Quantum-safe optical networks

NOKIA

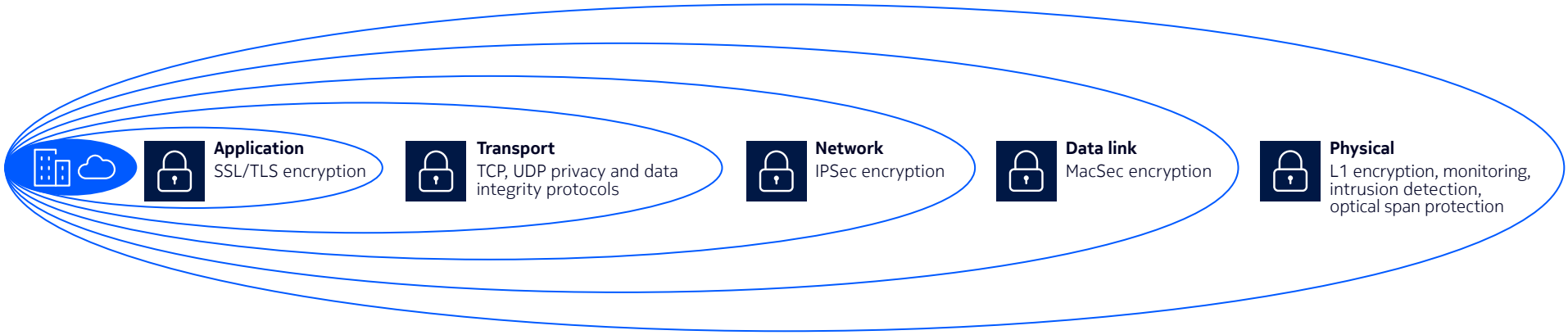
Quantum-safe networking with the Nokia 1830 SMS

Security breaches are growing at an alarming rate. Enterprises and network operators must secure business-critical information.

Quantum-safe Layer 1 encryption and key management are critical to an overall defense-in-depth strategy that protects business-critical data.

A multi-layered defense-in-depth strategy provides greatest security

Figure 1. Security layers as part of a defense-in-depth strategy



Breaches represent a serious financial risk

Since 2013, it is estimated that enterprises worldwide have had more than 14.7 billion data records lost or stolen as a result of security breaches. Of these breaches, only about 4 percent were "safe breaches" where the records were encrypted, rendering the stolen information useless.

The Ponemon Institute's Cost of a Data Breach report, which analyzes breaches, estimates that the average cost of a lost or stolen record is roughly $160. However, this cost varies by industry. Healthcare organizations average $375 per lost or stolen record, while education averages $250.

The public sector, at $80, has the lowest average of all. Regulated industries, such as healthcare and financial services, have the costliest data breaches. That's due to fines and the higher than average rate of lost business and customers. In 2020, the average cost per incident was about $4 million. The longer it takes to detect and contain a data breach, the more costly it becomes to resolve. The emergence of a cryptographically relevant quantum computer is thought to be likely by 2030. This implies that adversaries could be storing data today, waiting for later analysis and possible decryption. This harvest now, decrypt later (HNDL) scenario means that operators should be taking action today to protect data currently on their networks.

What does this mean for data security?

Enterprises and network operators need to strengthen security to minimize the risk of loss or breach of sensitive data. Because data is distributed well beyond the organization's boundaries, network firewalls and other network perimeter technologies are not sufficient in today's environment. These tools must be supplemented by technologies that protect the data itself, particularly when it is in-flight traversing the network. This means ensuring that data confidentiality and integrity are preserved and that the network is highly available and reliable.

The security strategy should include the coordinated use of multiple security countermeasures to protect the integrity of the enterprise's information assets. By using a multi-layered defense approach as shown in Figure 1, this defense-in-depth strategy offers a higher level of security for all data.

With this strategy, organizations can more effectively protect themselves from data breaches and HNDL attacks, while minimizing their impact. The Nokia 1830 Photonic Service Switch (PSS), Nokia 1830 Photonic Service Interconnect (PSI), and Nokia 1830 Security Management Server (SMS) are ideal for this role, providing quantum-safe security at the physical layer (Layer 1).

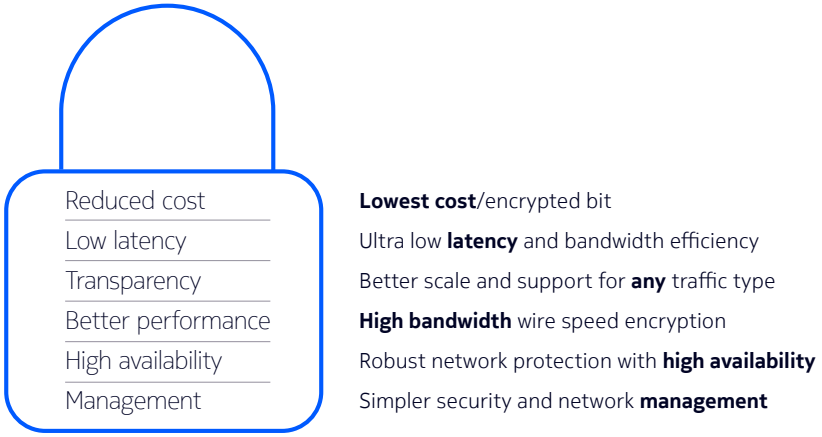
Layer 1 security as part of the overall security strategy

As part of the broader security strategy, Layer 1 security encryption and protection deliver important benefits:

- **Reduced cost:** Encryption at the higher network layers is costly because many security appliances are needed to protect each data stream, service protocol, and client. Data encryption at Layer 1 reduces the cost per encrypted bit by integrating the encryption function in the transport system.
- **Lower latency:** Layer 1 encryption yields better latency performance. Higher-layer encryption technologies add significant overhead and multiply the latency of the data stream, whereas Layer 1 encryption adds almost no additional latency (less than 150 nanoseconds) to the transport process. This makes it highly suitable for low-latency, business-critical applications.
- **Transparency:** Layer 1 encryption is protocol agnostic, which means that the network can offer the flexibility to support a variety of client and transport interfaces for both current and future services.
- **Improved performance:** Hardware-based Layer 1 encryption solutions support very high bandwidth with encryption of 10/100 Gbps wire speeds and higher. This provides the scale needed to support current and future services.
- **High availability:** Mission-critical data must be accessible to its rightful owners. The network must be highly available and reliable. By supporting optical span protection, the Nokia Secure Optical Transport solution avoids network disruptions in response to attacks.
- **Management:** Layer 1 encryption simplifies security and network management. Key management, exchange, and authentication can be labor-intensive and cumbersome when there are many separate encryption devices and encryption streams to manage. But with Layer 1 encryption, only one encrypted circuit needs to be managed as compared to many IPSec tunnels.

As part of the quantum-safe optical networking solution, the Nokia 1830 PSS and Nokia 1830 PSI provide AES-256 encrypted optical links, ensuring quantum-safe protection through symmetric key distribution. These systems leverage strong symmetric keys generated by the Nokia 1830 SMS as part of the encryption/decryption process. Benefiting from the service transparency of Layer 1 encryption, the solution supports multiple client interfaces including 8G/10G/16G Fibre Channel and 10GE/40GE/100GE Gigabit Ethernet.

Figure 2. Why Layer 1 security?



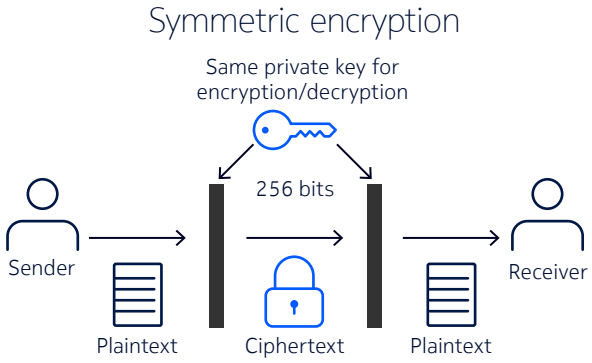
Key strength and the illusion of security

Cryptographic algorithms are considered “strong” not because they are mathematically impossible to break, but because they are computationally prohibitive. The longer it takes to decrypt a message without knowing the key, the stronger an algorithm is considered to be. In fact, an algorithm could take so much time to break, it would be far too costly a task.

Unbalanced crypto solutions marketed as AES-256 compliant may give the illusion of having 256-bit security strength, when in reality they are not because they use weak keys, distributed through asymmetric methods. There is a traditional trade-off between the strength of encryption and its impact on system performance that has led to the practice of using the minimum strength necessary. Asymmetric key negotiation providing 256-bit security key strength (e.g. RSA 15360) is computationally intensive, and as a result, many vendors have chosen asymmetric key negotiation that better fits their control plane processing power (e.g. RSA 2048). This choice weakens the security substantially. It is vitally important to match key strength to the encryption algorithm’s strength. That’s because the overall solution will only be as strong as the weaker of the two—just as the locks in a house are only as good as the weakest one. For this reason, a “top secret” security standard requiring 256-bit strength should use an AES-256 algorithm with 256-bit symmetrically distributed keys. This solution is generally viewed as "quantum-safe", meaning secure from compromise by any cryptographically relevant quantum computer in the foreseeable future.

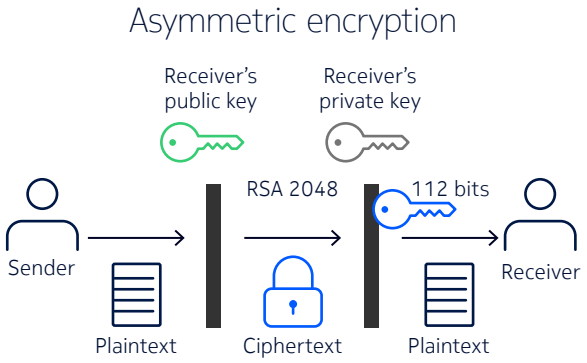
The Nokia 1830 SMS provides key management of strong AES-256 keys. The server interoperates with the 1830 PSI, the 1830 PSS and providing quantum-safe encryption to meet the most stringent security requirements.

Figure 3. Comparative stength of symmetric versus asymmetric encryption algorithms



Comparative key strength

Symmetric key size (bits)	Asymmetric key size (bits)
80	1,024
112	2,048
128	3,072
192	7,680
256	15,360

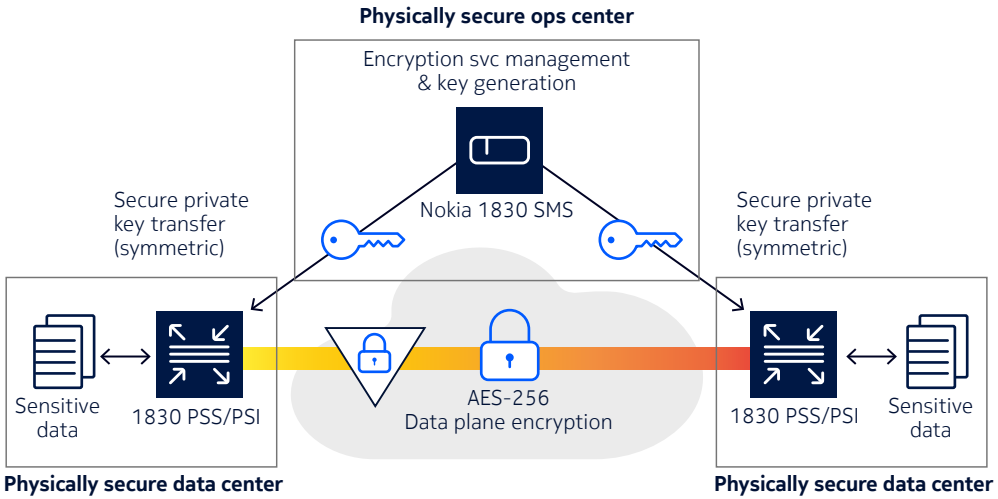


Centralized key management

To be most effective, key management should be centralized across the network. This offers these benefits:

- **Quantum-safe encryption:** Centralized, symmetric key management enables the creation of keys by the central key manager so they can be sent securely for “off-board” encryption/decryption. This frees up host CPU capacity on the hardware security module and allows the use of stronger, more complex keys. By distributing keys symmetrically, through a secure, discrete channel outside the data plane, we can ensure protection against quanutm computer attack.
- **Single point of trust:** Centralized key management limits the number of locations in which keys reside, minimizing the potential for exposure.
- **Consistent policy enforcement:** Centralized key management enables administrators to enforce standards and policies consistently across the network.
- **Streamlined administration:** Centralized key management streamlines administration by allowing updates to be made once (centrally) and cascaded automatically across the network. For example, this enables single-point key revocation and one point to force multi-tenant, synchronized key rotations.
- **Unified auditing and remediation:** Centralized key management simplifies network security audits, facilitates policy compliance, and streamlines remediation through the use of audit logs containing all key-related activities. These logs can be analyzed, enabling preventative measures to be continually improved.

The Nokia 1830 SMS delivers quantum-safe, centralized key management for the entire cryptographic life cycle of each encrypted wavelength service.



Importance of independent validation

Customers want confidence that the products they purchase and use will meet their security requirements. Product vendors may assert that they include cryptographic features in their products that are designed to meet industry standards and that they employ secure development practices. However, without independent certification, the level of assurance customers get from vendor assertions depends on vendor trustworthiness.

Independent confirmation of vendor claims by third-party validations can give customers greater confidence. Customers can gain even more confidence, if independent, third-party validations are performed using open, international standards where products are “certified to meet” these standards. Benefits of third-party validations include:

- **Higher confidence:** Examination against recognized industry standard metrics and criteria gives customers higher confidence that the measures are relevant and complete.
- **Consistent results:** Standardized validation methods help to guarantee consistent, unbiased results.
- **Credibility:** The credibility of the third party is the basis for trusting results. Third parties that use open processes for standards development and publication of results achieve the broadest credibility.

Regulatory compliance

Federal agencies and government contractors demand custom-developed enterprise and mobile applications for a diverse set of mission needs. Information security is always among the top requirements. Any federal information systems that need to meet the requirements of the Federal Information Security Management Act (FISMA), which did away with waivers to mandatory Federal Information Processing Standards (FIPS), must obtain support from a validated cryptographic module.

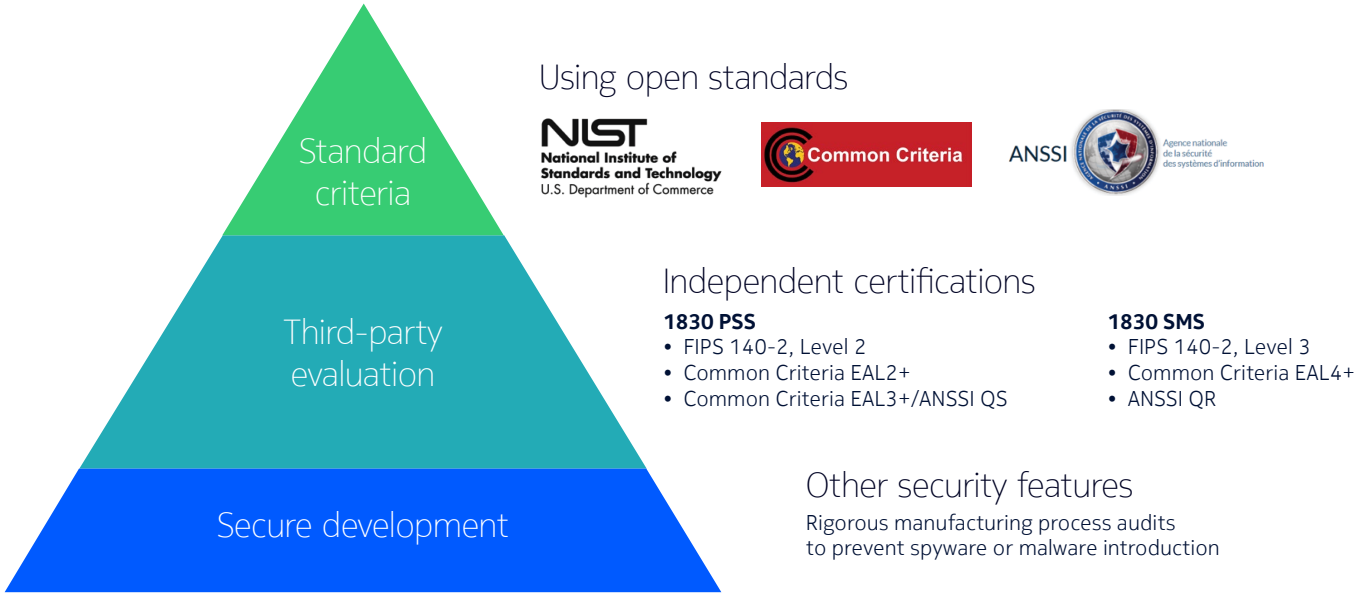
The Nokia Secure Optical Transport solution based on the 1830 PSS, 1830 PSI and 1830 SMS has been independently certified to meet numerous security standards as shown in Figure 4.

Versatility across industries and applications

The Nokia Secure Optical Transport solution is tailored to protect critical in-flight data in all of today's high-capacity applications. Key applications that can benefit from this solution include:

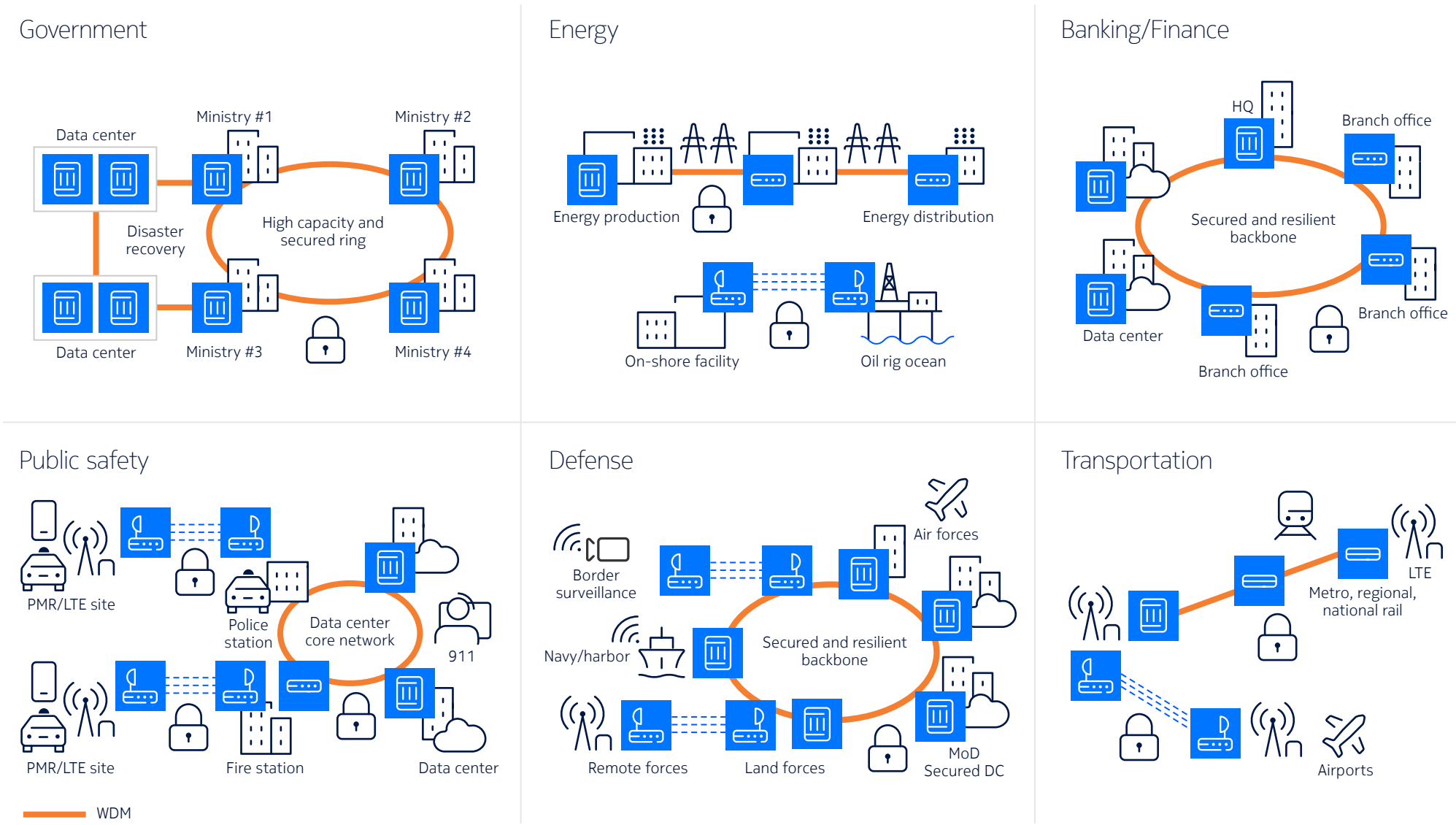
- Enterprises or cloud providers who require secure, encrypted connectivity across data centers (cloud DCI)
- Government and institutions that require certified, secure, high-speed communications between different locations
- Healthcare applications, such as telemedicine and telehealth with high-quality, low-latency and privacy requirements between healthcare stakeholders
- Smart city infrastructure providing connectivity to smart appliances and supporting the Internet of Things (IOT).
- Managed wavelength service applications requiring secure encryption
- Transportation applications, such as railway signaling or ITS, requiring high-capacity and low-latency communications across different endpoints
- Latency-sensitive applications, such as high-definition video, that require a secure, ultra-low-latency transport solution
- Utilities that want to protect their critical communication infrastructure and support smart grid, teleprotection, and SCADA applications.

Figure 4. The Nokia Secure Optical Transport solution is certified to meet strict security standards



The assurance pyramid

Figure 5. Industries where the Nokia optical transport security solution have been deployed



Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID200776

nokia.com

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.