WHITEPAPER

Security in the quantum era

Evaluating post-quantum solutions

NOKIA

Introduction

The computing power of a quantum computer renders obsolete the state-of-the-art, public-key cryptography deployed today. All the assumptions about the intractability of the mathematical problems that offer confident levels of security today no longer apply in the presence of a quantum computer.

Fortunately, research has produced several post-quantum cryptographic algorithms that will enable cryptography to survive in the quantum world. However, the transition to a post-quantum infrastructure is not straightforward and requires focused effort.

We are in the phase of engineering, pro-active assessment and evaluation of the available technologies, as well as careful product development approach, which helps pave a safe path through what otherwise could turn out to be cryptography's demise.

Nokia, including our industrial research lab Nokia Bell Labs, will stay at the forefront of these exciting advances. We evaluate the available post-quantum solutions, enhance our crypto-agility, and prepare for a smooth transition to a quantum-safe security infrastructure.

Evolving algorithm landscape

Quantum computing is no longer perceived as a conjecture of computational sciences and theoretical physics. There are considerable research efforts and enormous corporate and government funding invested in the development of practical quantum computing systems.

Examples of accelerated efforts towards large-scale quantum computers include, among others, Google's announcementon achieving quantum supremacy [1] and IBM's latest 433-qubit processor [2] and Nokia Bell Labs' topological qubit providing a promising solution for scalable quantum computers [3].

The existence of a quantum computer would mark a cornerstone in the humankind's technological evolution. In fact, it would mean that the computational problems that are considered intractable for the conventional computers of today would become tractable with quantum computing.

Professor Peter Shor and computer scientist Lov Grover, while at Bell Labs, developed two algorithms that were first seen to have significant impact on the way we think of security under the presence of a quantum computer.

Taking a closer look at "Grover's algorithm", it impacts the security of symmetric cryptographic algorithms in such a way that, theoretically, we would need to double the key sizes we use today to remain quantum-safe.

This is especially true for 128-bit algorithms, which means that AES-128-bit encryption would need to be replaced by AES-256-bit encryption. However, as we will explain in the next section, this is to some extent a misconception.

On the other hand, “Shor’s algorithm” efficiently solves the integer factorization problem and also the equivalent discrete logarithm problem, which offer the foundations of the public-key cryptography we use today.

This implies that many of today’s public-key cryptography algorithms including Rivest–Shamir–Adleman (RSA), Diffie-Hellman and Elliptic Curve Cryptography (ECC) as well as the accompanying digital signatures schemes and protocols would need to be replaced by algorithms and protocols that can offer cryptanalytic resistance against quantum computers.

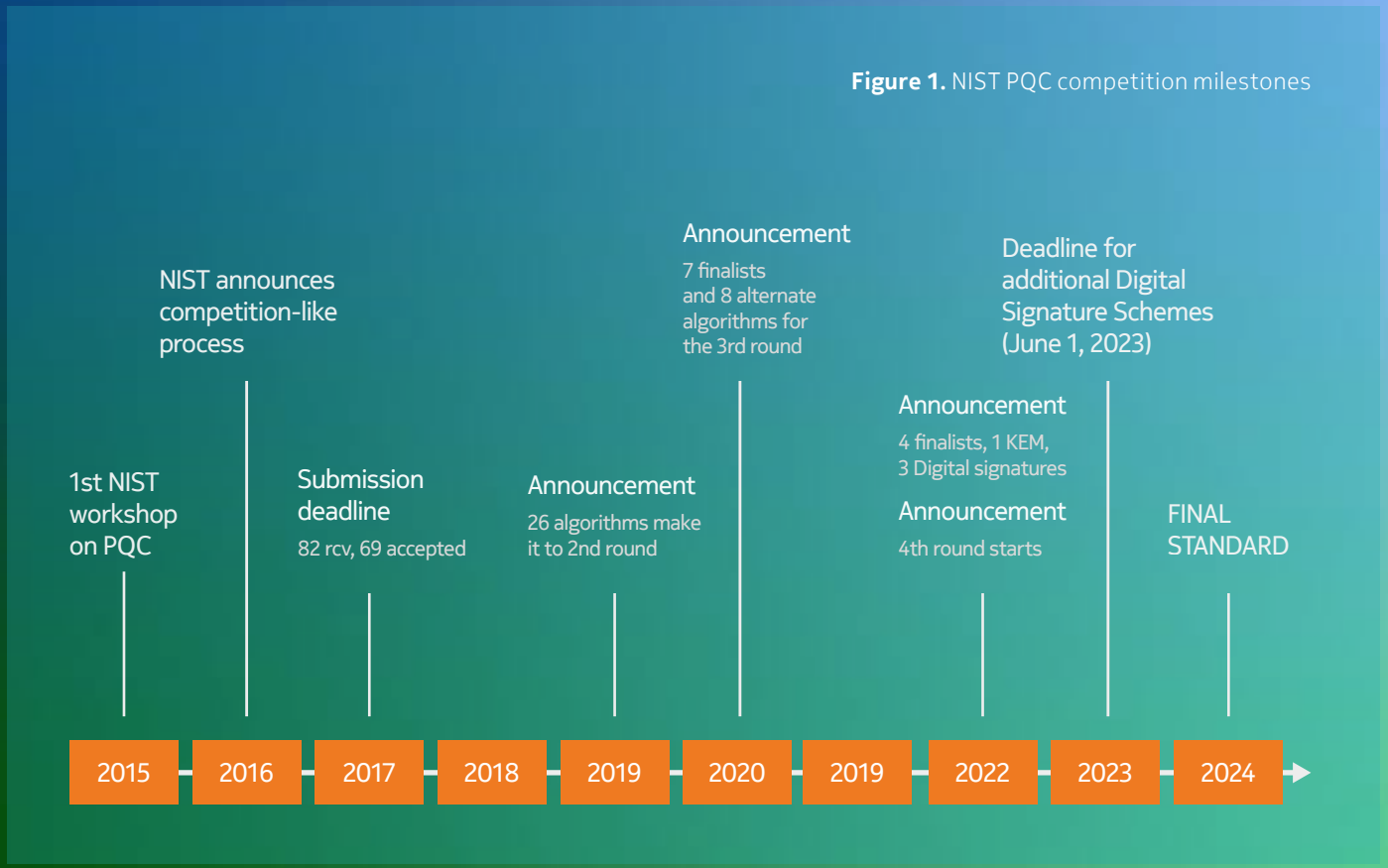
Much to everyone’s relief, modern cryptography does offer the tools to design such quantum-safe cryptosystems. In this whitepaper, we will review these solutions very briefly with emphasis on the challenging task of migrating towards a quantum-safe infrastructure. In the same framework, we highlight the crucial notion of crypto-agility and how Nokia exhibits due diligence and thought leadership by preparing timely for the transition to quantum-safe architectures.

Cryptography in the post-quantum era

Post-quantum cryptography (PQC) refers to a family of asymmetric cryptographic algorithms, which are conjectured to be quantum-resistant. In other words, they are based on mathematical problems that appear to be intractable even for a large-scale quantum computer. These algorithms will eventually replace the algorithms that underpin today's public-key infrastructure, such as the earlier-mentioned RSA, Diffie-Hellman and ECC, as well as the accompanying public-key encryption, key-exchange, and digital signature schemes.

The National Institute of Standards and Technology (NIST) is actively working to standardize PQC algorithms. Figure 1 illustrates the competition-like process that NIST initiated in 2016 to select new algorithms for standardization.

Figure 1. NIST PQC competition milestones



After three evaluation rounds, NIST selected for standardization four cryptographic primitives for Key Encapsulation

Mechanisms (KEM) and Digital Signatures, presented in Table 1. Note that the table does not include the Extended Merkle Signature Scheme (XMSS) and the Leighton-Micali Signature Scheme (LMS), which are stateful, hash-based, quantum- safe signature schemes and have already been standardized by NIST [4]. The reason is that NIST did not consider stateful algorithms for this competition.

Shortly after this announcement on July 5th 2022, researchers broke the Super-singular Isogeny Key Encapsulation (SIKE) algorithm [5], one of the candidates for the 4th round.

A first draft of the NIST standard is expected in 2023 and the final standard is anticipated by 2024. Apparently, each of these algorithms presents certain trade-offs, and NIST is currently evaluating the different options to compare the many aspects including security, performance, resistance to side-channel attacks, simplicity and flexibility [6].

The latter notion of flexibility pertains to a very important concept of cryptographic agility, which is extremely relevant to the migration process towards post-quantum cryptography. 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.

“

Nokia considers the task of evaluating our cryptographic agility a key step in understanding the implications of post-quantum cryptography on our products and the effort required to offer post-quantum cryptography solutions.

Table 1. NIST PQC 3rd round finalists and 4th round candidates

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

*Considered broken according to Castryck and Decru [4]

Symmetric cryptography

We mentioned earlier the assumption that Grover's algorithm theoretically requires us to double the key sizes of the algorithms we deploy today to achieve quantum resistance. This is because Grover's algorithm reduces the number of operations to break 128-bit symmetric cryptography to 2^64 quantum operations, which might sound computationally feasible. However, the following considerations illustrate that this is not the case:

- Whereas 2^64 operations performed in parallel are feasible for modern classical computers, 2^64 quantum operations performed serially in a quantum computer are not feasible.

- Grover's algorithm is highly non-parallelisable. Even if we deploy 2c computational units in parallel to brute-force a key using Grover's algorithm, it will complete in time proportional to 2^(128-c)/2, or put simply, running even hundreds of quantum computers in parallel would offer negligible advantage gains to attack the key [7], [8].

How can we then be sure that an improved algorithm won't outperform Grover's algorithm in the near future? Firstly, Christof Zalka has shown that Grover's algorithm, and in particular its non-parallel nature, achieves the best possible complexity for an unstructured search [9].

Secondly, in their evaluation criteria for PQC, NIST is considering a security level equivalent to that of AES-128. In other words, NIST has confidence in standardizing parameters for PQC that offer similar levels of security as AES-128 does [6]. As a result, 128-bit algorithms should be considered quantum-safe for the years to come. On a final note, we witness some interesting attacking advancements leveraging concepts from Quantum Signal Processing and we encourage the research and industry communities to stay alert for developments in this area [10].

The introduction of post-quantum cryptography is a complex and large-scale process. Next, we focus on the challenges it represents.

Challenges of post-quantum cryptography

There are several technical reasons that make it necessary to evaluate post-quantum cryptography options already today. On the implementation side, it is anticipated that, for many applications, PQC will be offered as a software-based solution. Current implementations indicate that PQC is well supported by the existing network infrastructure and hardware, however, further testing and benchmarking is required to fully understand their behaviour in different computational environments [11].

Industrial control systems represent a case with unique challenges. These systems adhere to very high standards of resiliency and safety, which means that they need to be upgraded without impacting the underlying industrial processes. Furthermore, as the recent cases of the NIST signature scheme candidates RAINBOW and SIKE have emphatically showcased [5] [12], PQC algorithms are no exception to cryptanalysis and so it is always possible that new vulnerabilities are discovered. As a result, mechanisms need to be in place to allow for a failover to safer PQC options.

Finally, although the incorporation of PQC algorithms in protocols such as Transport Layer Security (TLS), IPsec or Virtual Private Network (VPN) might not be technically very complicated, there is still a lot of work to be done and implementers should take into account the specific needs of their applications in order to choose an appropriate PQC scheme safely. In the upcoming years, more and more standards, libraries, and protocols will add support for PQC. Until then, we can leverage the existing libraries and start experimenting with post-quantum as well as hybrid versions of protocols such as TLS to better understand the characteristics and performance of these new algorithms [13].

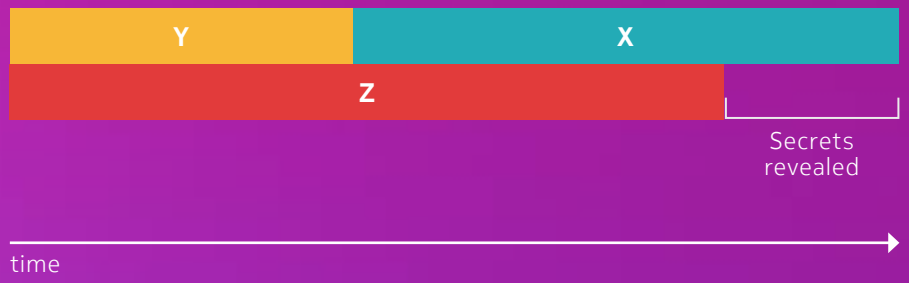
Shaping the future of cryptography

Apart from the technical difficulties outlined in the previous paragraph, there are several other reasons we need to stay vigilant and start evaluating PQC technologies already today.

First, we acknowledge the problem of “harvest-now-decrypt-later”, which means that malicious actors with adequate resources may be storing sensitive encrypted data today with the aim to decrypt the data once a quantum computer is available. This implies that every day we lose today by not implementing quantum-safe strategies can correspond to data being exposed in the future.

Moreover, cryptography is the type of technology that historically matures slowly. NIST acknowledges that it has taken almost 20 years to deploy a public-key infrastructure that we can trust. With regards to post-quantum cryptography, NIST expects a timeframe of 5-15 years after the release of the standards [14] while other analysts and academics give a more conservative estimate of 10-20 years [15].

Figure 2. The Mosca model for evaluating PQC migration timeframe



These challenges are illustrated nicely by the so called Mosca model in Figure 2 [16]. 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 remains vulnerable for the complete **x** years of their lifetime, thus the sum **x + y** gives us an estimate of the full timeframe that data remain insecure [15].

The model essentially asks the question of how we are preparing our IT systems during those **y** years, or on the other hand, how can we minimize those **y** years, so as to minimize the duration of the transition phase to a PQC infrastructure and hence minimize the risks of data being exposed in the future.

Additionally, we should not underestimate other factors that could accelerate the introduction of a large-enough quantum computer, such as faster-than-expected advances in quantum computing and more efficient versions of Shor's algorithm requiring less qubits. For 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 that will support more than 1000 qubits by 2025 and networked systems with 10k-100k qubits beyond 2026 [17].

Innovation often comes in waves, so it is to the industry's benefit to remain vigilant and prepare as early as possible.

Finally, there are other threat landscapes that do not pertain to quantum computing per se but can be utilized to attack legacy and post-quantum crypto, namely Artificial Intelligence (AI) and Machine Learning (ML).

Although it is still very early to judge their merits, some recent attacks employing the concept of "transformers" (used extensively in ML and AI models like GPT) clearly highlight that we cannot wait until the next breakthrough to take actions for our post-quantum migration journey [18].

Nokia takes a proactive approach to post-quantum security

We at Nokia believe that even though quantum computers are still in an experimental status, their security implications need to be addressed already today. We are getting prepared for the post-quantum era with proactive strategies.

The role of Nokia Bell Labs is to enable technology and knowledge transfer as well as foster collaboration to identify key areas that should be addressed during the initial steps for the introduction of quantum-safe solutions. Moreover, Nokia Bell Labs is partnering with leading universities to extend its in-house research and enable smooth integration and evaluation of PQC solutions in its 5G ecosystem. It is also looking into the specific challenges posed by key 6G drivers, such as environmental considerations and power consumption of the cryptosystems under evaluation.

Nokia also acknowledges the risks of the "harvest-now-decrypt later" threat. We understand that most of the encrypted data we transfer today for managing and controlling the network has only a short-term relevance, however, we have identified types of related data that might be prone to this threat.

Nokia has deployed a 5G system testbed in the NIST 5G Cybersecurity Lab at the National Cybersecurity Center of Excellence (NCCoE). In this testbed, Nokia plans to experiment with open-source implementations of PQC algorithms and protocols [19]. Additionally, we plan to evaluate these candidates while aiming to protect TLS, DTLS and IPsec traffic from quantum cryptanalysis so that all sensitive data can be protected. Several other proof-of-concept projects are also under planning to gain expertise for commercial support.

Looking forward, Nokia plans to add quantum-safe encryption support to the mid and long-term feature planning of our products and according to business needs. Nokia also expects to contribute to the standardization work and initiate feature life-cycle management for products with relevant business cases targeting commercial releases.

Impact analysis

At Nokia, we conduct continuous analysis of the impact that post-quantum cryptography will have on our products. We expect that these will be the key impact areas:

Hardware impact:
Several of our products leverage dedicated or embedded Trusted Platform Modules and hardware acceleration for current cryptographic algorithms, which might also be leveraged for NIST standardized PQC algorithms. We will of course take into account the impact of hardware-embedded security functions.

The availability of PQC algorithms on hardware level will be standardized in line with the state-of-the-art practices at the time.

We will align our implementation plans together with our vendor ecosystem. We will also plan the required adaptations of other parts of a system, including firmware/UEFI signatures for secure and measured boot sequences, key storage, and others.

Certificates:
Several of our products support X.509 certificates for many use cases according to today's best practice digital signature and key exchange algorithms. Nokia will support all necessary adjustments to certificates that PQC will require.

Crypto Software:
In due time, Nokia will replace all instances of current open-source crypto software with PQC-enabled open source software, thus offering leading security levels and product support globally.

Nokia will continue accelerating post-quantum cryptography evaluation and product preparedness to accommodate the new PQC algorithms

Conclusion

A quantum-world is definitely not as intimidating as one might expect from a security standpoint. We now have several PQC schemes we can test, cryptography experts around the world are working on the best possible solutions, and the first standards that will ease the introduction of post-quantum cryptography are being prepared.

It is of paramount importance to prepare for the era of quantum computing. We encourage all types of organizations and enterprises to start evaluating their cryptographic agility today, to assess the complexity of implementing PQC into their products, processes, and systems, as well as to develop a migration plan that achieves their security goals to the highest extent.

Nokia acknowledges the need for imminent action. We take all necessary steps to proactively prepare our product portfolio for the introduction of PQC, thus offering the best of breed security solutions to our customers.

Abbreviations

AI	Artificial Intelligence
CA	Certificate Authority
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
KEM	Key Encapsulation Mechanism
LMS	Leighton-Micali Signature Scheme
ML	Machine Learning
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PKI	Public-Key Infrastructure
PQC	Post-Quantum Cryptography
RSA	Rivest–Shamir–Adleman
SIKE	Supersingular Isogeny Key Encapsulation
TLS	Transport Layer Security
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
VPN	Virtual Private Network
XMSS	Extended Merkle Signature Scheme

References

[1] F. Arute, A. Kunal, B. Ryan, D. Bacon, J. C. Bardin, R. Barends, R. Biswas and S. Boixo, “Quantum supremacy using a programmable superconducting processor,” Nature, pp. 505-510, 2019.

[2] H. Collins and C. Nay, “IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two,” IBM, 9 November 2022. [Online]. Available: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

[3] R. L. Willett, K. Shtengel, C. Nayak, L. N. Pfeiffer, Y. J. Chung, M. L. Peabody, “Interference Measurements of Non-Abelian e=4 & Abelian e=2 Quasiparticle Braiding,” March 2023. [Online]. Available: https://journals.aps.org/prx/pdf/10.1103/PhysRevX.13.011028.

[4] David Cooper (NIST), Daniel Apon (NIST), Quynh Dang (NIST), Michael Davidson (NIST), Morris Dworkin (NIST), Carl Miller (NIST), “Recommendation for Stateful Hash-Based Signature Schemes,” NIST, 2020.

[5] W. Castryck and T. Decru, “An Efficient Key Recovery Attack on SIDH,” [Online]. Available: https://eprint.iacr.org/2022/975.pdf. [Accessed 24 08 2022].

[6] Q. E. D. Consortium, “A Guide to a Quantum-safe organization,” QED-C, 2021.

[7] “Post-Quantum Cryptography,” NIST, [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria).

[8] Bas Westerbaan, “NIST’s pleasant post-quantum surprise,” Cloudfare, 7 July 2022. [Online]. Available: https://blog.cloudflare.com/nist-post-quantum-surprise/. [Accessed 7 11 2022].

[9] C. Zalka, “Grover’s quantum searching algorithm is optimal,” Physical Review A, vol. 60, pp. 2746-2751, 1999.

[10] J. G. a. B. W. Y. Zheng, “New Quantum Search Model on Symmetric Ciphers and Its Applications.,” https://eprint.iacr.org/2023/327, Online, 2023.

References

[11] W. Barker, W. Polk and M. Souppaya, “Getting Ready for Post Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms,” 28 April 2021. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932330. [Accessed 9 May 2022].

[12] W. Beullens, “Breaking Rainbow Takes a Weekend on a Laptop,” Cryptology ePrint Archive, vol. 214, 2022.

[13] D. Stebila, “Post-quantum key exchange for the Internet and the Open Quantum Safe project,” Selected Areas in Cryptography (SAC), vol. 10532, pp. 1-24, 2017.

[14] W. Barker and M. Souppaya, “Migration to Post-Quantum Cryptography,” 2021. [Online]. Available: https://csrc.nist.gov/publications/detail/white-paper/2021/08/04/migration-to-post-quantum-cryptography/final.

[15] M. P. M. Mosca, “Quantum Threat Timeline Report 2020,” Global Risk Institute, 2020. [Online]. Available: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/.

[16] M. Mosca, “(2015) Cybersecurity in a quantum world: will we be ready? Invited talk at NIST workshop on Cyber Security in a Post-Quantum World (Gaithersburg, MD, 2015), National Institute of Standards and Technology (NIST),” 2015. [Online]. Available: https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf.

[17] IBM, “Our new 2022 Development Roadmap,” IBM, [Online]. Available: https://www.ibm.com/quantum/roadmap. [Accessed 24 08 2022].

[18] C. L. e. al., “SALSA PICANTE: a machine learning attack on LWE with binary secrets.,” https://eprint.iacr.org/2023/340, Online, 2023.

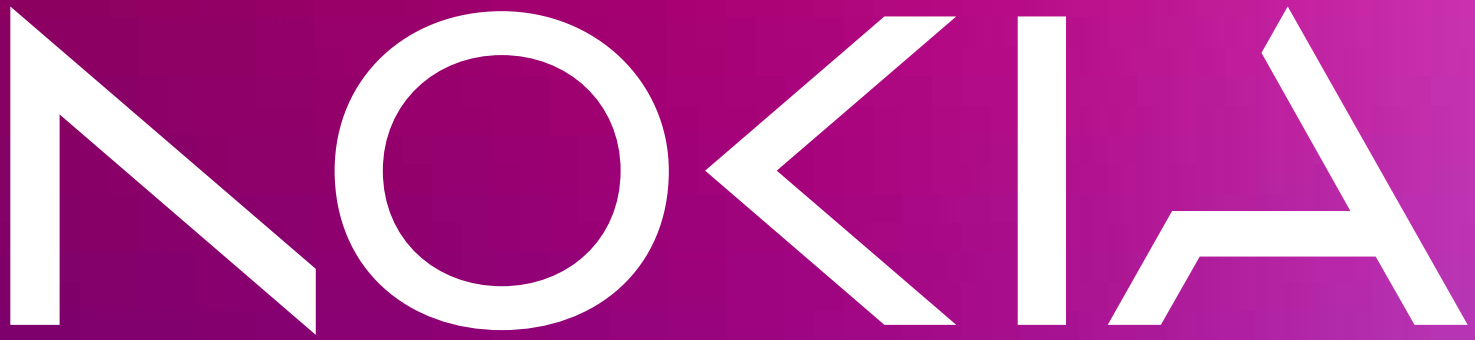
[19] “5G Cybersecurity,” National Cybersecurity Center of Excellence, [Online]. Available: https://www.nccoe.nist.gov/5g-cybersecurity.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 213086

nokia.com



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

As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry.

Through networks that sense, think and act, we work with our customers and partners to create the digital services and applications of the future.