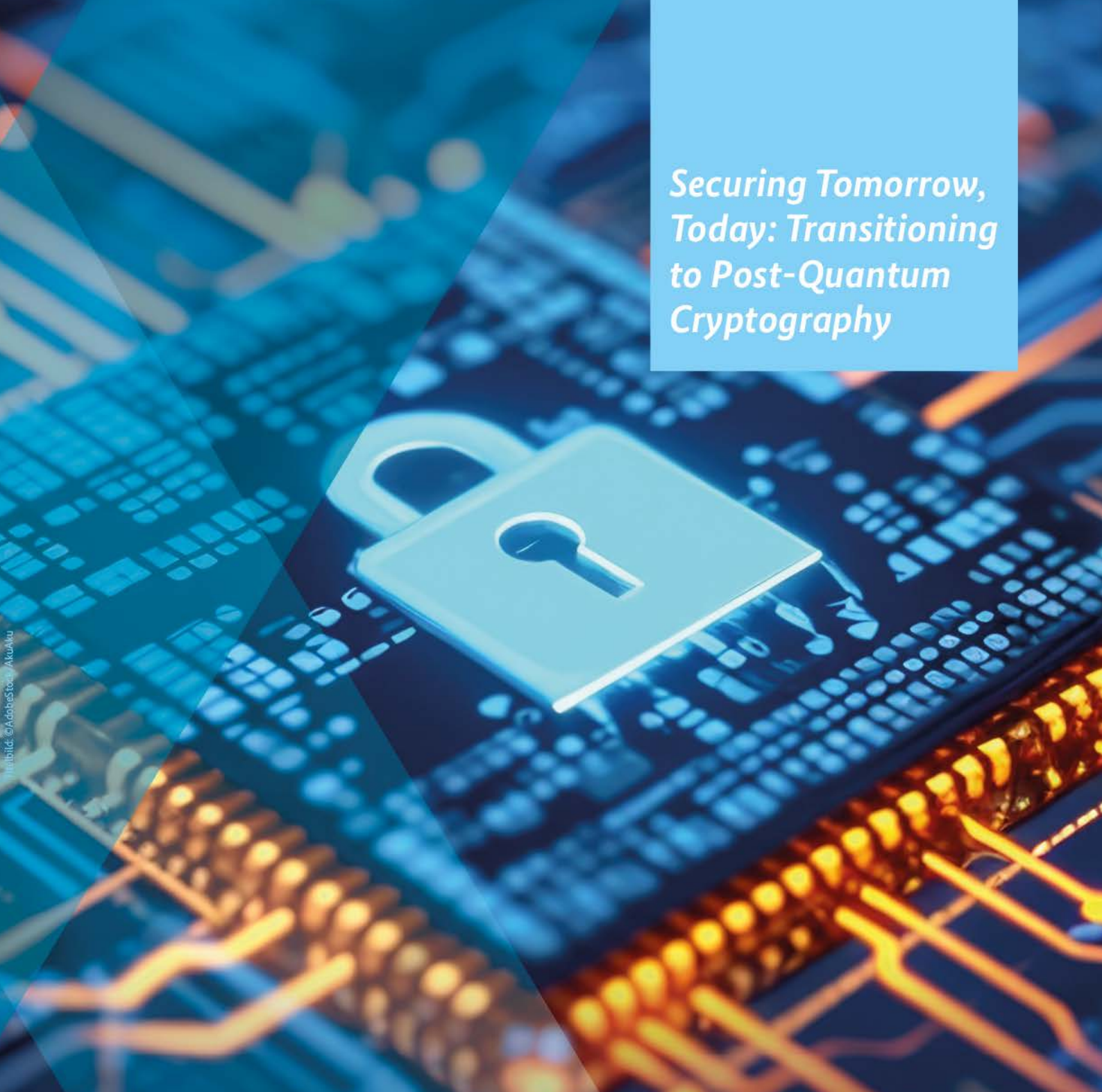
Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography



Titelbild: ©AdobeStock/AkuAku

A joint statement from partners from 18 EU member states:

Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish transport and Communication Agency, French National Agency for the Security of Information Systems, Federal Office for Information Security Germany, National Cyber Security Authority Hellenic Republic, National Cyber Security Centre Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, National Cyber Security Centre Ministry of Defense Lithuania, High Commission for National Protection Luxemburg, Netherlands National Communication Security Agency, Ministry of Interior and Kingdom Relations Netherlands, National Cyber Security Centre Ministry of Security and Justice Netherlands, Research and Academic Research Center Poland, Government Information Security Office Slovenia, National Cryptologic Center Spain

Bundesamt für Sicherheit in der Informationstechnik

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

A-SIT
Secure Information Technology Center - Austria
Zentrum für sichere Informationstechnologie - Austria

CENTRE FOR CYBERSECURITY BELGIUM

National Cyber and Information Security Agency

CENTRE FOR CYBER SECURITY

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

TRAFICOM
Finnish Transport and Communications Agency

National Cyber Security Authority
HELLENIC REPUBLIC

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

Ministry of Defence
Republic of Latvia

NATIONAL CYBER SECURITY CENTRE

MINISTRY OF NATIONAL DEFENCE
REPUBLIC OF LITHUANIA

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

National Cyber Security Centre
Ministry of Security and Justice

NASK

REPUBLIC OF SLOVENIA
GOVERNMENT INFORMATION SECURITY OFFICE
URSIV

CCN
centro criptológico nacional

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography

Public-key cryptography is crucial to securing a broad range of services having a direct impact on our daily lives. Those encompass, for instance, transferring money from a bank account, signing a digital contract, controlling smart home devices, or communication services such as messaging apps. If the currently deployed public-key schemes were to be broken, the consequences on our public digital infrastructure would be devastating. This threat to cryptography is posed by the development of a large-scale fault-tolerant quantum computer, which can break traditional public-key cryptographic schemes, based for example on RSA or elliptic curve cryptography (ECC), due to Shor's algorithm. While there are currently no such cryptographically relevant quantum computers (CRQC) available, their development is progressing rapidly [1].

Therefore, **preparing for the quantum threat should be considered an integral aspect of cyber security risk management**. In an attempt to quantify the risk, the 2023 issue of the Quantum Threat Timeline [2] conducted a survey among 37 international leading experts from academia and industry. Out of these, 17 estimated the risk that a CRQC appears within a 10-year timeframe higher than 5%. Moreover, 10 of these respondents even indicated a likelihood of about 50% or more.

Several well-studied post-quantum cryptography (PQC) alternatives to currently deployed vulnerable cryptography are either already standardized or ready to be standardized[1], and ready for use in production. For further in-depth recommendations and details, we refer to [3,4,5,6,7,8]. However, since they are relatively new and there is still developing experience with their implementation and cryptanalysis, we currently strongly recommend to **deploy PQC in hybrid solutions** for most use-cases, i.e. combining a deployed cryptographic scheme with PQC in such a way that the combination remains secure even if one of its components is broken.

Two main threat scenarios are currently of concern:

- **the 'store-now, decrypt-later' scenario**, where adversaries store encrypted data for decryption once a CRQC emerges. This is a threat when the confidentiality of data needs to be protected for a long time period (for instance sensitive personal data or commercial secrets);
- **long migration periods**, which occur for complex systems such as public key infrastructures (PKI) or devices with a long lifetime. Even if a system is not affected by ongoing attacks, as in the first scenario, the risk arises that the transition to quantum secure cryptography might not be completed in time, endangering the confidentiality and authenticity of all communication.

We urge public administration, critical infrastructure providers, IT providers, as well as all of industry, to **make the transition to post-quantum cryptography a top priority.** For the reasons outlined above, organizations and governments should **start the transition now** by working on the following steps (we refer to [5] and [6] for more details):

[1] Special-purpose PQC signature algorithm standards have been available for a while, allowing for post-quantum firmware and software updates. Moreover, new standards for post-quantum key establishment and signature algorithms have been published by NIST on August 13, 2024. Additional PQC standards from NIST and other SDOs, in particular ISO, as well as RFCs from the IETF are soon to be expected.

- perform a quantum threat analysis consisting of an inventory of the assets they need to protect as well as the applications that use cryptography;
- develop a risk-oriented roadmap for executing the transition, taking into account the sensitivity and the protection period of the information, as well as the need to mitigate 'store now, decrypt later' attacks and to protect long-lived systems against the quantum threat well before this threat materializes. The transition should also consider crypto-agility, allowing to ensure a more resilient transition to PQC;
- plan the migration, which includes a prioritization and involves all necessary business processes as well as budgeting the migration;
- promote the continuation of the extensive research on post-quantum cryptography and standardization efforts.

It is important to protect systems handling sensitive data against CRQCs well in time. Uncertainties regarding the progress of quantum computer development should not preclude us from moving ahead with the protection of the most sensitive use cases. To ensure an acceptable level of readiness, we recommend that these should be protected against 'store now, decrypt later' attacks as soon as possible, latest by the end of 2030. Moreover, we also recommend to develop detailed transition plans for public-key infrastructure systems in the same timeframe.

We are committed to working together towards protecting our IT systems from the quantum threat to cryptography, and to support all sectors in designing their transition plans in order to reinforce the global resilience of our society through updated cryptography.

To this end, a Work Stream on PQC, co-chaired by France, Germany and the Netherlands, has been created as part of the NIS Cooperation Group following a recommendation [9] of the European Commission. **We encourage active engagement from all EU member states in this work stream** throughout the process of preparing a roadmap for the transition to Post-Quantum Cryptography to ensure the quantum resilience of the European Union's digital infrastructures.

References:

[1]: BSI, The status of quantum computer development, available at https://bsi.bund.de/dok/study_status_quantum_computer
[2]: Global Risk Institute, Quantum Threat Timeline 2023 (2023), available at https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
[3]: ANSSI, ANSSI views on the Post-Quantum Cryptography transition (2022), available at https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition
[4]: ANSSI, Follow up position paper on Post-Quantum Cryptography (2023), available at https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography
[5]: BSI, Quantum safe cryptography - fundamentals, current developments and recommendations (2021), available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html
[6]: AIVD, CWI, and TNO, The PQC Migration Handbook (2023), available at https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/
[7]: ANSSI, AIVD, BSI, Swedish Armed Forces, Position Paper on Quantum Key Distribution, available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html
[8]: ACN, Crittografia Post-Quantum e Quantistica. Preparazione alla Minaccia Quantistica (2024), available at https://www.acn.gov.it/portale/documents/20119/85999/ACN_Crittografia_Quantum_Safe.pdf/d7eb595c-ee7f-848b-6c14-abf64cafb310?t=1721310015826
[9]: European Commission, Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, available at https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography