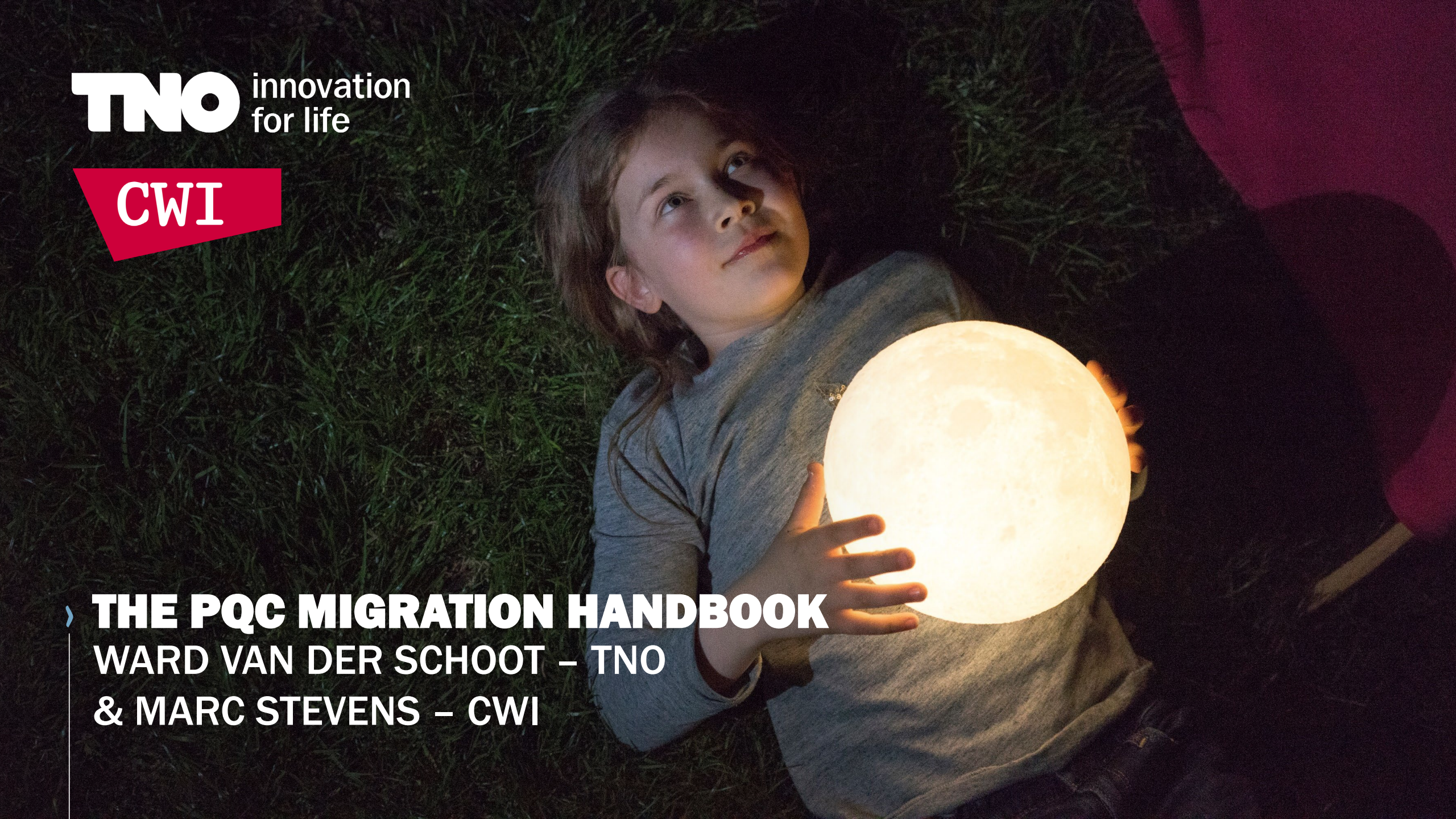


TNO innovation for life

CWI

THE PQC MIGRATION HANDBOOK

WARD VAN DER SCHOOT – TNO
& MARC STEVENS – CWI

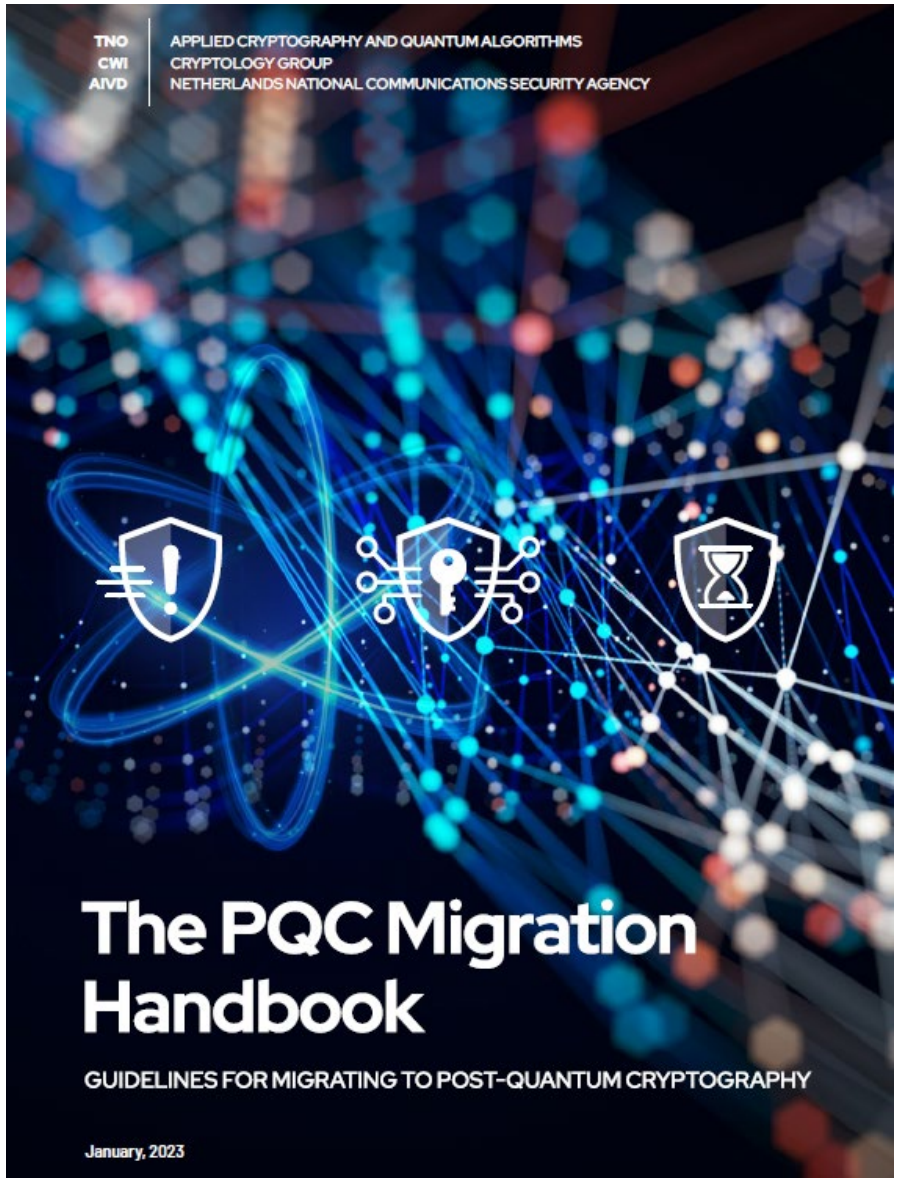
THE PQC MIGRATION HANDBOOK
GOAL & CONTRIBUTION

- Goal: pave the way for PQC migration in practice
  - Concrete, current and hands-on advice and action steps

- Strong points:
  - **Tailor -made** advice for each organisation
  - **Actionable:** 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.



THE PQC MIGRATION HANDBOOK

THREE-STEP APPROACH BY ETSI

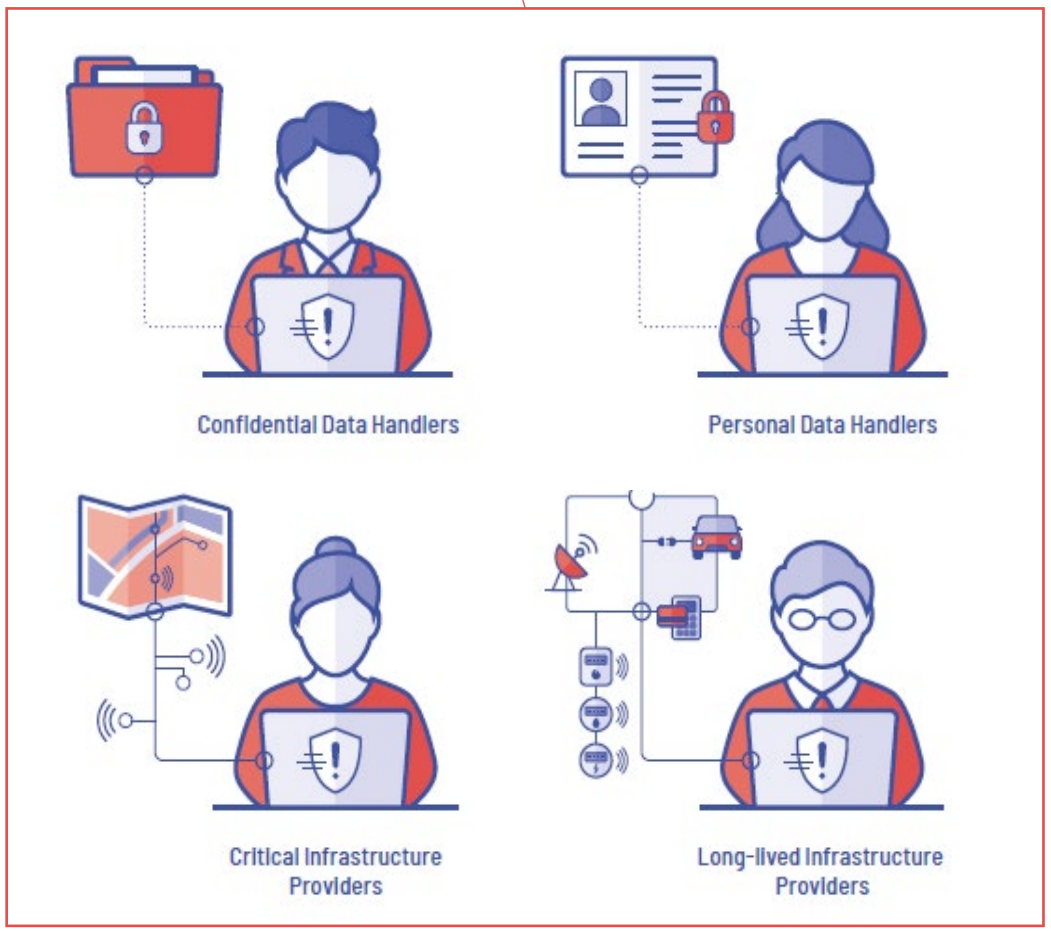
1. Diagnosis
   - Determine your stance towards PQC migration: PQC personas
   - PQC inventory
2. Planning
   - When? Determine your migration scenario
   - How? Business and technical planning
3. Execution
   - Choose migration per cryptographic asset
   - General strategies such as hybrid and pre-shared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

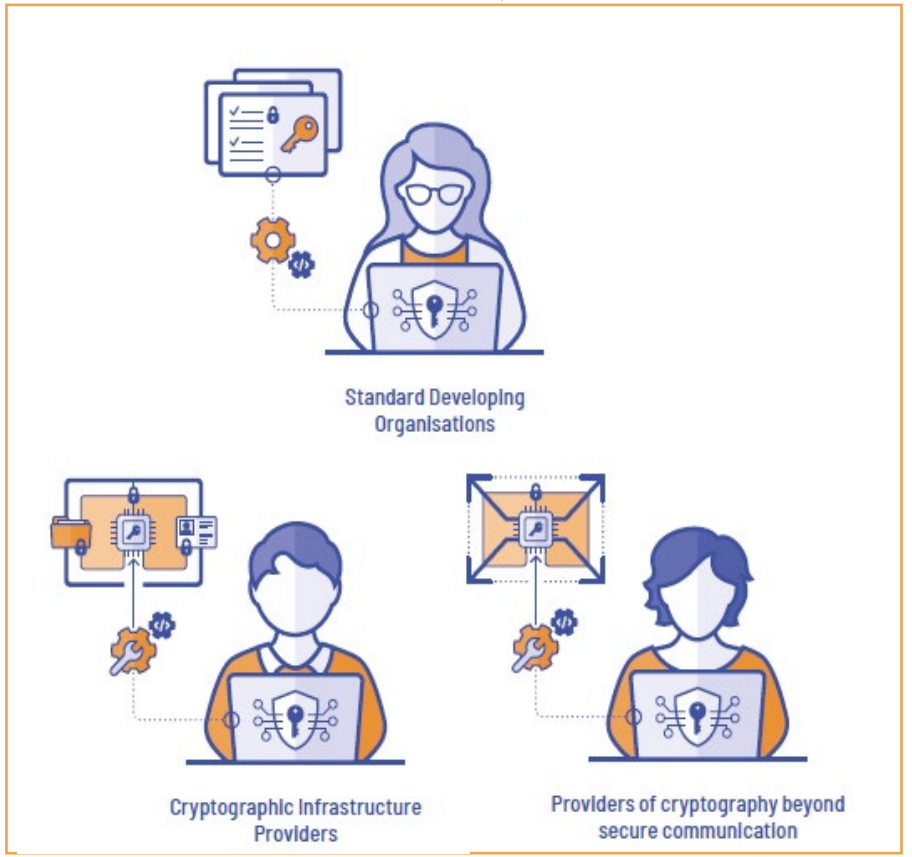
- Main contribution:
  - Collect advice and tailor it to each organisation with PQC personas

PQC PERSONAS

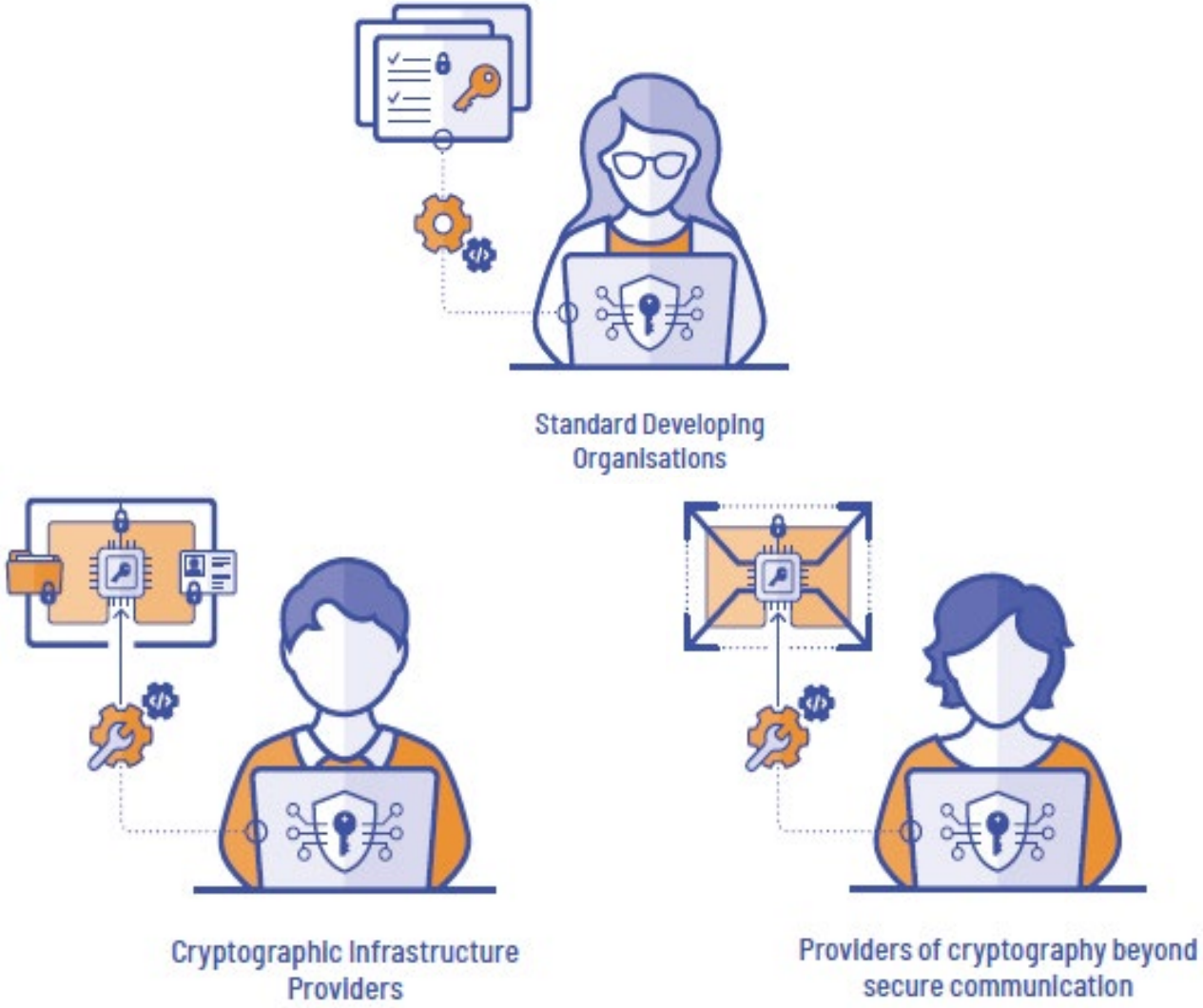
ALL PERSONAS

PQC PERSONAS
ALL PERSONAS



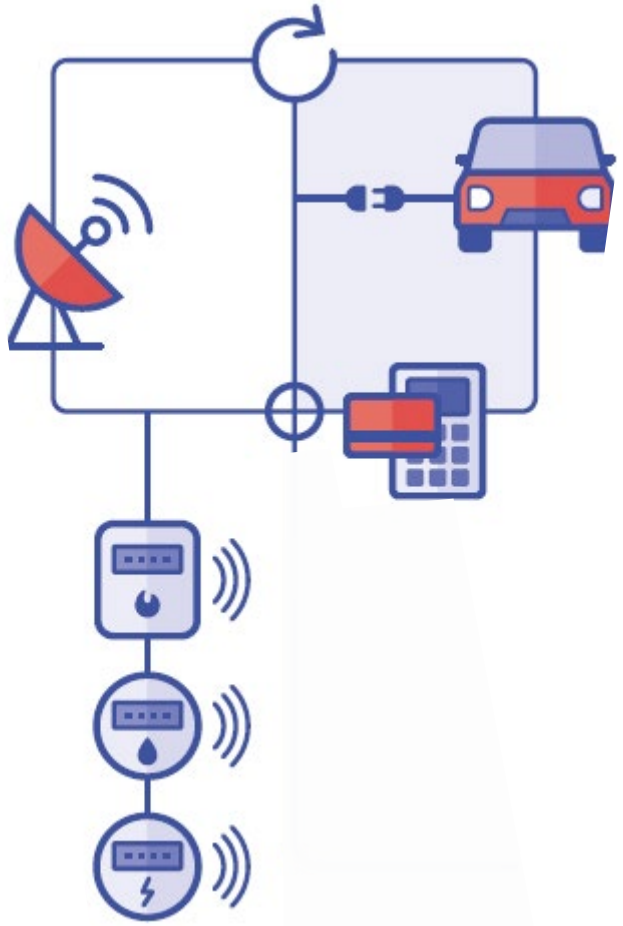


PQC PERSONAS
CRYPTO EXPERTS

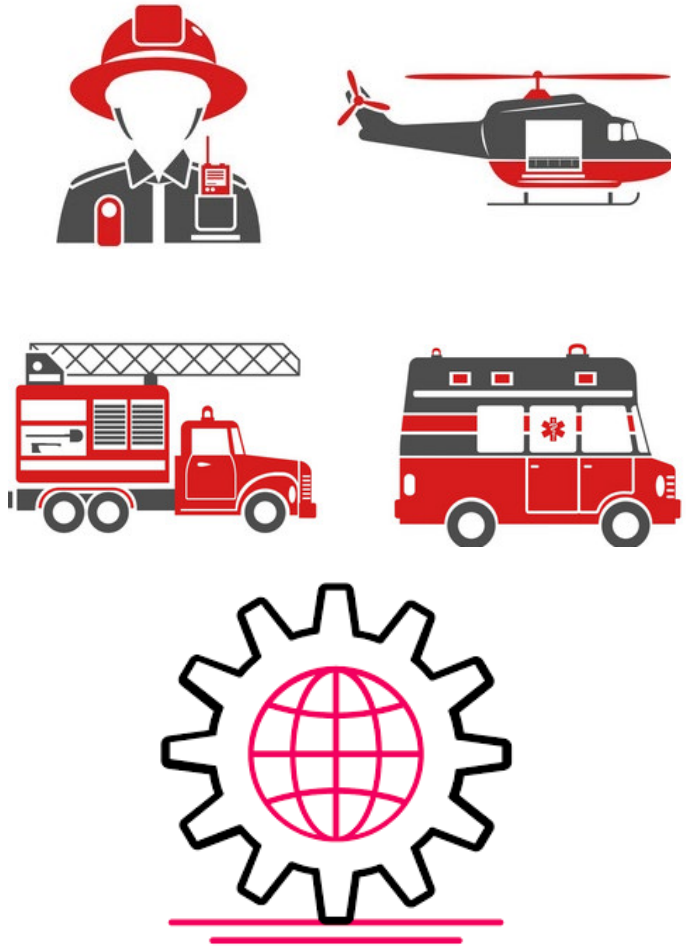


PQC PERSONAS
URGENT ADOPTERS

Store-now-decrypt-later attacks



Long-lived systems

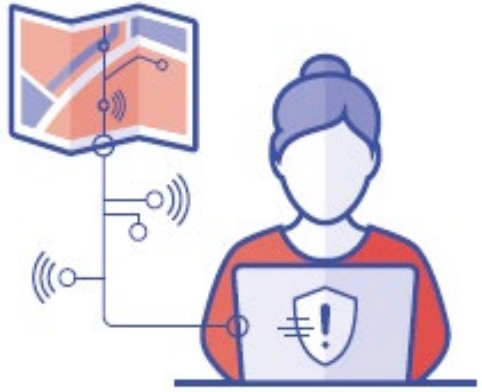


Vital infrastructure

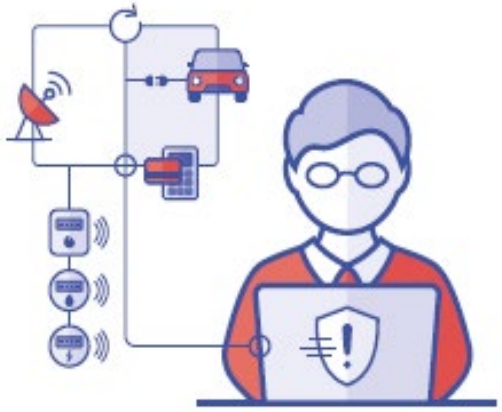
PQC PERSONAS
URGENT ADOPTERS

Confidential Data Handlers

Personal Data Handlers



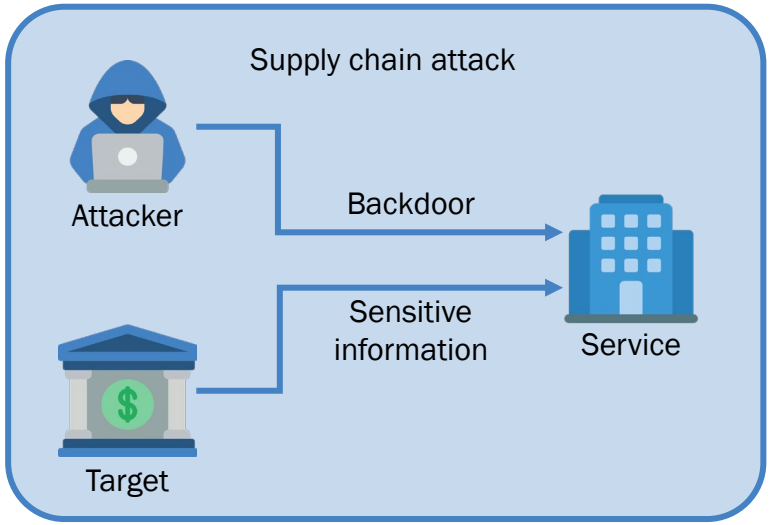
Critical Infrastructure Providers

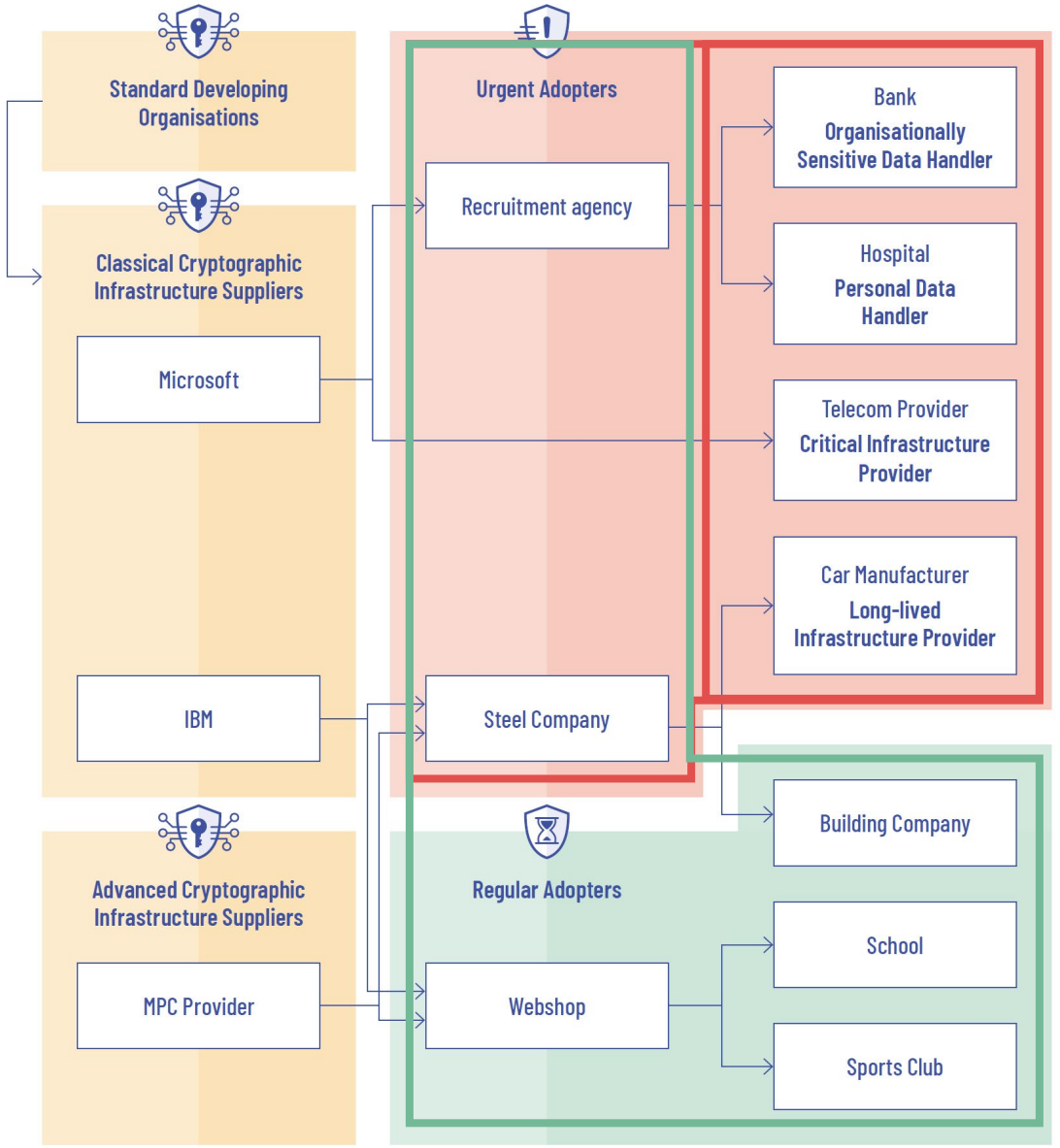


Long-lived Infrastructure Providers

PQC PERSONA'S
SUPPLY CHAIN

- Organisations are dependent on each other via collaboration and services
- This influences the migration in different ways:
  - Coordinated migration can be more efficient or even necessary
  - An organisation's persona can change due to supply chain risks





DIAGNOSIS
PQC INVENTORY

- Make a PQC inventory
  - Risk assessment
  - Inventory of cryptographic systems
  - Inventory of data
  - Inventory of cryptographic dependencies

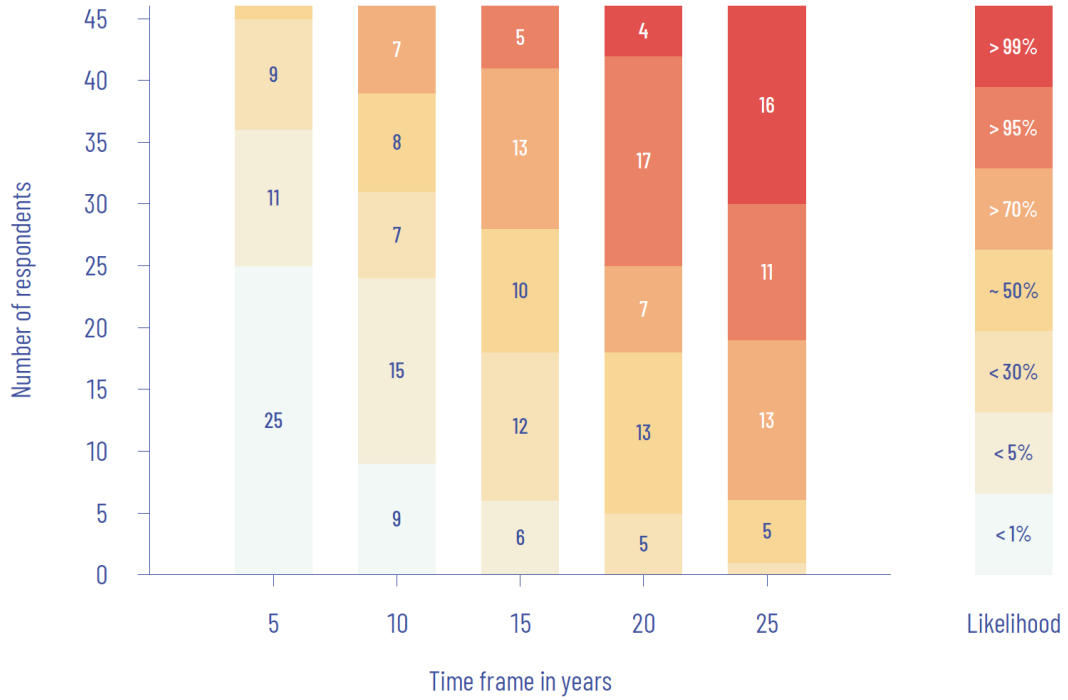
- Depending on ones persona, inventory has different focus
  - Data personas should have a thorough data inventory
  - Infrastructure personas should have a thorough systems inventory

- Each organisation is advised to prepare this already
  - Migration is a timely process
  - Increase readiness for future migration steps

PLANNING
WHEN TO MIGRATE?

- Migration equation: $X + Y < Z$:
  - Z: Time until old public-key crypto can be broken by a sufficiently large quantum computer
  - X: Time that information/systems need to stay protected
  - Y: Migration time

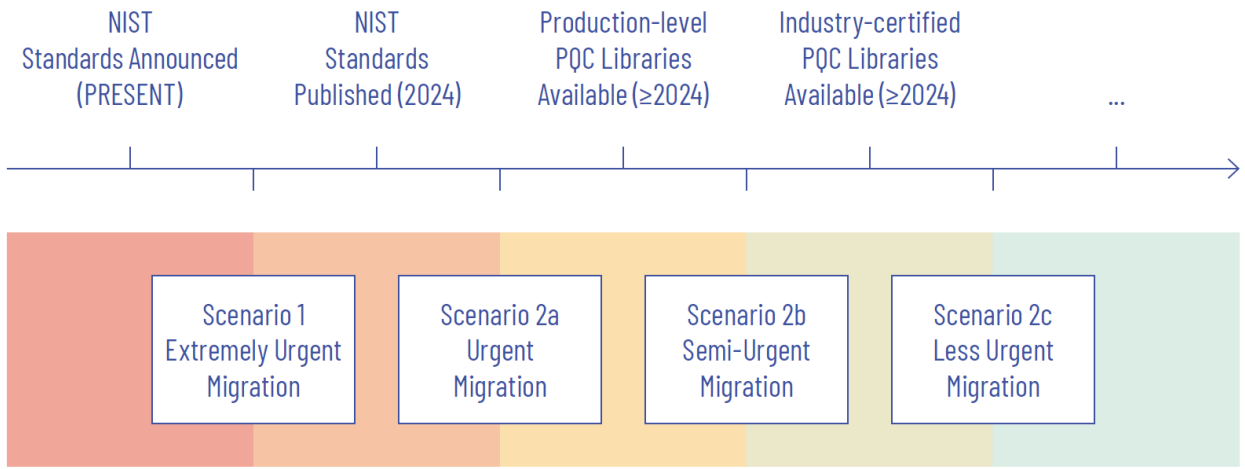
- Estimate Z on expert information and own risk appetite



- Urgent adopters:
  - Store-now-decrypt-later: larger X due to loss of control over encrypted information
  - Long-lived systems: larger X due to difficulty of migrating hardware/systems
  - Vital infrastructure: smaller Z

PLANNING
WHEN TO MIGRATE?

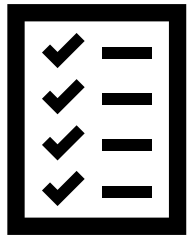
- Migration to be planned under 4 possible scenarios:

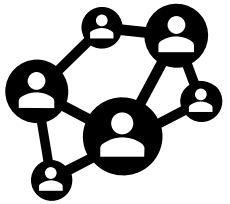


- Migration equation: $X + W_i + Y_i < Z$:
  - Z: Time until old public-key crypto can be broken by a sufficiently large quantum computer
  - X: Time that information/systems need to stay protected
  - W_i: Waiting time until scenario i
  - Y_i: Migration time under scenario i

PLANNING
ORGANISATIONAL PLANNING

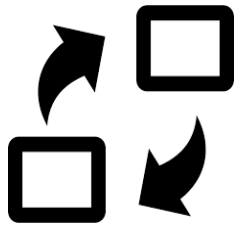
- Establish migration team
  - Migration manager with knowledge and access of overall organisation
  - 5-10 other people depending on size of organisation
- First steps migration team
  - Diagnosis
  - Prioritize assets to be migrated
  - Draw up migration plans
- Sufficient budget should be allocated for necessary migration steps
  - Financial & facilities resources
  - Time: Expect several years for the migration
- Interoperability: consider planning migration with community of similar and/or connected organisations

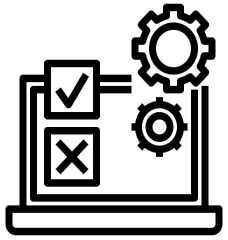




PLANNING
TECHNICAL PLANNING

- Identify *dependency of assets*
  - Decide order of migration
  - Maintain interoperability through 2 stages: PQC opportunistic ⇒ PQC mandated
- For each asset decide to either: *Replace*, *Redesign*, *Retire* (or something else)
- *Replace* or *Redesign*: choose which PQC depending on asset & usecase
- *Replace hardware* where needed
  - Acquisition, availability and deployment time should be taken into account
- In some cases *isolation of data/systems* is needed for protection
  - Especially against immediate store-now-decrypt-later protection
  - Temporary during switch-over to PQC
  - When timely migration is too costly
- *Test*, *test*, *test*

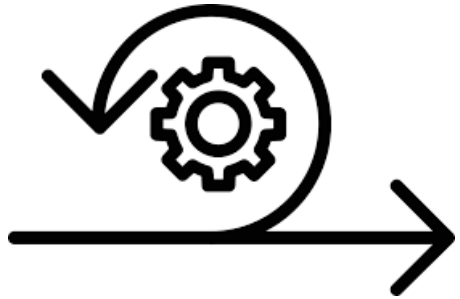




EXECUTION
GENERAL STRATEGIES

Cryptographic agility

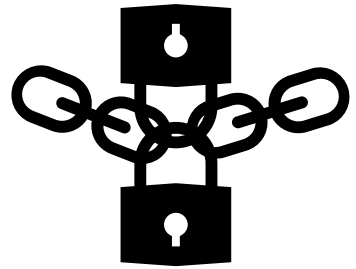
- Implement cryptography such that changes to cryptography can be made
  - Without significant changes to the systems
  - Without exposure to significant risk
- Why?
  - Need to change algorithms now, but future changes possible:
  - PQC is relatively young: better schemes, parameter tweaks, implementation bugs
  - Modernize cryptography, streamlined reporting, reduce risk of cryptographic failure
- Requires structuring people, processes and technology
  - Abstract cryptographic functionality from application code
  - Enforce crypto agility for new or updated systems
  - Integrate crypto agility in CI/CD systems



EXECUTION
GENERAL STRATEGIES

Hybrid solutions

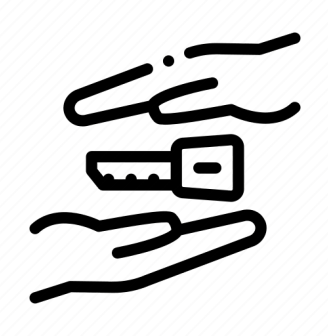
- Use PQC together with existing cryptographic standards
- Hydrid-AND: ‘Strongest link’ security
  - Attacker needs to break both algorithms
  - PQC protects against quantum attacks, while existing secure implementations are very mature
- Especially recommended for organisations that migrate under the early scenarios (1, 2a, 2b)
- Be careful for Hybrid-OR: ‘Weakest link’ security
  - Advertised hybrid solutions might use hybrid-OR instead of hybrid-AND
  - Opportunistic use of PQC for *backwards compatibility*
  - Introduces risk of *downgrade attacks*: security can be degraded to weakest option



EXECUTION
GENERAL STRATEGIES

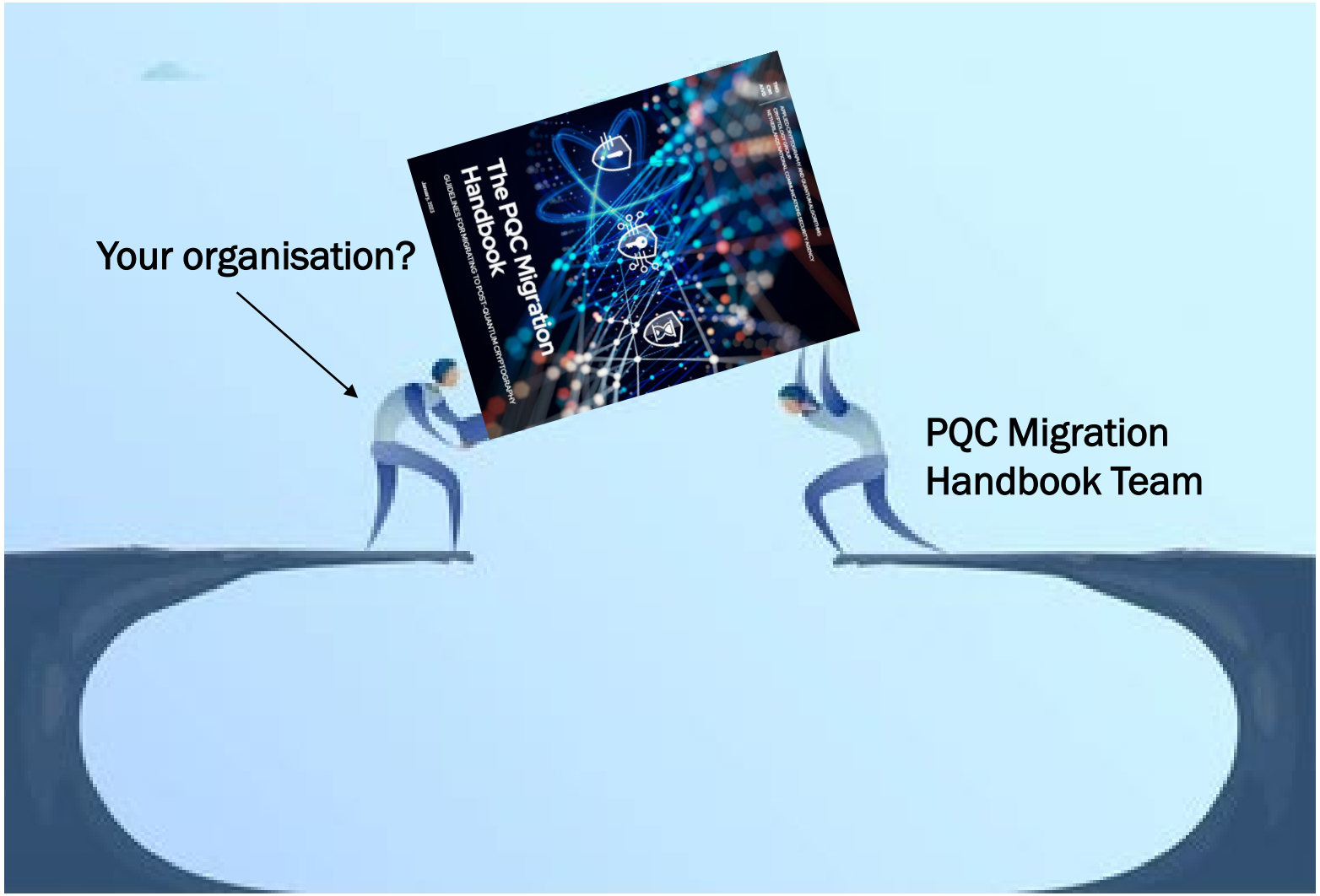
Pre-Shared Keys (PSKs)

- Use symmetric cryptography with PSKs
  - Replaces asymmetric cryptography entirely
- Pre-shared keys need to be established in physical way (courier, …)
  - Cumbersome process and scales badly
- Mostly applicable to very stringent cases:
  - Systems are fully controlled and trusted by organisation
  - There is a practical way of sharing secret keys
  - Adding or removing nodes happens rarely



THE PQC MIGRATION HANDBOOK

BRIDGING GAPS



THANK YOU
QUESTIONS?

Matthieu Lequesne

Marc Stevens

Thomas Attema

João Faria Miranda de Duarte

Vincent Dunning

Ward van der Schoot

TNO innovation for life

CWI

Email: ward.vanderschoot@tno.nl