
NOKIA
Quantum-safe data center interconnect networks

Contents

A new era of innovation

Today's enterprise data center faces a greater and more complex set of challenges: increases in scalability and bandwidth with improved performance–and a looming Q-Day threat. These challenges are being driven by increasing workloads for AI/ML and high performance computing (HPC).

As a result, enterprises are shifting data center workloads out to the network edge. This is driving demand for high-speed interconnect between them, creating an urgent need for greater capacity, security, resilience, and compliance across networks.

To address these challenges new solutions for data center interconnect (DCI) and quantum-safe networking are available and being deployed in modern data center networks. Nokia is leading the way in advanced networking, bringing powerful benefits to public and private sector enterprises around the world.

This guide explores this new era of innovation while explaining the global trends, enterprise challenges, and solutions to this growing problem.

> "Nokia is at the leading edge of developing quantum-safe IP and optical networking solutions to keep customers data safe today."
>
> **James Watt,** Vice President, Optical Networks business, Nokia

Watch Quantum Networks Summit 2025 keynote address - M. Charbonneau

Continuous enterprise data center expansion

There's no such thing as too much capacity

As enterprises digitize more processes, applications and services, it's creating an incessant demand for more processing, storage and bandwidth with higher performance and lower latency. The biggest consumers of these networking resources, besides service providers, are enterprises in banking, insurance, securities and trading, manufacturing, and energy industries.[1]

Enterprises have deployed multi-cloud and hybrid-cloud networks, moving more workloads to them expecting costs and efficiency improvements. But as the bills for these clouds have increased, enterprises are reassessing this strategy and shifting some workloads back to gain more cost control. There's also mainstream enterprise adoption of AI/ML use cases including enhanced customer support, hyper-personalized product recommendations, and retrieval-augmented generation (RAG).

And we've seen an upsurge in big data analytics workloads, the expansion of Industry 4.0 and IoT, and acceleration of digital transformation initiatives. Other business dynamics such as data privacy and sovereignty concerns are contributing to the rise in data centers numbers.

[1] Global Interconnection Index, Equinix, 2025
[2] Data Center Market to Grow by USD 535.6 Billion from 2025-2029, Technavio, February 2025

39%

Enterprises are growing at a 39% CAGR[1]

34%

The five-year CAGR forecast for interconnection bandwidth[1]

15.6%

CAGR growth in global data center market by 2029[2]

Escalating threats

A growing need for stronger security and greater resilience

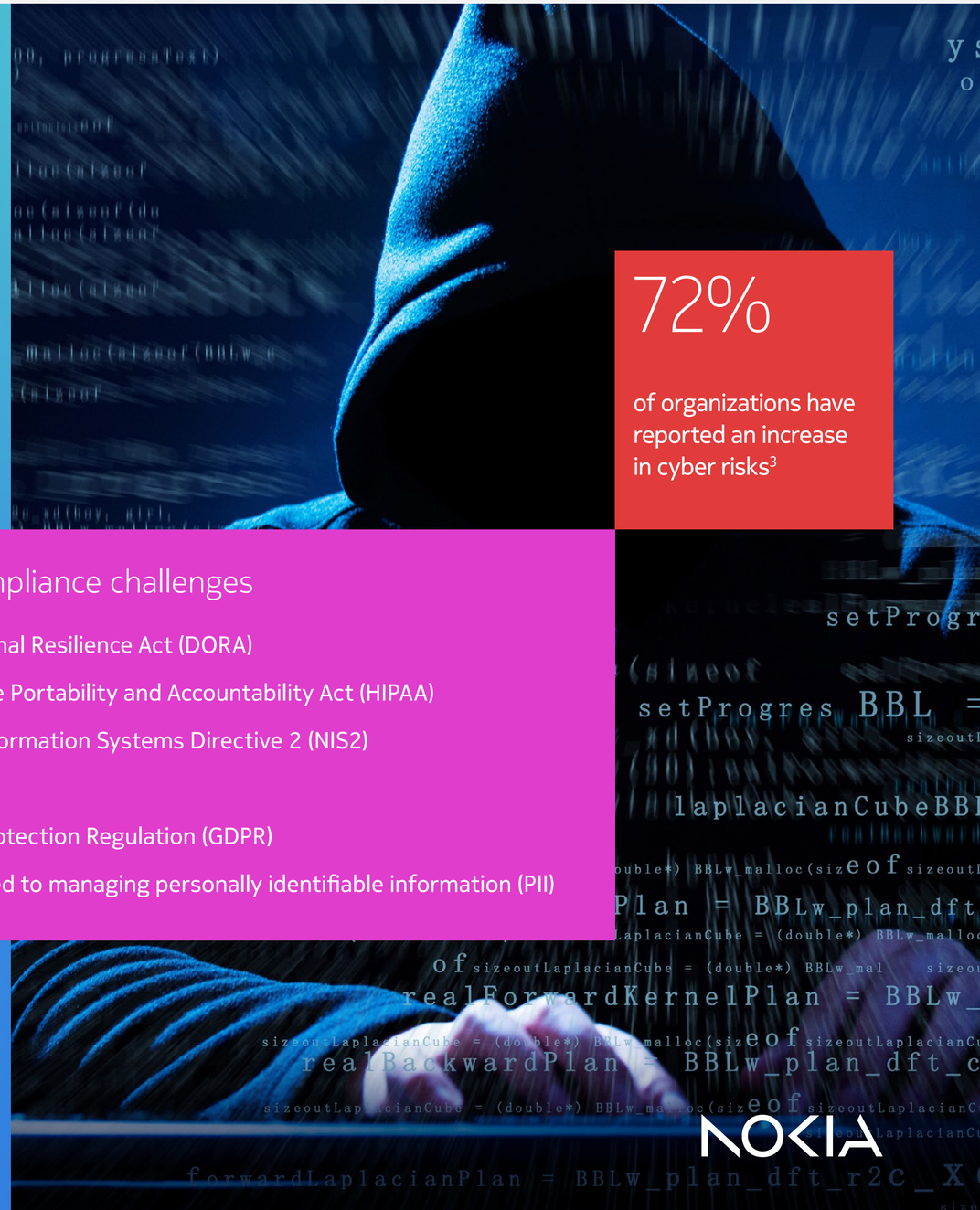
Lurking behind the data center network expansion trend is the growing prevalence, volume and sophistication in global cybersecurity threats, including nation-state-sponsored attacks.

This is due to many factors. With advances in quantum computing and AI, there is a real threat that existing security protections could be compromised. Quantum computers hold promise for many of the world's most difficult computational problems. But in the wrong hands, a sufficiently powerful machine could break through the level of encryption that currently protects networks against attacks from conventional computers.

We don't know when this will be possible, but it will be a bad day. Some call it Q-Day. It's likely that cyber criminals are already storing encrypted data until Q-Day, in what's often called a harvest now, decrypt later (HNDL) attack.

In addition, enterprises face rising regulatory and compliance pressures in areas including data privacy, cyber resiliency, and personal data protection to maintain business continuity standards.

[3] Global Cybersecurity Outlook 2025, World Economic Forum, January 2025



72%

of organizations have reported an increase in cyber risks[3]

Mounting compliance challenges

- Digital Operational Resilience Act (DORA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Network and Information Systems Directive 2 (NIS2)
- ISO/IEC 27001
- General Data Protection Regulation (GDPR)
- Standards related to managing personally identifiable information (PII)

The need for quantum-safe DCI

Essential network and security technologies

Enterprises must act now to satisfy the demand for bandwidth and to meet regulatory requirements for business continuity and disaster recovery (BC/DR). At the same time, they must mitigate the growing security risks from many threats, including quantum computers in criminal hands. All network operators, including enterprises and service providers, need to act today and deploy strategies over time to protect tomorrow's data integrity.

But before the solution can be implemented, a trusted consultant must perform a threat and risk assessment to evaluate the resiliency of the infrastructure security. Expert consulting services may also be needed to design the data network and edge infrastructure architecture and make recommendations for adding capacity where it's needed.

This design will include optical and IP networking (or some combination of both) that addresses enterprise connectivity challenges. This partner-focused solution will be quantum-safe by design and ensure larger network capacity as well as stronger security measures.

> "We see a lot of uptake in the banking and financial industry, for sure, but on top of this, government, public sector, MODs, military, and research and education, healthcare and transportation. So basically, the addressable market for us is actually expanding in terms of our technologies, realizing data center interconnect, data center cloud access and campus network to be quantum-safe-enabled."
>
> **Martin Charbonneau** Head of Quantum-Safe Networks, Nokia

What is data center interconnect?

Definition and characteristics

DCI joins data centers over physical or virtual links so they can share computing and storage resources. This helps enterprises overcome the challenges of matching data management to their business needs while securely handling huge data volumes across varying distances. It means organizations can adopt cloud architectures that fit their business requirements without incurring additional security risk.

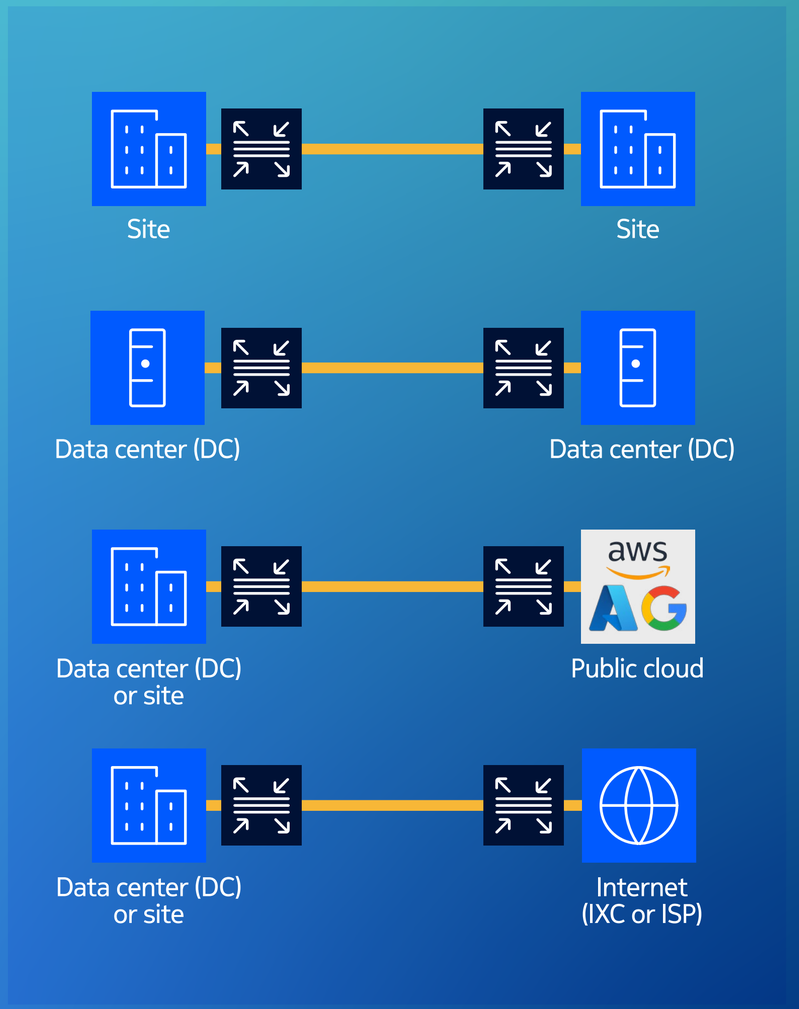
DCI provides high-capacity connectivity through leased dark fiber or managed Ethernet services between either enterprise-owned or cloud service provider data centers. Connectivity can be at various network layers, using protocols matched to the operator's existing infrastructure.

Common examples include wavelength over dark fiber, virtual extensible LAN (VXLAN), Ethernet virtual private network (EVPN) and MPLS VPN extensions.

Leased or dark fiber is ideal for DCI

Typical characteristics

- **Network topology:** Often point-to-point (P2P) and sometimes point-to-multi-point for complex projects.
- **Interfaces:** Ethernet, fiber channel, and optical transport network (OTN).
- **Distances:** DCI can be used between data centers less than 10 km apart, within metro areas (10-20 km), across regions (20-200 km), or across countries, continents or oceans (more than 200 km).
- **Deployment and operations models:** IT or Telco-centric data center design configurations, network management, toolsets and automation platforms.



Nokia data center network architecture

Anatomy of Nokia solutions

Nokia Data Center Network (DCN) solutions consist of the Nokia Data Center Fabric (DCF), Nokia Data Center Gateway (DCGW), Nokia Data Center Interconnect (DCI), and DCN management and automation.

1. The management layer

This manages all the network assets and automates the DCI's deployments, configurations and testing. It abstracts and exposes the solution to other tools and orchestrators sitting above. And it supports network security through the secure management and distribution of keys.

2. The IP/Ethernet layer

This consists of two elements:

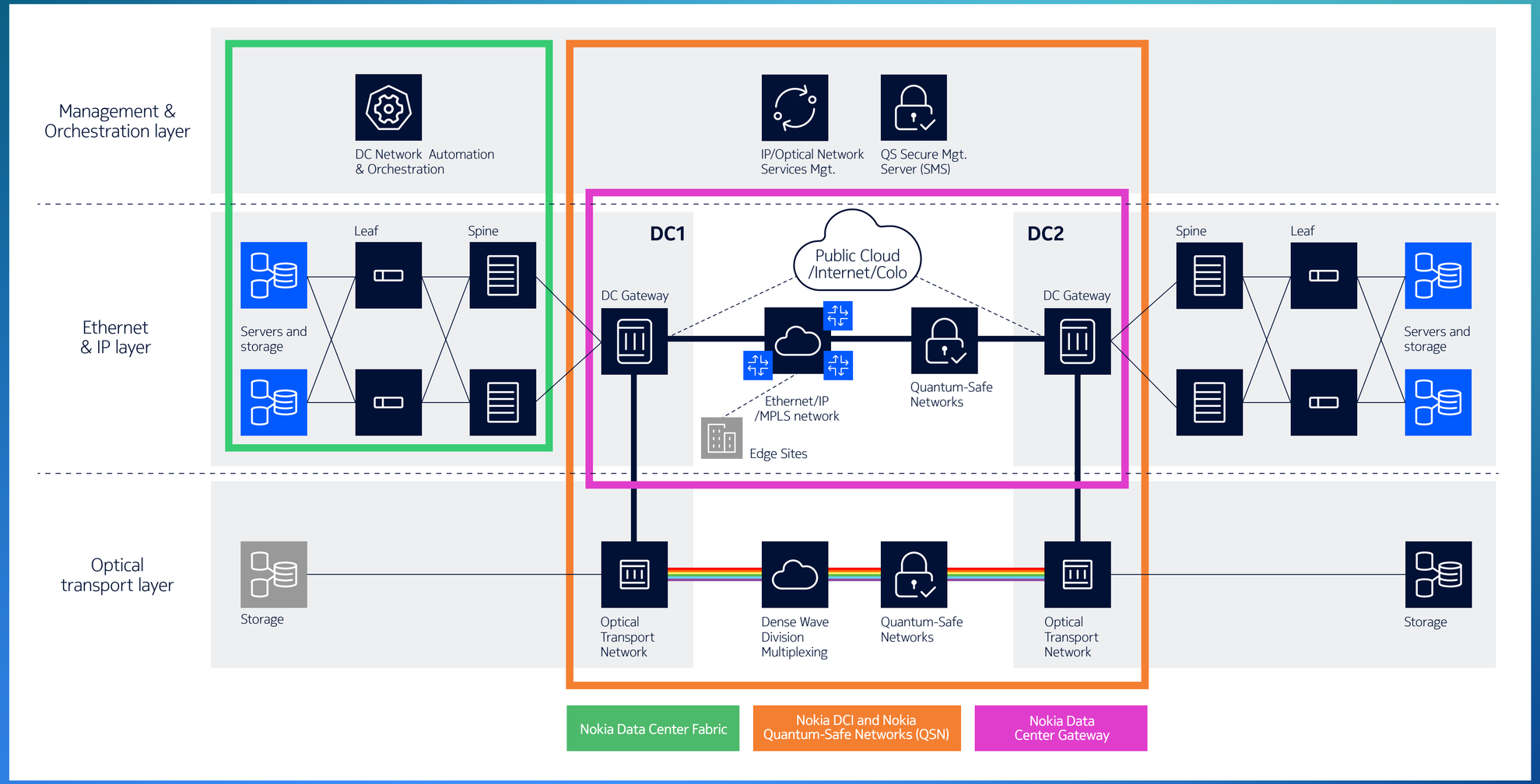
a. A DC fabric leaf and spine switching solution reliably connects servers and storage devices at high speeds in an automated NetOps model.

b. The DC gateway connects to the external world and other data centers and clouds supporting multi-domain and multi-VPN interworking and border gateway protocol (BGP) internet peering.

3. The optical transport layer

This layer physically interconnects data centers. It aggregates multiple high-speed connections from the IP layer and storage fiber channels. And it's typically underpinned by dark fiber that uses the latest DWDM technology and is protected with OTNSec.

Nokia DCN architecture: end-to-end network solutions



Preparing for Q-Day

The risks and benefits of quantum computing

Advances in quantum computing and the threat to security.

Unlike conventional computers that use bits (0 or 1) as a unit of data to process and transmit, quantum computers use qubits which can exist in superposition (combinations of both 0 and 1 state simultaneously) enabling them to perform complex computation orders of magnitude much faster than conventional computers. This solves industry problems like optimizing factory processes or global supply chain logistics, genetic research or complex financial trading algorithms. They also retrieve and store data in a super-efficient way, support advanced AI/ML algorithms and capabilities, and enhance cryptography.

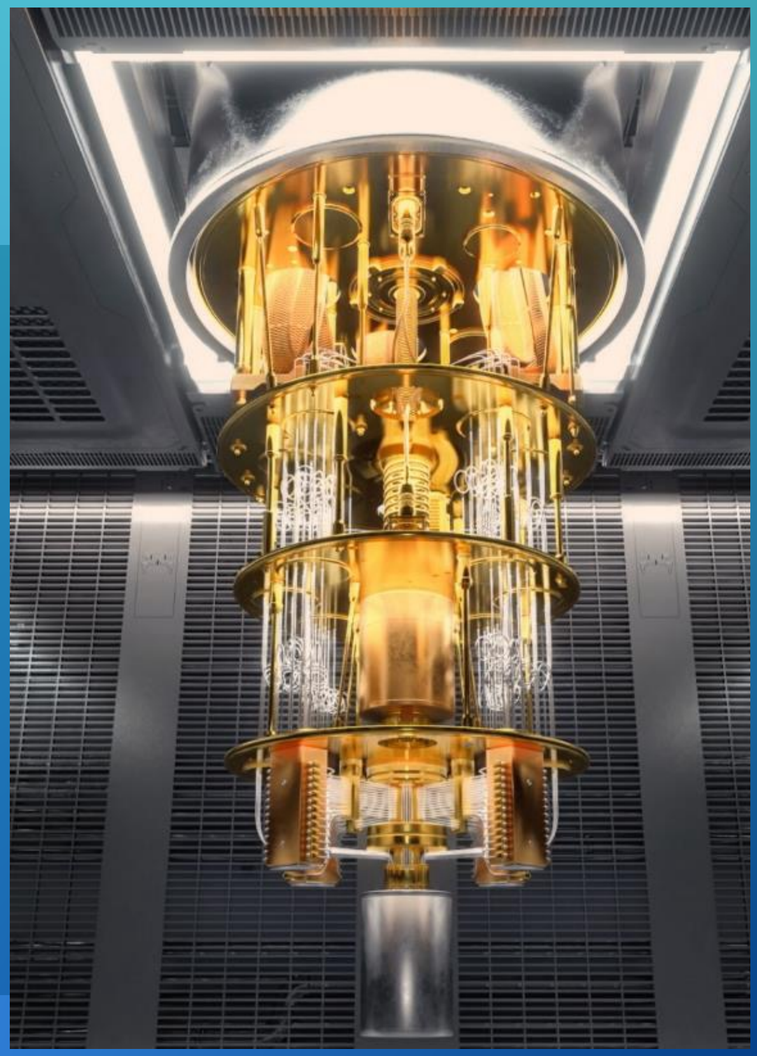
Quantum computing is still nascent. But just like AI, the technologycould be used for nefarious purposes. Government and security experts are concerned that cyber criminals are already making efforts to develop cryptographically relevant quantum computers (CRQCs) one day in the future.

Q-Day: a very real threat

Q-Day will arrive when a CRQC is available that can break today's commonly used asymmetric encryption ciphers. This will allow cyber criminals to launch attacks that could expose sensitive data—such as government secrets, enterprise and personal heath care records, financial data, or industrial intellectual property data—to threats including ransomware, jeopardizing global internet trust and confidence.

Quantum computer cyber attacks are a real threat. And it takes years to develop new ciphers, commercial products, and system change-outs to defend against these attacks. But we can get prepared for all eventualities with the right quantum-safe solutions.

Governments, service providers and enterprises must take proactive steps to protect their networks. A quantum-safe DCI solution consists of multiple protections that secure the operator's data. Planning for this outcome should start today, with technology deployments integrated into the operator's network maintenance and upgrade plans.



Ingredients of quantum-safe networks

Quantum-safe networks

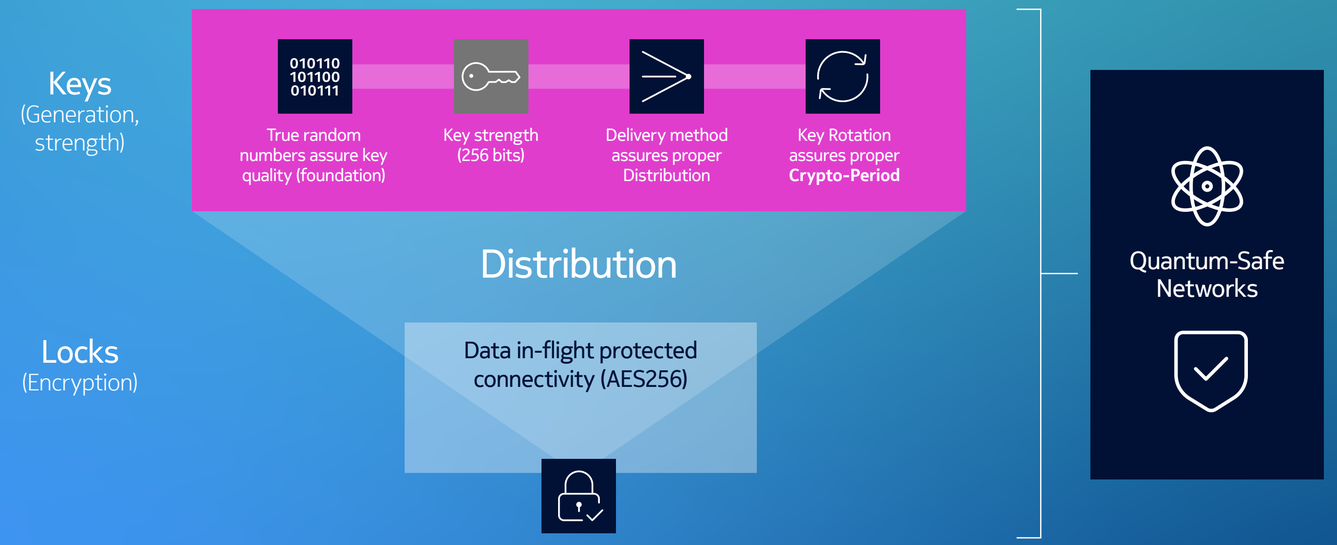
Quantum-safe networks (QSNs) protect data at various connectivity points across network layers. This usually includes the physical, data link, and network layers, as well as the application layer. Historically, we've believed that encrypting a single layer was sufficient for data security. Quantum computing changes this assumption.

Protecting against attacks from a quantum computer executing Shor's algorithm requires tools that make use of the best-known implementations of various encryption mechanisms. Encryption has three essential elements:

1. Locks are engines which converts plain text into cipher text through an established method. The Advanced Encryption Standard (AES) is a gold standard block cipher which has never been broken.
2. Keys are used by engines to lock data before transmission. They're random in nature to be difficult to predict. Keys are generated from a source of randomness, or entropy. They have a defined length in bits. They're used by the lock to create cipher text.
3. Key distribution methods get keys to the sending and receiving ends of a communication link. Pre-shared, symmetric keys and public, asymmetric keys are common key distribution methods in the industry.

QSN toolkit

Shor's algorithm tells us that commonly used asymmetric ciphers, such as RSA2048, are vulnerable to quantum computing attack. Grover's algorithm tells us that symmetric key distribution to an AES-256 encryption lock can withstand a quantum computing attack. These are the initial building blocks for a QSN.



The combination of locks and keys assure quantum-safe networks

Nokia QSN solution

A multi-layer, defense-in depth approach

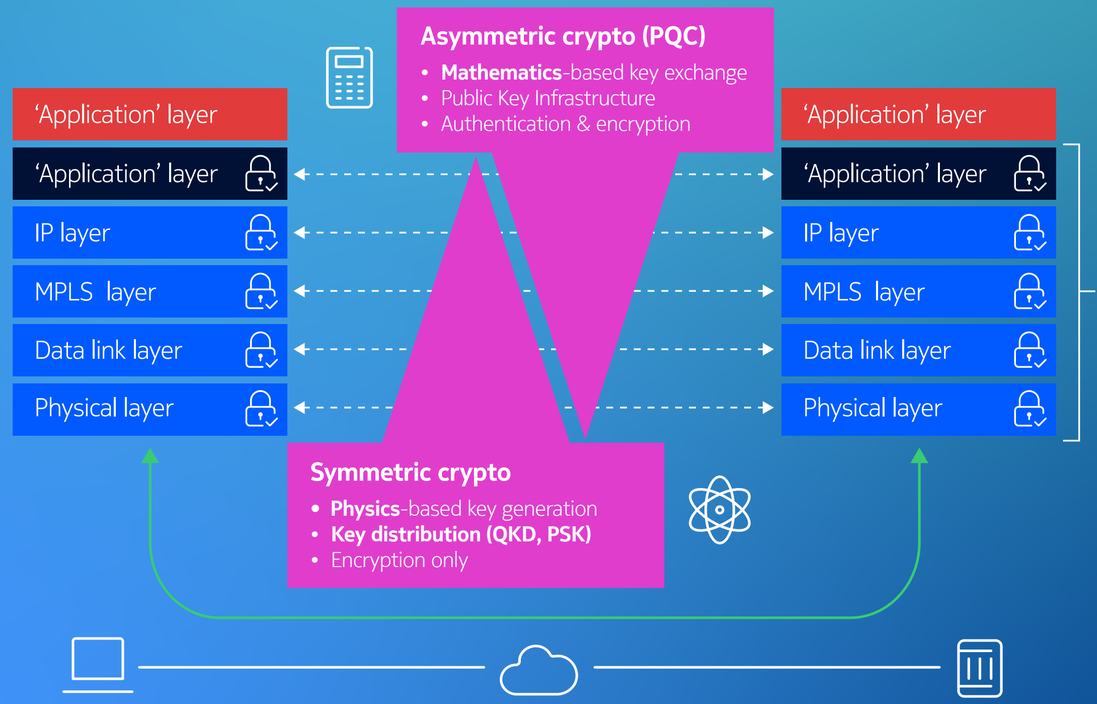
Adaptable, resilient quantum-safe networks

Nokia QSN solutions provide protection at multiple points in the network through a set of tools. Different networks and the data they carry will dictate the selection of which tools, where they are deployed, and when they are used.

Typically, the first line of defense is created by securing the physical layer, often optical transport links between data centers, using Nokia 1830 Photonic Service Switch with encrypted transponders. This is supported by a symmetric centralized key management system, the Nokia 1830 Secure Management Server (SMS), using classic, physics-based keys. In some cases, this will be enhanced through quantum-generated keys in a quantum key distribution (QKD) architecture.

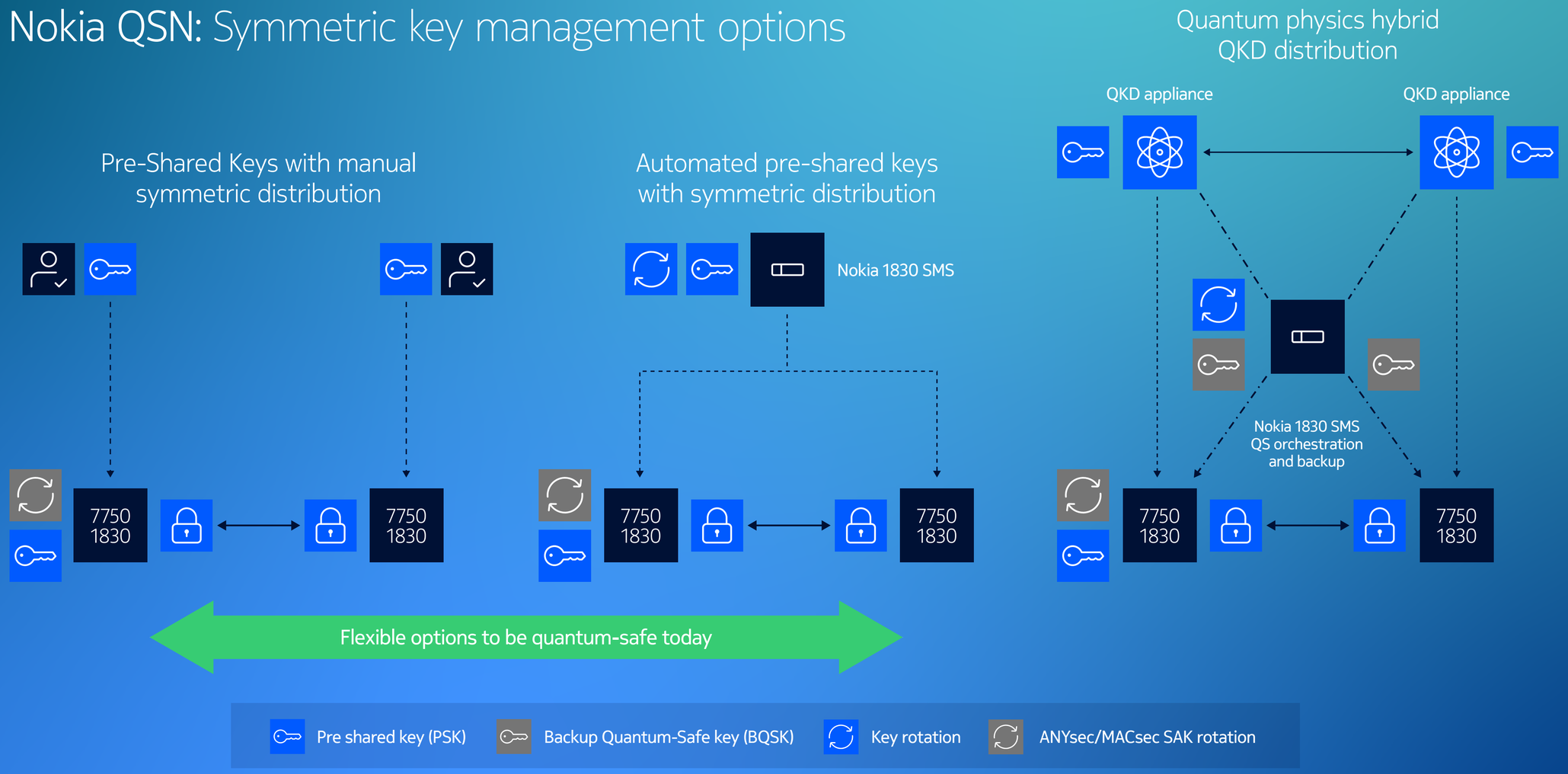
Next, protection can be layered at higher layers through a similar symmetric key distribution approach supporting IPsec or MACsec encryption, both of which are supported by Nokia 7750 Service Routers (SR). Together, this would bring three layers of defense-in-depth protection.

Finally, protection can be added using post-quantum cryptography (PQC). These are newer, asymmetric ciphers, designed to be immune from attack by a quantum computer running Shor's algorithm. Their standardization is new, and implementations are still unproven, but they would add another flexible layer of protection.



Watch: How to protect ands secure your data with a Nokia Quantum-Safe Network

Nokia QSN: Symmetric key management options



Use case
Mainframe modernization

Summary

Nokia improves your network security and resiliency with quantum-safe mainframe data center interconnectivity.

Click on the links below to find out more
Nokia's Optical Data Center Interconnect solution
Nokia Quantum-Safe Network solutions

Enterprise challenges

- Integrating legacy mainframes with modern data center technologies and operating processes.
- Closing the skills gap for mainframe technologies.
- Overcoming the risks of data theft and corruption during migration.
- Minimizing potential interruptions to critical business operations.
- Ensuring standardized and effective tools and methodologies.
- Ensuring compliance with relevant regulatory standards or directives.

The Nokia Quantum-Safe Mainframe DCI

- As your trusted networking partner, we can help accelerate the modernization of your mainframe application, data and infrastructure to extract value from your hybrid cloud environment.
- Nokia's Optical Data Center Interconnect solution with new IBM GPDS certified high-speed interfaces for mainframe modernization projects provides a cost-effective option using your own dedicated fiber links allowing you to migrate from a shared network service provider infrastructure.
- For improved security against emerging quantum cyber-threats, mainframe DCI optical connections can be enhanced with the Nokia Quantum-Safe Network solution delivers the same high bandwidth and very low latency over highly secure and resilient network with quantum-safe cryptography for business-critical data and applications.
- Nokia's optical network transport technology is field-proven and easy to operate and manage.

Business benefits

- Better performance against SLA targets and data security requirements compared to a shared network service provider.
- Full control over your DCI network infrastructure, with fast service turn-up time and agility.
- Excellent data security with quantum-safe encryption.
- Lower total cost of ownership (TCO) versus shared carrier leased alternatives.
- High speed mainframe-GPDS-certified interconnectivity for IBM z16 and z17 projects.

Case study
Modernizing a financial network

Summary

A financial services enterprise required a data center interconnect refresh between their sites and took the opportunity to include a quantum-safe network solution to protect their in-flight business-critical data.

Customer challenge

- The current infrastructure is nearing its end of life (EOL), necessitating an upgrade.
- The financial services enterprise requires a high-performing and reliable DCI solution.
- Data privacy is a significant concern in the quantum era.
- The solution should include SLAs that are tailored to meet specific needs.
- Strict adherence to a deployment schedule is critical.

An end-to-end Nokia solution

- Implemented the Nokia market-leading Photonic Service Switch (PSS) solution.
- Operated with Nokia WaveSuite NOC application.
- Ensured an adapted, scaled and evolvable solution.

Benefits

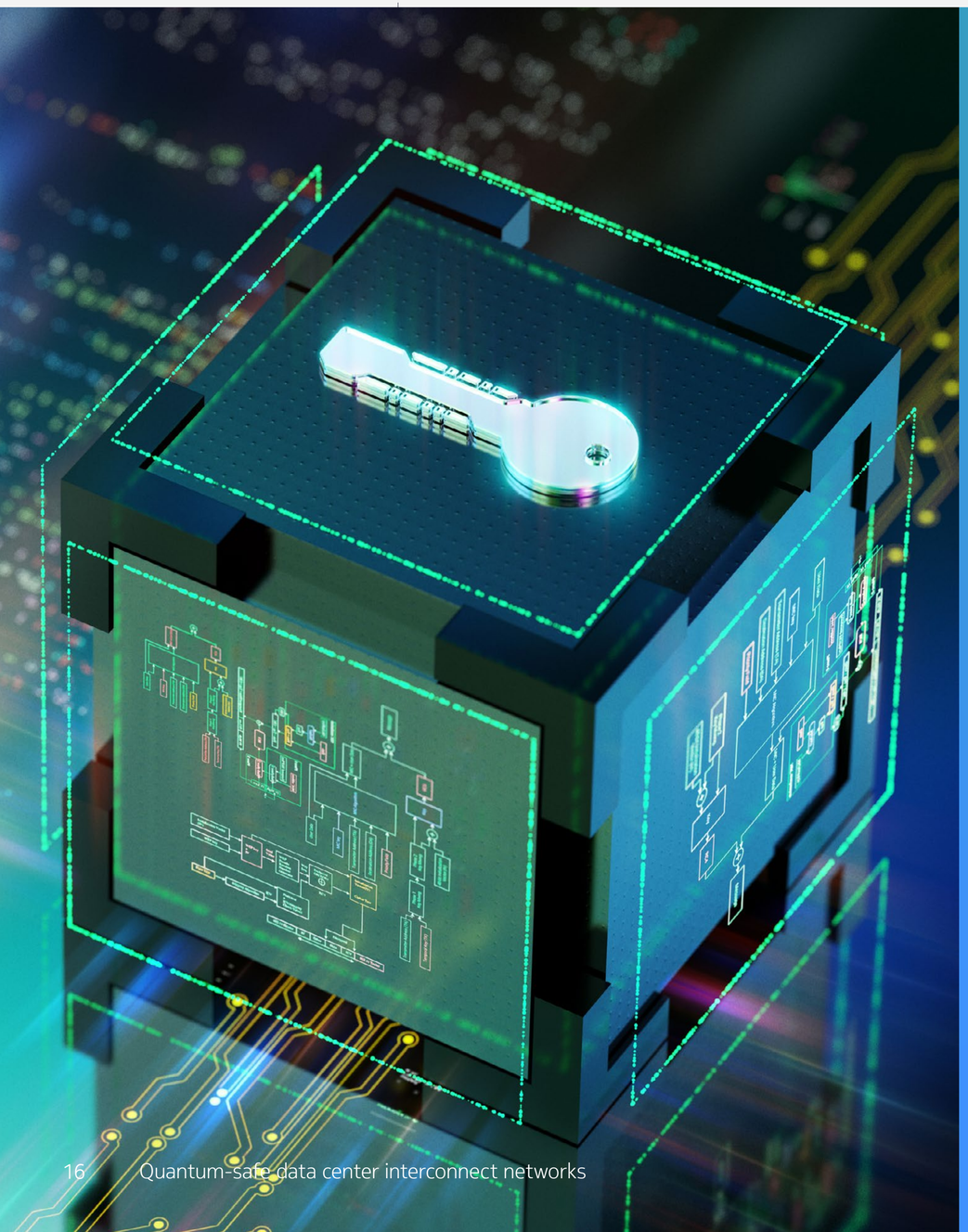
- High-capacity optical data center interconnect solution.
- Safe encryption of client data (data privacy).
- Trusted network.

Business benefits

- Better total cost of ownership (TCO) than the existing solution.
- Fast ROI.
- A better business case than connectivity service provider (CSP) connectivity.
- Dedicated infrastructure owned by the client brings flexible connectivity and a quantum-safe cryptography SLA.

Powerful business outcomes

- End-to-end project delivery based in leading and high performing future-proofed Nokia technology.
- Fast supply to accommodate EOL substitution.
- More secure, higher-capacity and greater performance with lower latency than the existing solution.
- 10-30% lower TCO than CSP connectivity.
- Immediate security risk protection against potential future decryption threats with the Nokia Quantum-Safe Network solution.



Action starts right now

No Plan B for trust in your data

Data centers play a fundamental role in keeping our networks secure. But the game is changing fast. It's time for a new era in technologies to ensure that our data centers can safely and compliantly deliver on these demands. Smart investments in data center interconnect and quantum-safe network security solutions could be the missing piece towards enterprise success.

> "Let's not wait. The dialogue, the assessments, and the action starts right now. And there are technology options; there are actually ways that we can help you today to start mitigating your risk towards Q-Day. Let's just remember one thing, if we lose trust in our data, in our digital infrastructure, there's no Plan B anymore."
>
> **Martin Charbonneau** Head of Quantum-Safe Networks, Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 214755