NÚKIB's view on transition to post-quantum cryptography

THE FUTURE CRYPTOGRAPHY CONFERENCE

Tallinn, Estonian Academy of Sciences, 13 May 2024

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

NÚKIB activities for PQC

Národní úřad pro kybernetickou a informační bezpečnost

White papers/recommendations (July 2023):

- [8] Quantum computer attacks can break current encryption: the solution is the timely and effective implementation of new standards
- [9] Minimum requirements for cryptographic algorithms
- [10] Quantum threat and quantum-resistant cryptography

NÚKIB activities for PQC

- Conferences:
  - Prague Cyber Security Conference (March 2024)
  - CyberCon (September 2024, national)
- Invited presentations
- National Quantum Strategy (colaboration on its preparation)

Quantum computer attacks can break current encryption: the solution is the timely and effective implementation of new standards[8]

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Quantum computer attacks can break current encryption

- strategic analysis at managerial level
- description of the nature of the quantum threat for non-experts

Recommendations:

- use of post-quantum cryptography - with emphasis on proper implementation
- cryptographic agility - ability to replace individual components or algorithms if needed

MINIMUM REQUIREMENTS FOR CRYPTOGRAPHIC ALGORITHMS[9]

Cryptographic Security Recommendations

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Minimum Requirements for Cryptographic Algorithms

- (some) subjects regulated by the Act No. 181/2014 Coll. (**Cyber Security Act**) need to be compliant, e.g., critical infrastructure (unless their risk analysis justifies not to)

- provides a list of **recommended algorithms** in cryptography

version 1.0 in 2018
version 2.0 in 2022 – addition of algorithms for password hashing
version 3.0 in 2023 – **Quantum-Resistant Public-Key Cryptography**

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Quantum-Resistant Public-Key Cryptography

a) Hybrid quantum-resistant cryptography for key establishment

It is required to combine:

- a classical key establishment algorithm (one of the recommended ones)
- **CRYSTALS-Kyber**, **FrodoKEM** or **Classic McEliece** (each of them in **level 3 or 5**)

b) Stand-alone post-quantum key establishment algorithm

- CRYSTALS-Kyber Level 5 (Kyber-1024), implemented according to the NIST standard
- Note: Since the NIST standard has not yet been published, this solution has not yet been approved.

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Quantum-Resistant Public-Key Cryptography

c) Stand-alone post-quantum digital signature algorithm for firmware and software integrity protection

- LMS
- XMSS

d) Stand-alone post-quantum digital signature algorithm for general use

- CRYSTALS-Dilithium Level 5, implemented according to the NIST standard

e) Hybrid quantum-resistant cryptography for digital signatures

It is required to combine:

- a classical digital signature algorithm (one of the recommended ones)
- CRYSTALS-Dilithium, SPHINCS+ or Falcon

Quantum Threat and Quantum-Resistant Cryptography[10]

Appendix to the document
Minimum Requirements for Cryptographic Algorithms

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Quantum Threat and Quantum-Resistant Cryptography

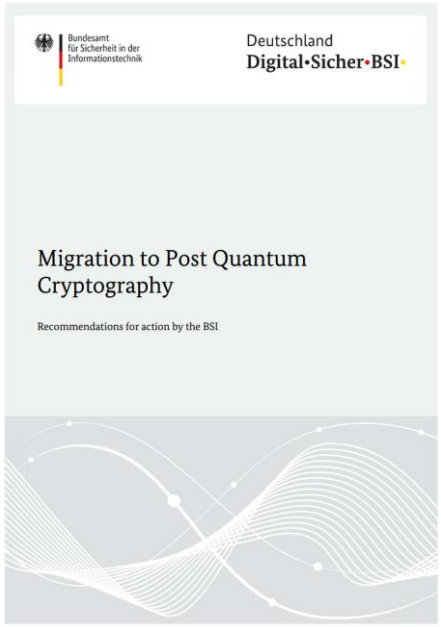
- Added to version 3.0 of Minimal Requirements to explain the cryptographic aspects of the quantum threat in more detail and to justify the updated requirements
- Describes possible reactions to the quantum threat
- Differentiates algorithms that are quantum-safe and quantum-vulnerable
- Assesses the urgency of replacement for the quantum-vulnerable ones

Quantum threat – news around the globe

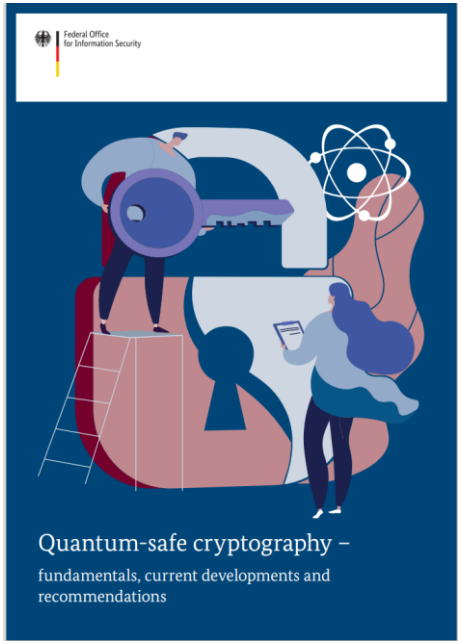
(How other institutions react to the quantum threat)

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

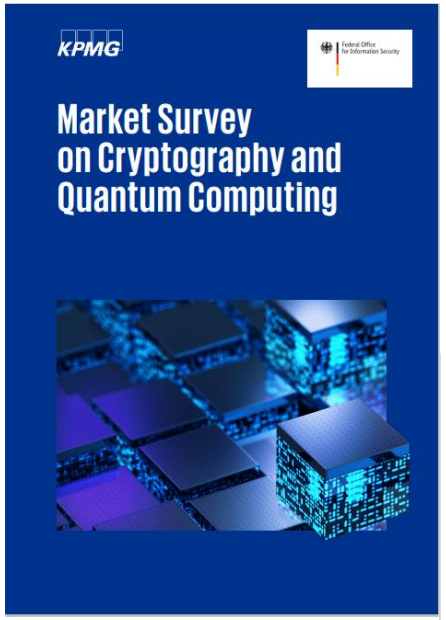
BSI



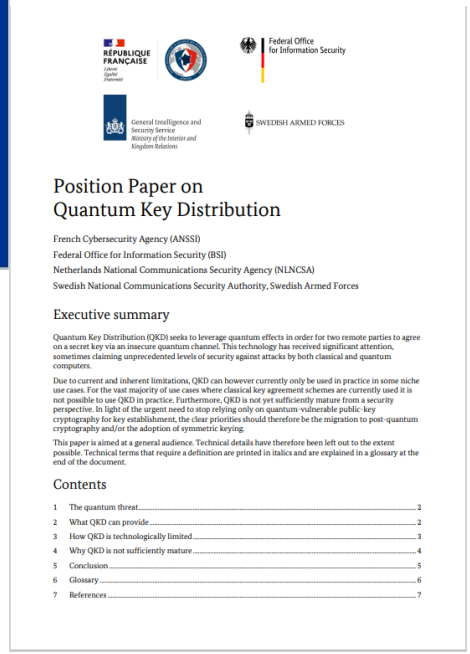
August 2020 [3]



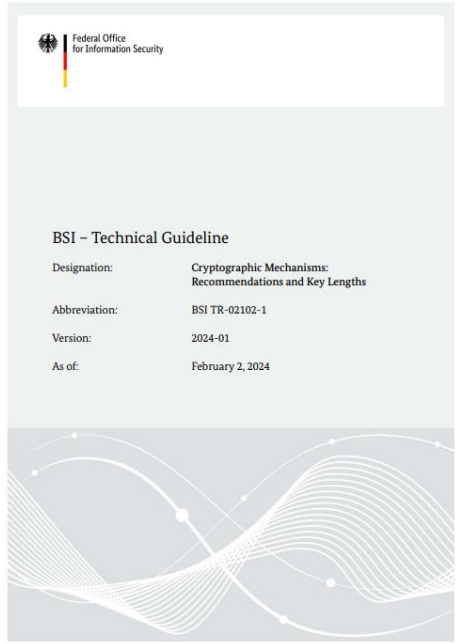
December 2021 [4]



August 2023 [5]



January 2024 [6]

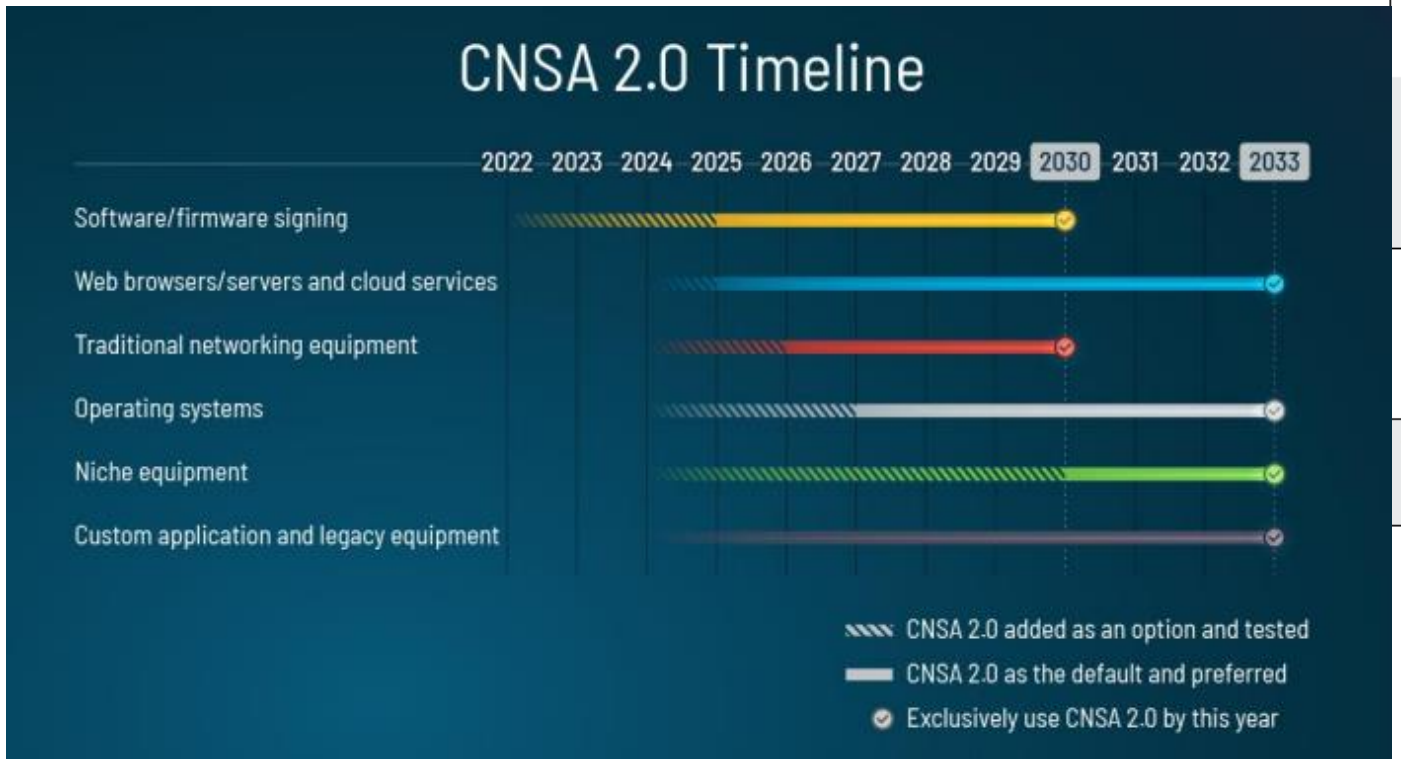


January 2024 [7]

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NSA – CNSA suite 2.0



Source: [1]

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

Source: [1]

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

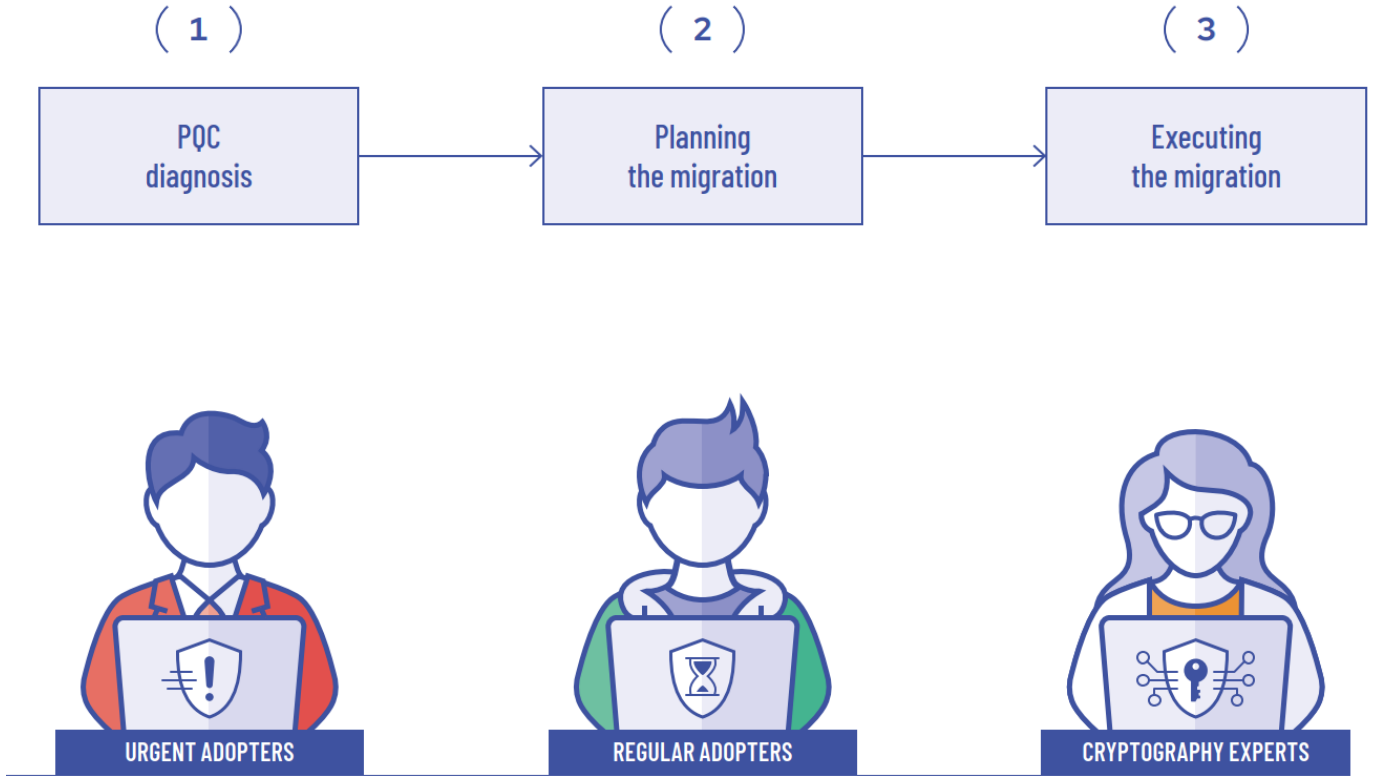
ETSI – Technical reports

- ETSI TR 103 619 V1.1.1 (July 2020) "Migration strategies and recommendations to Quantum Safe schemes"

  Three stages:
  1. Inventory Compilation
     (map dependencies of cryptographic assets on organizational assets, specific hardware or software infrastructure)
  2. Preparation of the migration plan
  3. Migration execution

- ETSI TR 103 616 V1.1.1 (September 2021) "Quantum-Safe Signatures"
- ETSI TR 103 823 V1.1.1 (September 2021) "Quantum-Safe Public Key Encryption and Key Encapsulation"

The Netherlands – PQC Migration Handbook (TNO, CWI, AIVD)



April 2023 [11]

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

EU Commission

EU COMMISSION RECOMMENDATION, 11 April 2024 [2]

Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

"*encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronised transition among the different Member States and their public sectors*"

Tomáš Rabas

Cyber Security Officer
Department of Security of Information and Communication Technologies (OBIT), NÚKIB

E-mail: tomas.rabas@nukib.gov.cz

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

References

[1] CSA_CNSA_2.0_ALGORITHMS_.PDF (defense.gov)

[2] Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography | Shaping Europe's digital future (europa.eu)

[3] BSI - Quantum Technologies and Quantum-Safe Cryptography - Migration to Post Quantum Cryptography (bund.de)
[4] Quantum-safe cryptography – fundamentals, current developments and recommendations (bund.de)
[5] Market Survey on Cryptography and Quantum Computing (bund.de)
[6] Position Paper on Quantum Key Distribution (bund.de)
[7] Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2024-01 (bund.de)

[8] Utoky s vyuzitim kvantoveho pocitace mohou prolomit soucasne sifrovani resenim je vcasna a efektivni implementace novych standardu.pdf (gov.cz)
[9] Minimum Requirements for Cryptographic Algorithms (gov.cz)

[10] Doporučení v oblasti kryptografických prostředků (gov.cz)
[11] The PQC Migration Handbook | Publication | AIVD