



Protecting your network from the quantum threat

Solution brief

Modern enterprises, governments and service providers know they need to keep upgrading their security solutions to protect their confidential data from attacks and breaches by threat actors. But the emergence of quantum computers that can quickly break down trusted encryption methods is poised to upset the cybersecurity landscape and put business-critical data and services at risk. Organizations of all types need to start making their networks quantum-safe.

This solution brief describes how the Nokia Quantum-Safe Networks solution can help your organization build a defense system within multiple layers of the network to protect your data against harvest now, decrypt later quantum threats—starting today. Discover how you can adopt multilayered cryptography and the important role it plays in a defense-in-depth approach that shields your network from current and future quantum computing attacks while flexibly adapting to your business needs.

Contents

Introduction	3
A complex new threat to data integrity	3
Pioneering threat tolerance for the quantum computing age	4
A comprehensive, defense-in-depth approach to quantum security	5
Make your network quantum-safe today	6
QSN solution benefits	7
A trusted optical and IP cryptography partner	8
Fostering collaboration on quantum-safe networks	9
Accelerating CSP adoption of QSN	10
Resources for further reading	10
Nokia contacts	10

Introduction

Modern enterprises, government agencies and service providers rely on business-critical data. This data enables them to deliver a host of essential services, from providing energy to power homes, cities and transportation, to processing business transactions for the world's supply chain and enabling communications to drive social media interactions and commercial business decisions.

As the value of confidential data transmitted across networks increases, it is becoming a more attractive target for threat actors seeking to extract it for financial gain. Attacks and breaches are on the rise.

A complex new threat to data integrity

At the same time, emerging practical quantum computers pose an immediate threat to data integrity. These computers can seamlessly decrypt many types of protected data without the network operator knowing about the breach. With more content and services moving to the cloud, network operators need better ways to protect in-flight data.

High-speed, low-latency and secure transport has become increasingly crucial and relevant for mitigating quantum computing attacks by unknown threat actors. Applications such as artificial intelligence (AI), critical infrastructure and financial transactions rely on networks being resilient to these attacks. But network operators have work to do to achieve this resiliency.

The quantum threat looms large over organizations. Quantum computers have the potential to swiftly break cryptographic ciphers. This means they can compromise widely used encryption methods and endanger secure online transactions, confidential communications and sensitive file transfers.

One of the main quantum threats is known as a harvest now, decrypt later (HNDL) attack, where a malicious actor harvests encrypted data today, anticipating decryption in the future when quantum computing matures. Existing encryption methods provide a false sense of security. Intercepted data will easily be decrypted by a threat actor that gains access to a cryptographically relevant quantum computer (CRQC).

Our industry needs to view the timeline for migration to quantum-safe cryptography through the lens of the Mosca Equation, which reinforces that there is vulnerability today—a zero-day vulnerability.

Pioneering threat tolerance for the quantum computing age

The Nokia Quantum-Safe Networks (QSN) solution enables you to protect your business-critical data against HNDL attacks and impending quantum computing threats.

As quantum computing evolves, so does the threat landscape. QSN offers a dynamic, defense-in-depth approach that integrates layered quantum-safe cryptography using mathematical and physics-based Quantum Safe Keys (QSKs) in an incremental way to fortify networks against attacks. The solution will also integrate Post-Quantum Cryptography (PQC) once the standards evolve and become ratified. More than mere encryption, QSN ensures the longevity and resilience of your digital infrastructure.

The magnitude of the quantum threat becomes clear if we compare the security levels provided by popular ciphers when they face conventional and quantum computing attacks. As shown in the table below, most ciphers cannot prevent penetration by quantum computing attacks (expressed as 0 bits). Only two provide some protection. The key strength and algorithm play a significant role. Choosing the right QSK generator—such as the Nokia 1830 Security Management Server (SMS)—is essential for implementing a proper defense-in-depth strategy.

Algorithm	Key length	Effective key strength/security level	
		Conventional computing	Quantum computing
RSA-1024	1013 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

A comprehensive, defense-in-depth approach to quantum security

Delivering quantum-safe connectivity demands a comprehensive strategy. The QSN solution's defense in-depth approach integrates multilayered cryptography that's designed to flexibly adapt to your business and use case needs. It gives you the confidence to scale your quantum-safe network deployment while ensuring that your network can evolve with the quantum landscape.

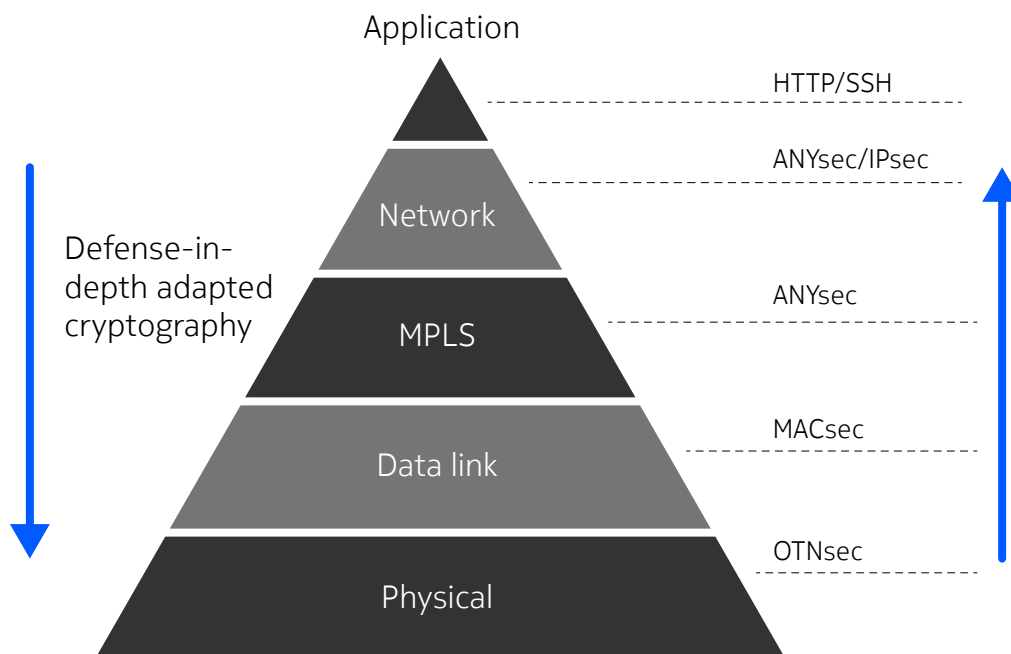
Not all layers require cryptography in our defense-in-depth approach. What is necessary is the incremental and complementary application of cryptography at one or multiple layers, depending on the network's operational model.

For instance, some of your networks may operate without the optical transport network (OTN) layer. This eliminates the need for encryption at layer 1. In contrast, your longer-distance regional or long-haul networks will likely rely on OTN. This means you need to build resiliency into a new layer to provide protection from threat actors seeking to use methods of intrusion as a starting point for HNDL attacks.

QSKs grounded in mathematics and physics are foundational to our approach, along with appropriate key distribution and PQC keys once these are standardized. These PQC keys can be applied to all layers ubiquitously to provide the greatest encryption strength and protection where it matters.

AES-256 network encryption enhances this foundation by providing multiple layers of additive optical, Ethernet, MPLS and IP cryptography to complement application-level cryptography and ensure quantum-safe data transit.

QSN is more than a singular solution. As illustrated by the figure below, it's a holistic strategy that yields a clear outcome: quantum-safe network connectivity.





Symmetric encryption uses a single pre-shared key (PSK) to encrypt and decrypt data, establishing a shared secret among communicating parties. This shared key must be kept confidential to maintain the security of the communication link. Symmetric encryption is fast and computationally efficient, making it suitable for bulk data encryption.

In contrast, asymmetric encryption, used in public key cryptography (PKC), uses two keys—a public key for encryption and a private key for decryption. The public key is openly accessible, while the private key remains confidential. Asymmetric encryption makes it easy to scale key distribution by allowing public key sharing without compromising security.

Make your network quantum-safe today

The QSN solution provides flexible options for making your network quantum-safe today. For example, you can generate keys manually and securely hand-deliver them to end-point locations, although this process can be time- and effort-intensive. Alternatively, you can choose an automated key generation, orchestration and distribution method that accelerates service fulfillment, shortens time-to-market and reduces errors by eliminating the manual workloads involved in generating and delivering the keys. This option ensures that you will have an efficient encryption mechanism as your networks grow in size or capacity.

Our approach incorporates physics- and mathematics-based keys. For physics-based keys, we support evolving classical (PSK) and quantum physics (QKD) for key exchange.

You can apply these keys to layer 1 optical, Ethernet, MPLS and layer 3 IP connections. They enforce a high degree of security across all Nokia infrastructure systems and deliver a flexible and robust solution that protects your business from quantum attacks. Our automated approach introduces a centralized key management system that efficiently generates, rotates and distributes keys across the network. These capabilities enable agile operations and synchronized key rotation across endpoints.

QSKs produced and rotated by the Nokia 1830 SMS protect your network against a quantum computer attack. If there is a data breach, it would take millions of years for a threat actor to crack a key. You can adapt the 1830 SMS by reconfiguring the key size to rectify any foreseen vulnerability to the system.

Our QSN architecture uses trusted physics-based sources to improve scalability and secure engineered connections, utilizing PSK as Secret Session Keys¹ to ensure quantum-safe connectivity. You can refer to our QSN blueprints summary document for more information on supported blueprints.

¹ Secret Session Keys are randomly generated single-use symmetric keys for encrypting and decrypting data within a communication session.

QSN solution benefits

Feature	Benefits
Secure layer 1 to 3 connections	• Enable layered, incremental defence in-depth security across multiple network layers • Implement performant AES-256 encryption (OTNsec, MACsec, ANYsec, IPsec) to provide robust protection against quantum threats • Ensure data confidentiality and integrity in a post-quantum era
Scalable connectivity blueprints	• Use a flexible architecture that integrates seamlessly with Nokia IP and optical transport technologies • Support reach and capacity extensions to service diverse geographical network configurations • Adapt easily to support a variety of network operator business applications
Automated PSKs	• Provide automated key distribution orchestration and configurable key rotation to various network layers • Support symmetrical distribution of key exchange for classic and quantum physics technologies • Provide an architecture that will expand to include PKC/PQC mathematical algorithms as standards become ratified



A trusted optical and IP cryptography partner

Nokia optical and IP cryptography solutions are the trusted choice of more than 100 communications service providers (CSPs) and enterprises worldwide. Customers have deployed more than 4,000 of our optical encryption-based cards. Our Quantum-Safe MACsec cryptography solution has already enabled several customers to realize quantum security.

> 50 enterprise customers and success stories

Product line configuration and endorsements

IP Telecom enlisted Nokia to expand its fiber optic networks in Portuguese metro areas. The company wanted to deploy a quantum-safe encrypted optical data center interconnect solution that could support robust data rates of 100 Gb/s and 200 Gb/s and provide a foundation for 400GE services.

1830 Photonic Service Switch (PSS)
1830 Photonic Service Interconnect – Modular (PSI-M)
1830 Security Management Server (SMS)

Our QSN architecture fortified IP Telecom's cloud data center against data theft and extended its reach to additional nodes in Portugal. Having QSN capabilities also strengthened the company's position in the information and communication technology (ICT) ecosystem.

Nokia is collaborating with GRNET and NKUA on a quantum-safe networking proof-of-concept for HellasQCI, the Greek National Quantum Communication Infrastructure consortium. The project aims to help HellasQCI implement quantum-safe networks for critical infrastructure security across Greece.

"We are very pleased with the successful completion of the PoC with Nokia, which is one of the key milestones for the HellasQCI project."

Dr. Ognjen Prnjat, Director for European Infrastructures and Projects Directorate, GRNET

The trials demonstrate the live use of a hybrid encryption method that combines classic and quantum physics methods. The approach symmetrically generates and distributes out-of-band keys, allowing for the delivery of quantum-safe cryptography services.

In June 2023, Nokia and Belgian mobile operator Proximus completed a trial of hybrid quantum encryption keys in a live network. The trial solution combined classic and quantum physics to symmetrically generate and distribute out-of-band keys for the delivery of quantum-safe cryptography services. Proximus used the solution to successfully encrypt and transmit data between data centers located in Brussels and Mechelen, Belgium.

"Working with Nokia and its partners, we're confident that we'll be able to continue to safeguard our critical systems and successfully navigate the ever-evolving threat landscape in the quantum computing world."

Geert Standaert, Chief Technology Officer, Proximus



Fostering collaboration on quantum-safe networks

Collaboration is essential for developing holistic quantum-safe optical networks. By forging key partnerships with Quantum Key Distribution (QKD) experts and Public Key Infrastructure with Post Quantum Cryptography (PKI-PQC) specialists, we aim to achieve genuine quantum safety within the OSI layer and the highest degree of security for network operators.

Starting from the optical layer, these alliances provide the foundation for shaping a reliable, secure, end-to-end solution that can be used across other layers to build a complete quantum-safe network architecture. By introducing automated key distribution and key rotation to the transport layer, the solution has a significant impact that can scale to span all optical layer 1 connections in the transport part of the network. By leveraging the same technology in other layers, it ensures that you can adapt your business to target security in depth, and scale and tailor security across the rest of the network, which can include many other different types of service connections.

Our partnership initiatives foster collaboration, unifying diverse entity experts who invest in the pursuit of a resilient, future-proof communication infrastructure to protect our customers' networks. These initiatives ensure that our QSN solution blueprints can leverage a variety of QKD technologies that can be validated—each having its own core tolerances—to avoid the need for vendor lock-in.



Accelerating CSP adoption of QSN

[SK Telecom QKD proof point](#)

[IP Telecom press release](#)

[Proximus press release](#)

[HellasQCI PoC press release](#)

Resources for further reading

[Nokia Quantum-Safe Networks page](#)

[Nokia Quantum-Safe Networks white paper](#)

Nokia contacts

Martin Charbonneau, Head Quantum Enablement & Quantum-Safe Networks

Sylvain Chenard, Quantum Enablement Solution leader

Chris Janson, Pino Dicorato & Nick Cadwgan, Quantum-Safe Networks Product Marketing

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2024 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID213993 (May)