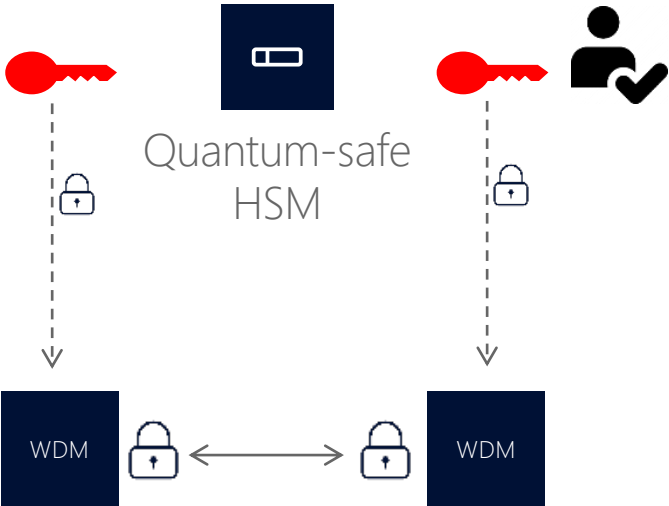
Links:

(1)Post-Quantum Cybersecurity Resources

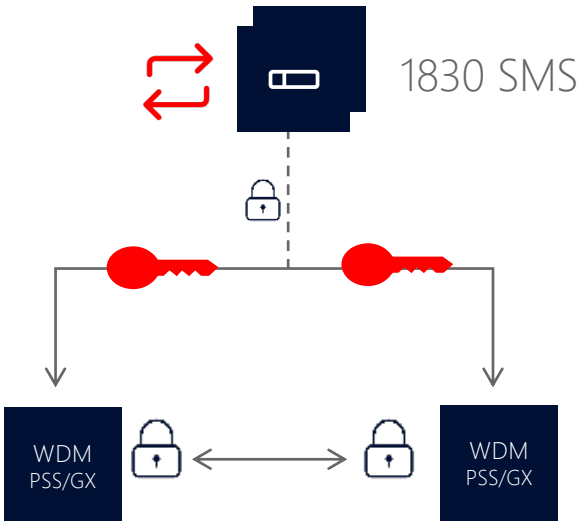
(2)Why Google Is Betting On Post-Quantum Cryptography (Not QKD) - NETCONFIG

Quantum Safe DWDM - Networks Blueprints

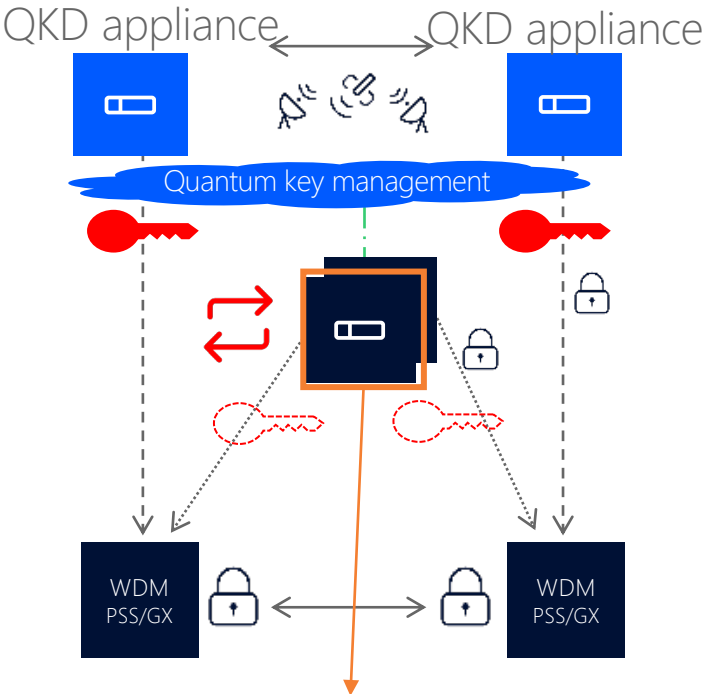
Pre-shared keys with manual symmetric distribution



Automated symmetric keys distribution and rotation



QKD with backup symmetric distribution



Nokia 1830 SMS orchestration and backup



Backup Quantum-Safe Key (BQSK)



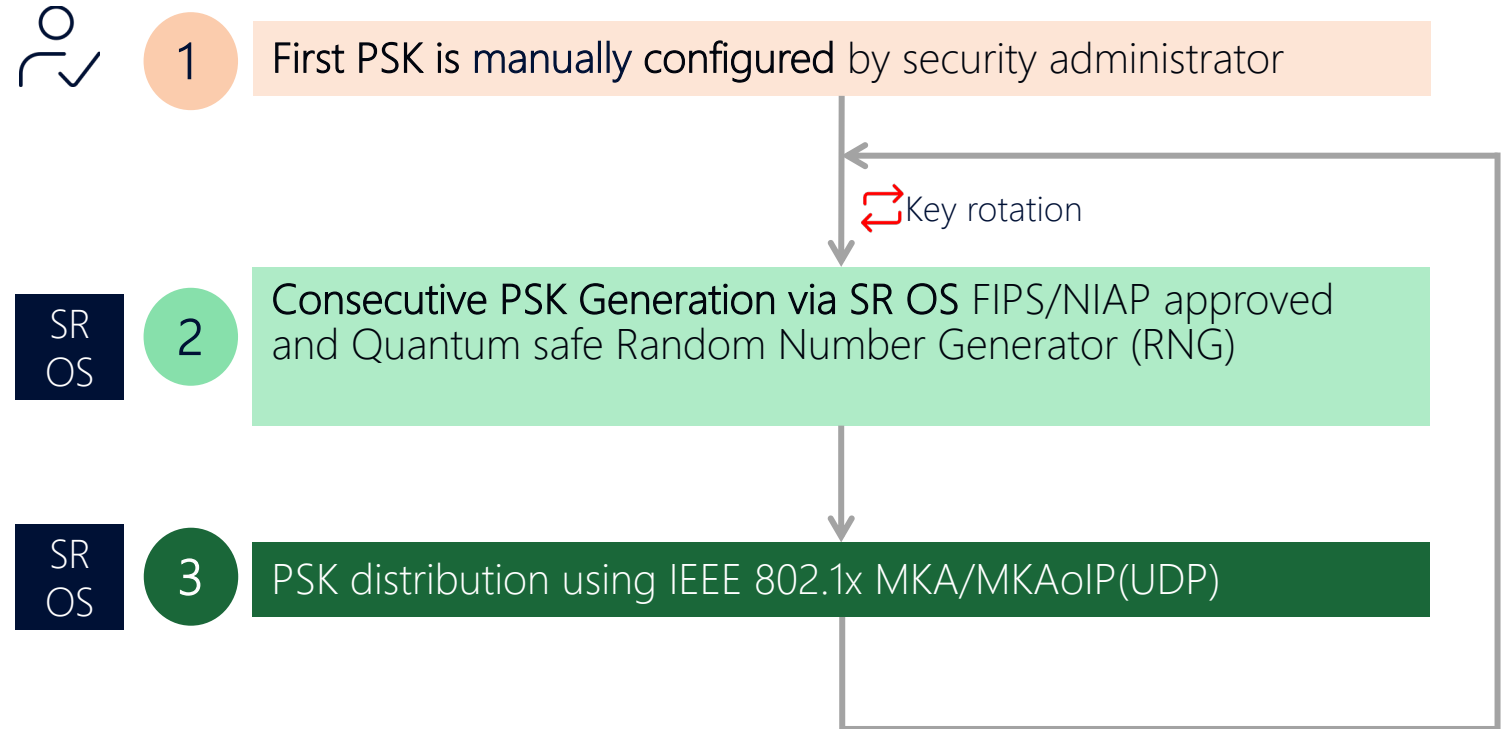
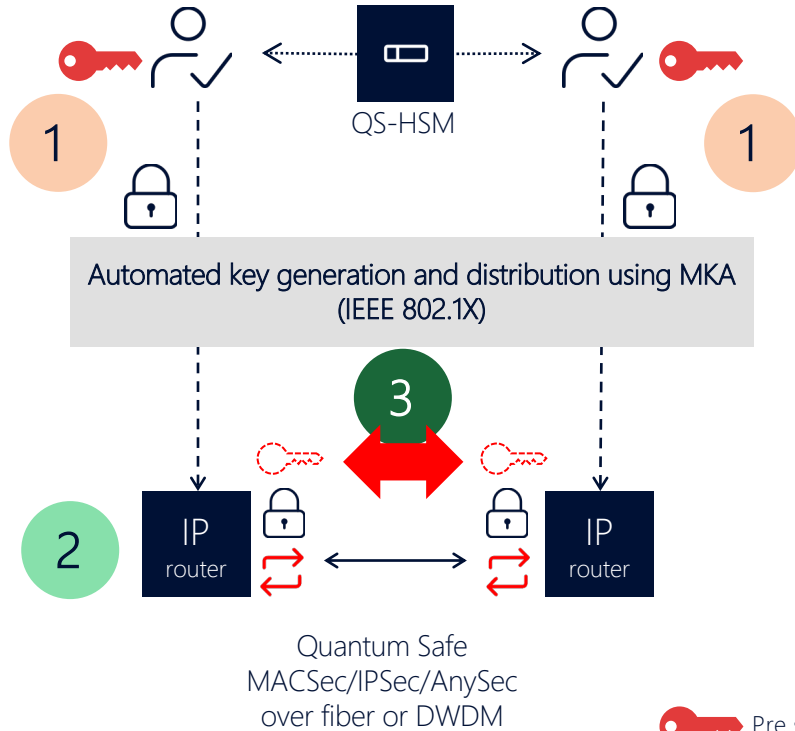
Key rotation

Quantum Safe IP WAN

Automated rotation – **SR OS** based automatic key generation and distribution

SR OS based key management

Manual pre-shared key configuration with automated key generation and distribution



Pre shared key (PSK)



Backup Quantum-Safe key (BQSK)



Key rotation

QS-HSM = Quantum-Safe Hardware Security Module

NOKIA