Jak se připravit na post-kvantovou kryptografii

+ příklad budování inventáře a migrace

18.10.2023

AFCEA – BS72 – Bezpečnostní seminář:
Kvantová a postkvantová kryptografie

Roman Cinkais

3KEYCOMPANY

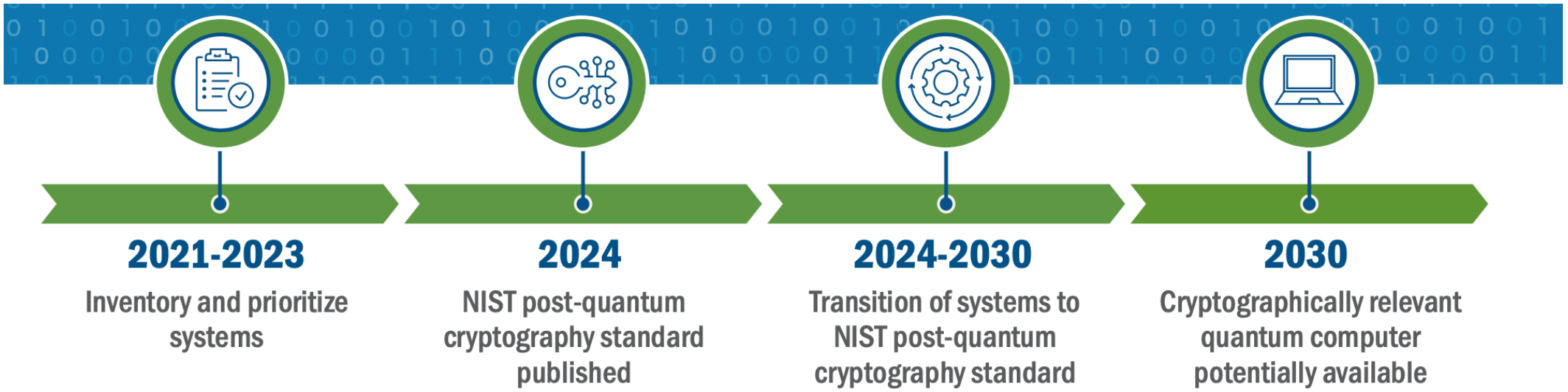
KVANTOVÁ HROZBA

Kvantové počítače mají potenciál prolomit mnoho v současnosti používaných kryptografických algoritmů, které jsou založeny na obtížnosti určitých matematických problémů. Na rozdíl od klasických počítačů, které používají k ukládání informací bity ve formě 0 nebo 1, kvantové počítače používají qubity, které mohou existovat ve více stavech současně, což jim umožňuje zpracovávat informace exponenciálně rychleji než klasické počítače. Toto nové výpočetní paradigma pravděpodobně umožní kvantovým počítačům prolomit šifrovací klíče, které se používají k ochraně citlivých dat, čímž se současné metody kryptografie s veřejným klíčem stanou zastaralými.

Harvest Now – Decrypt Later

Symetrická kryptografie - Grover

Asymetrická kryptografie - Shor



STANDARDY A REGULACE

Post-Quantum Cryptography - Integration study
- není zaručeno, že postkvantový kryptosystém, který projde přes proces standardizace, je bezpečný
- výskyt chyb v nových implementacích, rozšíření současných kryptosystémů místo nahrazení
- přidávání dalších vrstev šifrování nebo podepisování pomoci PQC

ANSSI VIEWS ON THE POST-QUANTUM CRYPTOGRAPHY TRANSITION
- Fáze 1 (dnes): hybridizace, která má zajistit dodatečnou postkvantovou obranu, hybridní bezpečnost
- Fáze 2 (nejdříve v roce 2025): hybridizace, která poskytne dlouhodobu postkvantovou bezpečnostní záruku a zabrání regresi
- Fáze 3 (pravděpodobně ne dříve než v roce 2030): implementace a nasazení samostatných PQC algoritmů

TR 103 619 - Migration strategies and recommendations to Quantum Safe schemes
- Postupný přechod na PQC pomoci hybridního módu
- Použití hybridních certifikátů a kryptografické pružnosti
- Hybridní mód nepřestavuje konečný stav, ale představuje mezikrok

Migration to Post-Quantum Cryptography – NCCoE SP 1800-38A
- Standardizace PQC algoritmů pro šifrování a podepisování
- Doporučení pro migraci infrastruktury a zavedení hybridních nebo kompozitních certifikátů
- Validace implementace PQC algoritmů

NÚKIB

NÚKIB

MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY

doporučení v oblasti kryptografické bezpečnosti

NÚKIB

KVANTOVÁ HROZBA A KVANTOVĚ ODOLNÁ KRYPTOGRAFIE

Příloha k dokumentu: Minimální požadavky na kryptografické algoritmy

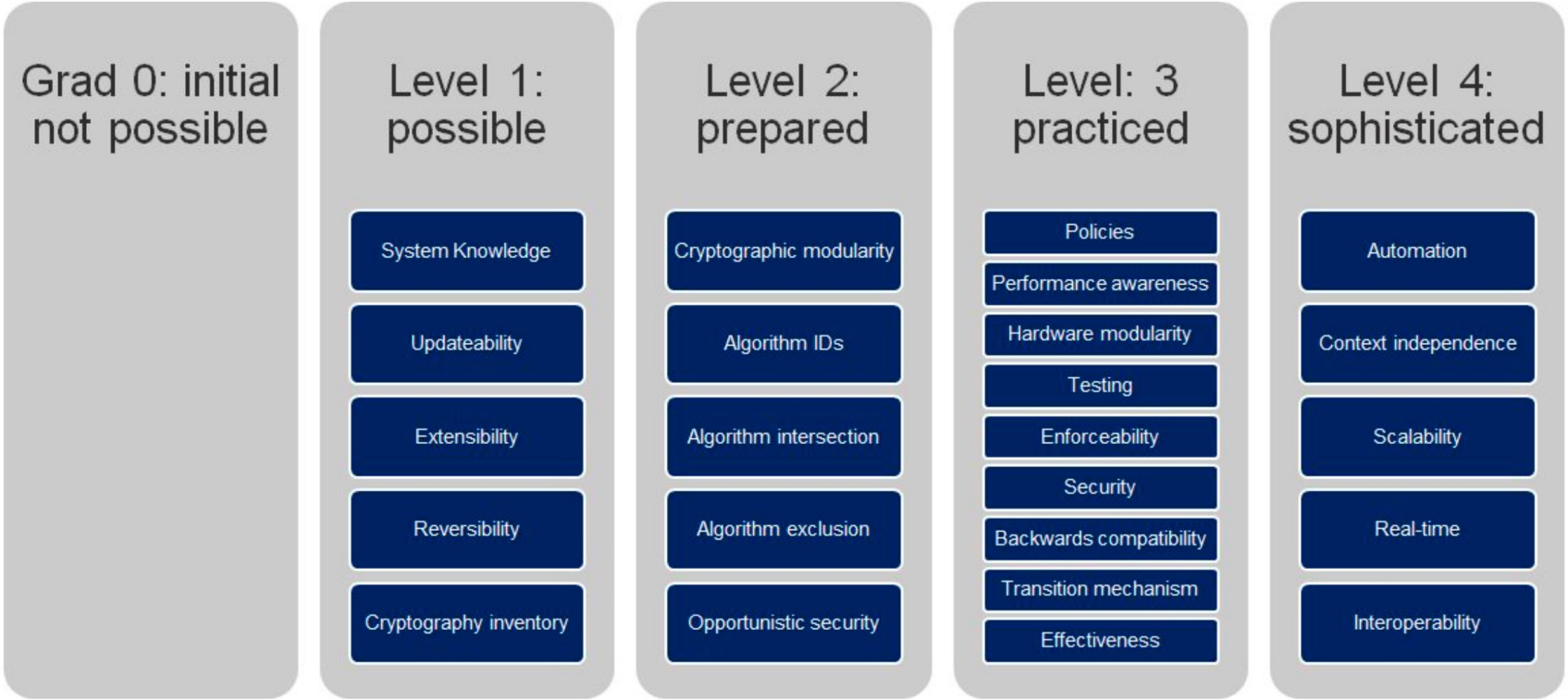
Kryptografická pružnost je schopnost rychle nahradit kryptografické algoritmy na základě jejich bezpečnostních atributů a požadovaných funkcí, aniž by to mělo zásadní dopad na technologii.

- Vysoce prioritní oblast – do konce 2027
- Prioritní oblast – kolem roku 2030
- Ostatní oblasti

Doporučení se řídí doporučením NIST pro přechod na PQC algoritmy a jejich požadavky na bezpečnost (úroveň 1 až 5)

CAMM

Cryptographic Agility Maturity Model



Part of the project Agile and Easy-to-use Integration of PQC Schemes within the ATHENE Cryptography (PQC) research area. It is jointly conducted by the UCS and ACSD research groups at the CS department at Hochschule Darmstadt – University of Applied Sciences.

PQC ALGORITMY

Úroveň	AES/SHA3 náročnost	Algoritmy
1	Odpovídá náročnosti útoku hrubou silou na AES-128	Kyber512, Falcon512, Sphincs+SHA256 128f/s
2	Odpovídá náročnosti generického hledání kolizí SHA-256	Dilithium2
3	Odpovídá náročnosti útoku hrubou silou na AES-192	Kyber768, Dilithium3, Sphincs+SHA256 192f/s
4	Odpovídá náročnosti generického hledání kolizí SHA-384	Na této úrovni nebyl testován žádný algoritmus
5	Odpovídá náročnosti útoku hrubou silou na AES-256	Kyber1024, Falcon1024, Dilithium5, Sphincs+SHA256 256f/s

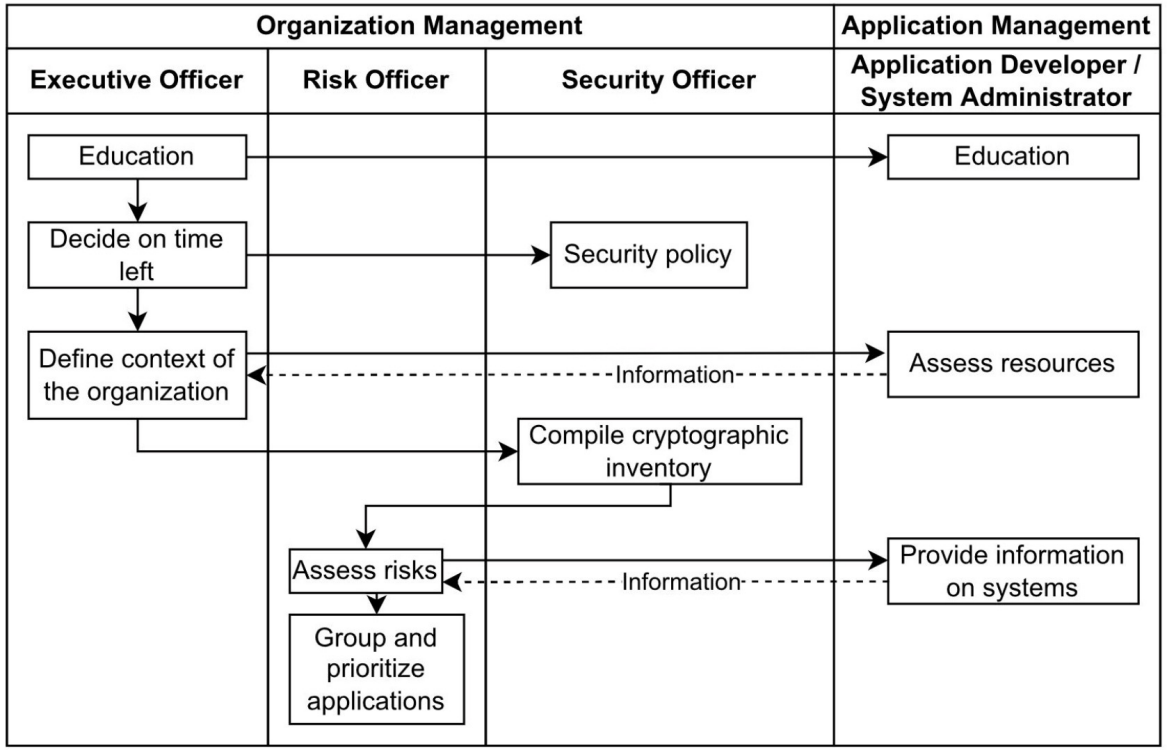
- **SP 800-208**, Recommendation for Stateful Hash-Based Signature Schemes, LMS (RFC 8554) and XMSS (RFC 8391)
- **FIPS 203**, Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM), rooted in CRYSTALS-Kyber
- **FIPS 204**, Module-Lattice-Based Digital Signature Standard (ML-DSA), drawing strength from CRYSTALS-Dilithium
- **FIPS 205**, Stateless Hash-Based Digital Signature Standard (SLH-DSA), inspired by the prowess of SPHINCS+

ALGORITMY A DÉLKY

Úroveň	Algoritmus	Délka veřejného klíče (byte)	Délka privátního klíče (byte)	Délka podpisu/šifrovaného textu (byte)
1	Kyber512	800	1632	768
1	Falcon512	897	1281	666
1	SPHINCS+-{SHA2,SHAKE}-128s	32	64	7856
2	Dilithium2	1312	2528	2420
3	SPHINCS+-{SHA2,SHAKE}- 192s	48	96	16224
3	Kyber768	1184	2400	1088
3	Dilithium3	1952	4000	3293
5	Falcon1024	1793	2305	1280
5	SPHINCS+-{SHA2,SHAKE}- 256s	64	128	29792
	RSA2048	256	256	256
	P256	64	32	64
	P256_HKDF_SHA256	65	32	65
	P521_HKDF_SHA512	133	66	133

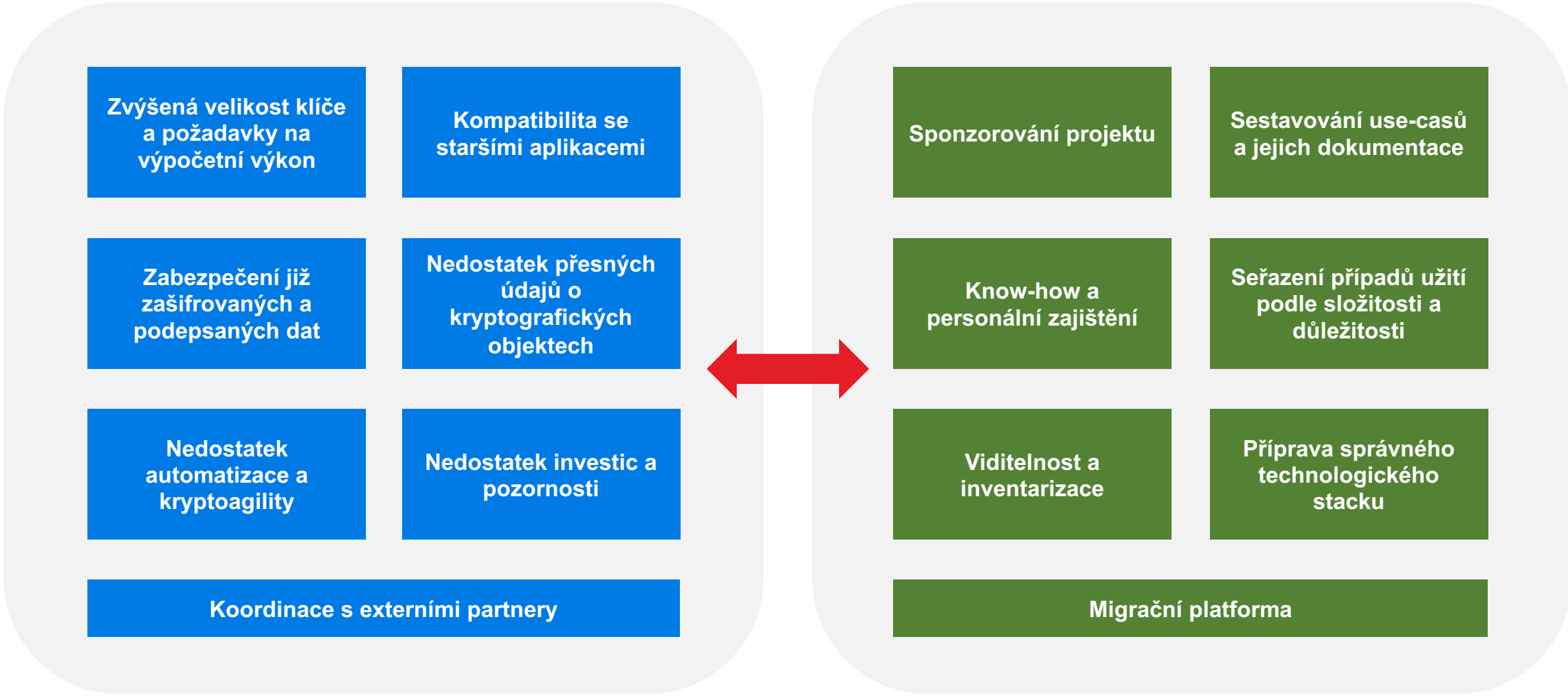
MIGRACE

- Vzdělávat decision makery
- Rozhodnout o časovém plánu pro mitigaci kvantové hrozby
- Konzultovat a upravovat bezpečnostní politiky
- Definovat kontext organizace a zhodnotit zdroje
- Shromáždit znalosti o systému, poradit se s partnery
- Sestavit inventář kryptografických objektů (pokud možno automatizovaně)
- Posoudit současné rizika (na základě kontextu)
- Seskupit systémy a stanovte jejich priority, vytvořit skupiny aplikací a systémů.
- Zajistit kompatibilitu systémů



N. von Nethen, A. Wiesmaier, O. Weissmann, and N. Alnahawi. Managing the Migration to Post-QuantumCryptography. Submitted to ACNS'23, 2023. Preprint: https://arxiv.org/abs/2301.04491.

VÝZVA A PŘEDPOKLADY



MOSCOVA VĚTA

X Jak dlouho bude trvat implementace kvantově bezpečného řešení do vaší stávající infrastruktury?

Y Jak dlouho potřebujete mít zašifrovaná data zabezpečená?

Z Jak dlouho bude trvat vývoj dostatečně výkonného kvantového počítače?

KOMPROMITACE

PKIC - PQCCM

Seznam softwarových aplikací, knihoven a hardwaru, které podporují postkvantovou kryptografii.

- Crypto4A
- Securosys
- Utimaco
- Thales
- Bouncy Castle
- Entrust
- Keyfactor
- Fortanix
- I4P
- CZERTAINLY
- IBM
- MTG AG
- ISC
- Botan

Algorithm	Reference
Composite certificates	https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-keys/
Hybrid certificates	https://datatracker.ietf.org/doc/html/draft-truskovsky-lamps-pq-hybrid-x509-01
Chameleon certificates	https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/
X.509 Alternative Signatures (section 9.8)	https://www.itu.int/rec/T-REC-X.509-201910-I
LMS	https://www.rfc-editor.org/rfc/rfc8708.html
XMSS	https://datatracker.ietf.org/doc/html/rfc8391
Falcon	https://falcon-sign.info
Dilithium	https://pq-crystals.org/dilithium/resources.shtml
SPHINCS+	https://sphincs.org
Kyber	https://pq-crystals.org/kyber/index.shtml
BIKE	https://bikesuite.org
McEliece	https://classic.mceliece.org
HQC	https://pqc-hqc.org
NIST Recommendation for Stateful Hash-Based Signature Schemes	SP800-208

3KEYCOMPANY

3Key Company s.r.o.

Roman Cinkais

roman.cinkais@3key.company