ANYsec quantum-safe network cryptography to help protect your AI and digitalization ambitions

Application note

NOKIA

Abstract

We live in a world that's being transformed by rapid digitalization and the continuing growth of the digital economy. This transformation needs to be underpinned by hyperconnectivity. Telecommunications networks have become business- and society-critical infrastructure because they support digitalization with secure and trusted connectivity.

But this infrastructure faces a serious new threat. The rapid evolution of quantum computing technology means that threat actors could soon gain access to powerful computing capabilities that can break down the cryptographic technologies that currently protect critical networks and data.

At the same time, we are seeing the emergence of, and continued investment in, technologies such as artificial intelligence (AI). However, the effectiveness and reliability of AI technologies depend heavily on the trustworthiness of the data on which they operate. Without secure and trusted data, we cannot have full confidence in the outcomes of AI operations.

Secure and trusted data connectivity must be anchored in scalable, automated and resilient cryptography technologies.

The ANYsec technology in the Nokia 7705 Service Aggregation Router (SAR), 7730 Service Interconnect Router (SXR) and 7750 Service Router (SR) platforms fulfills this role by extending the low latency and simplicity of MACsec security technology to a new generation of engineered quantum-safe networks based on IP, multiprotocol label switching (MPLS) and segment routing. With quantum-safe ANYsec technology, operators can secure an IP connection or service by turning on network cryptography whenever and wherever it's required.

Contents

Introduction

Networks and data have never been at greater risk. Most of the world's content and economies are becoming digitalized, which means that corporate, government and personal data traverses public and private networks in petabyte volumes. As the Quantum 2.0 era begins, the emergence of quantum computing presents a profound and urgent challenge to the cryptographic technologies that protect digital infrastructures. The threat is not hypothetical: Quantum computers will make widely used asymmetric cryptographic methods obsolete and expose organizations to systemic risk across their operations, supply chains and customer ecosystems.

The growing use of AI compounds this liability and changes the cyberthreat landscape in potentially alarming ways. As enterprise and AI infrastructures become more distributed through multiple private data centers, distributed cloud services or a hybrid of the two, data spends more time in transit over public or private networks.

At the same time, the operators responsible for transporting these data flows are embracing open technologies, third-party transport options and globalization. All of these choices can make their networks more porous and vulnerable to attacks. Organizations are increasingly concerned about the confidentiality and integrity of data in flight, or more specifically, the growing vulnerability of data flows to interception and manipulation.

The challenge is clear: Organizations of all types need secure and trusted data connectivity to unlock the potential and value of investments in digitalization and AI.

Cryptography requirements for mission-critical IP networks

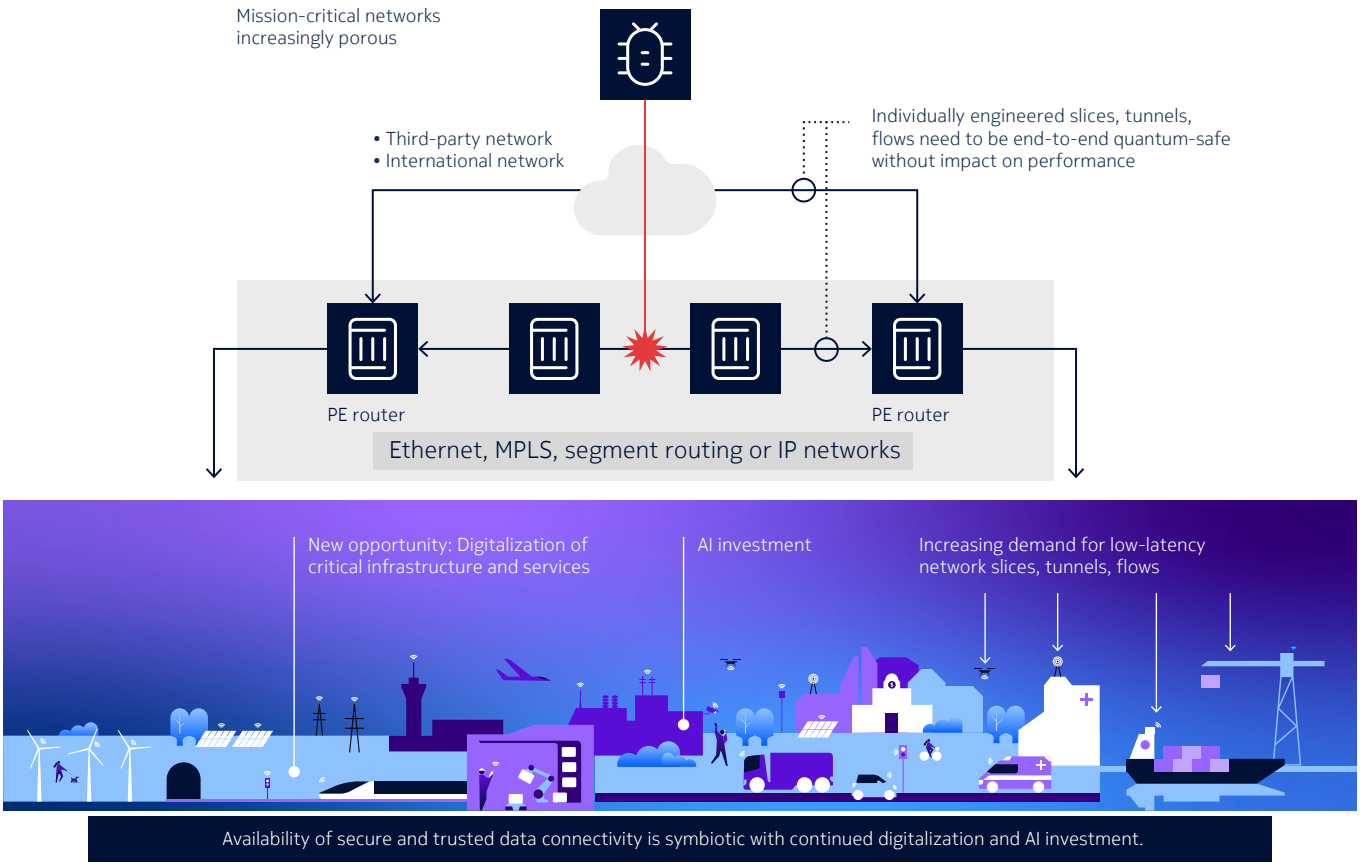
While many mechanisms are used to protect the confidentiality and integrity of data flows, the most secure and prevalent option is cryptography. Historically, most cryptography, and its inherent encryption, has been applied at the application layer and at the transport layer or above using asymmetric cryptography and protocols such as the Transport Layer Security (TLS) protocol.

But TLS only cryptographically encrypts application layer payloads, so it leaves mission-critical IP and other network data exposed as packets transit operators' networks. It also puts the security onus on the application developer and the user to protect the data in flight. Some organizations work around this by configuring and deploying specialized cryptographic equipment at all their sites, but this approach entails significant ongoing operational and capital costs, and it limits the kinds of network connectivity and services they can leverage.

Operators can help resolve these issues and enable new IP connections or service types through the flexible application of cryptography in their networks. To instill user confidence and open up new service opportunities, operator-based cryptography must provide:

- **Low latency** to support the many new networked applications and services that are an integral part of organizations' digitalization and AI strategies.
- **Simplicity and low cost** to enable mass-scale deployment.
- **Flexibility** to support the use of individually engineered tunnels, slices and flows using segment routing and MPLS to build next-generation IP transport infrastructure. Cryptographic technologies must be able to encrypt these flows as well as IP, Ethernet and virtual LAN (VLAN) frames and packets.
- **High security** to support quantum-safe networking with the requisite key entropy, strength and distribution combined with 256-bit network encryption standards.

Figure 1: Quantum-safe connectivity is a growing network imperative



Traditional cryptographic options

Until now, operators have tried to provide data flow confidentiality and integrity with limited deployments of MACsec, IPsec or proprietary technologies. None of these options have been able to fulfill more than one or two of the cryptography requirements described above.

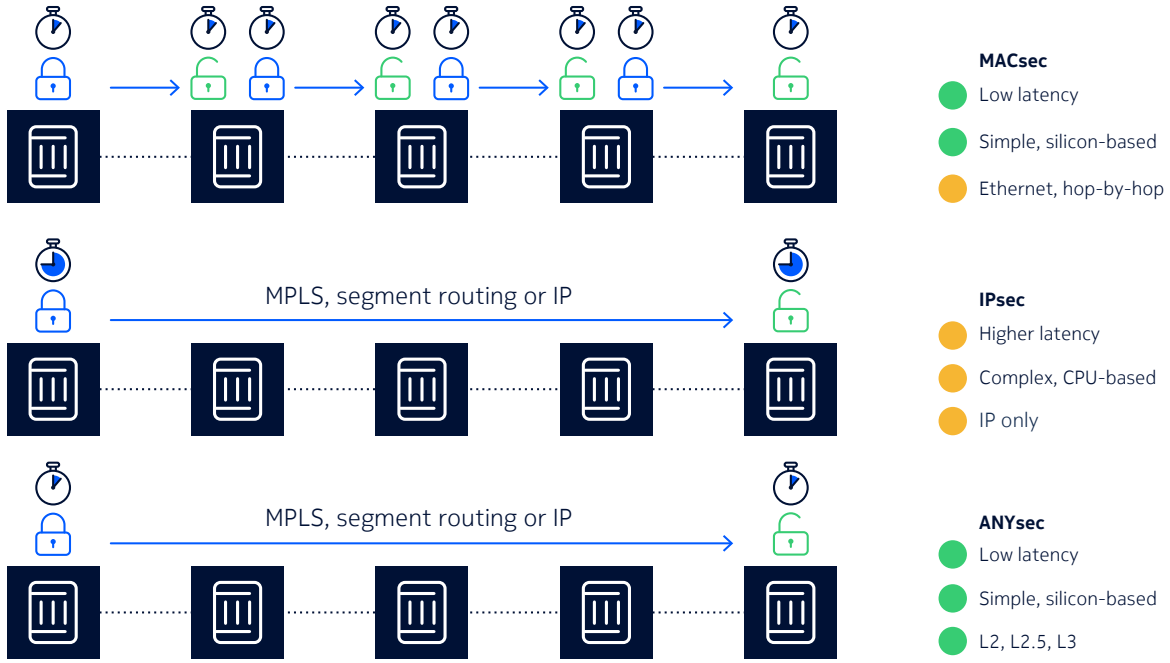
The big advantage of MACsec is its simplicity. It allows for silicon-based implementations that deliver the low latencies required by some digitalization and AI applications. But MACsec was designed for point-to-point Ethernet links, which means it must be implemented hop by hop in MPLS, segment routing or IP networks. Each cryptographically encrypted hop must be individually configured, making deployment operationally complex. Frames must be decrypted at every hop to determine the next hop, thereby increasing the security risk and adding to the overall latency.

IPsec, on the other hand, was designed specifically for single-hop encryption across a wide area network (WAN). IP packets are encrypted at one end of an IP network and decrypted at the other. But IPsec requires a more complex control plane that involves software intervention and CPU processing. It must be implemented in CPU-based platforms such as specialized appliances or specialty CPU blades that consume precious real estate within routers. CPU processing also means that IPsec latencies are much higher. This makes it unsuitable for time-sensitive networking. Finally, because IPsec is an IP-only technology, it cannot natively encrypt tunnels, flows and slices engineered using MPLS and segment routing.

ANYsec quantum-safe cryptography

To address these gaps, Nokia delivers ANYsec symmetric cryptography on the 7705 SAR,7730 SXR and 7750 SR series routers.

Figure 2: Comparing ANYsec with traditional network cryptography options



ANYsec provides the benefits of MACsec—low latency, simplicity, Advanced Encryption Standard (AES) network encryption—and adds flexible quantum-safe key entropy, strength and distribution. It extends these attributes beyond Ethernet links and VLANs to include MPLS, segment routing and IP transport networks.

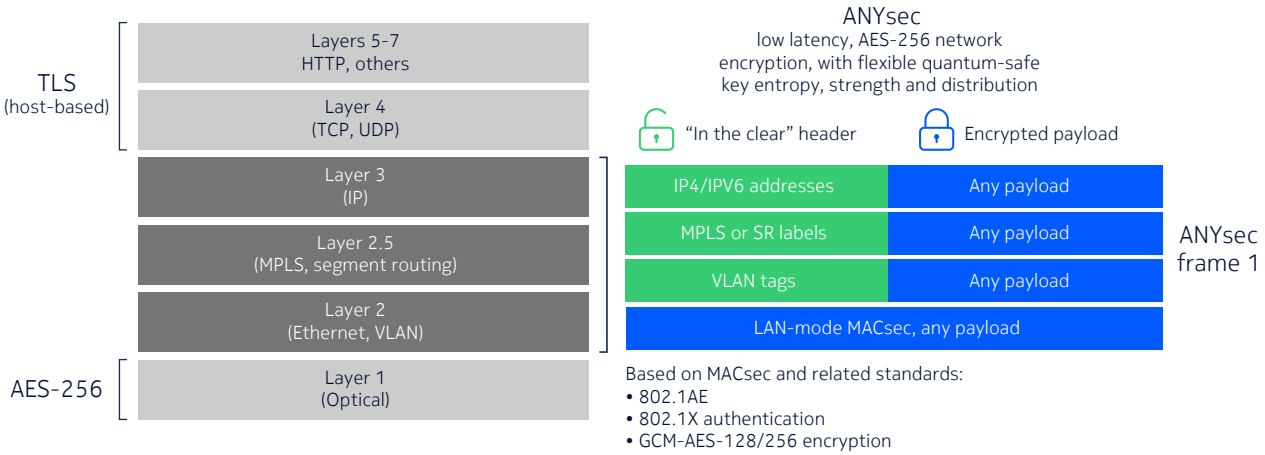
With ANYsec, operators can cryptographically encrypt individually engineered tunnels, flows and slices at network ingress, switch or route them natively across existing IP, MPLS or segment routed networks, and decrypt them when the tunnel, flow or slice is terminated on the other side. The cryptographic encryption is always optimized for the network payload and chosen transport method.

To provide the required latency, performance and universal network capability, best-of-breed network technology is fused with best-of-breed quantum-safe cryptography (quantum-safe key generation, distribution and network encryption) to deliver quantum-safe outcomes— just like packet forwarding, a high-performance, universal capability of the network itself.

Figure 3 provides a summary of ANYsec options and packet formats. ANYsec supports traditional MACsec network cryptography in LAN and WAN modes. It extends MACsec-related standards such as 802.1AE, 802.1X authentication and Galois/Counter Mode (GCM) AES-128 or AES-256 network encryption to all other network payloads, and it allows any in-the-clear (unencrypted) network headers to be inserted. This includes traditional Ethernet and VLAN tags, as well as MPLS labels, segment routing labels and IP addresses—whatever is necessary to optimize the transport of cryptographically encrypted frames, packets and flows across a network.

Where MACsec and ANYsec operate simultaneously on a router, a hybrid operation is supported with interworking between these protocols with seamless network encryption and decryption.

Figure 3: ANYsec delivers quantum-safe network cryptography for all network layers (2, 2.5 and 3) and payloads



ANYsec use cases

ANYsec provides operators with the freedom to make IP-based connections and services quantum-safe on demand. Instead of treating cryptography as an expensive, complex and limited capability that requires significant advanced planning, operators can flip a switch to turn on the cryptographic encryption whenever and wherever it is required, no matter what service or network transport is being used.

Figure 4 shows how ANYsec can be used to transform internal or wholesale transport connections and services into quantum-safe network outcomes. Tunnels or slices that correspond to individual customers or service quality characteristics can all be cryptographically encrypted from provider edge to provider edge with no impact on performance or latency.

Figure 4: Quantum-safe transport services (internal or wholesale)

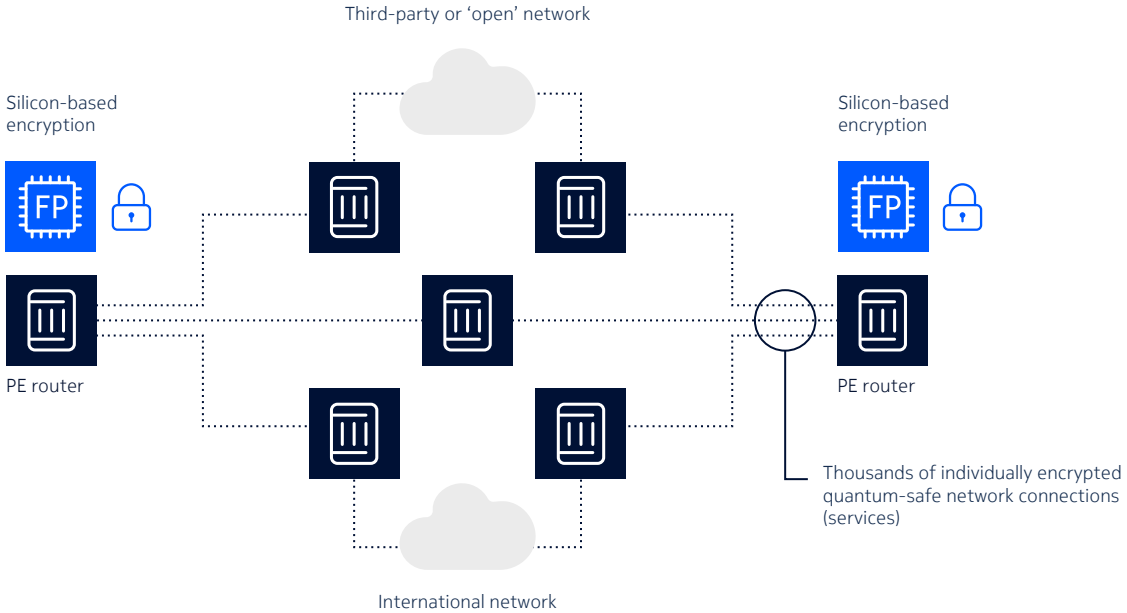
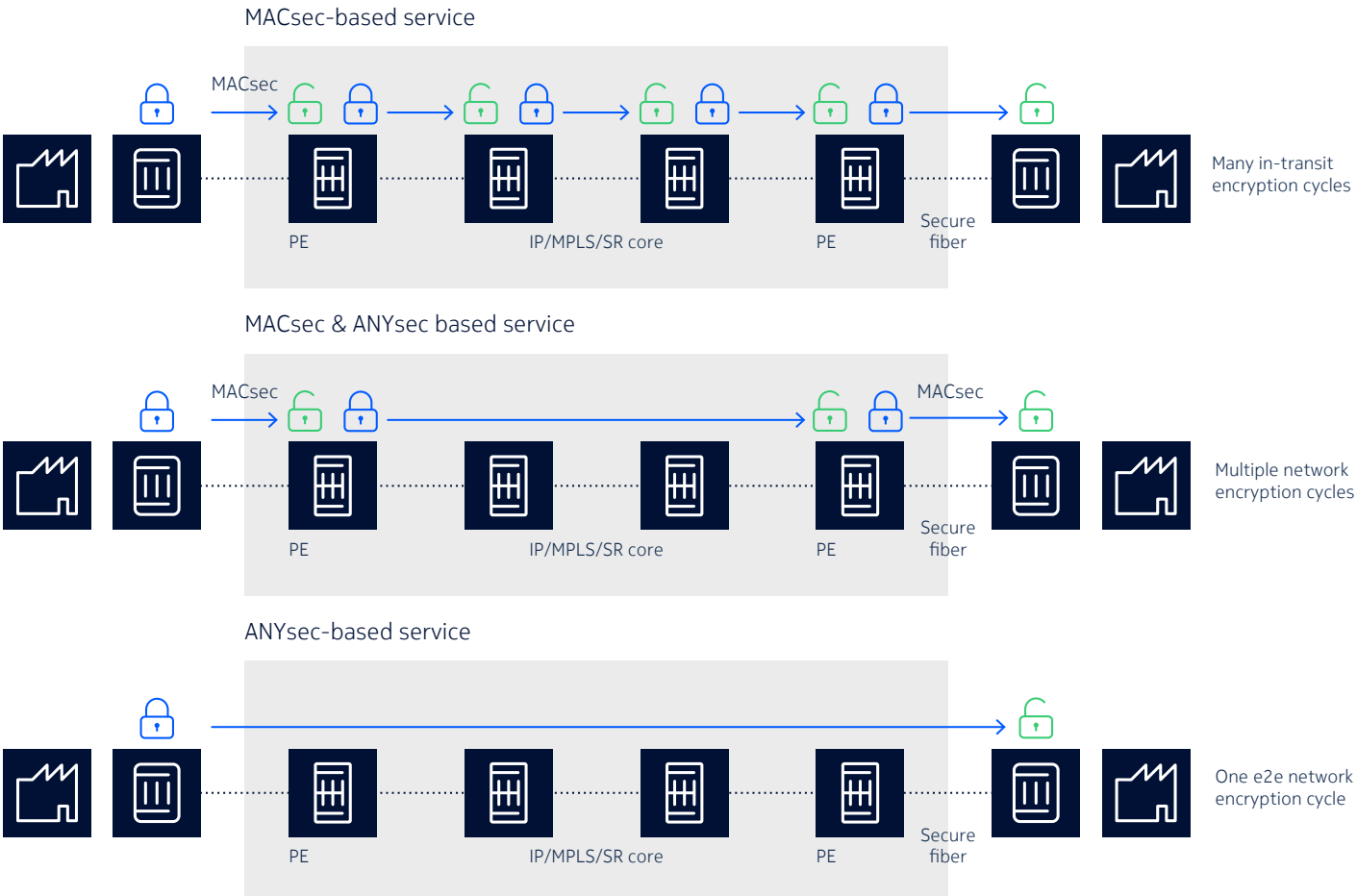


Figure 5 shows how ANYsec can be used to deliver high-performance, secure VPN services. While MACsec technically provides the low latency required, it requires hop-by-hop configuration within IP/MPLS and segment routing networks. This is time-consuming to configure and manage, it increases security risks by requiring decryption at each hop, and each decrypt/encrypt cycle adds to the total latency of the service. With ANYsec, the operator simply turns on cryptographic encryption on all MPLS and segment routing tunnels associated with a particular customer, thereby eliminating the latency, security risk and operational complexity.

Figure 5: ANYsec-based secure VPN services



Summary

As the Quantum 2.0 and AI eras dawn, the stakes for digital security, trust, sovereignty and resilience have never been higher. The rapid emergence of quantum computing and AI threatens to undermine the network security foundations that protect digital economies and societies. Organizations that fail to act now risk falling behind in a world where trust, compliance and continuity are paramount.

Nokia has redefined and redesigned network security by adopting a multilayer approach to IP network security. Offered on our 7705 SAR, 7730 SXR and 7750 SR series routers, ANYsec is a multilayer quantum-safe network cryptographic capability. It extends the low latency and simplicity of MACsec to MPLS, IP and segment routed networks so that operators can secure any connection or service across any network.

With this approach, operators can deliver high-performance and comprehensive quantum-safe protection for IP network users, connections and services today—and maintain this protection as AI and quantum technologies evolve.

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, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. 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 OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (September) CID210676