Post-Quantum

Cryptography Conference

A structured approach to the quantum-safe transformation

Efstathia Katsigianni
IBM Quantum Safe Project Executive at IBM Research & Development

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

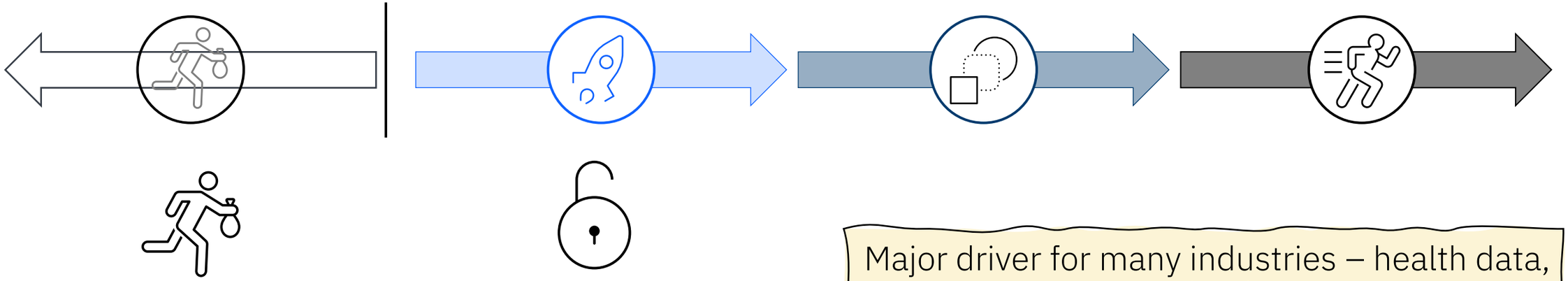
A structured approach to the quantum-safe transformation

Dr. Efstathia Katsigianni
IBM Quantum Safe Project Executive
IBM Research

PKI Consortium Post-Quantum Cryptography Conference

Kuala Lumpur, 29th October 2025

Primary threats and drivers



Harvest confidential data
in order to decrypt them later

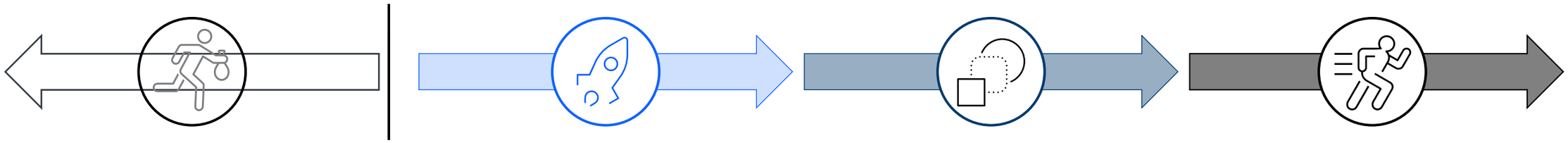
Decrypt lost or harvested confidential data through stealing encryption keys

Major driver for many industries – health data, governments, private banking

Requires targeted actions for risk mitigation

Requires prioritization; which are the data that are highly sensitive & exposed?

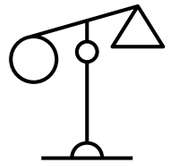
Primary threats and drivers



Complex multi-year project, whole business ecosystem affected

Remediation needs establishing a foundation for efficient, controlled, risk-based execution, in line with current ways of working

Manipulate firmware updates & transactions through fraudulent **authentication**



Manipulate digitally signed contracts & legal history by **forging digital signatures**

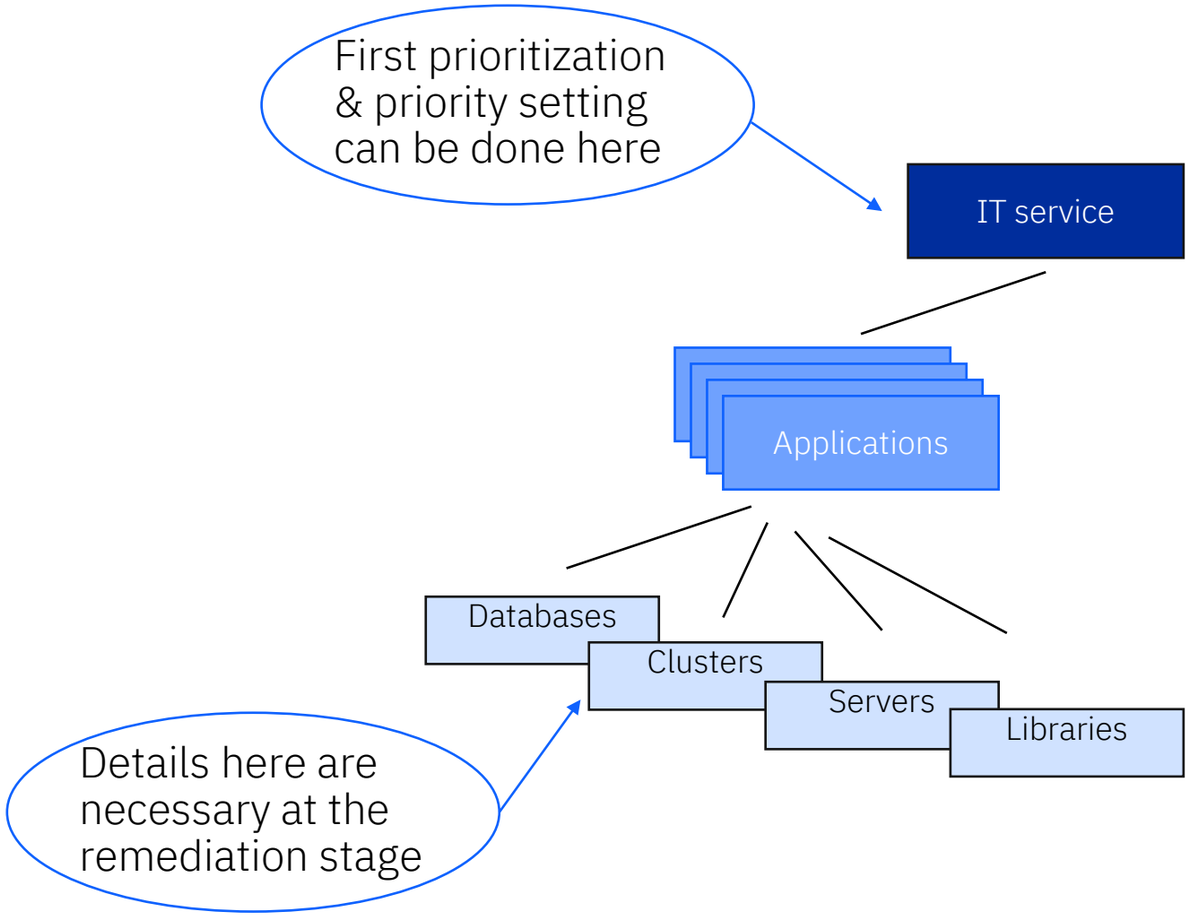
High relevance for industries, such as government, banking, insurance

Transformation key constraints

A typical organization faces many challenges from the beginning of their Quantum Safe transformation:

- Obtaining management buy-in & getting mandate to act
- Defining responsibilities, finding the right information
- Prioritizing activities against normal business & against other security threats
- Being able to “absorb” the extent of necessary activities
- “Distractions”

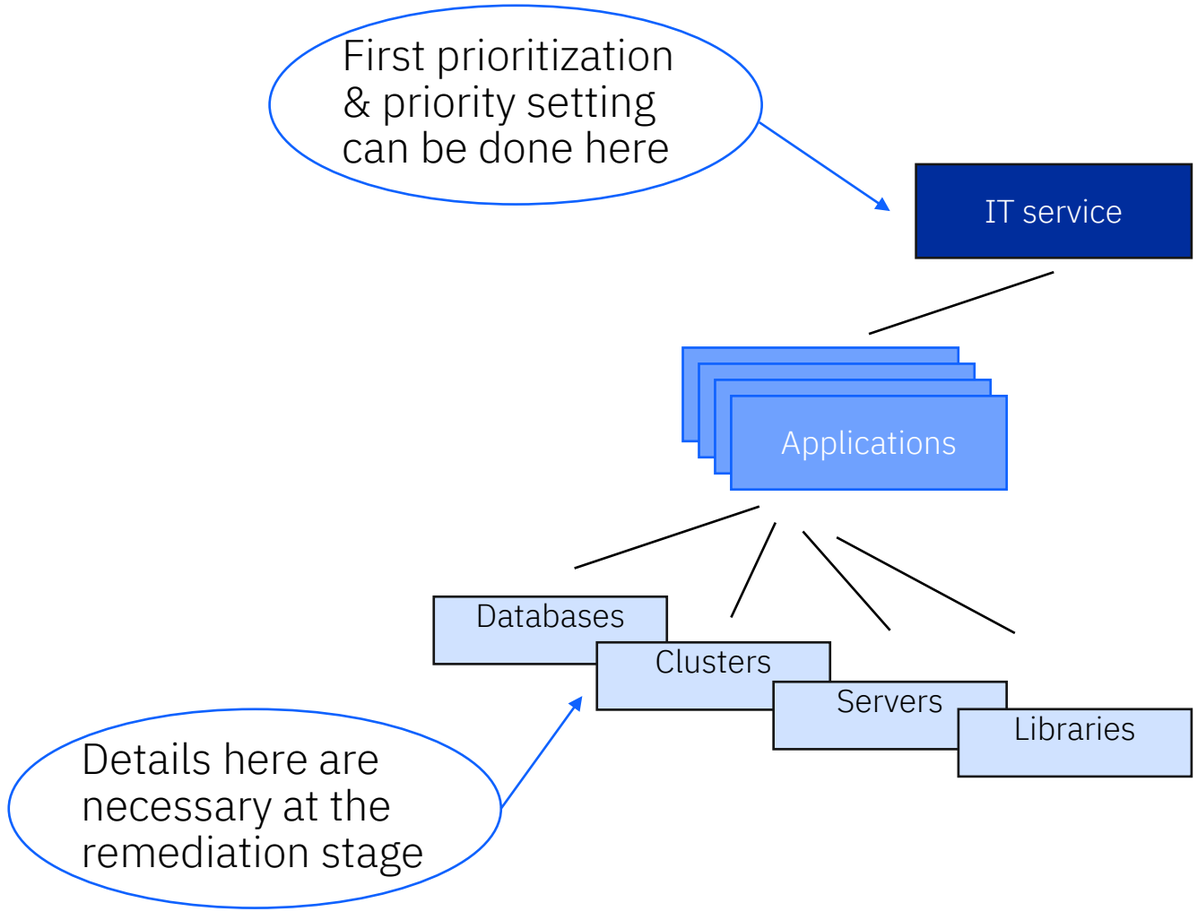
Where to start?



Initial focus was set by many on a *detailed inventory* for cryptography in the network and source-code, but:

- Using the collected insights is hard without context – they often do not help to make a plan
- Very high initial effort with limited gains – outdated fast
- You can easily “miss the forest for the trees”

Where to start?



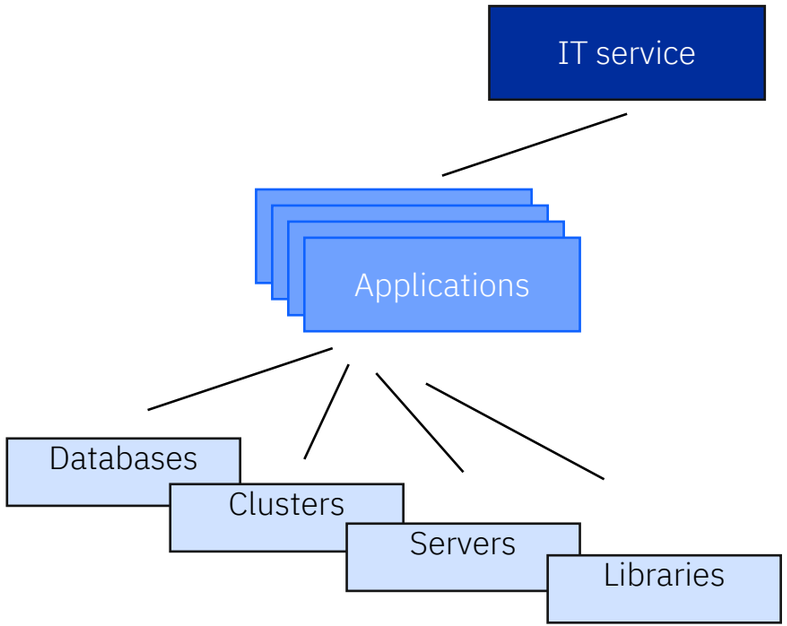
Prioritization should be driven by business criticality of an asset – this information is often gathered and can be done on IT Service level

Focusing on **external** critical flows, it is possible to define urgent actions

Analysis & remediation actions will be in any case be directed to the respective service owner (teams)

Identify **dependencies** in more and more depth during the transformation to drive the migration planning

Focus on a high-level cryptographic inventory



Understand the highly critical elements affected, within:

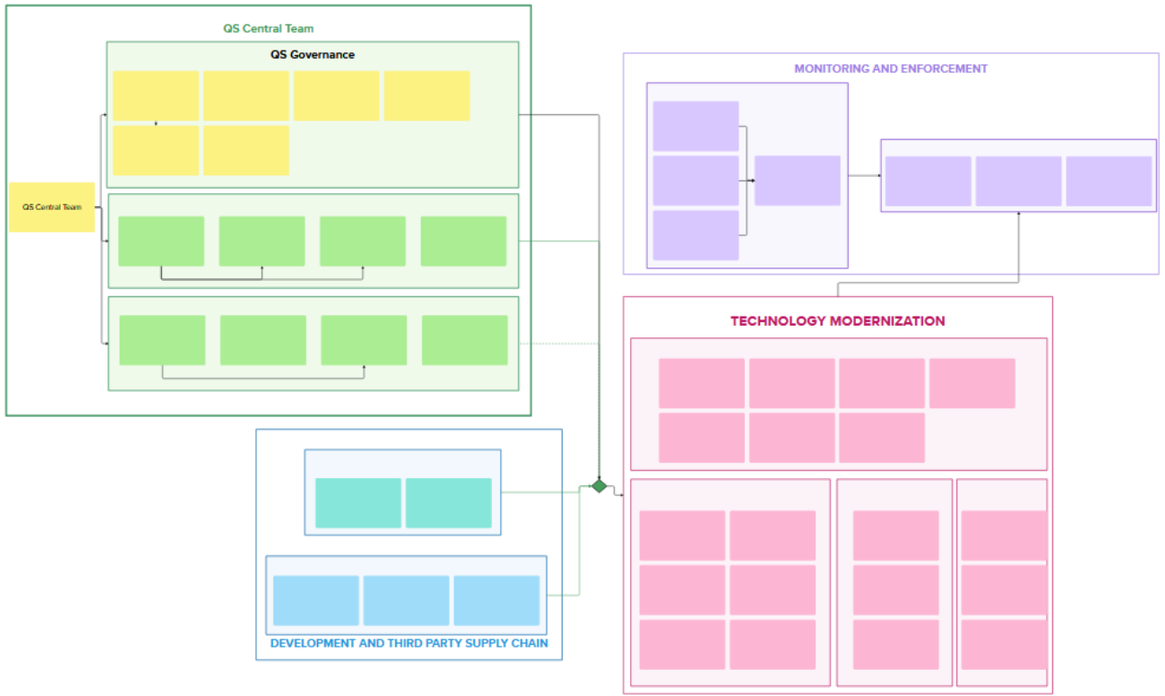
- Policies & standards (cryptographic governance)
- PKIs & Key management systems
- IT Services/Applications/Products
- Network architecture
- Infrastructure

Use the insights to understand, quantify, and communicate effort of the actual transformation

Create a blueprint of necessary capabilities

There are 4 key categories, into which actions are often divided:

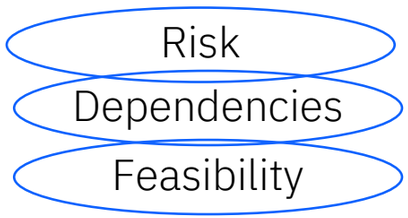
- **Centrally-driven**: fundamental capabilities that are ideally driven by a Quantum Safe Central Team.
- **Development & 3rd Party Supply Chain**: includes the pre-requisites for technology modernization both from the point of view of *internal development* practices as well as *3rd party requirements*.
- **Technology Modernization**: covers the migration of technology infrastructure, systems, and applications to Quantum-safe algorithms.
- **Monitoring & Enforcement**: involves continuously observing systems, networks, and applications to identify remaining quantum unsafe cryptography and related vulnerabilities as well as the retirement of non-QS cryptography.

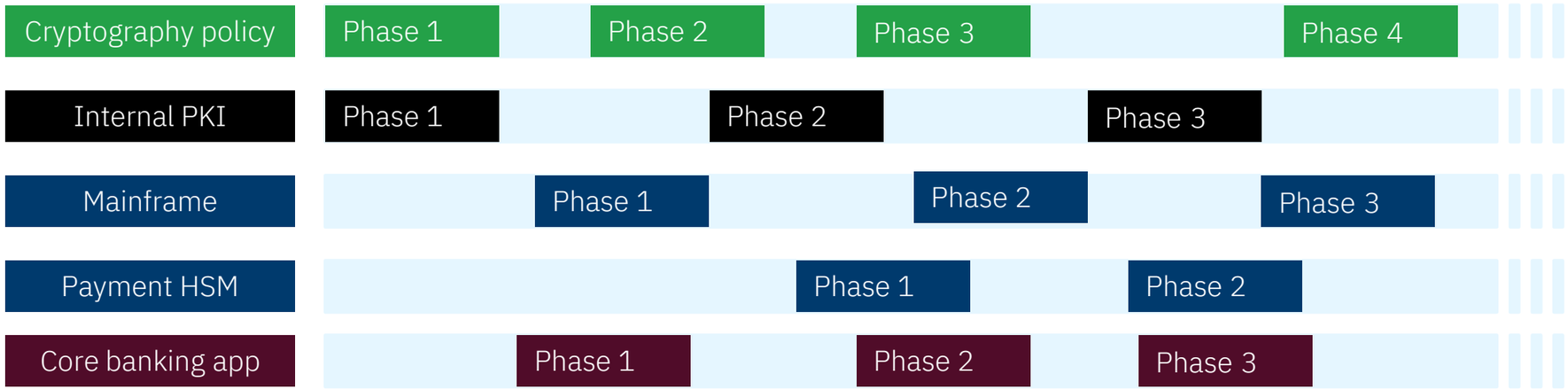


Create an agile transformation roadmap

The transformation plan needs to be **constantly refined and adjusted**

Periodical actions in fundamental domains will be necessary throughout this transformation





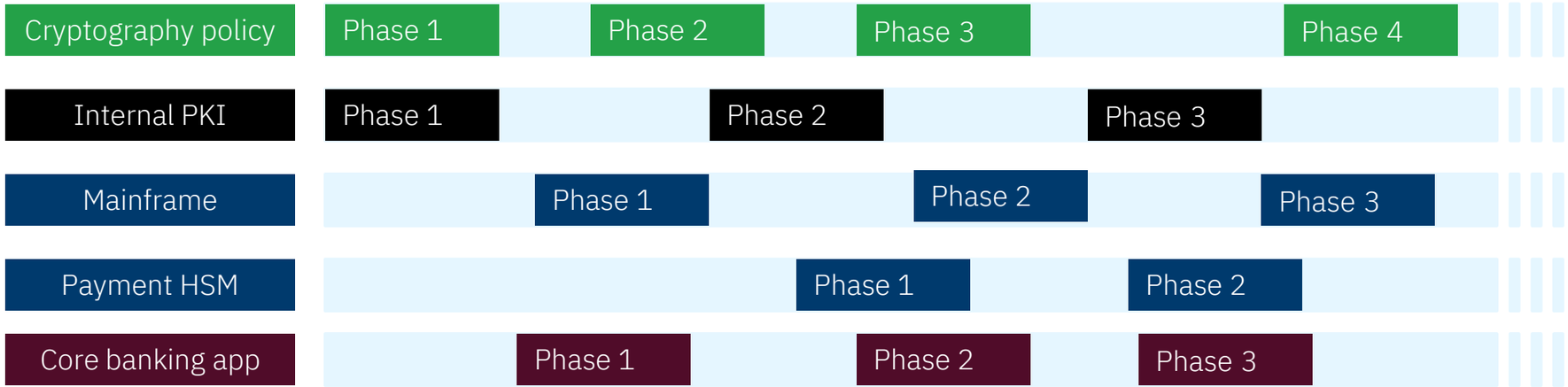
Execute in line with ways of working in the organization

Align changes with normal product update cycles

Use architectural ‘remediation patterns’

Create central guidance for application teams

Set-up processes for alignment and monitoring of actions



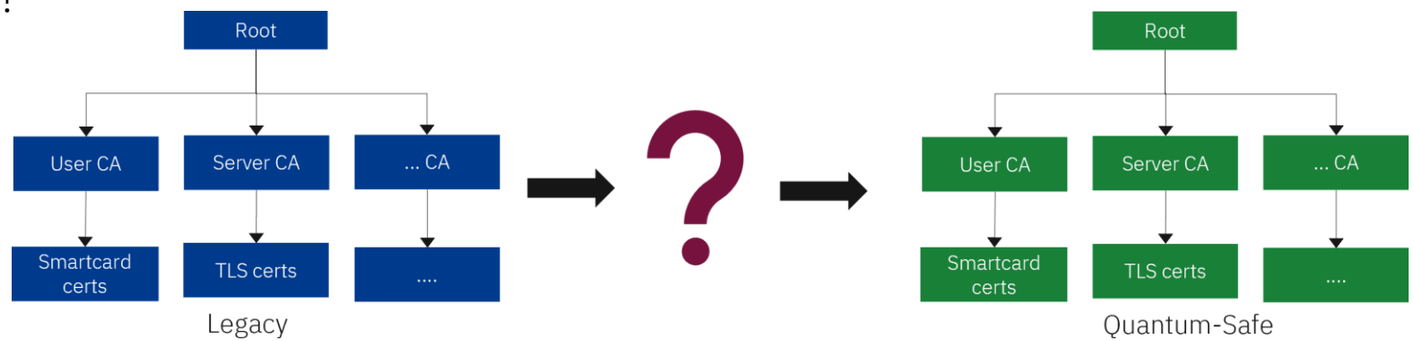
Key focus area examples – Public Key Infrastructures

What kind of an intermediate PKI is needed until a purely QS-PKI can be used?

What is the solution that can make adoption as *fast* as possible & management as *simple* as possible?

How and when are the use-cases in scope of the PKI going to migrate to using quantum-safe certificates?

Not all „**hybrids**“ are the same and not all are always needed – often a parallel PKI approach is enough



Key focus area examples – Cryptographic agility

Organizations starting early have a chance to make this transformation in a more efficient and ‘agile’ way – even use this chance to address broader cryptographic issues

But …

This involves much more than creating a cryptographic inventory – *long-lasting changes* in processes, guidance, and cryptographic governance

You may spread *resources* thin to make every aspect of cryptographic governance perfect all at-once

Crypto agility involves *cost and potential risks*

You *don’t need to be perfectly agile* in order to start or go through the Quantum Safe transformation

Key focus area examples – Cryptographic agility

Organizations starting early have a chance to make this transformation in a more efficient and ‘agile’ way – even use this chance to address broader cryptographic issues

Organizations should start with:

➔ defining how much they actually need

➔ adding requirements to internal guidelines (own-development) - periodically

➔ adding requirements to procurement artefacts – RfPs - periodically

Key take-aways

Organizations need to identify their **critical** assets and prioritize their efforts

Industry experience is valuable, should be shared and re-used

Cryptography is difficult to replace – a **central team** approach is required to manage the complexity & give guidance

If quantum-safe is seen as part of the overall **cryptographic governance**, these efforts will not be “wasted”


IBM