ETSI/IQC Quantum Safe Cryptography Event

THE PQC MIGRATION HANDBOOK

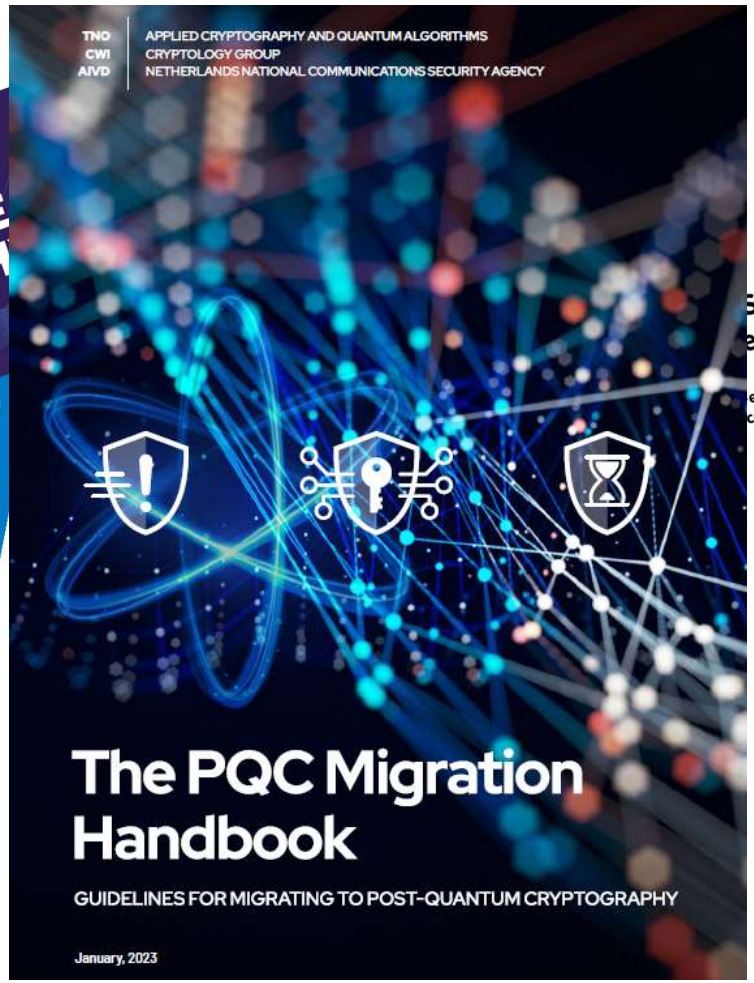
GUIDELINES FOR MIGRATING TO PQC

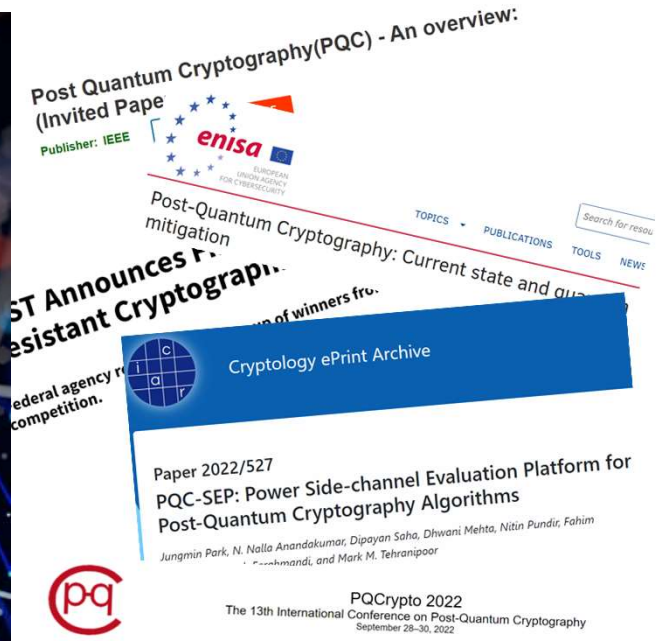
Ward van der Schoot MMath

TNO innovation for life

14/02/2023

POST-QUANTUM CRYPTOGRAPHY
CURRENT STATE OF AFFAIRS





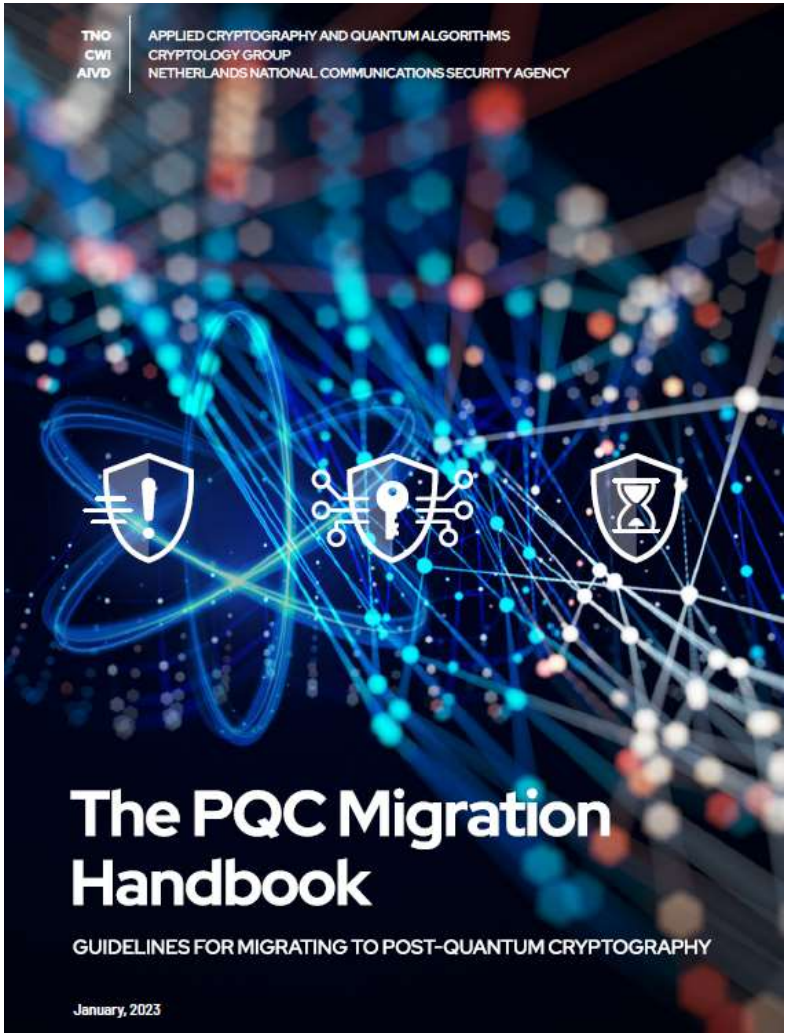
TNO innovation for life

THE PQC MIGRATION HANDBOOK
CONTRIBUTION

- Bridges the gap between technology and urgency
  - Sweet spot between **detail** and **high-level**
  - **Tailor-made** for organisations with few(er) crypto knowledge
  - Concrete, current and hands-on advice
  - Checklists, decision trees and step-by-step guides

- **Layered** approach. Describe full migration for:
  - Management, policymakers, strategists, technical audience, etc.

- Collection of state-of-the-art advice from NIST, ETSI, IETF, etc
  - Corporate insights from Deloitte, KPMG, KPN
  - Governmental insights from (Dutch) ministeries of defence, foreign affairs and health and infrastructure.



TNO innovation for life

THE PQC MIGRATION HANDBOOK
THREE-STEP APPROACH BY ETSI

1. Diagnosis
   - Determine your stance towards PQC migration: PQC personas
   - PQC inventory
2. Planning
   - When? Determine your migration scenario
   - How? Business and technical planning
3. Execution
   - Choose migration per cryptographic asset
   - General strategies such as hybrid and pre-shared keys
   - Cryptographic agility

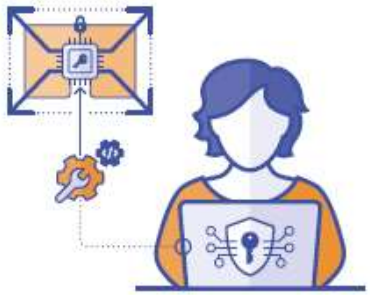
- Main contribution: collect advice and tailor it to organisations

ETSI TR 103 619 V1.1.1 (2020-07)

PQC PERSONAS
ALL PERSONAS

Standard Developing Organisations

Cryptographic Infrastructure Providers



Providers of cryptography beyond secure communication

URGENT ADOPTERS

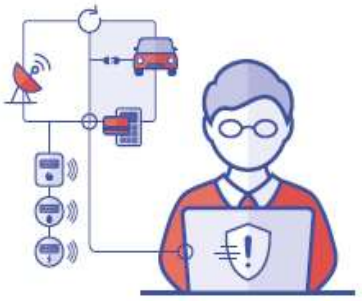
REGULAR ADOPTERS

CRYPTOGRAPHY EXPERTS

Confidential Data Handlers

Personal Data Handlers

Critical Infrastructure Providers

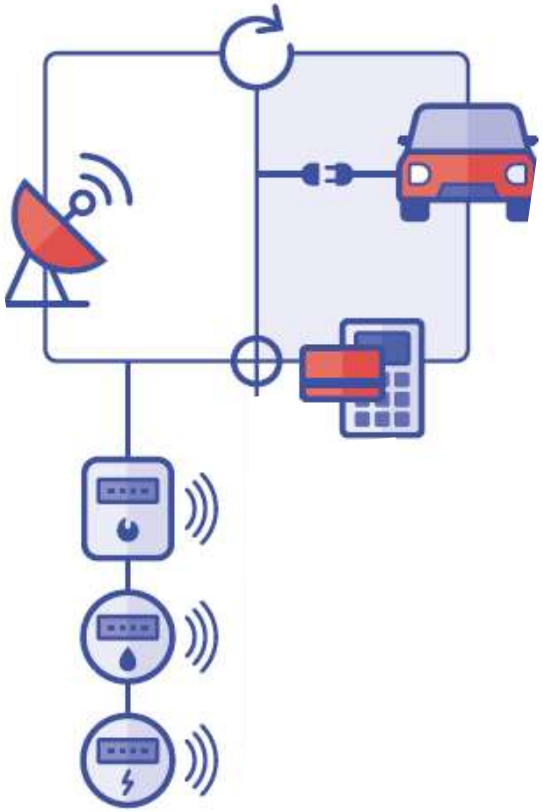


Long-lived Infrastructure Providers

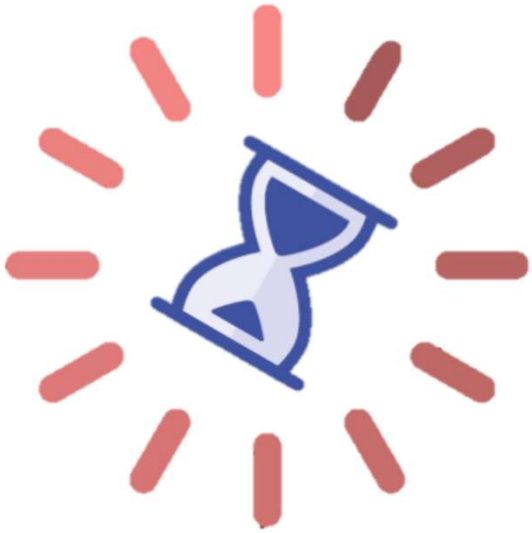
TNO innovation for life

PQC PERSONAS
URGENT ADOPTERS

Store-now-decrypt-later attacks



Long-lived systems

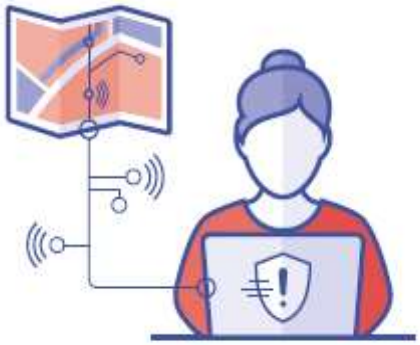


Migration is time-consuming

PQC PERSONAS
URGENT ADOPTERS

Confidential Data Handlers

Personal Data Handlers



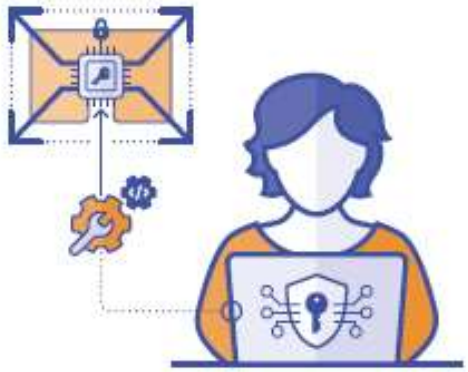
Critical Infrastructure Providers

Long-lived Infrastructure Providers

PQC PERSONAS
CRYPTOGRAPHY EXPERTS

Standard Developing Organisations

Cryptographic Infrastructure Providers



Providers of cryptography beyond secure communication

THE PQC MIGRATION HANDBOOK
WHAT ELSE?

- Diagnosis
  - PQC personas: stimulates collaboration
  - Make PQC inventory

- Planning
  - Choose your migration scenario based on Mosca's inequality $X + W_i + Y_i < Z$
  - Business and technical process planning

Migration time from scenario *i*

Waiting time until scenario *i*

- Execution
  - General strategies such as hybrid and pre-shared keys
  - Cryptographic agility
  - Detailed overview and advice on protocols, primitives, (a)symmetric cryptography, hashes and MACs

TNO innovation for life

THE PQC MIGRATION HANDBOOK

HANDS-ON ADVICE

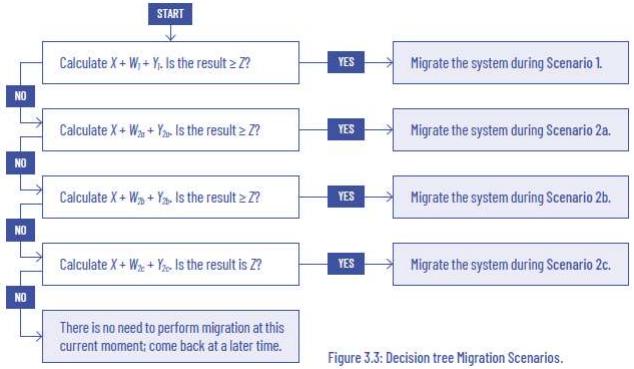


Figure 3.3: Decision tree Migration Scenarios.

Type	Functionality	Recommended	Acceptable	Do not use
Symmetric	*Block Cipher*	AES-256	Camellia-256	AES-128, AES-192 (T)DES, IDEA, and Blowfish
Symmetric	*Stream Cipher*	ChaCha20 with 256-bit key	-	RC4
Asymmetric (All scenarios)	*Public-Key Encryption/KEMs*	CRYSTALS-KYBER	Classic McEliece, FrodoKEM	Any classical PKC
Asymmetric (Scenario 1 with Stateful Hash-based Signatures)	*Digital Signatures*	XMSS, XMSS^{MT} LMS, HSS	Any NIST (Draft) Standards	Any classical PKC
Asymmetric (Scenario 1 without Stateful Hash-based Signatures)	*Digital Signatures*	Any NIST (Draft) Standards	-	Any classical PKC
Asymmetric (Scenario 2)	*Digital Signatures*	Any NIST (Draft) Standards	XMSS, XMSS^{MT} LMS, HSS	Any classical PKC
Hash	*Hashing*	At least SHA3-256 or SHA-256	BLAKE2, SHAKE256	SHA1, MD5, SHAKE128, SHA3-224, SHA-224
MACs	*Block Cipher Construction*	CMAC-AES-256	CMAC-Camellia	CBC-MAC
MACs	*Hash Constructions*	HMAC with at least SHA-256 or SHA3-256	BLAKE2-MAC	HMAC-MD5
MACs	*Universal Hashing*	Poly1305	-	-

Table 4.1: Recommended, Acceptable and Do not use Cryptographic Primitives per functionality.

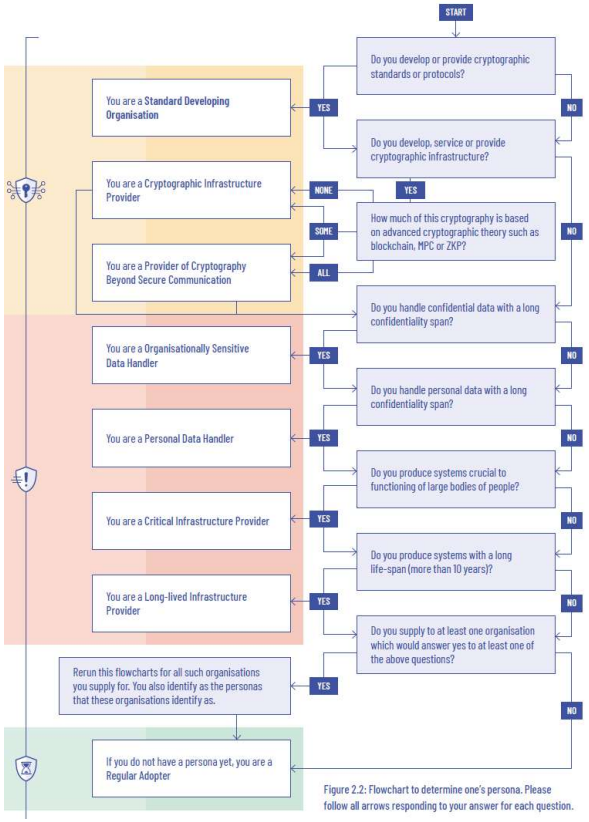


Figure 2.2: Flowchart to determine one's persona. Please follow all arrows responding to your answer for each question.

	Features			Speed			Memory		
	QUANTUM SAFE?	MATURITY	VERSATILITY	KEY GEN	ENCRYPTION	DECRYPTION	PUB KEY	PRIV KEY	CIPHERTEXT
RSA									
Elliptic-curve									
CRYSTALS-DILITHIUM									
CRYSTALS-KYBER									
FrodoKEM									
FALCON									
BIKE									
Classic McEliece									
HQC									
SPHINCS+									

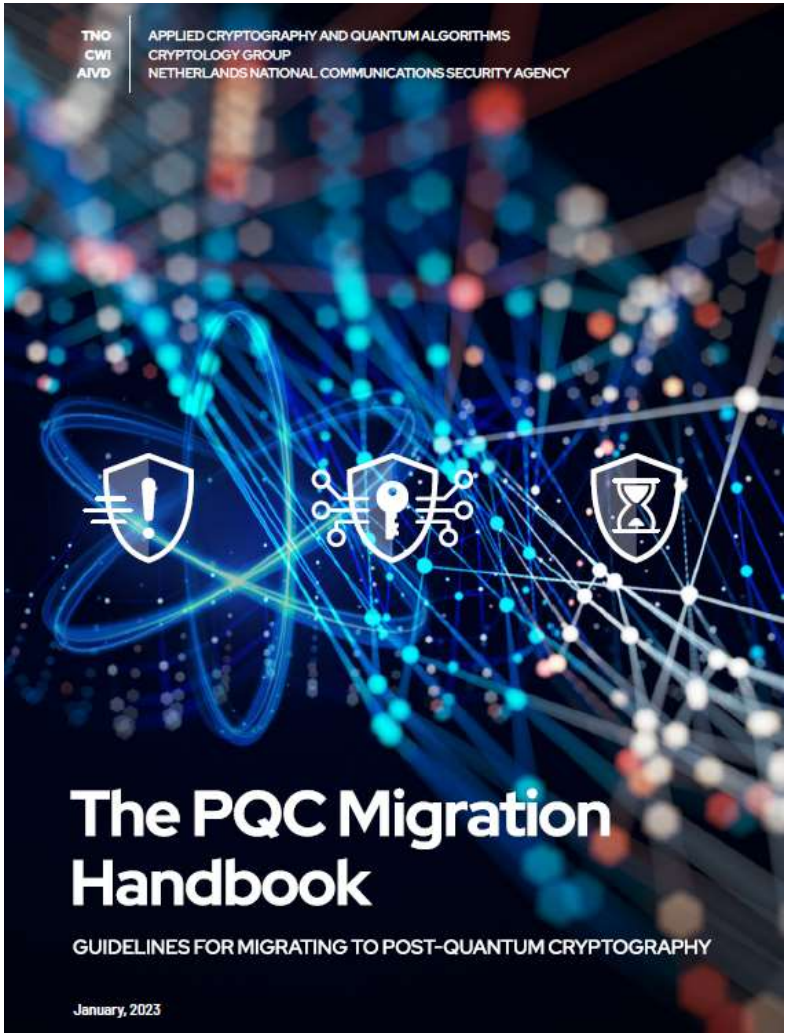
Symmetric	Asymmetric	Hash	MAC	HBS
AES	RSA	SHA Family	HMAC Constructions	XMSS
(T)DES	ElGamal	MD5	BLAKE2-MAC	XMSS^{MT}
ChaCha20	ECDSA	BLAKE2	CMAC Constructions	LMS
Blowfish	EdDSA		CBC-MAC Constructions	HSS
RC4	ECDH		Poly1305	
Camellia				
IDEA				

THE PQC MIGRATION HANDBOOK
WHAT'S NEXT?

- The 'Dutch standard' in PQC migration
  - Written by Dutch national security agency and renowned knowledge institutes
  - Official handover to minister of digital security in March
  - Publish on dcypher
  - Note: just as relevant for foreign organisations

- Want to collaborate?
  - Partner? Sounding board?
  - Approach me or email to ward.vanderschoot@tno.nl

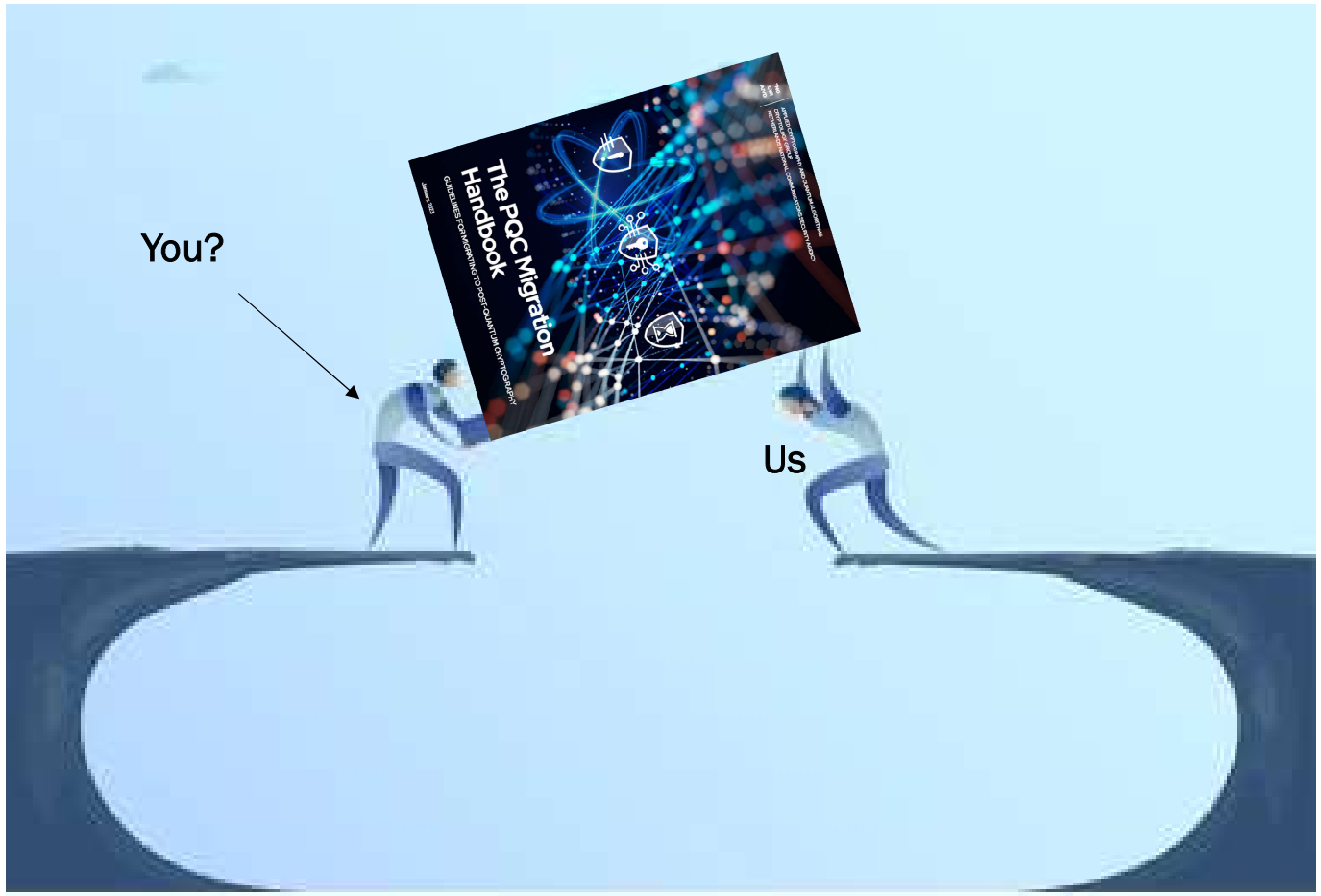
- Pick up a copy of the manual in the front
  - Kick-start your own migration



TNO innovation for life

THE PQC MIGRATION HANDBOOK

BRIDGE THE GAP



TNO innovation for life

THANK YOU FOR YOUR TIME
SPECIAL THANKS TO THE TEAM

Matthieu Lequesne

Marc Stevens

Thomas Attema

João Faria Miranda de Duarte

Vincent Dunning

Ward van der Schoot

TNO innovation for life

Contact: ward.vanderschoot@tno.nl