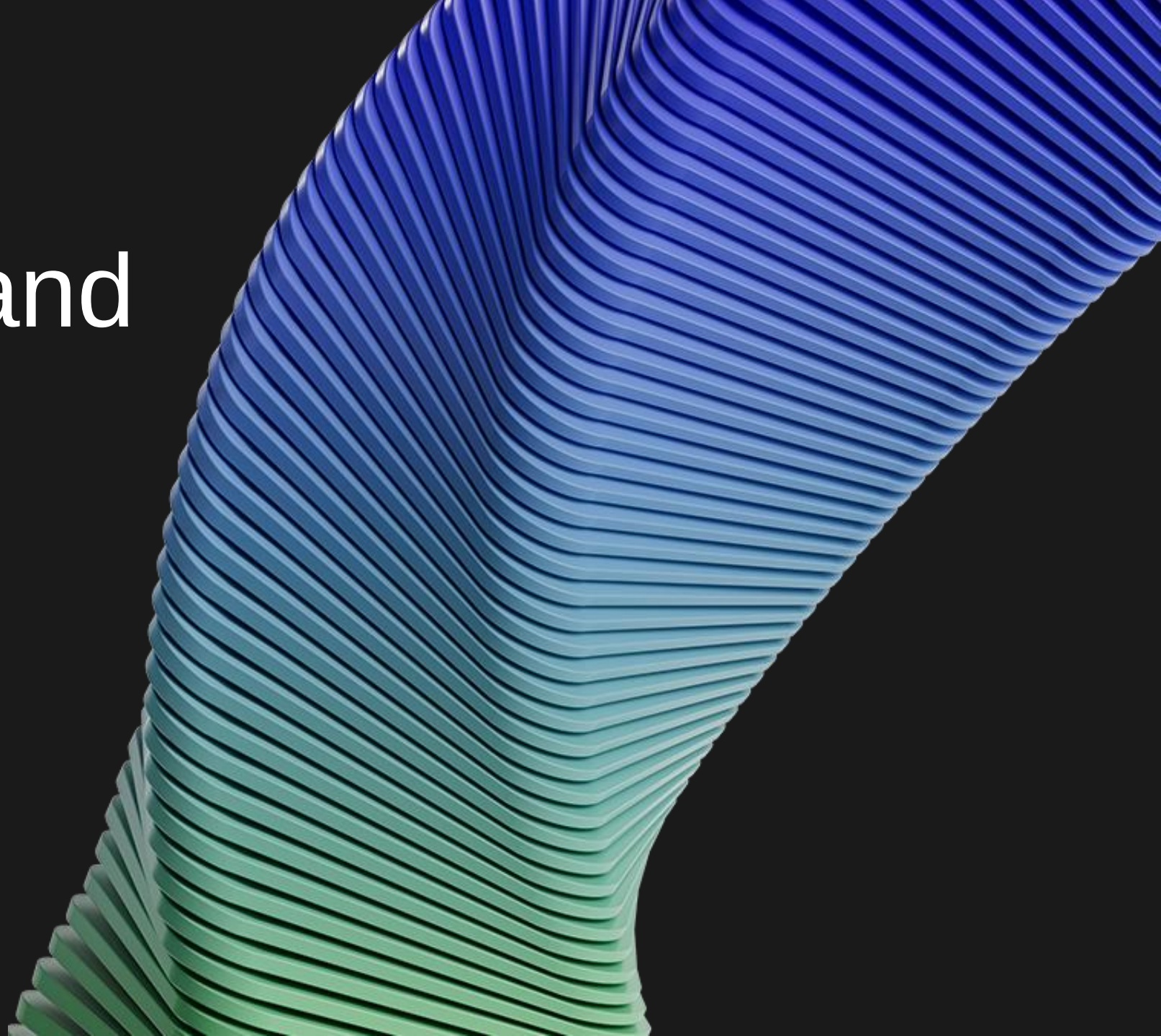
# Tackling new compliance requirements, with crypto agility and infrastructure modernization


Tomas Gustavsson

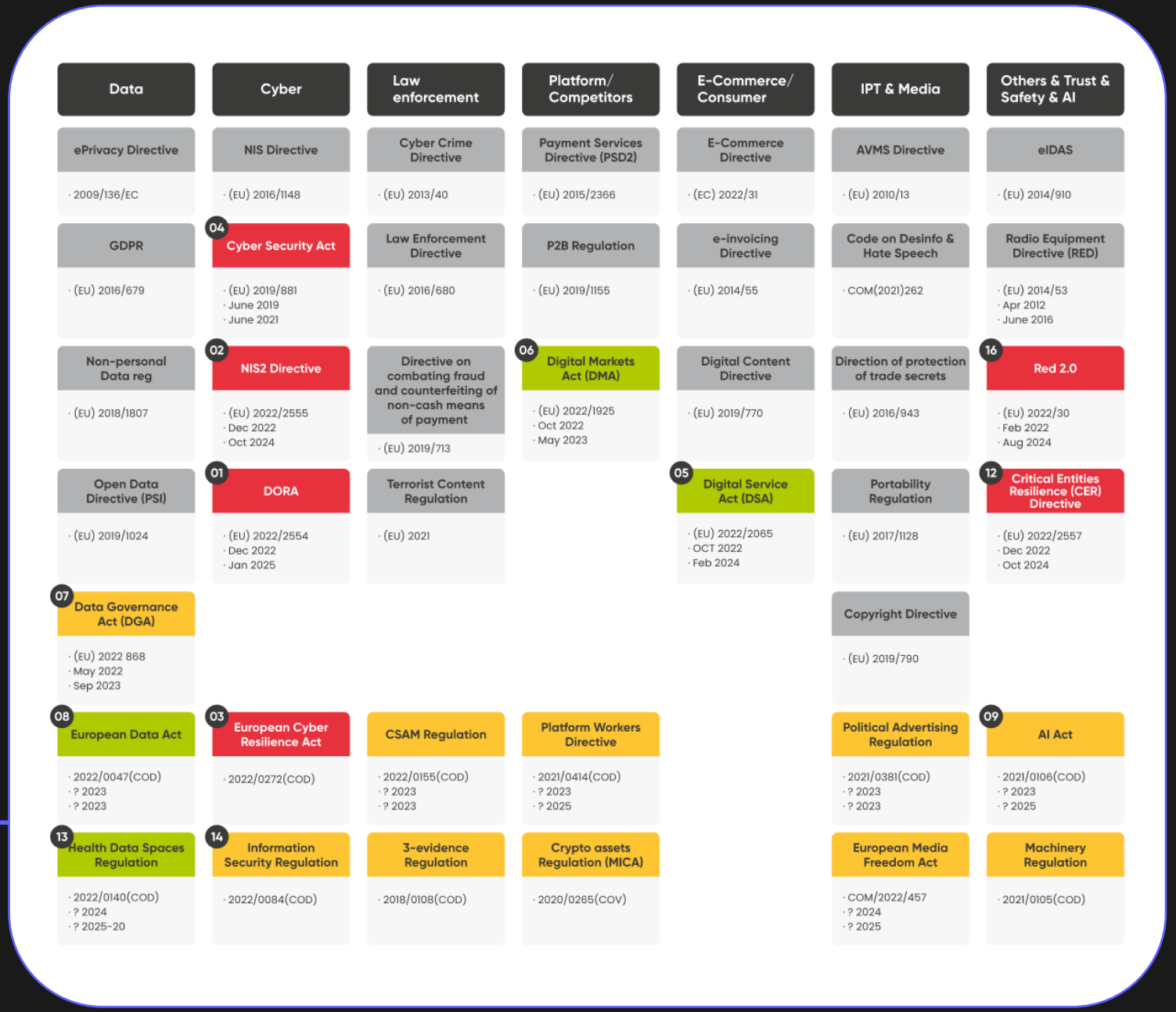
Chief PKI Officer KEYFACTOR


# Regulatory Landscape and Compliance



KEYFACTOR

# Regulatory Landscape (EU)




Impact on Cyber Security Requirements: Low | Medium | High

01. The Digital Operational Resilience Act - (DORA)
02. The NIS 2 Directive
03. The European Cyber Resilience Act - (CRA)
04. The Cybersecurity Act
05. The Digital Services Act - (DSA)
06. The Digital Markets Act - (DMA)
07. The European Data Governace ACT - (DGA)
08. The European Data Act
09. The Artificial Intelligence Act
10. The European ePrivacy Regulation
11. The eIDAS Regulation
12. The Critical Entities Resilience Directive - (CER)
13. The European Health Data Space - (EHDS)
14. The EU Information Security Regulation
15. The EU Cybersecurity Regulation
16. The Red Delegated Act

KEYFACTOR

# DORA

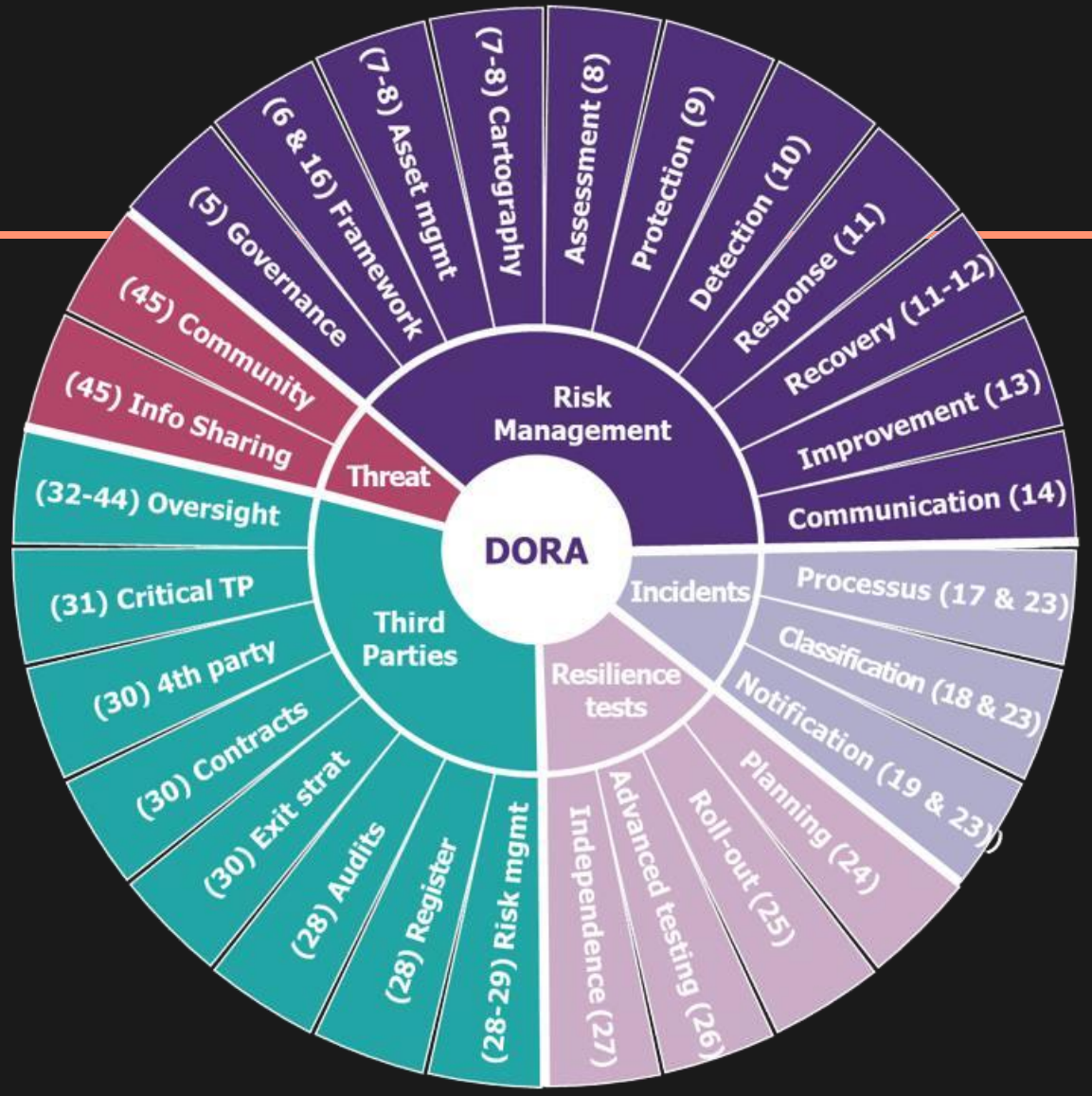
**01**
ICT risk management

**02**
ICT-related incident management, classification and reporting

**03**
Digital Operational resilience testing

**04**
Managing of ICT third-party risk (supply chain)

**05**
Information and intelligence sharing (see NIS2)




KEYFACTOR

# CRA

**01**
Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;

**02**
Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;

**03**
Enhance the transparency of security properties of products with digital elements, and,

**04**
Enable businesses and consumers to use products with digital elements securely.

KEYFACTOR

# NIS2

Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

KEYFACTOR

# NIS2

Article 21 (2) “Cybersecurity risk-management measures”

(2) The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

KEYFACTOR

# ICAO

## Doc 9303

## Machine Readable Travel Documents (MRTDs)

Part 1: Introduction

Part 2: Design, Manufacture and Issuance

Part 3: Common Specifications

Part 4-6: Machine Readable Passports and Travel Documents

Part 7: Machine Readable Visas

Part 8: Emergency Travel Documents

Part 9: Biometric Identification and Electronic Storage of Data in eMRTDs

Part 10: Logical Data Structure (LDS)

Part 11: Security Mechanisms for MRTDs

Part 12: Public Key Infrastructure

Part 13: Visible Digital Seals

KEYFACTOR

# CA/B Forum

**01**
A voluntary gathering of Certificate Issuers and suppliers of Internet browser software and other applications that use certificates (Certificate Consumers).;

**02**
The CA/Browser Forum advances industry best practices to improve the ways that certificates are used to the benefit of Internet users and the security of their communications;

**03**
The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates describe a subset of the requirements that a certification authority must meet in order to issue digital certificates for SSL/TLS servers to be publicly trusted by browsers;

**04**
WebTrust for CAs:
SSL, Code Signing, S/MIME, Network Security.

# CA/B Forum

What's new?

- Linting
- Weak-keys
- S/MIME
- Code Signing
- Validation / CAA / CT
- QWAC

KEYFACTOR

# CA/B Forum

What is so scary?

- Hundreds of details that must be followed, technical and procedural
- A failure in one aspect results in Misissuance
- Hard revocation requirement (24h – 5 days)
- No flexibility

KEYFACTOR

The core topic today

# *So, you need Crypto Transparency*

PQC: to replace keys and upgrade ciphers you should first find them
→ Can be scoped with IT-ownership
→ No owner = no fix (no budget anyway)

NIS2: all assets and services you depend on are in scope for compliance

→ This includes your shadow IT and your supply chain

→ The hardest part in NIS2 – things that should be encrypted, but aren’t

**This shouldn’t be an IT-project; it is a security process**

KEYFACTOR

# More Use Cases – More CAs

- Zero Trust
- TLS/mTLS
- Code / Container signing
- Service Mesh / SPIFFE
- SBOM Attestations
- Wallets

- Matter / IoT / Manufacturing
- Point PKI Solutions
  - Off-load to a "real" PKI

Any RSA, EC, Ed25519, DH, ECDH will change.

Avoid sub-optimization!

KEYFACTOR


Recent
Incidents
KEYFACTOR

# Entrust

## Distrusted by Chrome and Mozilla

Google's decision to part ways with Entrust's public certificate authorities (CAs) is due to an *"observed pattern of compliance failures, unmet improvement commitments, and the absence of tangible, measurable progress in response to publicly disclosed incident reports."* Digital certificates have been mis-issued which has led to overall security implications.

While unfortunate, Google's response is intended to preserve the integrity of Web public key infrastructure (PKI). In today's increasingly digital world, PKI is critical to protect the confidentiality and authenticity of communication between web browsers and web content servers. PKI is what ensures digital trust in our online world.

KEYFACTOR

# DigiCert

## Revokes >83000 certificates

DigiCert has asked customers to replace SSL and TLS certificates due to strict CA/Browser Forum (CABF) regulations.

On July 30, DigiCert publicly disclosed the incident regarding incorrect certificate issuance, making the revocation necessary. According to DigiCert, the root cause was traced to a malfunctioning system of the certificate authority, which resulted in the issuance of certificates without non-compliant validation checks.

The revocation affects more than 6800 customers, including organizations in critical infrastructure sectors.

KEYFACTOR

# What can we learn?

**01**
The importance of CA-agility;

**02**
The critical need for crypto-agility. For end points where publicy PKI is needed a high level of crypto-agility and automation is needed in order to avoid disruptions;

**03**
Businesses shouldn’t put all their eggs in one public CA’s basket;

**04**
This situation is an early warning sign of what’s to come for post-quantum cryptography (PQC);

**05**
There are risks by using public CAs that many organizations may not have considered. Every CA may, and all larger CAs have, become subject to revocations due to compliance issues that are in most cases not security related;

**06**
If an organization can not be crypto-agile enough to handle unexpected revocations with tight deadlines, Private PKI should be used;

KEYFACTOR

# Public vs Private PKI

**01**
For some use cases, especially those involving external uses, publicly trusted PKI is an absolute must;

**02**
Private PKI is often the best choice for other use cases involving internal-only networks;

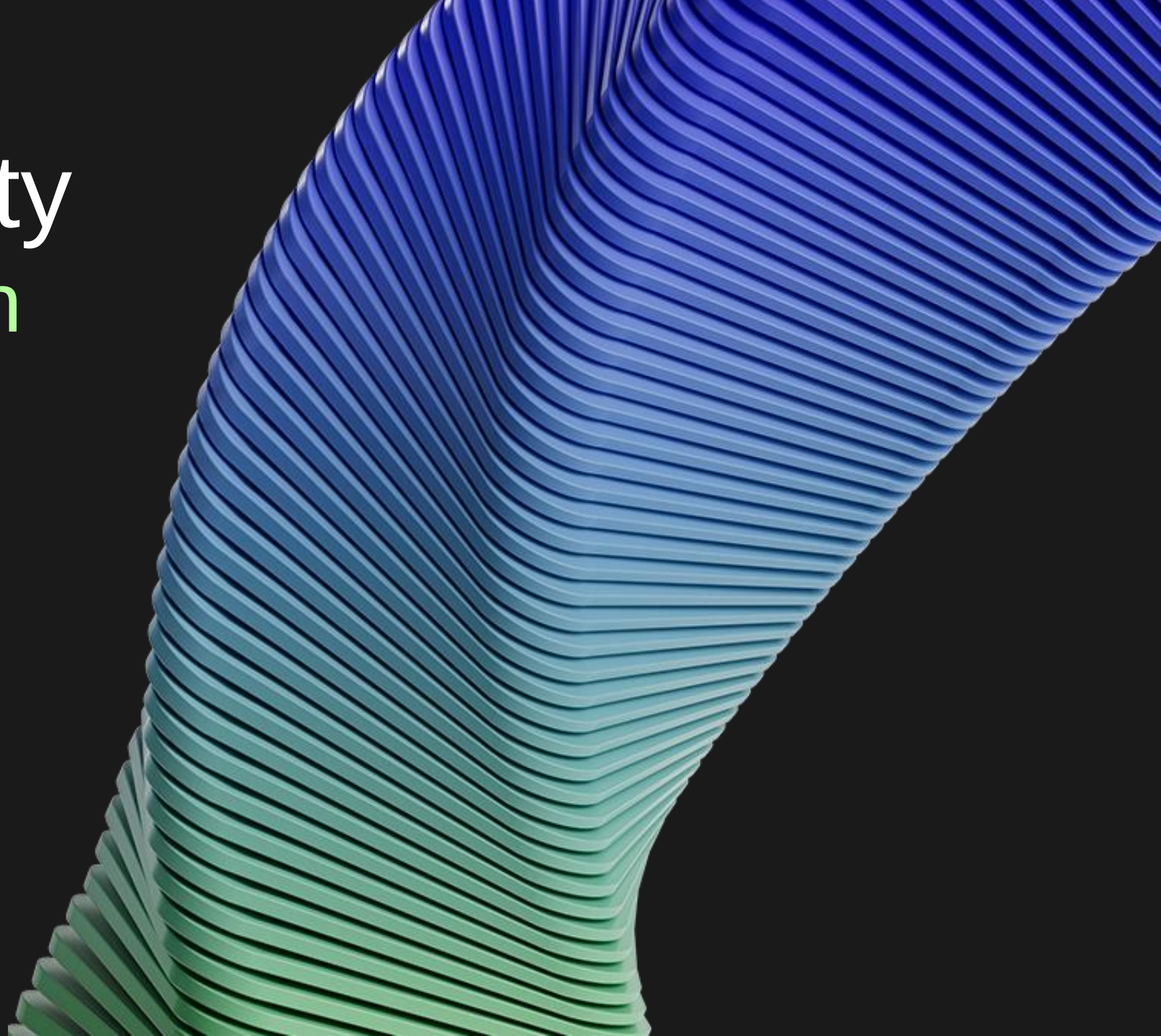
**03**
It is essential to have a high level of crypto-agility and automation to handle unexpected revocations with tight deadlines;

**04**
Having the ability to use multiple root CAs in parallel help by providing fall-back options;

**05**
If that level of crypto-agility is not possible (even with a fallback), a private PKI is likely the better option to ensure business continuity;

KEYFACTOR

# Crypto Agility
## where to begin



KEYFACTOR


~~Dilithium~~
ML-DSA / FIPS 204
~~Kyber~~
ML-KEM / FIPS 203
~~SPHINCS+~~
SLH-DSA / FIPS 205

KEYFACTOR

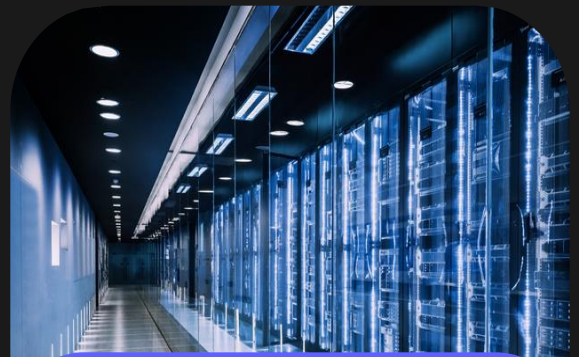
# What’s the story?

## Quantum is coming

Quantum computers are being developed by tech giants and nation states.

## That means new risks

These computers will be capable of cracking the algorithms we rely on today.



## We need new algorithms

New quantum-resistant algorithms are already here and was standardized in August 2024.

## It’s time to prepare

Making the transition to PQC will take years – the time to plan and prepare is now.

KEYFACTOR

# This is the starting point on the PQC migration journey.

- More new algorithms will come in the future.
- Maintaining crypto agility is a must.

KEYFACTOR

Recommendations

# Seize the Opportunity

1. Start now, 2030 is not far away
2. Design in crypto-agility - **updatability** of algorithms, keys, device identities, and Roots of Trust
    - Require crypto-agility by vendors, in procurement
    - All new development must be crypto agile
3. PQ Code Signing is a must
4. Use existing data classification to plan for an algorithmic changeover
5. Get an inventory of algorithms and keys you don't know

# Order of PQC Migration

**Confidentiality** → **Integrity** → **Identity**,

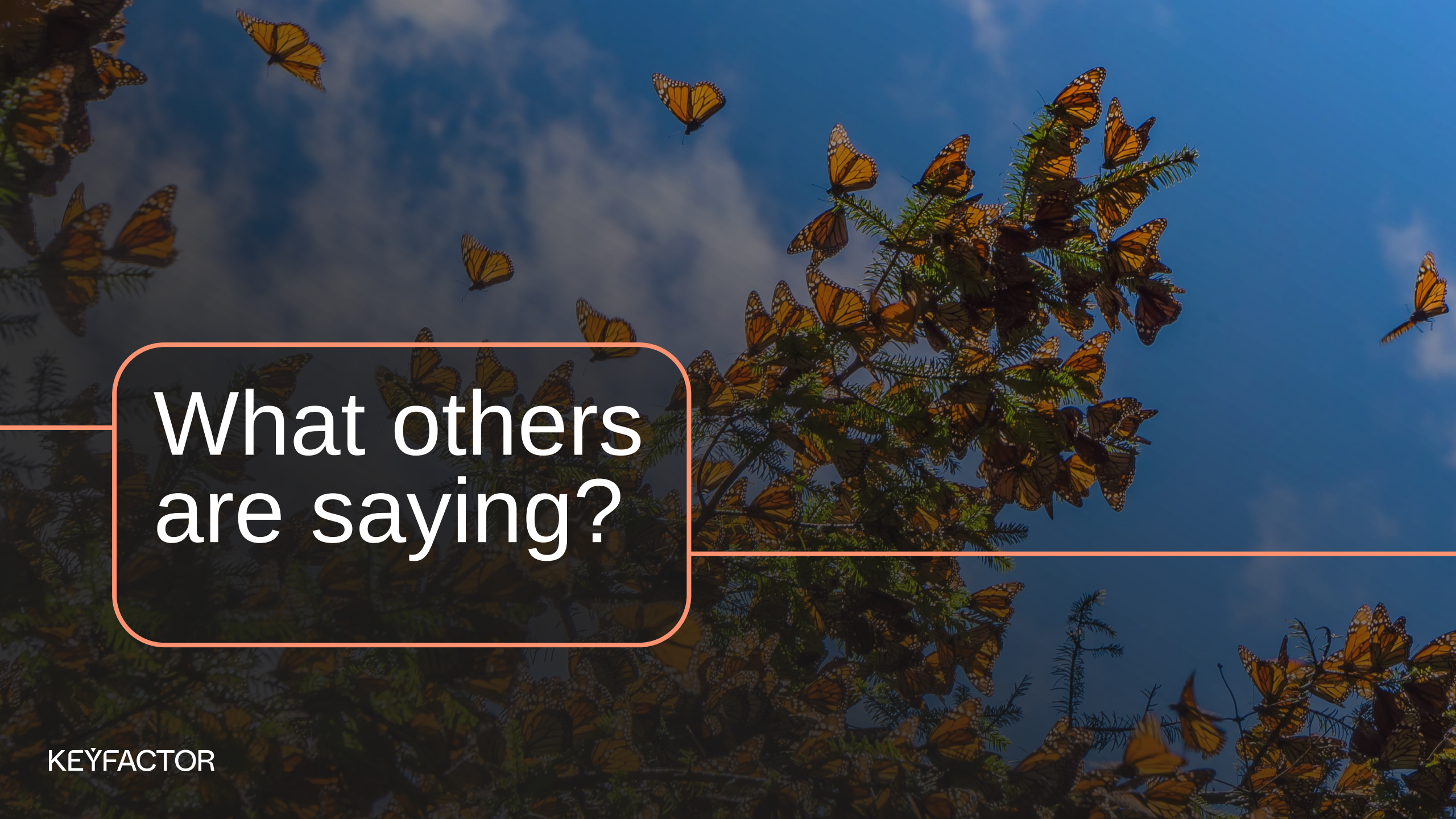
or

**Integrity** → **Confidentiality** → **Identity**
(depending on who you ask)

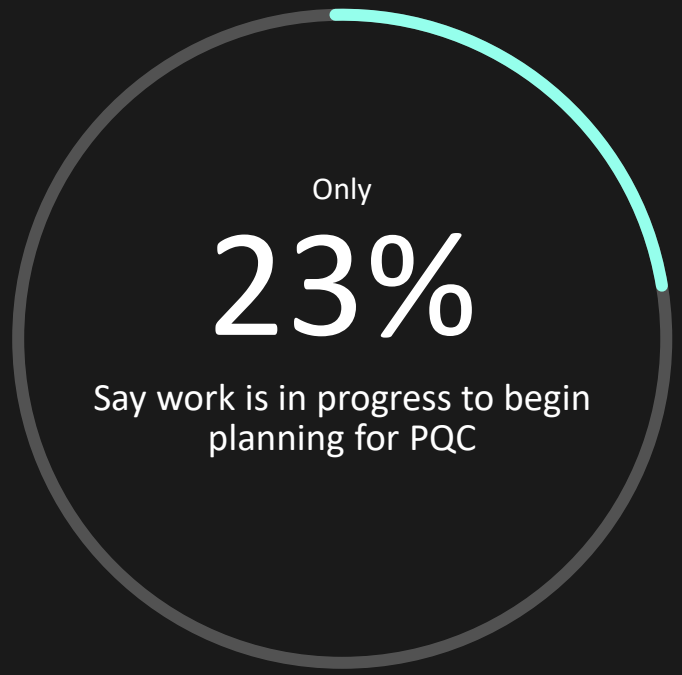
## Industries

- Government
- Regulated industries
  - Financial
  - Critical infrastructure
  - Telecom
  - Supply chain vendors
- *Everyone*

KEYFACTOR




KEYFACTOR




CISA

"Although NIST will not publish the new post-quantum cryptographic standard for use by commercial products until 2023, CISA and NIST strongly recommend organizations start preparing for the transition now"

KEYFACTOR


EU Commission

“

This Commission Recommendation 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.

The strategy should define clear goals, milestones, and timelines resulting in the definition of a joint Post-Quantum Cryptography Implementation Roadmap.

(See also ETSI TR QSC - A Repeatable Framework for Quantum-Safe Migrations)

https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

# There will be costs

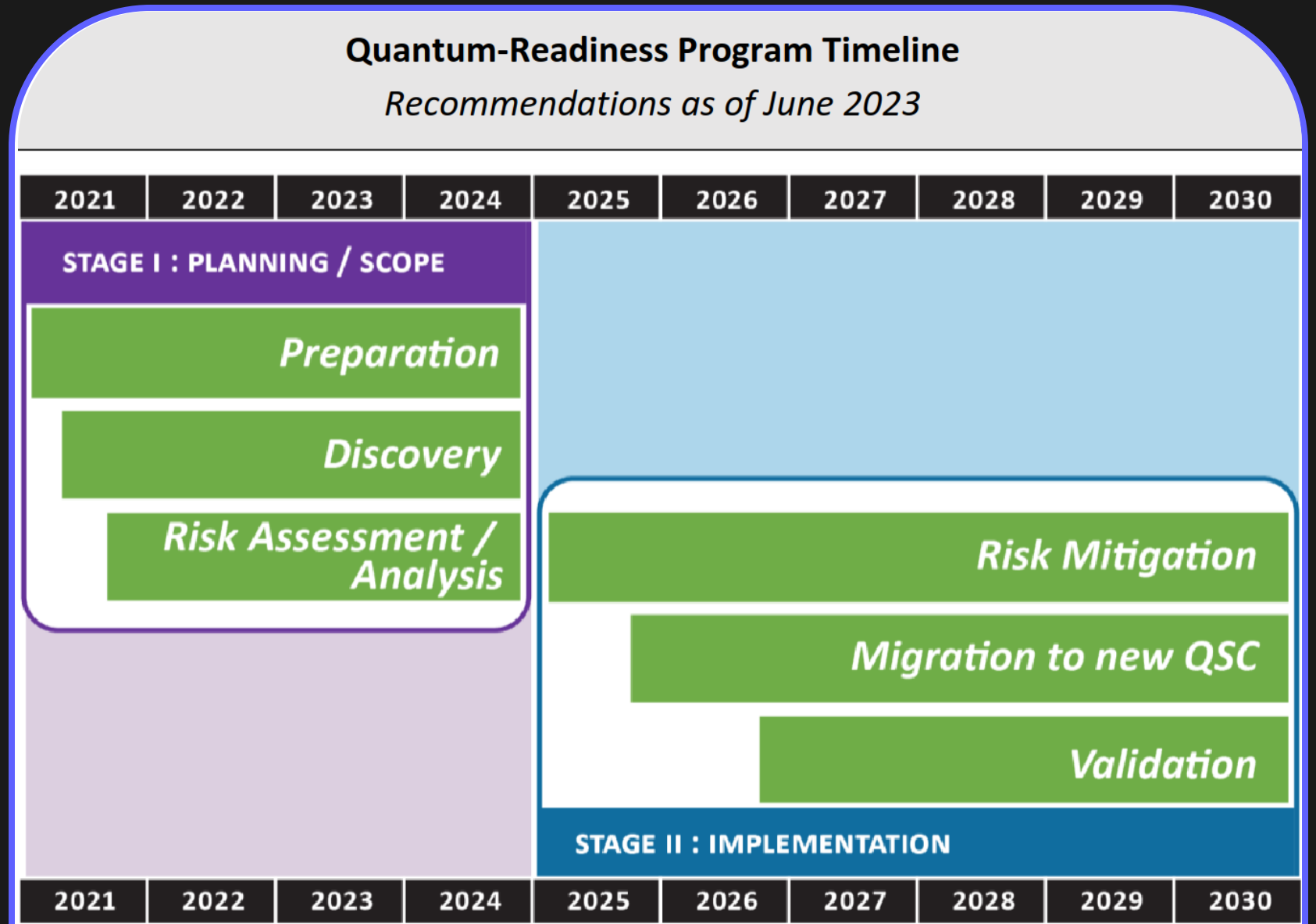
ONCD projects that that the total government-wide cost required to perform a migration of prioritized information systems to PQC between 2025 and 2035 will be approximately $7.1 billion in 2024 dollars.

Quantum Computing Cybersecurity Preparedness Act

White House report on post-quantum cryptography

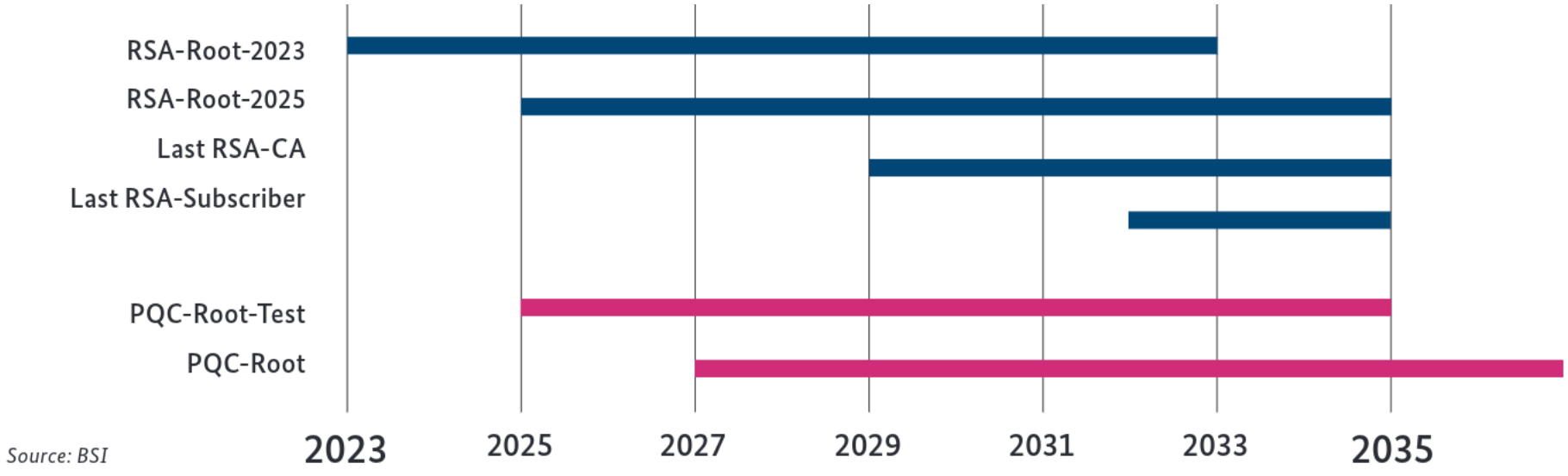
KEYFACTOR

# Canada, CFDIR




https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf

# Government Plans




Source: BSI

*Exemplary illustration of a migration with a parallel approach. The individual bars each represent validity periods, the certificate validation is carried out according to the shell model. In this example, it is assumed that a final RSA root will be issued in 2025 and that the root certificates will each be valid for ten years, the (sub)CA certificates for six years and the end-user certificates for three years. PQC stands for Post-Quantum Cryptography.*

KEYFACTOR

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2023-01.pdf
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf

# Gartner Post Quantum recommendations

**Why This Is Important**

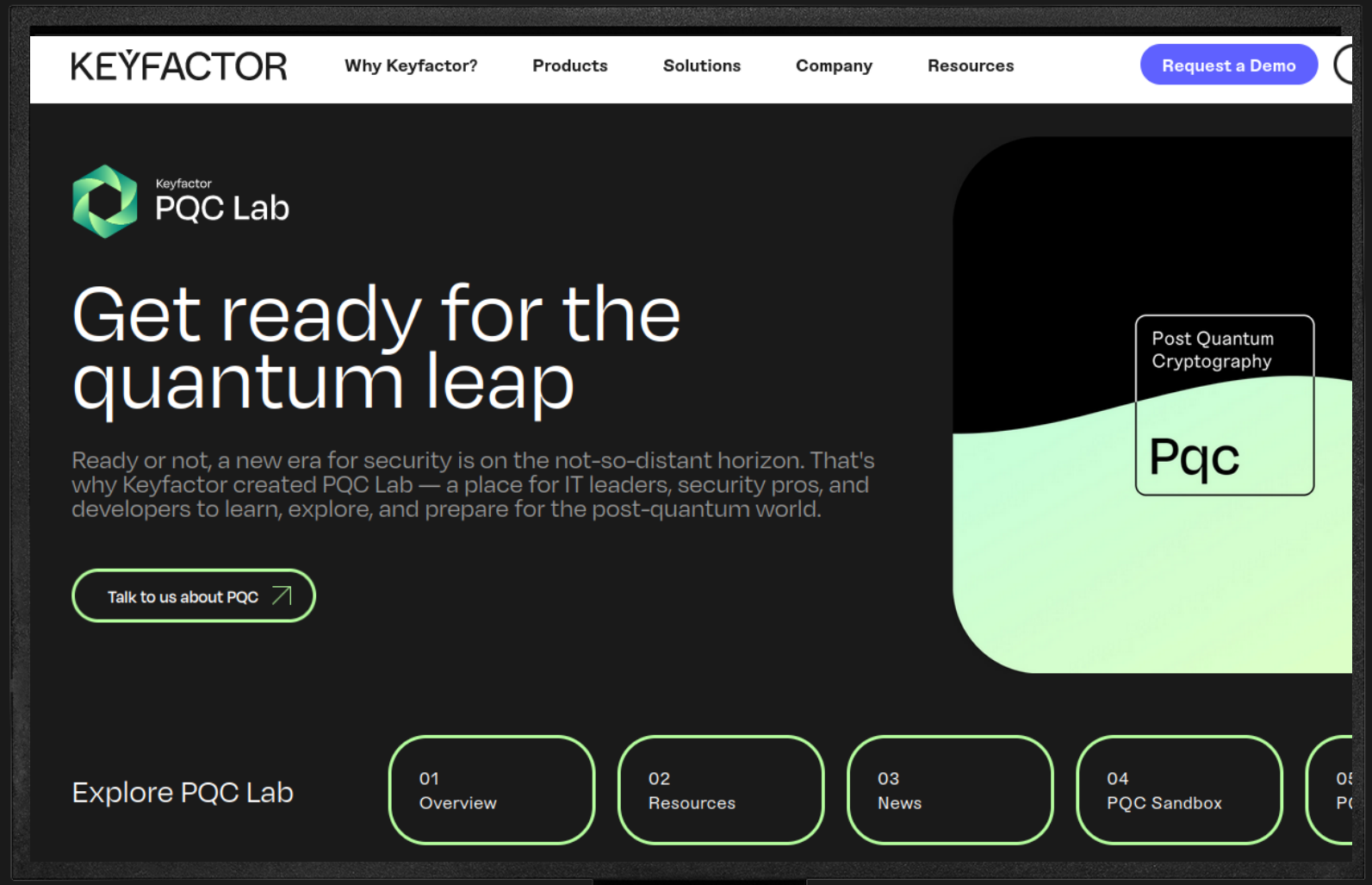
- Existing asymmetric algorithms like Diffie-Hellman, RSA and ECC are vulnerable and will be unsafe to use by the end of the current decade, requiring replacement for common cryptographic functions such as digital signatures, public key encryption, blockchains and key exchanges.
- PQC offers organizations a level of cryptographic protection, which will remain strong as quantum computers enter the mainstream.

**User Recommendations**

- Develop crypto policies for easing the transition to new algorithms. Adopting a policy-based program for cryptographic replacement will reduce confusion and arbitrary choices and increase manageability.
- Build a cryptographic metadata database of all in-use cryptographic algorithms. Use it to perform an exercise for data identifying the expected end-of-life targets in the short-, mid- and long-term time scales, and create a key life cycle policy to reflect risks to asymmetric keys.
- Implement crypto-agile application development and stage to production after extensive testing. Vet and test new PQC algorithms to understand their characteristics, uses and performance.
- Implement crypto-agility initiatives with an object-based approach to address future changes in PQC algorithm updates and replacement.

Keyfactor is one of Gartner's recommended Vendors in the post-quantum arena, within Gartner's Hype Cycle for Digital Banking.

Gartner®




https://www.keyfactor.com/post-quantum-cryptography-lab

KEYFACTOR

# Tomas Gustavsson

Chief PKI Officer KEYFACTOR

## Any Questions?

KEYFACTOR