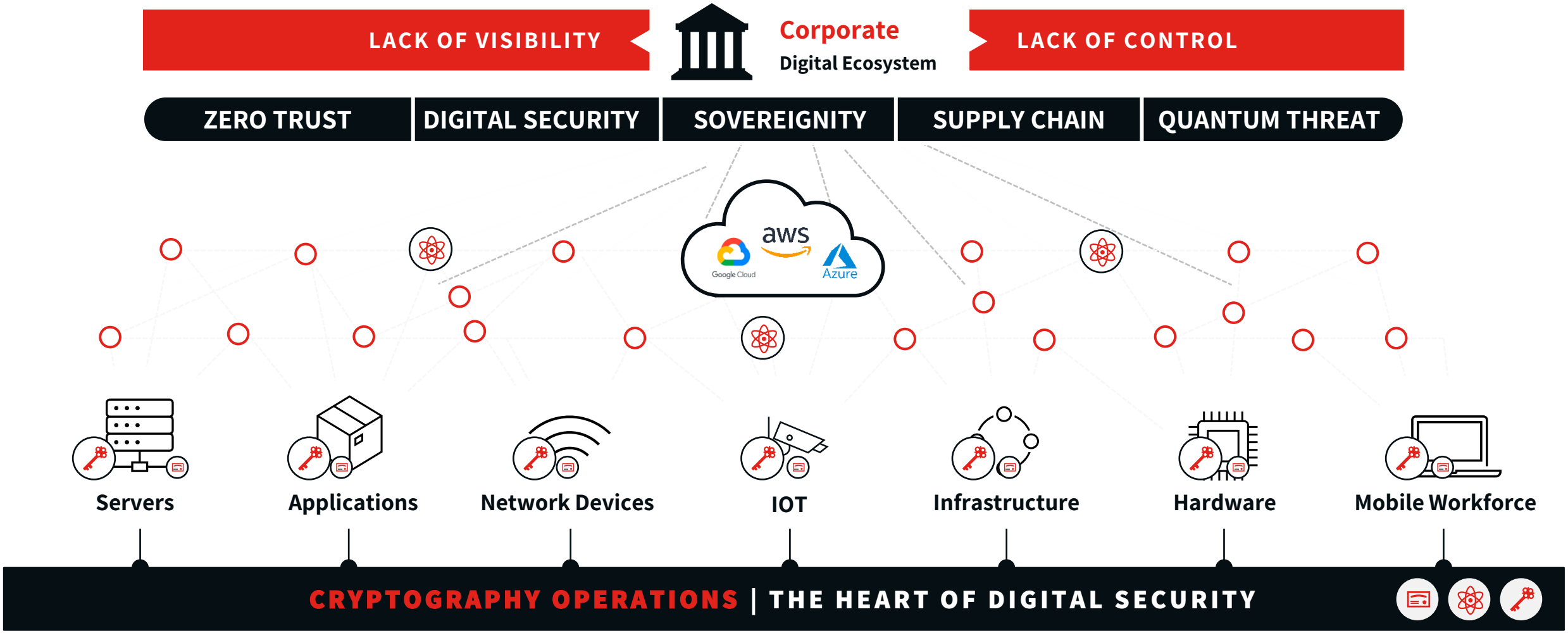
Cryptographic Lifecycle Management: Discovery and Agility

Discover, Remediate, Protect and Prepare for Migration

Dr. Vladimir Soukharev

Problem | Cryptography is everywhere

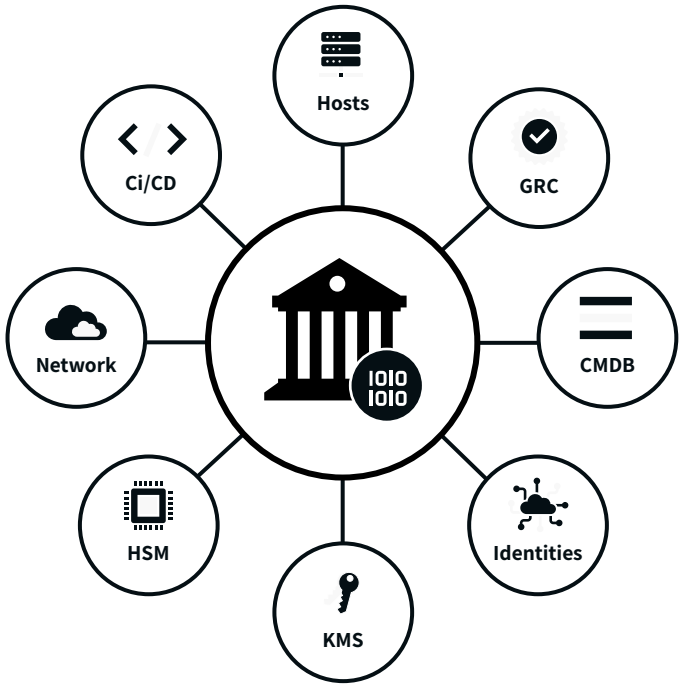


INFOSEC GLOBAL
a Keyfactor company

Threat | Quantum Computer

Classical Cryptography

Static | Reactive | Unmanaged



Cryptographic
Transformation Journey

Crypto Agility & Management

Full Visibility | Automated | Controlled

NIST

THE WHITE HOUSE WASHINGTON

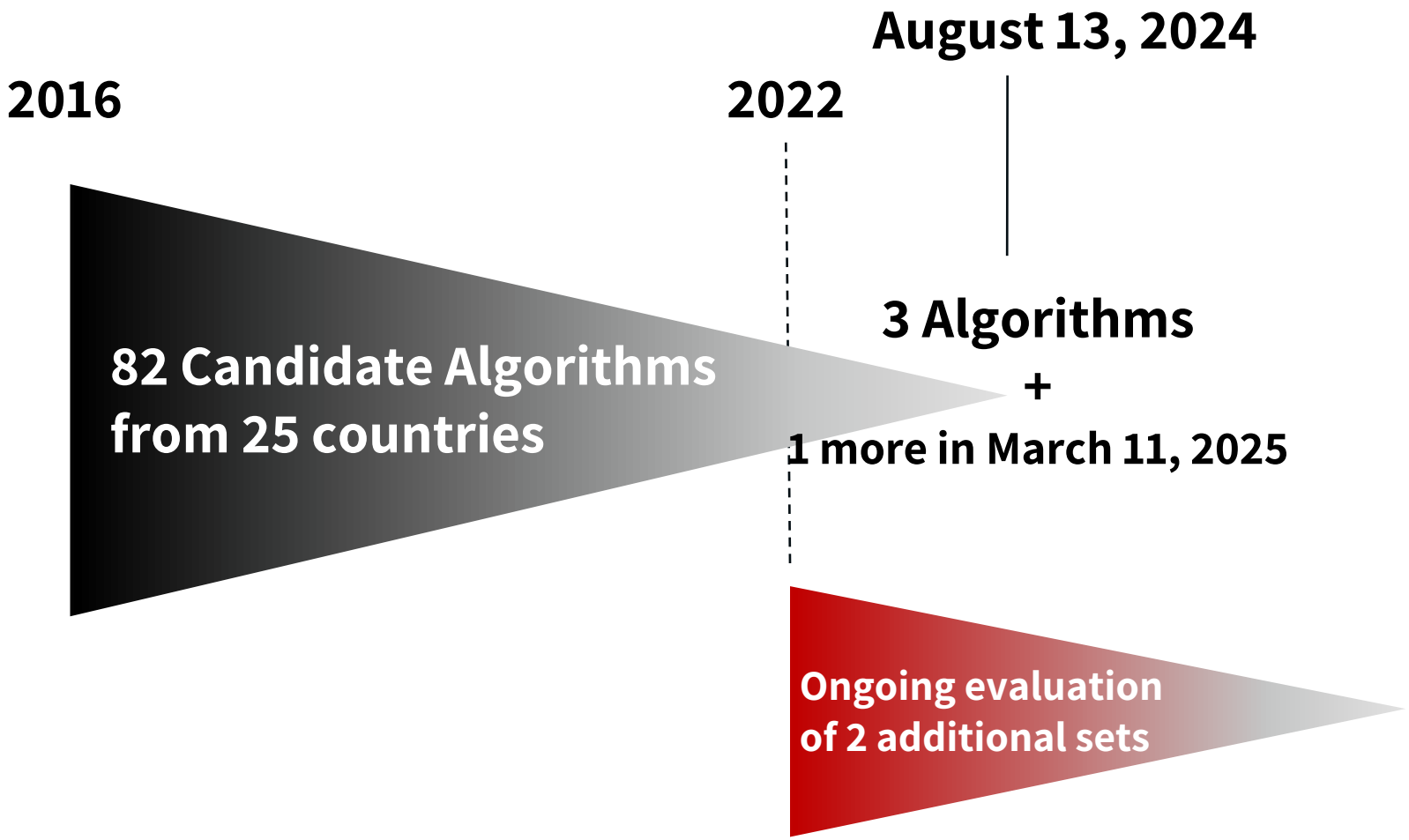
PCI DSS COMPLIANT 4.0

FS-ISAC

And Others…

Discover ▶ Remediate ▶ Transition ▶ Control

News | NIST Releases First 3 Finalized Post-Quantum Encryption Standards (August 13, 2024)



Timeline | Quantum Policy

2018

National Quantum Initiative (NQI) Act

Establish goals & priorities for a 10-year plan to accelerate the development of QIS and technology applications

2019

NSM-8: Improving the Cybersecurity of National Security, DoD, & Intelligence Community Systems

Requires all federal agencies to assess all uses of vulnerable cryptography in classified systems & develop a timeline to transition to quantum resistant cryptography

2020

Executive Order 14028: Improving Our Nation's Cybersecurity

Modernizing Federal government cybersecurity through Zero Trust Architecture

2021

OMB Memorandum Mitigating to Post Quantum Cryptography (M-23-02)

New guidance to initiate governmentwide transition to post quantum cryptography

2022

NSM-10: Promoting US in Quantum Computing, Mitigating Risks to Vulnerable Cryptographic Modernizing Federal Systems

Requires all federal agencies to assess all uses of vulnerable cryptography in unclassified systems & develop a timeline to transition to quantum resistant cryptography

2023

Quantum Computing Cybersecurity Preparedness Act (HR 7535)

Codifies NSM-10 and NSM-8 into law

2024

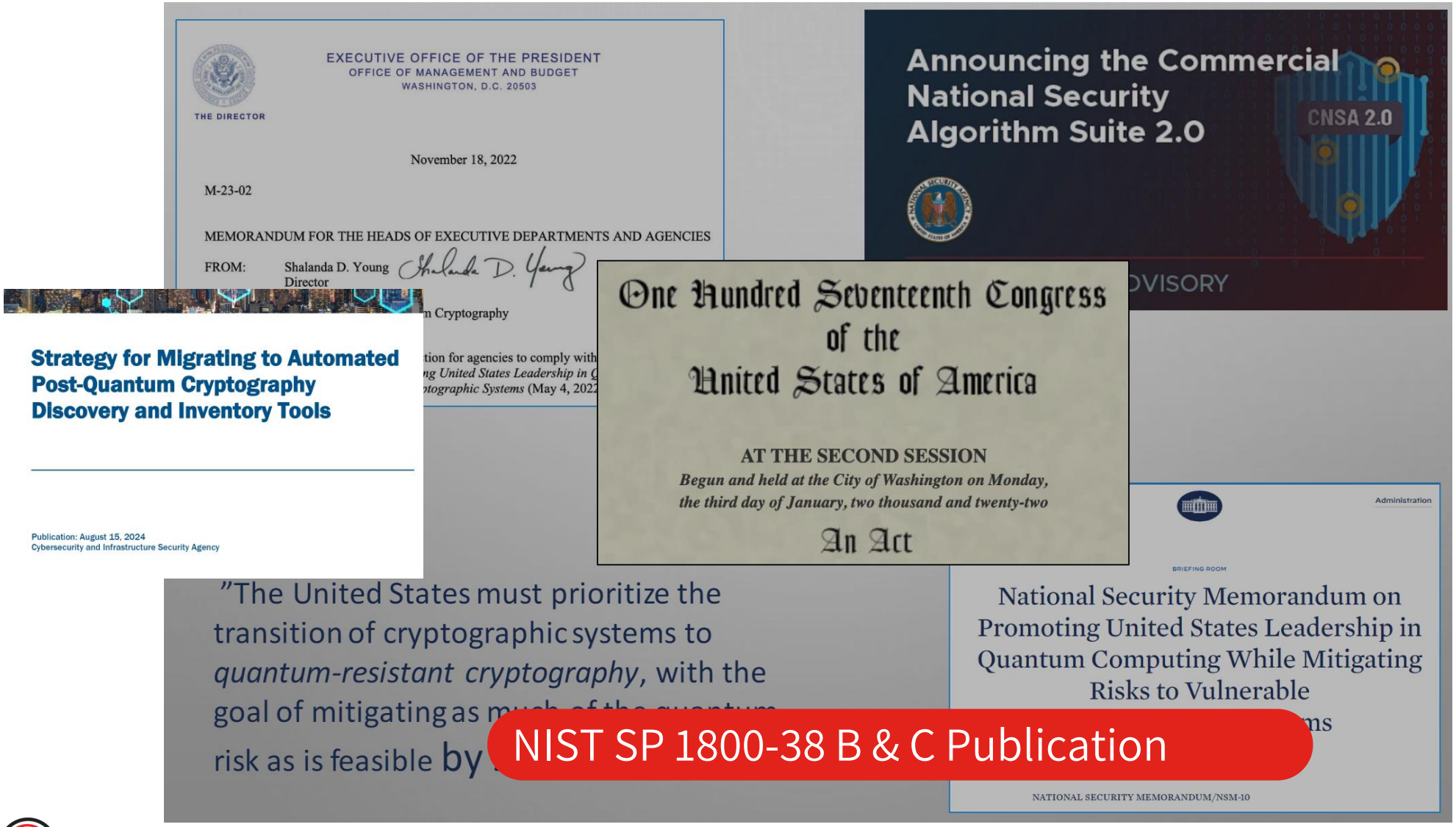
First Federal Inventory of Cryptographic Systems

NIST IR 8547 Transition to Post-Quantum Cryptography Standards

INFOSEC GLOBAL
a Keyfactor company

Source: https://csrc.nist.gov/csrc/media/Presentations/2024/u-s-government-s-transition-to-pqc/images-media/presman-govt-transition-pqc2024.pdf

Readiness | Government on PQC Migration and Readiness



NIST SP 1800-38 B & C Publication

INFOSEC GLOBAL
a Keyfactor company

Source: ref: https://csrc.nist.gov/csrc/media/Presentations/2024/update-on-the-nist-pqc-standardization-project/images-media/moody-are-we-there-yet-pqc-pqc2024.pdf

NCCoE | PQC Evolution

NIST Cryptographic Inventory

INFOSEC GLOBAL
a Keyfactor company

Migration to Post-Quantum Cryptography

The advent of quantum computing technology will compromise many of the current cryptographic algorithms, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to criminals, competitors, and other adversaries. It is critical to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

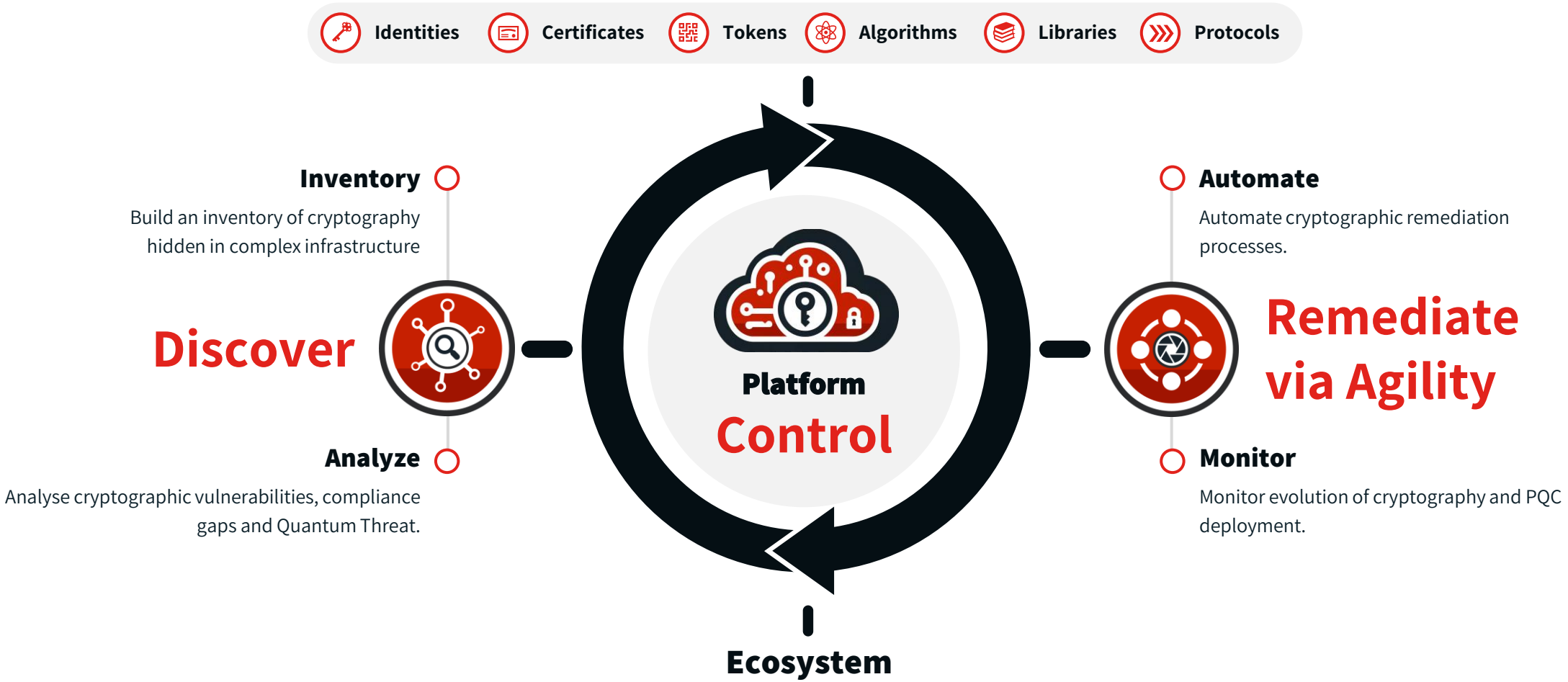
INFOSEC GLOBAL
a Keyfactor company

- Selected by NCCoE
- Cryptographic Inventory
- Solution installed by NIST
- Unique Analysis Approach
- Building PQC Discovery
- Interoperability

https://csrc.nist.gov/Projects/post-quantum-cryptography

NIST SP 1800-38 B & C Publication

Vision | Cryptographic Posture Management Platform



INFOSEC GLOBAL
a Keyfactor company

The Problem with Cryptography

A single vulnerability can lead to disaster

Material Financial Impact

Heartbleed

$500M

Large Scale Impact

Estonian eID Cards

German eID Providers

Several High-Security Solutions (TPM / SSH / GPG)

ROCA

Million broken high security chipset

Complex Identification

Heartbleed, FREAK, SSLv3, SHATTERED, ROCA, And more...

Long Time Exposure

60% US Company need 1+ Year to fix weak crypto

Gartner

New Strict Regulations

GDPR

PCI DSS COMPLIANT

IoT

Dev. Failure

cryptographic issues: VERACODE

n°2 vulnerability found in apps

Quantum Threat

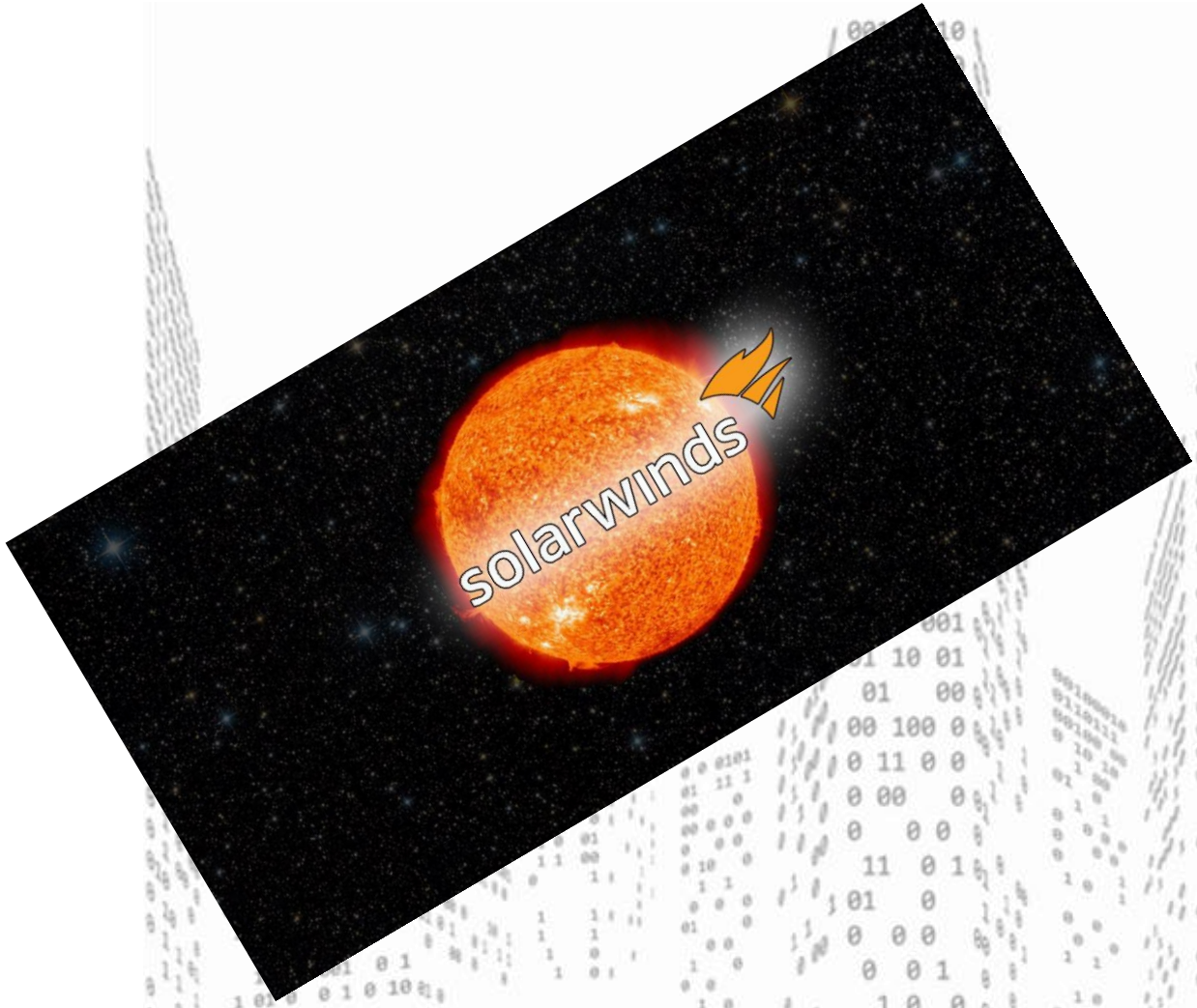
Unpredictable global impact

Plan Transition to Quantum Safe

INFOSEC GLOBAL
a Keyfactor company

The Problem with Cryptography

A single vulnerability can lead to disaster



deepseek

Cryptographic Bill of Material

The following table includes the list of cryptographic materials or mechanisms detected by AgileSec Analytics within the Target.

Algorithm	Instances
Algorithm: jca-generic	13
Algorithm: jca-md5	7
Algorithm: jca-aes	6
Algorithm: jca-sha256	3
Algorithm: jca-des-ecb	2
Certificates	Not Found
Keys	Not Found
Libraries	JCA
Keystores	Not Found

INFOSEC GLOBAL
a Keyfactor company

Discover | AgileSec Analytics

Discover
Cryptography Ecosystem

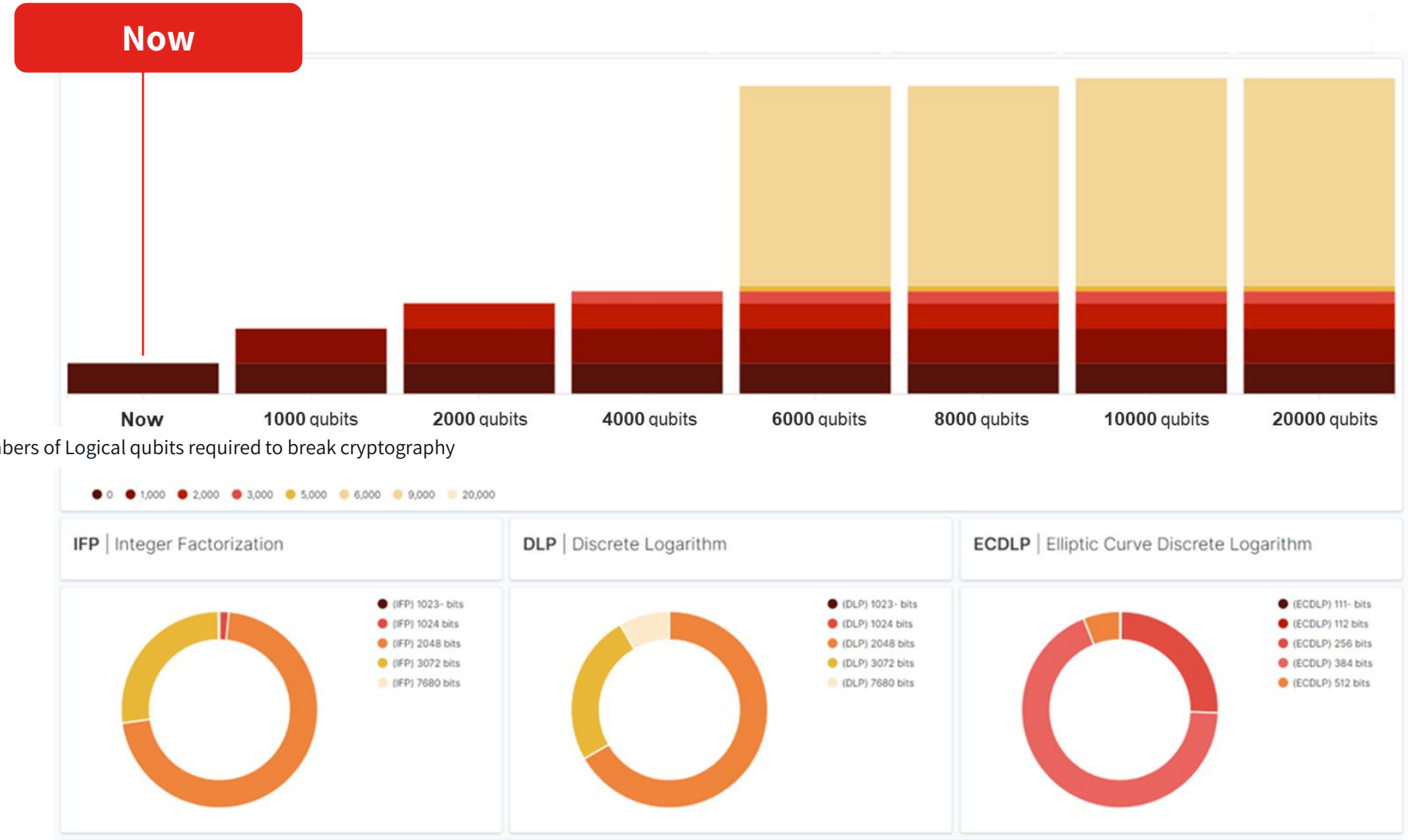
Analyze
Cryptographic Compliance, Security & Correlation

Automate
Cryptographic Processes

Sample Integrations

Crowdstrike | ServiceNow | Utimaco* | Gitlab | Github | Venafi | Thales CTM* | Azure Vault | Ansible | Entrust | Tanium | Windows | RedHat | Others

Solution | Understand Quantum Vulnerability Roadmap



Numbers of Logical qubits required to break cryptography

INFOSEC GLOBAL
a Keyfactor company

Use-Cases | Discover

1

Cryptographic
Vulnerabilities

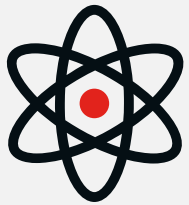
Identify and remediate critical cryptographic vulnerabilities hidden in the digital landscape.

2

Cryptographic
Keys in the Wild

Hunt cryptographic keys and secrets across infrastructure to ensure compliance and security.

3



Cryptographic
PQC Migration

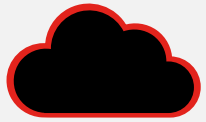
Prepare transition to Quantum Safety by monitoring deployment of Post-Quantum Cryptography.

4

Cryptographic
Threats

Uncover complex cryptographic threat vectors based on identities, secrets and cryptography.

5



Cryptographic
Cloud Migration

Understand current uses of cryptography to prepare for transition from on-prem to cloud.

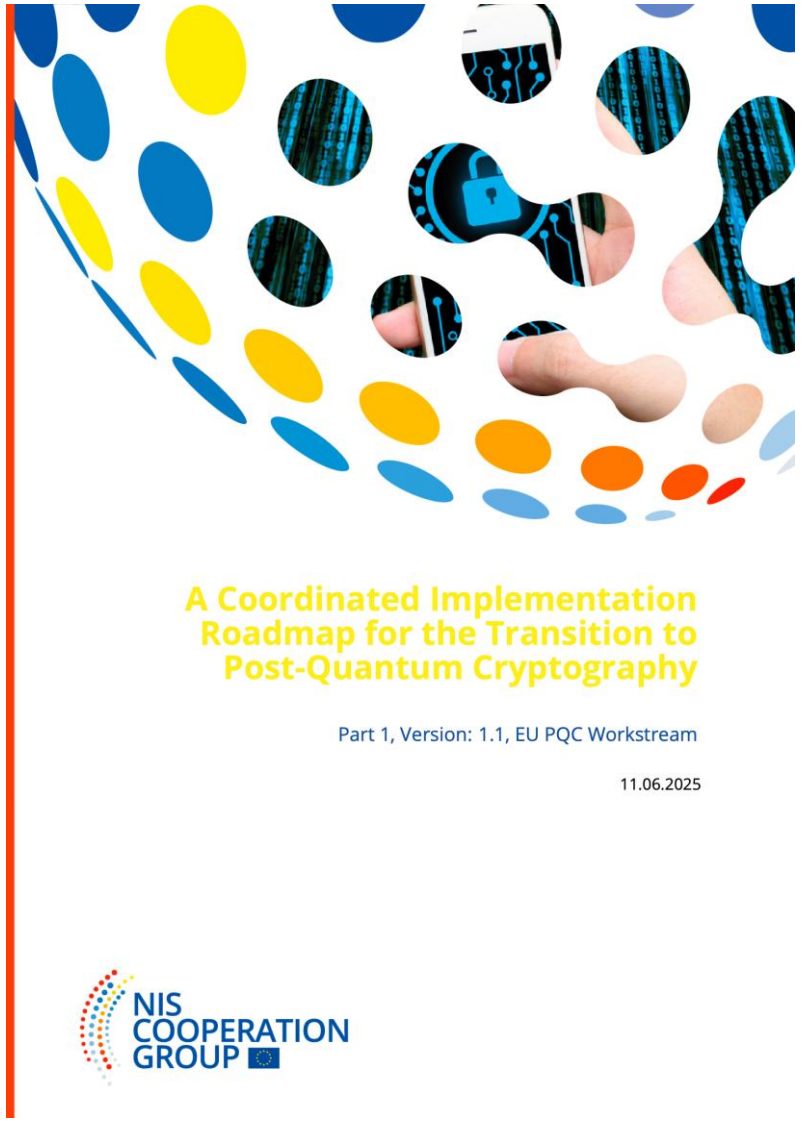
Cryptography Inventory

EU Member States Warn of the Quantum Threat and Call for the Transition to Post-Quantum Cryptography

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

- “Store now, decrypt later”
  - A threat when the confidentiality of data must be protected for a long time
    (e.g. governmental data, sensitive personal data, trade or business secrets)

- Long transition period
  - Migrating complex systems can take 5-10 years, necessitating immediate action



Timeline for the Transition to PQC

- Create and maintain **cryptographic inventory**
- Identify internal and third-party **dependencies**
- Perform **quantum risk analysis**
- Develop a timeline and an **implementation plan**
- Initiate transition **planning for high-risk** use cases

- Support **cryptographic agility** and a quantum-safe upgrade path
- **Allocate resources** for the transition
- **Implement pilot** use cases and contribute to testing centers
- Completion of **PQC transition for high-risk** use cases
- Initiate transition **planning for medium-risk** use cases
- **Enable Crypto-agility**

- Completion of **PQC transition for all use cases**

Recommendations | Government Initiatives

Agence nationale de la sécurité des systèmes d'information

"Encourage the initiation of progress towards crypto-agility as much as possible for future products."

Government of Canada

"Canada National Quantum Readiness Best Practices & Guidelines."

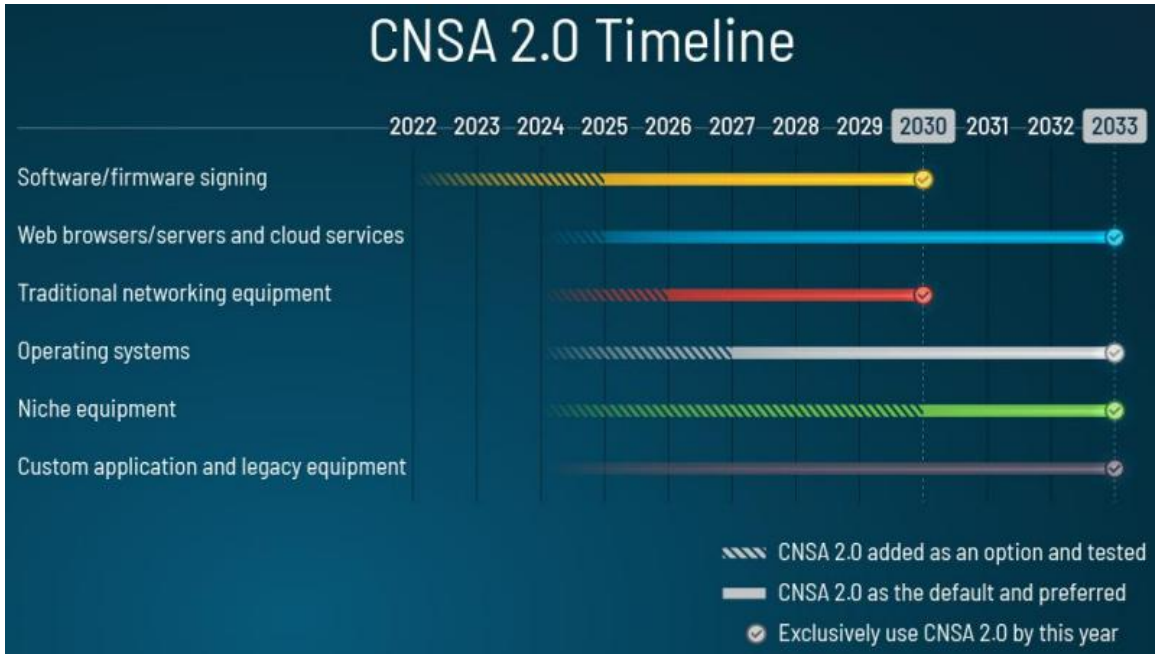
Bundesamt für Sicherheit in der Informationstechnik

"From the BSI's point of view, the question of "if" or "when" there will be quantum computers is no longer paramount. First post-quantum algorithms have been selected by NIST for standardisation and post-quantum cryptography will be used by default."

National Cyber Security Centre
a part of GCHQ

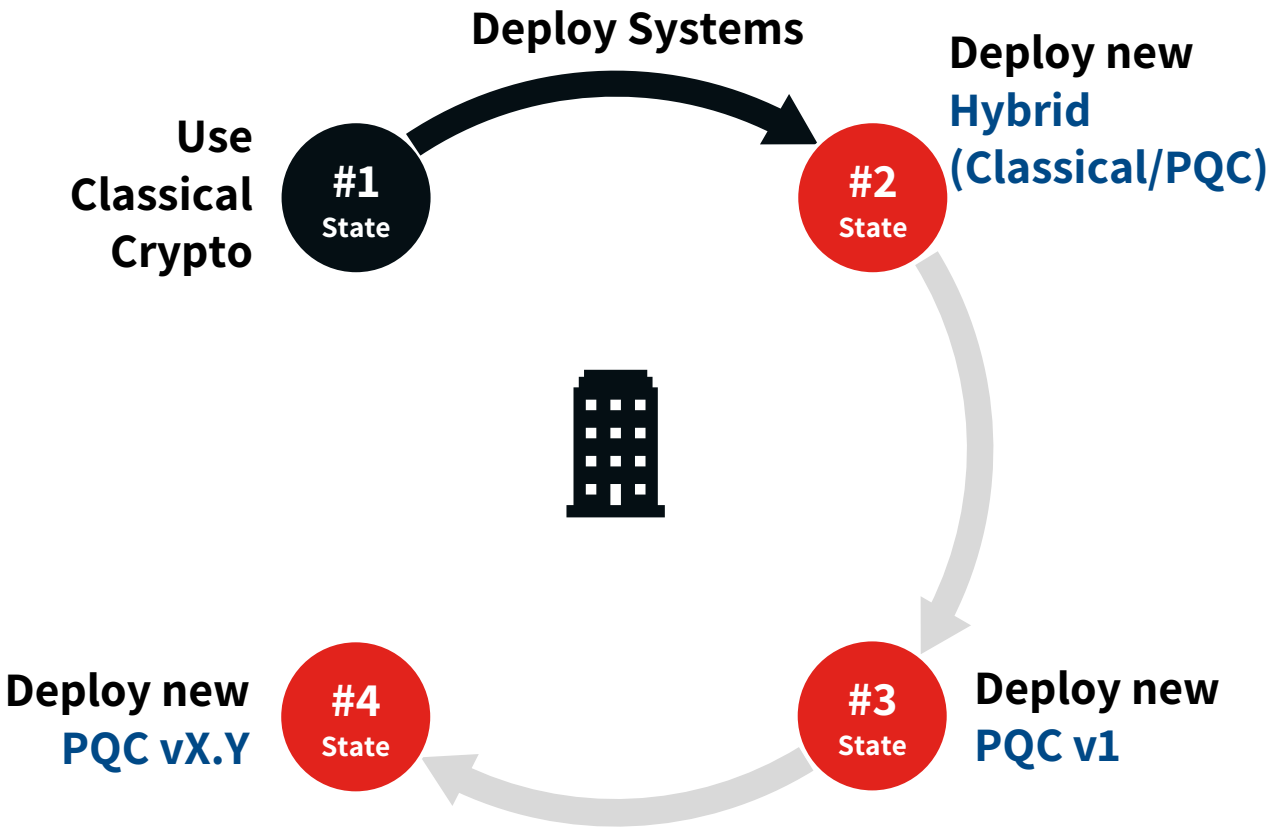
"As quantum technology advances, upgrading our collective security is not just important – it's essential."

Timeline | PQC Transition Timeline



Announcing the Commercial National Security Algorithm Suite 2.0

Transition | Multiple Stages

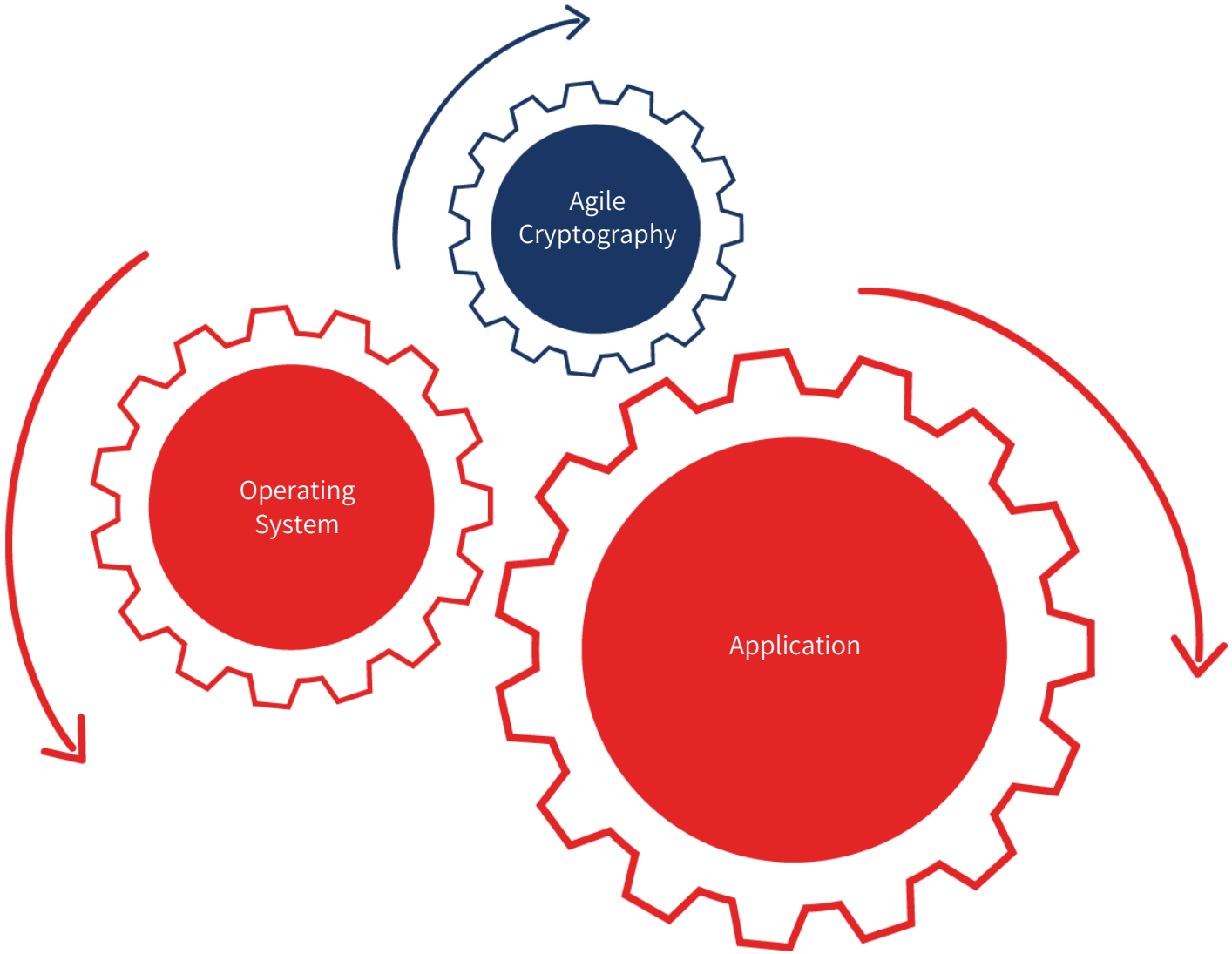


KEY BENEFITS OF CRYPTO AGILITY

- Streamline Development of Core Cryptographic Functions
- Allow to Support Client's Cryptography (Software/Hardware)
- Readiness for up-coming cryptographic standards
- New Technology Differentiator for customers
- Trust anchor for end-customers

Agile Cryptography

Decouple Applications from Cryptography



Design Principles | Implementation of independence

- Application code must be independent from cryptographic implementations
- No hard coded dependencies on specific algorithms

INDEPENDENCE

Design Principles | Implementation Simplicity

- The interface to cryptography must be simple to reduce the risk of errors
- Clear and easy understandable guidelines must be available

SIMPLICITY

Design Principles | Implementation abstraction

- The interface to cryptography must offer a high level of abstraction to support implementation independence and simplicity.
- Implementation details should be hidden

ABSTRACTION

Design Principles | Dynamic exchangeability and extensibility

- Systems must be able to change cryptographic algorithms dynamically
- Systems must be able to add new algorithms dynamically
- Application should not needed to be changed

EXCHANGEABILITY

Design Principles | Manageability

- Usage of cryptographic algorithms must be manageable separately from the application
- Usage of cryptographic algorithms must be configurable after application deployment
- Application should be able to be deployed without specific instances of cryptographic algorithms

MANAGEABILITY

Design Principles | Portability

- The framework providing cryptographic agility must be highly portable to make it available on as many platforms as possible
- Overhead should be as small as possible to enable cryptographic agility even on the smallest devices

PORTABILITY

Design Principles | Performance

- It must be possible to implement algorithms such that highest performance can be achieved

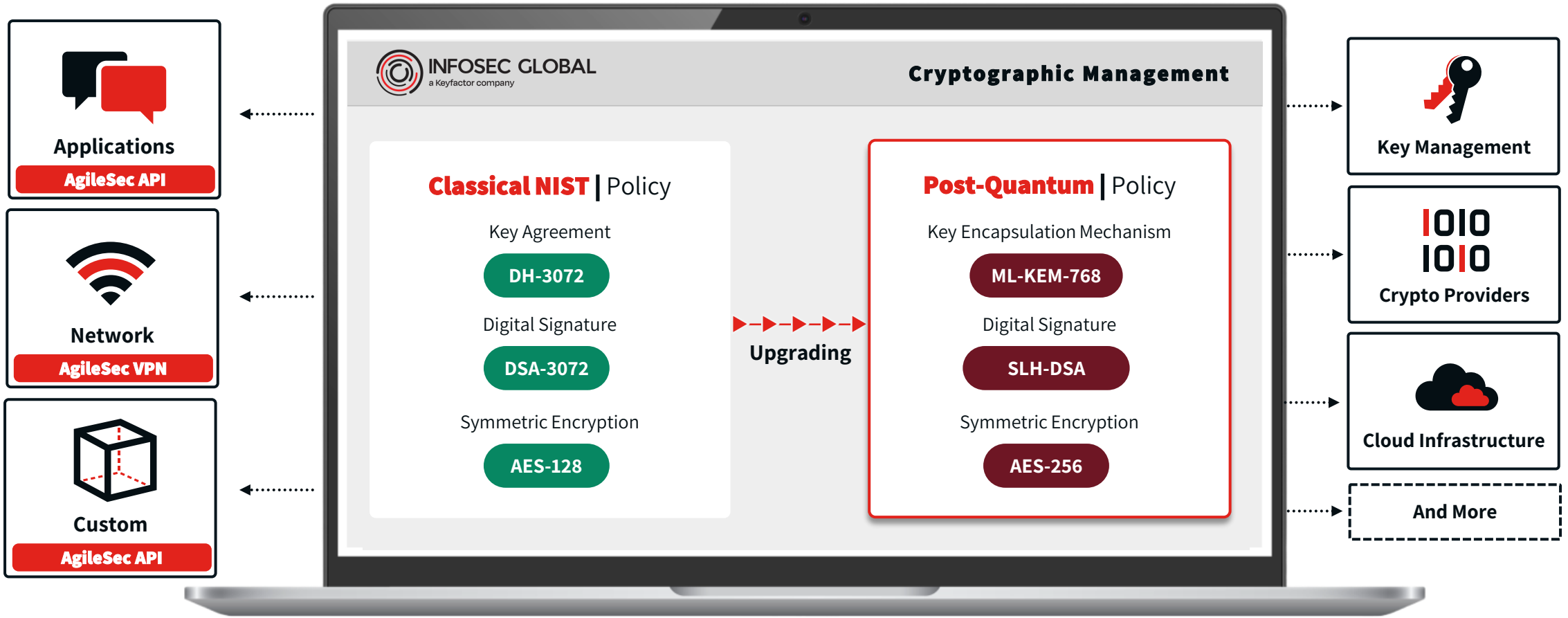
PERFORMANCE

Control | AgileSec Management

Control
Cryptographic Policy in Use

Manage
Cryptographic Policies, Algorithms, Keys and Settings

Integrate
Cryptographic Systems



Sample Integrations

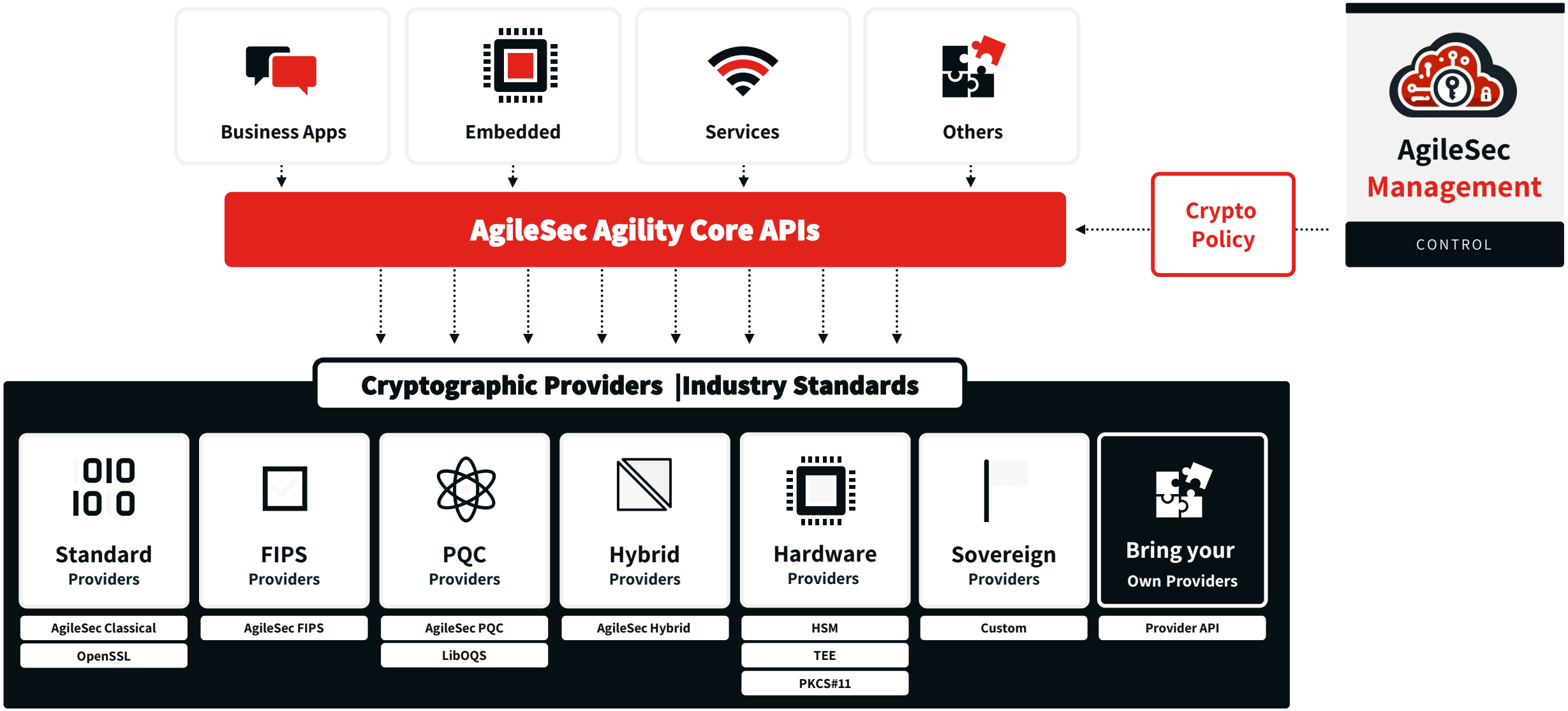
TRoot · Luna SA7 · Bouncycastle · OpenSSL · Marvell* · Utimaco* · Wireguard · QKD

NIST Cybersecurity White Paper
NIST CSWP 39 2pd

Considerations for Achieving Crypto Agility

Strategies and Practices

Control | Agility



INFOSEC GLOBAL

a Keyfactor company