Post-Quantum Cryptography Standards and Roadmapping, PQC in Legislation

Workshop PQC – 27. 3. 2025, Brno

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Standardizace samotných PQC algoritmů

- NIST
- ISO
- Čína a Jižní Korea?

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

NIST

2016: únor – Ohlášení soutěže, prosinec – oficiální začátek

2017: listopad – konec přihlášek, prosinec – 69 kandidátů splnilo podmínky (z celkových **82 kandidátů**)

2019: leden – postoupení 26 kandidátů do druhého kola

2020: červenec – ohlášení 7 finalistů a 8 alternátů do třetího kola **(**únor 2022 - **Rainbow** ☹ [A1R]**)**

2022: červenec – Oznámení 4 algoritmů pro standardizaci (z 7 finalistů) a 4 postupujících algoritmů do čtvrtého kola **(**červenec/srpen – **SIKE** ☹ [A1S, A2S, Microsoft]**)**

2023: leden – ohlášení nové soutěže pouze pro digitální podpisy, srpen – vydání draftů standardů pro 3 algoritmy

2024: srpen – FIPS 203, 204, 205 - CRYSTALS-KYBER (**ML-KEM**), CRYSTALS-Dilithium (**ML-DSA**) and SPHINCS+ (**SLH-DSA**); Falcon stále čeká na draft (konec roku 2024…?)

Březen 2025: z 4 kandidátů čtvrtého kola vybrán **HQC** pro standardizaci

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

ISO

ISO/IEC 18033-2:2006(en) Asymmetric ciphers – a co PQC?

Oficiálně nikde nic… nebo?

Autoři Classic McEliece publikovali dokument jako draft potenciálního standardu ISO.

NIST v reportu ze čtvrtého kola prohlásil, že nestandardizuje Classic McEliece, mimo jiné z obavy dvou nekompatibilních standardů téhož [IR8545].

Autoři FrodoKEM v rámci konference IETF [slides]:

- ❑ Ongoing standardization by ISO (started on April'23)
  - To be included as Amendment 2 of ISO/IEC 18033-2 (together with ML-KEM and Classic McEliece)
  - Currently approved for Draft Amendment (DAM), Sept/Oct'24

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Jižní Korea

2021 – ohlášení soutěže; 2022 – začátek prvního kola s 16 kandidáty (7 KEMs, 9 dig. podpisů);

2023 – 8 kandidátů prošlo do druhého kola; leden 2025 – ohlášení 4 vítězů

KEMs: **SMAUG-T** a **NTRU+**; digitální podpisy: **HAETAE** a **AIMer** [KpqC]

Čína

První akademická **národní** soutěž **2018-2019**: 36 kandidátů, organizováno CACR (Chinese Association for Cryptologic Research); uzavřeno pro čistě národní vývojce, vše v čínštině; tři algoritmy získaly první místo [QApp, NCTA, CACR]

Únor 2025 – ICCS (Institute of Commercial Cryptography Standards) ohlásil mezinárodní soutěž pro čínské standardy pro **asymetrickou** kryptografii, **hashovací funkce** i **symetrické blokové šifry [NGCC].**

Doporučení algoritmů (PQC)

- V ČR - NÚKIB
- Vybrané ze zahraničí (s formálním vlivem na ČR)
  - SOG-IS (ACM)

Minimální požadavky na kryptografické algoritmy

Doporučení v oblasti kryptografické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Minimální požadavky na kryptografické algoritmy

- Je seznamem **schválených algoritmů** pro kryptografii od NÚKIB [odkaz]:

verze 1.0 v 2018
verze 2.0 v 2022 – přidání algoritmů hašování hesel
verze 3.0 v 2023 – **Postkvantová kryptografie**
verze 4.0 v 5.2.2025 – reference na **standardy NIST** + další malé úpravy

Jaký je právní význam tohoto dokumentu?

- Podle § 26 písm. d) vyhlášky č. 82/2018 Sb. „vyhláška o kybernetické bezpečnosti“ mají **povinné osoby** podle zákona č. 181/2014 Sb. „zákon o kybernetické bezpečnosti“ povinnost **zohlednit doporučení** v oblasti kryptografických prostředků vydaná Národním úřadem pro kybernetickou a informační bezpečnost za účelem ochrany aktiv informačního a komunikačního systému.

- Vyhlášky č. 316/2021 Sb. „*Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu*“, přílohy č. 2*: „Poskytovatel **umožňuje** ochranu zákaznického obsahu **šifrováním** při přenosu a v úložištích ve službě cloud computingu **pomocí některého z algoritmů** uvedených v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách.“*

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Kvantově odolná kryptografie s veřejnými klíči

a) Hybridní kvantově-odolná kryptografie pro ustanovení klíčů

Je vyžadována bezpečná kombinace:

- Klasického algoritmu pro ustanovení klíčů (jednoho ze schválených)
- **ML-KEM/CRYSTALS-Kyber**, **FrodoKEM** nebo **Classic McEliece** (**level 3 a 5**)

  (Po standardizaci NIST je pravděpodobné i přidání HQC)

b) Samostatný postkvantový algoritmus pro ustanovení klíčů

- **ML-KEM-1024** (level 5)

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Kvantově odolná kryptografie s veřejnými klíči

c) Samostatný postkvantový algoritmus digitálního podpisu pro ochranu integrity firmware a software

- LMS
- XMSS

d) Samostatný postkvantový algoritmus digitálního podpisu s obecným použitím

- ML-DSA - level 5
- SLH-DSA - level 3 a 5 (bezpečnostně více robustní)

e) Hybridní kvantově odolná kryptografie pro digitální podpis

Je vyžadována bezpečná kombinace:

- Klasického algoritmu pro digitální podpis (jednoho ze schválených)
- ML-DSA/CRYSTALS-Dilithium (level 3 a 5), SLH-DSA/SPHINCS+ (level 3 a 5) nebo Falcon (zatím není rozhodnuto – pravd. level 5)

SOG-IS – Agreed Cryptographic Mechanisms 1.4

-> např. vliv na doporučení ETSI: TS 119 312 „Electronic Signatures and Infrastructures (ESI); Cryptographic Suites“

-> vliv na důvěryhodné certifikační autority v ČR [MV, I.CA, PostSignum]

- Zatím nezveřejněno.

A co standardy protokolů?

Malá rešerše vybraných protokolů

Standardy protokolů relevantních ke kvantové hrozbě

- SSH
  - draft-ietf-sshm-mlkem-hybrid-kex-00 - PQ/T Hybrid Key Exchange in SSH
- TLS
  - RFC 8773: TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key
  - RFC 9257 - Guidance for External Pre-Shared Key (PSK) Usage in TLS (ietf.org)
  - draft-ietf-tls-hybrid-design-12 - Hybrid key exchange in TLS 1.3
- IPsec, IKEv2
  - RFC 8784 - Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security (ietf.org)
  - RFC 9370 - Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) (ietf.org)
  - RFC 9242: Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2) (rfc-editor.org)
  - Hybrid Non-Composite Authentication in IKEv2 (ietf.org)
- PGP
  - draft-ietf-openpgp-pqc-07 - Post-Quantum Cryptography in OpenPGP
- X.509 certificates
  - draft-ietf-lamps-kyber-certificates-08 - Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
  - draft-ietf-lamps-kyber-certificates-08 - Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
  - draft-ietf-lamps-kyber-certificates-08 - Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)

Roadmapping v EU

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*"

Securing Tomorrow, Today

- Pouze doporučení, nikoli legislativně závazné
- Do 2030 pro vysoce a kriticky citlivé informace (tj. citlivé i po deseti letech)
  - Šifrování – hotovo
  - Podpisy – mít plán
- Vznik pracovní skupiny pro PQC pod NIS Cooperation Group za účelem vytvoření detailnějšího plánu pod vedením Francie, Německa a Nizozemska
- Národní úřad pro kybernetickou a informační bezpečnost - Členské státy EU varují před kvantovou hrozbou a vyzývají k přechodu k postkvantové kryptografii

Tomáš Rabas

Vedoucí Oddělení kryptologických analýz (OKA), Odbor bezpečnosti informačních a komunikačních technologií (OBIT), NUKIB
E-mail: tomas.rabas@nukib.gov.cz