Quantum-Safe networks: today and into the future

White paper

Introduction

As quantum computers continue to advance, they will pose a significant threat to cybersecurity. Most communications infrastructure presently using encryption to protect confidentiality are already vulnerable to a harvest now, decrypt later attack by any adversary capable of eavesdropping on encrypted data. This is because the current method of generating asymmetric encryption keys to protect the confidentiality is already known to be exposed as soon as a strong enough quantum computer is available.

Quantum computers can perform calculations immensely faster than classical computers, allowing cyber criminals to break public key-based encryption algorithms and perform cyber-attacks that are currently not possible. Decision makers responsible for telecommunications infrastructure need to immediately inventory and prioritize which portions of their networks are most at risk and provide countermeasures to assure that today's customers' data is staying secure from future unauthorized decryption.

Nokia's Quantum-Safe Networks offer a solution to this challenge by allowing parties to securely exchange keys that can be used to encrypt and decrypt data. This paper describes the threats and countermeasures already available and additional technologies under development that will complement these protections. Together, this forms a quantum-safe, defense-in-depth protection well into the future.

Contents

The quantum threat

Quantum computing is a rapidly emerging field that has the potential to revolutionize a wide range of industries, from healthcare and transportation to finance and cybersecurity. But what exactly is quantum computing, and how does it differ from the classical computers that we use every day?

At its core, quantum computing is based on the principles of quantum mechanics, which describe the behavior of particles at the atomic and subatomic level. Quantum computers use quantum bits, or qubits, to store and process information. Unlike classical computers, which use bits that can only represent either a 0 or a 1, qubits can represent both 0 and 1 simultaneously, a property known as superposition. This allows quantum computers to perform certain types of calculations much faster than classical computers, making them particularly well-suited for tasks that require a lot of processing power, such as searching large datasets or optimizing complex systems.

But the potential capabilities of quantum computers also pose a new challenge to cybersecurity. Quantum computers have the potential to break certain encryption algorithms that are currently considered secure. This could enable attackers to perform cyber-attacks that are currently infeasible or impractical, potentially leading to the theft of sensitive data and the disruption of critical infrastructure.

As the world becomes increasingly reliant on digital systems and networks, the security of data and communications has become a critical concern.

Connectivity and Cybersecurity in the “Quantum era”

Rapid digitalization of industries, government and individual consumers over the past ten years has led to an insatiable need for connectivity. By 2023, digitalization had far exceeded simple transactions like order placement, inventory management or logistics optimization- it had embraced cloud-based compute & store, process automation and AI-based customer experiences. All of this means that network connectivity is vital to most any organization or individual.

While much attention has been on the speed, availability and reliability of this connectivity, less attention has been paid to security. But in a world where data connectivity is the lifeblood of commerce, basic infrastructure and individual safety, one must place a higher emphasis on protecting networks against threat from attack. This includes attacks which seek to steal data as well as disrupt the organizations that rely upon connectivity.

Network connectivity security measures traditionally have addressed attacks from conventional binary computers, as well as disruptive attacks, such as denial of service. For this paper, we set aside denial of service attacks to focus on data theft.

Why act now?

Quantum computers are rapidly become real and tangible, so now is the time to start the quantum security journey and prepare for “harvest now, decrypt later” attacks.

Harvest now, decrypt later (HNDL) refers to an attack where threat actors store encrypted data from target organizations today, anticipating that data can be decrypted later when quantum computing reaches a maturity level capable of rendering some existing cryptographic algorithms obsolete, according to Deloitte. This implies that, **every day we lose today by not implementing quantum-resistant strategies, might correspond to data being exposed in the future.**

Deloitte surveyed over 400 professionals from organizations that have considered quantum computing benefits and found that over half (50.2%) of respondents believe their organizations are at risk for HNDL attacks.

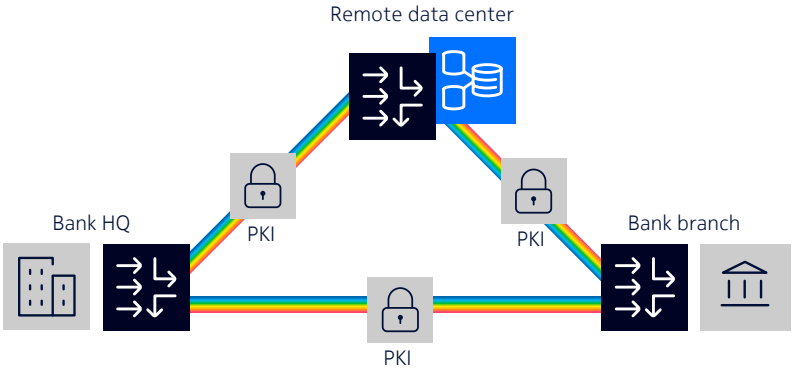
Many enterprises are employing encryption

The United States government is also urging organizations to prepare for post-quantum threats. The White House issued a memo on mitigating vulnerable cryptographic system risks, while the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) released quantum-resistant (QR) algorithms recommendations and requirements for critical infrastructure and national security systems based on the post-quantum cryptography selections from National Institute of Standards and Technology (NIST).

Deloitte's report showed that 27.7% of respondents stated that their organizations' quantum computing security risk management efforts will advance following regulatory pressure to adopt legislation or policies.

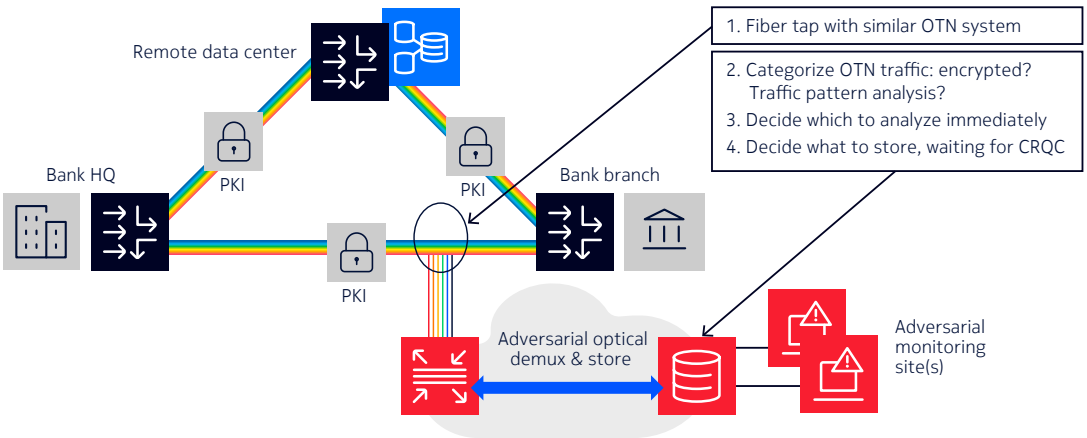
Nokia believes HNDL is a clear and present danger faced by all network operators. For example, imagine a bank, with a headquarters location connected to a remote data center and branches, as shown in the simple diagram below. In this case, the bank is using commonly available PKI (Public Key Infrastructure) encryption:

Figure 1. Harvest now, decrypt later (HNDL) threat



The threat is from a future quantum computer which could easily decipher the private PKI key in data stored now from the bank's network. An HNDL attack unfolds over an extended period. First, an adversary accesses the bank's DCI (Data Center Interconnect) infrastructure through an inexpensive fiber tap found anywhere in the optical span. Using commercially available optical terminal equipment, an entire OTN (Optical Transport Network) connection can be replicated and transmitted to a monitoring site through the internet, without detection for years. Once a CRQC is available, the adversary can decrypt the bank's data. Figure 2 illustrates this attack.

Figure 2. How the HNDL threat unfolds



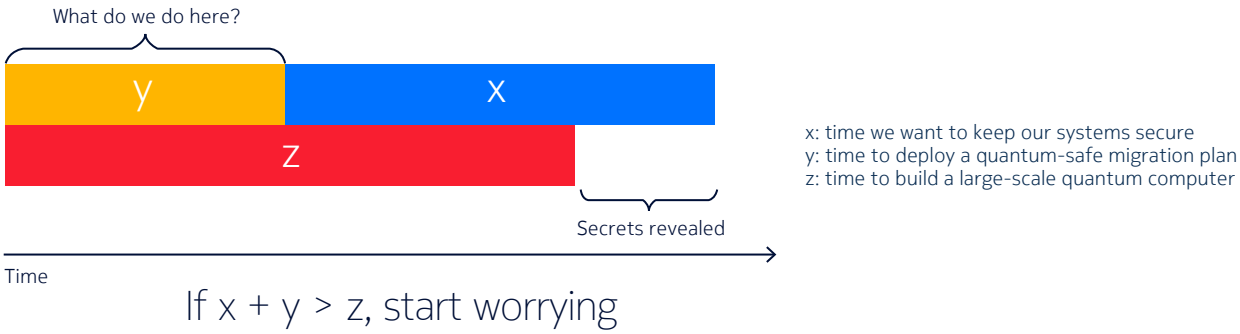
A cryptographically relevant quantum computer (CRQC) can decrypt widely used asymmetric security protocols, such as the commonly used RSA (Rivest Shamir Adleman) or elliptical curve algorithms and present **a zero-day vulnerability.**

Post-Quantum Cryptography (PQC) algorithms are under development to address this vulnerability but ratification, standardization, implementation & deployment will take years. This time delta, for many, is not acceptable.

Cryptography is a technology that historically matures slowly; NIST notes that it has taken almost 20 years to deploy a public-key infrastructure that we can trust. NIST also expects a similar period of 5-15 years after the release of PQC standards (Barker & Souppaya, 2021) while other analysts and academics give a more conservative estimate of 10-20 years (Mosca M. P., 2020).

The risk is well-illustrated by the Mosca model shown in Figure 3 (Mosca M., 2015). In the figure, x denotes the time that our systems and data need to remain secure, y the number of years to migrate to a PQC infrastructure and z the time until a practical quantum computer that can break current cryptography is available. The model assumes that encrypted data can be intercepted and stored before the migration is completed in y years. This data stays vulnerable for the complete x years of their lifetime, thus the sum x+y gives us an estimate of the full period that data stay insecure (Mosca M. P., 2020). The model asks the question of how we are preparing our IT & telecom systems during those y years (or in other words how we can minimize y years), to minimize the transition phase to a PQC infrastructure and hence, minimize the risks of data being exposed in the future.

Figure 3. The Mosca model



We should not underestimate other factors that could accelerate the introduction of a large-enough quantum computer, for example faster-than-expected advances in quantum computing and more efficient versions of Shor's algorithm requiring less qubits. As an example, IBM, one of the leading actors in the development of a large-scale quantum computer, has recently published a roadmap committing to new quantum processors supporting more than 1000 qubits by 2025 and networked systems with 10k-100k qubits beyond 2026. Innovation often comes in waves, so it is to the industry's benefit to remain vigilant and prepare as early as possible.

It's worth noting that HNDL is but one vulnerability due to the emergence of a CRQC. While HNDL poses an immediate threat, there are also other types of attacks to be concerned with. Obviously, post-quantum attacks would result in theft of live network data, compromising all manner of commercial, infrastructure and government systems. But more insidious events such as masquerade or counterfeiting attacks brought on by stolen authentication certificates could wreak havoc in ways not at once detected. Certainly, these attacks allow more time than HNDL for implementing countermeasures but are worth consideration today.

Building a quantum-safe network

A quantum-safe network protects against the imminent threat imposed by quantum computing. It is characterized by inherent resistance against theft and intrusion due to the emergence of cryptographically relevant quantum computers (CRQC). A quantum-safe network provides the highest level of known protection against a CRQC attack. This protection is achieved through multiple mechanisms including data encryption, strong key generation, management and distribution, independent certification, and other factors which together ensure:

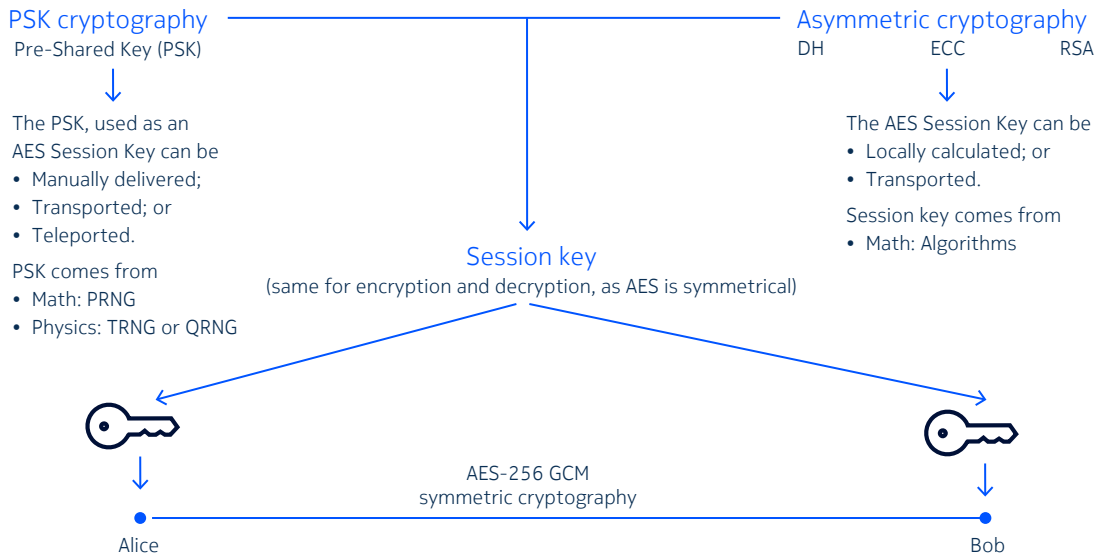
- **Data confidentiality**: protecting enterprise sensitive data from access, disclosure or use by unauthorized parties
- **Integrity**: protecting data from theft or corruption in-transit across the network
- **Non-repudiation**: that no party can deny that it sent or received a message via encryption
- **User and end-point authentication**: protect access to systems that manage encryption keys or related systems

Fortunately, network operators have many tools available to protect their data today from the quantum threat. Adopting a defense-in-depth approach that maximizes protection at once while allowing for adoption of emerging technologies ensures investment protection while taking best effort actions to protect against HNDL or other attacks.

As mentioned above, multiple mechanisms exist. In this paper, we will focus on data in-flight protection and integrity using encryption & strong key generation, management, and distribution. Locks are the encryption engines, embedded in our connectivity enablers, that implement a cipher, such as AES-256 GCM, rendering plain text into ciphertext for transmission across a network. A key is, as the name implies, the 256 bit value that allows an authorized user to unlock ciphertext back into plain text. Key distribution, also an important notion, is the method used to share or to agree on the key between ends of a network link.

Figure 4 shows a baseline key distribution canvas.

Figure 4. Key distribution comparison



Focusing on data in-flight protection and integrity, our attention shall be on how we enable a Quantum-computer resistant connection between endpoints. To detail this out, let's use industry terms of Alice and Bob. Alice, one endpoint, wants to have a Quantum-Computer resistant connection with Bob, the other endpoint.

Let's focus first on the connection itself, and more specifically, its ability to ensure secure communication and data protection. For this we make use of AES (Advanced Encryption Standard) symmetric encryption algorithm, and we will refer to this functionality as a lock. A lock employs a block cipher with varying key lengths of 128, 192, or 256 bits, providing strong encryption and efficient processing for secure transmission of sensitive information.

It is important to understand that in AES, both endpoint locks need to have access to the same secret key to encrypt and decrypt traffic. Thus, let's now focus our understanding on how we can derive the AES secret session key. As shown in the diagram, two methods are possible to derive the AES secret session key:

- Pre-Shared Key (PSK) cryptography; or
- Asymmetric cryptography.

Pre-Shared Key (PSK) cryptography uses a single secret session key for both encryption and decryption of data. It ensures confidentiality and integrity of information, as the same pre-shared key is used between the communicating parties. Here the challenge is how to create and distribute these Pre-Shared Key to both Alice and Bob, ensuring the secure communication and data protection.

The Pre-Shared Key (PSK) can come from

- PRNG (Pseudorandom Number Generator): An algorithm that generates random numbers using a seed value. However, the output is deterministic and predictable if the seed is known, making it unsuitable for Quantum-Computer resistant solutions;
- TRNG (True Random Number Generator): It derives randomness from unpredictable classical physical processes, such as electronic noise or radioactive decay. It produces genuinely random numbers, making it suitable for Quantum-Computer resistant solutions; and
- QRNG (Quantum Random Number Generator): It leverages quantum phenomena to generate random numbers. It uses properties like quantum superposition and entanglement, ensuring provable randomness, making it suitable for Quantum-Computer resistant solutions.

And the Pre-Shared Key (PSK) can be delivered to the lock via

- Manual processes;
- Transported and distributed by a Quantum-Resistant protocol; or
- Teleported, or locally created at both endpoints thanks to the law of Quantum mechanics.

We will deepen how the PSK can be distributed in the next section.

The other method, called asymmetric cryptography, or public-key cryptography, uses a pair of keys (public and private) for encryption and decryption. The public key is shared openly, while the private key remains secret. It ensures secure data exchange and authentication, enabling parties to communicate securely without prior key sharing. That said, asymmetric cryptography, like RSA or ECC, can be used to facilitate the AES secret key exchange. The sender encrypts an AES key (i.e.: secret session key) with the recipient's public key, which can only be decrypted using the corresponding private key held by the recipient. Once the AES key is securely exchanged, both parties can use AES symmetric encryption for efficient and secure communication.

Asymmetric cryptography uses complex mathematical algorithms like RSA or ECC to generate key pairs for encryption and decryption. These algorithms involve problems that are easy in one direction but computationally difficult in reverse. RSA relies on factoring large numbers, while ECC is based on the discrete logarithm problem on elliptic curves. The security stems from the complexity of these mathematical operations, ensuring robust key exchange and secure data encryption. In context of Quantum-Resistant cryptography, we need to understand that Quantum computers have the capability to perform certain mathematical operations, such as factoring large numbers or solving the discrete logarithm problem, much faster than classical computers. As a result, the security provided by these algorithms may be compromised when facing a powerful quantum computer, rendering them vulnerable to attacks. We will deepen in the next chapter how the industry is planning to address this with post-quantum cryptography (PQC) algorithms.

Lastly, to ensure Quantum-Computer resistant connection, and regardless of the method used, we will strictly recommend the usage of 256 bits secret session key. This is due to the Grover's algorithm, which effectively halves the key size's security level for symmetric encryption (i.e., AES) and hash functions. For example, an AES-256 cipher would effectively be reduced to 128 bits, still considered adequately protected.

Quantum-Safe network tools

Optimizing a Quantum-Safe network necessitates employing various key generation and distribution methods. To facilitate effective communication on this topic, predefined blueprints will be utilized as reference models, guiding the achievement of desired outcomes for enabling a Quantum-Safe network. As mission-critical networks are intricate systems, many of these blueprints will become requirements in real-life implementations. Embracing heterogeneous realities of telecommunication infrastructures and the pursuit of a defense-in-depth Quantum-Safe Networking will demand the incorporation of diverse approaches. This comprehensive approach ensures resilience and robust security, addressing the complexities of safeguarding sensitive data in the quantum era.

Our initial focus will be on Pre-Shared Key (PSK) cryptography-based blueprints. These are deployable today, providing the capability to safeguard sensitive data immediately and address the Harvest Now Decrypt Later paradigm. These blueprints will apply most to the engineered connectivity layers of the OSI model, namely the OTN, MAC and MPLS layers. By prioritizing PSK blueprints, we can fortify our security posture and protect mission-critical information in the quantum era.

Our plan is to address Asymmetric cryptography-based blueprints in a future update to this paper, once Post Quantum Cryptography (PQC) algorithms are standardized. These blueprints will be applicable to dynamic connectivity layers like application, presentation, and session layers in the OSI model. Asymmetric cryptography, applied also with IPsec at the networking layer, will also play a vital role in safeguarding sensitive data for the telecommunication infrastructure's management and control plane in the quantum era.

Thus, we will focus at this stage on the following Pre-Shared Key (PSK) cryptography-based blueprints:

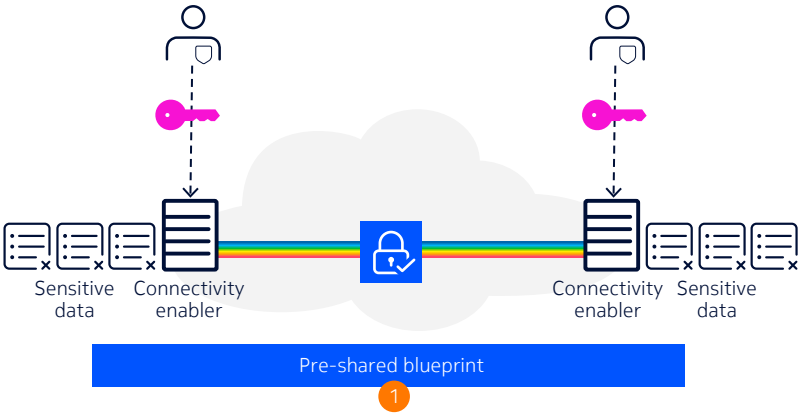
- Manual Pre-Shared Blueprint
- Classical Blueprint
- QKD-Hybrid Blueprints

Manual Pre-Shared Blueprint

Manual, pre-shared keys are the simplest form of Pre-Shared Key (PSK) cryptography-based blueprints. Both sides of a connection are pre-configured with a highly guarded secret key. This connection could be of any type; from a layer 1 optical or microwave link, or a layer 3 IP connection. Best practices determine how the keys are manually handled and delivered to the link ends. While quantum-safe, this method requires resources to maintain and scale. Figure 5 shows a system employing manual, pre-shared keys.

Shown in figure 5, it is one of the oldest and most widely used forms of encryption, and it is used in a variety of applications, including secure communication, data storage, and access control.

Figure 5. Manual Key Distribution Network



Nokia Classic Blueprint

This blueprint makes use of a centralized key management approach, where the Pre-Shared Key (PSK) are computed off board in a single (central) physical location. Centralized key management is preferred and approved by the certification authorities because it provides a single point of trust where the key management system assumes responsibility for the entire life cycle and becomes the “Pre-Shared Key (PSK) authority.”

In this blueprint, the Pre-Shared Key (PSK) and their associated policies, are centrally generated and stored. Keys are distributed to suitably authenticated and authorized applications or endpoints on request.

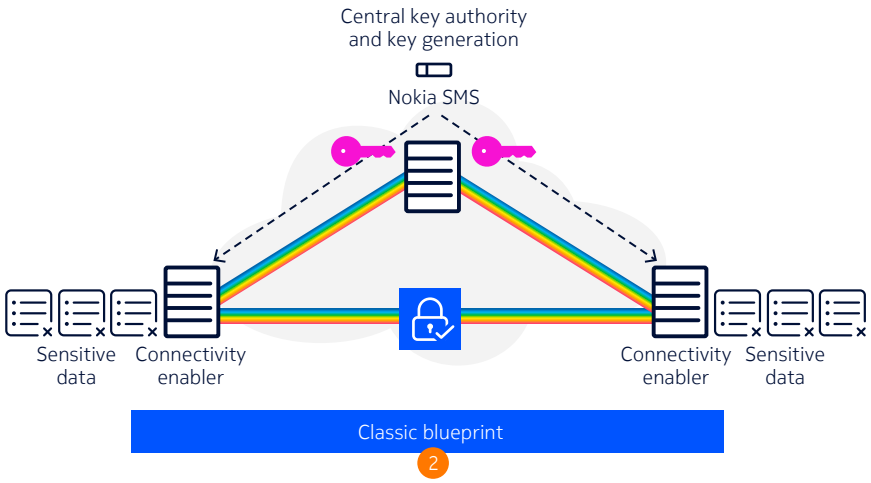
The main advantages of a centralized key management approach are:

- Single point of trust (single point to protect) – Pre-Shared Key (PSK) generation is enabled from a single point of trust, helping the system operator to administer from a single repository instead of from geographically distributed end points.
- Single point Pre-Shared Key (PSK) revocation – The system provides a system-wide, multitenant, single access point to force synchronized key rotation.
- Clear separation of tasks – A clear separation of duties exists in critical applications, ensuring that no single administrator or privileged user can weaken the system security or integrity of keys.
- Unified key management, encryption policies and system-wide key revocation – Agile operation is permitted as part of system key administration.
- Consolidated audit information – A system-wide, single point is provided to extract and consolidate audit logs across different endpoints.

- Low-cost automation – The scripting and automation of the centralized key management process enables us to scale the system and reduce OpEx in managing multiple scripts on multiple nodes.
- Simpler controlled access – Security is improved because key management is done centrally, making it easier to physically secure the key management infrastructure.

Utilizing a trusted, classic physics-based source (i.e., TRNG) as a central key authority improves the ability to scale the network and support many pre-engineering connections among link ends. This architecture utilizes a centralized key server, such as Nokia SMS, connected to each connectivity enabler through its own quantum-safe connection, separately from the data plane. Shown in Figure 6, this is the Classic key distribution network.

Figure 6. Classic Key distribution network



This blueprint is fully productized with the Nokia Optical Networking AES-256 GCM enabled connectivity. In this case, the Pre-Shared Key (PSK) are used as the Secret Session Keys by the AES-256 GCM engines. This blueprint can also be used with our Nokia IP Routing Networking portfolio that supports AES-256 GCM enabled connectivity. In this case, the Pre-Shared Key (PSK) are used as the Key Encryption Key (KEK), used by the routers to ensure Quantum-Safe key wrapping of the Secret Session Keys.

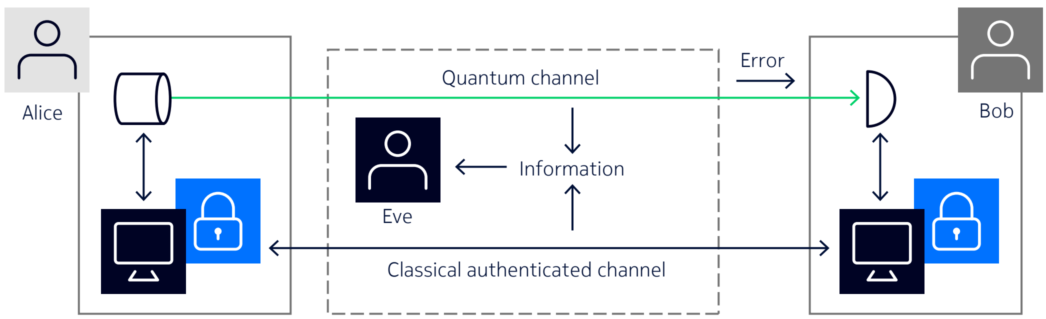
Nokia QKD-Hybrid Blueprints

Similarly, a Pre-Shared Key (PSK) can also come from quantum physics and be distributed through a quantum key distribution network.

Quantum key distribution (QKD) covers all the methods for distributing keys between two distant parties, whose security can be demonstrated by arguments from the theory of quantum mechanics. They offer a long-term quantum-safe alternative to asymmetric cryptography. In a paper published in 1970, J. L. Park demonstrated the impossibility of designing a measurement device, even a theoretical one, which does not disturb the quantum states being measured. In 1982, this same result was independently re-demonstrated in a slightly different context by W. H. Zurek and W. K. Wootters and by D. Dieks. The authors demonstrated the impossibility of creating an identical and independent copy of an arbitrary unknown quantum state. This fundamental result for quantum key distribution is called the no-cloning theorem.

Charles Bennett and Gilles Brassard proposed in 1984 the first key distribution protocol with security based on quantum mechanical theory. The founding idea is based on the non-cloning property of a quantum state. In short, Alice sends Bob polarized photons on a quantum channel. The eavesdropper cannot perfectly clone or divide the photons. She must measure them and generate new ones to send to Bob with the measured polarization. In doing so, she introduces errors in the protocol, that betray her presence. The protocol assumes that Alice and Bob also have access to an authenticated classical channel, to monitor the protocol and identify if the channel is being eavesdropped on.

Figure 7: QKD principle



As already mentioned, one of the possible physical quantities to implement the BB84 protocol is the polarization of photons. Alice transmits random bits to Bob by encoding them on an orthonormal basis. For example, a horizontal polarization, noted |↔ >, encodes a 0, and a vertical polarization, noted | ↕ >, a 1. Alice has at her disposal a second basis inclined by a 45° angle: a polarization of 45° to the left, noted | ↕ >, encodes a 0, and a polarization of 45° to the right, noted | ↕, > encodes a 1. For each bit to be transmitted, Alice randomly chooses the encoding basis and the bit with uniform probability. Bob is not informed of her choice.

For his measurement, he chooses arbitrarily one of the two bases. If his choice does not coincide with Alice's, the polarization he measures is random, and the information is unusable. Using the authenticated channel, Alice and Bob communicate to each other their basis choices and dismiss the bits measured with incompatible bases. This step of the protocol is called sifting. What if Eve tries to eavesdrop on the channel? Since she cannot clone or divide a photon, any action will introduce errors. For instance, she can measure the polarization, and then generate a new photon to send to Bob corresponding to her measurement. This basic attack is called intercept-and-resend. Like Bob, she must decide on the basis to use, with probability 1/2 of making a mistake. This induces a 1/4 error probability in the bit read by Bob. Thus, if Alice and Bob reveal a fraction of their bits on the authenticated channel to estimate the bit error rate, they can estimate the quantity of information leaked to Eve. In fact, Eve can make subtle attacks consisting of imperfect cloning of the photons. In this case, she still introduces an error rate of 11%.

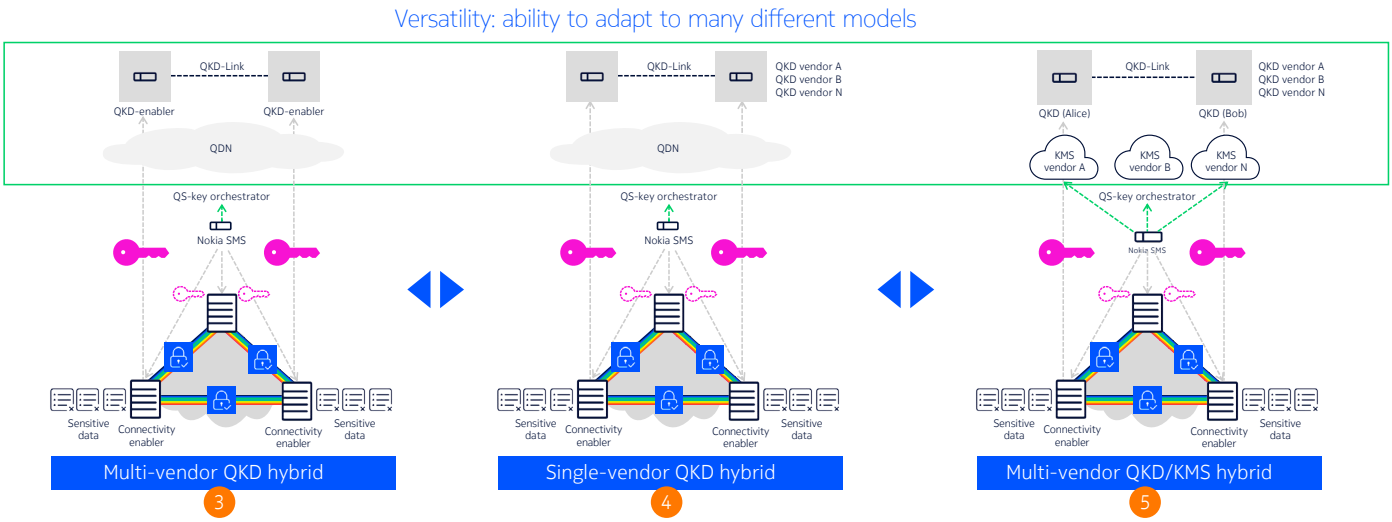
Most available QKD protocols use quantum states taken in a finite-dimensional Hilbert space. For example, the states in the BB84 protocol are qubits in a two-dimensional Hilbert space. This context allows for simple security analysis but typically requires complex practical implementation. Such protocols are referred to as discrete variable (DV-QKD). Another way to proceed is to consider a Hilbert space of infinite dimension, in which the observables have continuous eigen-spectra. Typical example of such observables are the quadratures in the phasor diagram of the electromagnetic field of a light beam. Such protocols are called continuous variable (CV-QKD). Their theoretical analysis is more difficult than that of DV-QKD.

However, their practical implementation is simplified by their proximity to classical communications. Indeed, the most efficient systems in optical communication use phase and amplitude modulation of coherent light beams. It is therefore possible to benefit from the state-of-the-art equipment available and from modern digital processing techniques.

The first CV-QKD protocol proposals involved squeezed-states, with discrete modulation in phase space, and then Gaussian modulation. F. Grosshans and P. Grangier proposed in 2002 a protocol, called GG02, that used coherent states with Gaussian modulation. The use of coherent states allowed us to avoid the practical difficulty of technological generation of squeezed states, allowing a fast experimental validation. In the GG02 QKD protocol, Alice generates coherent states |α>, |α2>, . . . with α1, α2, . . . chosen independently at random from a complex circular Gaussian distribution. The quantity of interest to detect the presence of Eve, like the bit error rate in BB84, is the covariance matrix between Alice's and Bob's data. The quadratures of a coherent state present a fundamental noise called shot noise, or vacuum noise. The presence of Eve is typically betrayed by the presence of an additional noise, called excess noise.

Thus, to develop and deploy keys based upon quantum physics, we propose Blueprints 3, 4 and 5, as shown in figure 8.

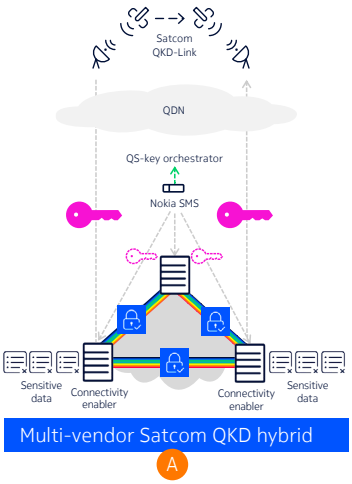
Figure 8. QKD blueprints



These expand upon blueprint 2, adding quantum key sources and QKD links to allow for use of quantum keys in a hybrid fashion alongside the classic keys of blueprint 2. These hybrid classic-quantum key blueprints provide a very robust solution where quantum keys are orchestrated and backed-up by a central authority such as Nokia SMS. In Blueprint 3, multiple QKD vendors are orchestrated through a single platform such as Nokia SMS. In Blueprint 4, specific QKD vendors are optimized to the key orchestrator using their unique KMS. In Blueprint 5, multiple QKD vendors and their respective KMS interoperate with the central key orchestrator. These are subtle but crucial differences that offer interoperability among the QKD solutions available to network operators. These QKD blueprints are shown in figure 10.

Finally, we consider Blueprint A, shown in figure 9. This is a special case, where satellite communications links are used to overcome inherent limitations to using optical fiber for quantum key teleporting. As with the hybrid QKD blueprints, blueprint A utilizes a central trusted orchestrator to manage and back-up quantum keys with classical keys. This blueprint allows for global key distribution, limited only to local weather conditions, and ground station construction practicalities in reaching link endpoints.

Figure 9. Space-based quantum-key generation and distribution



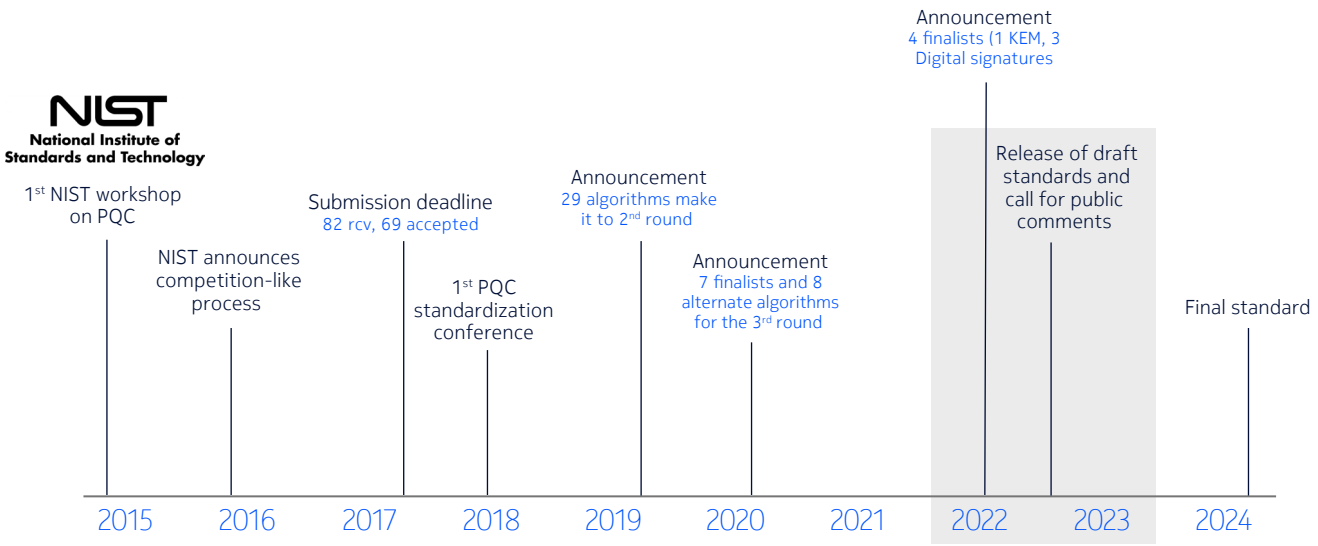
Asymmetric cryptography-based blueprints

As mentioned above, our plan is to address Asymmetric cryptography-based blueprints in a future paper, once Post Quantum Cryptography (PQC) algorithms are standardized. These blueprints will be applicable to dynamic connectivity layers like application, presentation, and session layers in the OSI model. Asymmetric cryptography, applied also with IPsec at the networking layer, will also play a vital role in safeguarding sensitive data for the telecommunication infrastructure's management and control plane in the quantum era. That said, we believed constructive to touch the basic of Post Quantum Cryptography (PQC) to ensure completeness.

Post-quantum cryptography (PQC) is a family of asymmetric cryptographic algorithms which are conjectured to be quantum-resistant, i.e., they are based on mathematical problems that are intractable even for a large-enough quantum computer. These algorithms will eventually replace the algorithms that underpin today's public-key infrastructure, namely RSA, Diffie-Hellman, ECC and the accompanying public-key encryption, key-exchange, and digital signature schemes.

PQC is best for any to any connections that connect two strangers together, for example, making purchases over the Internet using a browser interface, and is on-track to be the foundation for telecommunication network management and control. The browser knows the list of trusted certificate authorities and warns you if you are accessing an untrusted web site. However, there could be imperfections in the quality of certificate authorities as registrations tend to go to the lowest bidder, so users need to understand the trust of the PKI system they are using. At this point, there are no standardized PQC as trusted as a responsibly managed pre-shared key.

Figure 10: PQC timeline



The National Institute of Standards and Technology (NIST) is actively working to standardize PQC algorithms. NIST began a competition-like process in 2016 and after three evaluation rounds four cryptographic primitives for Key Encapsulation Mechanisms (KEM) and Digital Signatures were selected for standardization (see Figure 1 and Table 1); shortly after this announcement on July 5th, 2022, researchers broke SIKE, one of the candidates for the 4th round (Castryck & Decru). Note that, Table 1 does not contain the stateful, hash-based signature schemes XMSS and LMS, which are also Quantum-Resistant and have already been standardized by NIST.

(David Cooper (NIST), Daniel Apon (NIST), Quynh Dang (NIST), Michael Davidson (NIST), Morris Dworkin (NIST), Carl Miller (NIST), 2020); the reason is that NIST did not consider stateful algorithms for this call. A first draft of the standards is expected in 2022-2023 and the final standard is anticipated by 2024. Each of these algorithms presents certain trade-offs, and NIST is currently evaluating the different options to compare security, performance, resistance to side-channel attacks, simplicity and flexibility, etc. (Consortium, 2021).

Table 1. NIST finalists after the 3rd evaluation round

Specification	To be standardized	Alternatives (4th round)
KEM/Encryption	CRYSTALS-KYBER	BIKE Classic McEliece HQC SIKE*
Signatures	CRYSTALS-Dilithrium FALCON SPHINCS+	

*Considered broken according to (Castruyck & Decru)

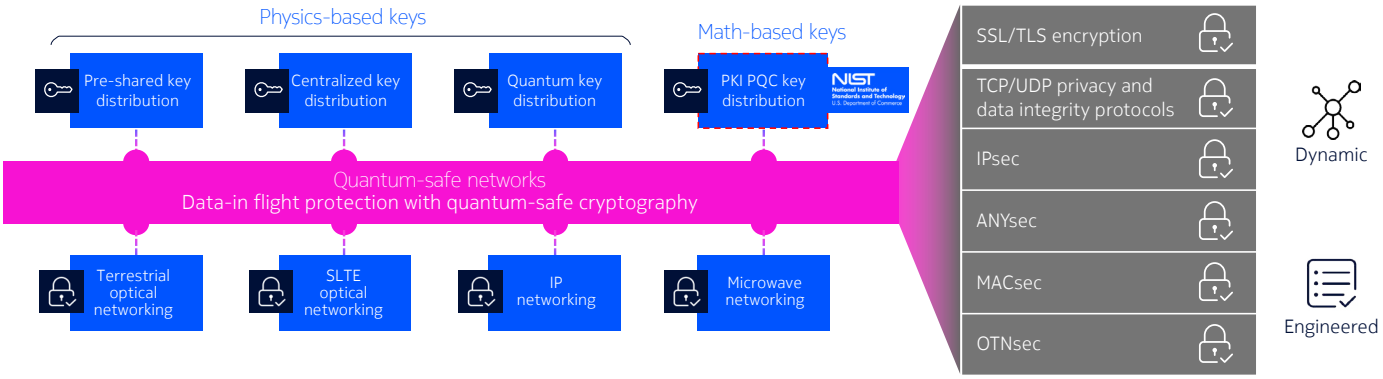
The latter notion of flexibility pertains to an important concept which is extremely relevant to the migration process towards PQC, that is “cryptographic agility”. Cryptographic agility refers to the capacity of a system to accommodate, exclude or update new and obsolete algorithms, without severe impact to the existing infrastructure.

Summary

This paper has outlined the existing and expanding threat posed by development of CRQC's. Network operators of all types should take note of this trend and consider actions to protect their data and related operations.

Building quantum-safe networks can be done today though readily available tools including manual, pre-shared keys, classic physics-based keys of sufficient length, distributed through a symmetric key distribution system and through use of quantum physics-based key distributed through a hybrid distribution system. In the future the solution tools are likely to include mathematical-based keys, designed specifically to be safe from quantum computer attack while also being well suited for use in ephemeral, dynamic connectivity applications. Together, these tools for a quantum-safe ecosystem, as shown in figure 11, which we expect to continue to evolve as the quantum threat becomes clearer.

Figure 11. Summary: Quantum-safe networks ecosystem applied



Nokia is the industry leader in quantum-safe network solutions and can help you determine the best solutions that match your unique protection needs.

Learn more at www.nokia.com

Abbreviations

AES	Advanced encryption standard
CRQC	Cryptographically relevant quantum computer
CRNG	Classic random number generator
CSP	Communications Service Provider
CV-QKD	Continuous Variable Quantum key distribution
DCN	Data Communications Network
DV-QKD	Discrete Variable Quantum Key Distribution
ECC	Elliptic curve cryptography
GCM	Galois counter mode

HNDL	Harvest now decrypt later
ISP	Internet Service Provider
KEK	Key encryption key
KMS	Key management system
NIST	National Institute of Standards and Technology (US)
NSA	National Security Agency (US)
OAM	Operations and Management
OTN	Optical transport networking
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
PRNG	Pseudo random number generator
PSK	Pre-Shared Keys
QDN	Quantum distribution network
QKD	Quantum key distribution
QKDN	Quantum key distribution network
QRNG	Quantum random number generator
RSA	Rivest-Shamir-Adleman
TRNG	True random number generator

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

Document code: (August) CID213258