Post-Quantum

Cryptography Conference

Perspectives on the transition to PQC in the financial sector

The race towards post-quantum cryptography has started. While several organizations in the finance sector are taking steps to prepare for the transition, the focus seems to still be building up. This session will provide an update on the status of the transition to PQC in the financial sector, including relevant regulations such as DORA, PCI-DSS, CNSA2, and NIST IR 8547, and how these regulations collectively drive the need for improved cryptography management; the ongoing collaboration in initiatives like the Europol Quantum Safe Financial Forum or the FS-ISAC PQC Workgroup; and the Santander Quantum Threat Program.

Jaime Gómez García
Head of Quantum at Banco Santander and Chair of the Quantum Safe Financial Forum

January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium Inc. is registered as a 501(c)(6) non-profit entity (“business league”) under Utah law (10462204-0140) | pkic.org

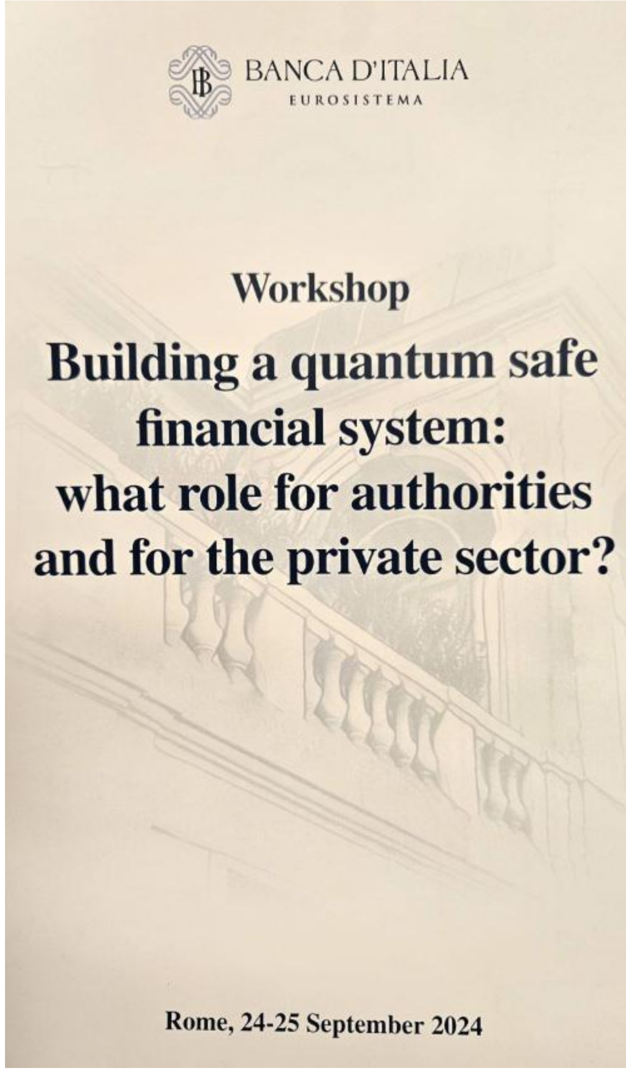
PKI Consortium

Santander
Block›chain

Perspectives on the transition to PQC in the financial sector

Jaime Gómez García
PQC Conference - Jan. 16th, 2025

G7 Workshop hosted by Banca d’Italia



BANCA D'ITALIA
EUROSISTEMA

Workshop

Building a quantum safe financial system: what role for authorities and for the private sector?

Rome, 24-25 September 2024

12 financial institutions (Banca d’Italia, Swift, Bundesbank, JP Morgan, Banque de France, Santander, BIS, Bank of Canada, Intesa Sanpaolo, US Treasury, Reserve Bank of Australia and World Bank Group), among many other specialists.

Key statements from Alessandra Perrazelli (Deputy Governor of Banca d’Italia):

- **Main obstacles slowing the transition**:
  - 😰 High short-term risk mitigation costs
  - 😰 Lack of consensus on migration approaches and technical standards
  - 😰 Fragmented regulatory and capability frameworks across jurisdictions
- **Key requirements for a common roadmap:**
  - 👉 Build on existing regulations to avoid over-regulation
  - 👉 Standardize risk mitigation strategies across jurisdictions
  - 👉 Include input from financial industry players and tech providers
  - 👉 Ensure interoperability and service quality throughout the transition
  - 👉 Maintain strong international coordination

Despite growing awareness, a clear, unified action plan to ensure a smooth and secure quantum transition is still lacking.

https://www.bancaditalia.it/media/notizia/alessandra-perrazzelli-at-the-g7-workshop-on-building-a-quantum-safe-financial-system/

INSTITUTE OF INTERNATIONAL FINANCE

2024 IIF QUANTUM BOOTCAMP

AGENDA

Philip Intallura, Group Head of Quantum Technologies, HSBC

QUANTUM IN PRACTICE
CHANGE MANAGEMENT AND APPLICATIONS IN PRACTICE

Carmen Recio Valcarce, Director, Quantum Computing, Moody's

QUANTUM IN PRACTICE
CHANGE MANAGEMENT AND APPLICATIONS IN PRACTICE

Alex Manson, Chief Executive Officer, SC Ventures by Standard Chartered

QUANTUM IN PRACTICE
CHANGE MANAGEMENT AND APPLICATIONS IN PRACTICE

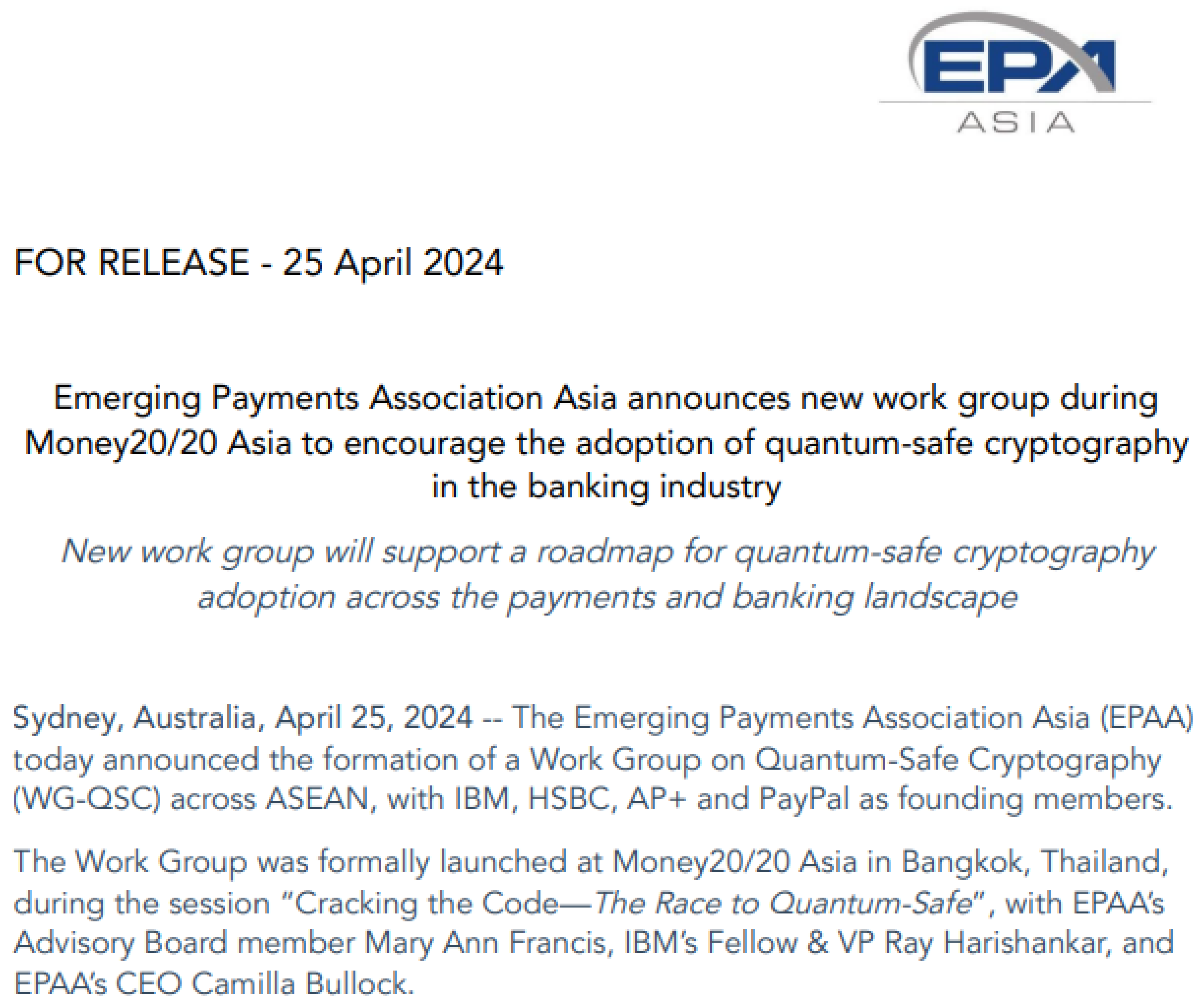
Marco Pistoia, Managing Director, Distinguished Engineer, Global Head of Applied Research, Global Head of Quantum Computing, JPMorganChase

QUANTUM TECHNOLOGY
FOCUS ON RISKS, CRYPTOGRAPHY STANDARDS AND DATA SECURITY

Jaime Gómez García, Head of Quantum, Banco Santander

QUANTUM TECHNOLOGY
FOCUS ON RISKS, CRYPTOGRAPHY STANDARDS AND DATA SECURITY

EPAA Workgroup on Quantum-Safe Cryptography



EPA ASIA

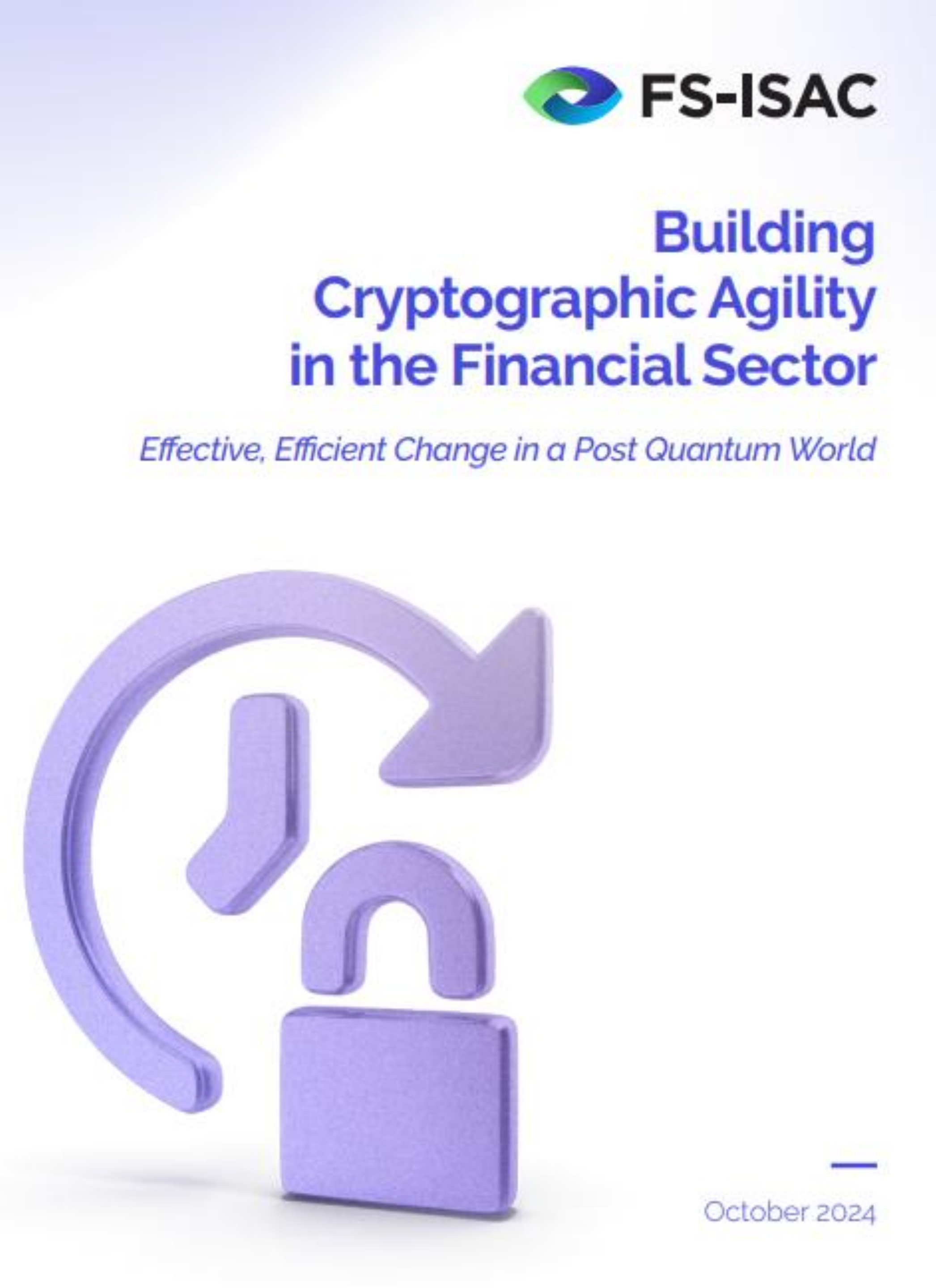
FOR RELEASE - 25 April 2024

Emerging Payments Association Asia announces new work group during Money20/20 Asia to encourage the adoption of quantum-safe cryptography in the banking industry

New work group will support a roadmap for quantum-safe cryptography adoption across the payments and banking landscape

Sydney, Australia, April 25, 2024 -- The Emerging Payments Association Asia (EPAA) today announced the formation of a Work Group on Quantum-Safe Cryptography (WG-QSC) across ASEAN, with IBM, HSBC, AP+ and PayPal as founding members.

The Work Group was formally launched at Money20/20 Asia in Bangkok, Thailand, during the session "Cracking the Code—*The Race to Quantum-Safe*", with EPAA's Advisory Board member Mary Ann Francis, IBM's Fellow & VP Ray Harishankar, and EPAA's CEO Camilla Bullock.



FS-ISAC

Building Cryptographic Agility in the Financial Sector

Effective, Efficient Change in a Post Quantum World

October 2024

> ***Cryptographic Agility*** *is a measure of an organization's ability to adapt cryptographic solutions or algorithms (including their parameters and keys) quickly and efficiently in response to developments in cryptanalysis, emerging threats, technological advances, and/or vulnerabilities.*
>
> *It is also a design principle for implementing, updating, replacing, running, and adapting cryptography and related business processes and policies with no significant architectural changes, minimal disruption to business operations, and short transition time.*

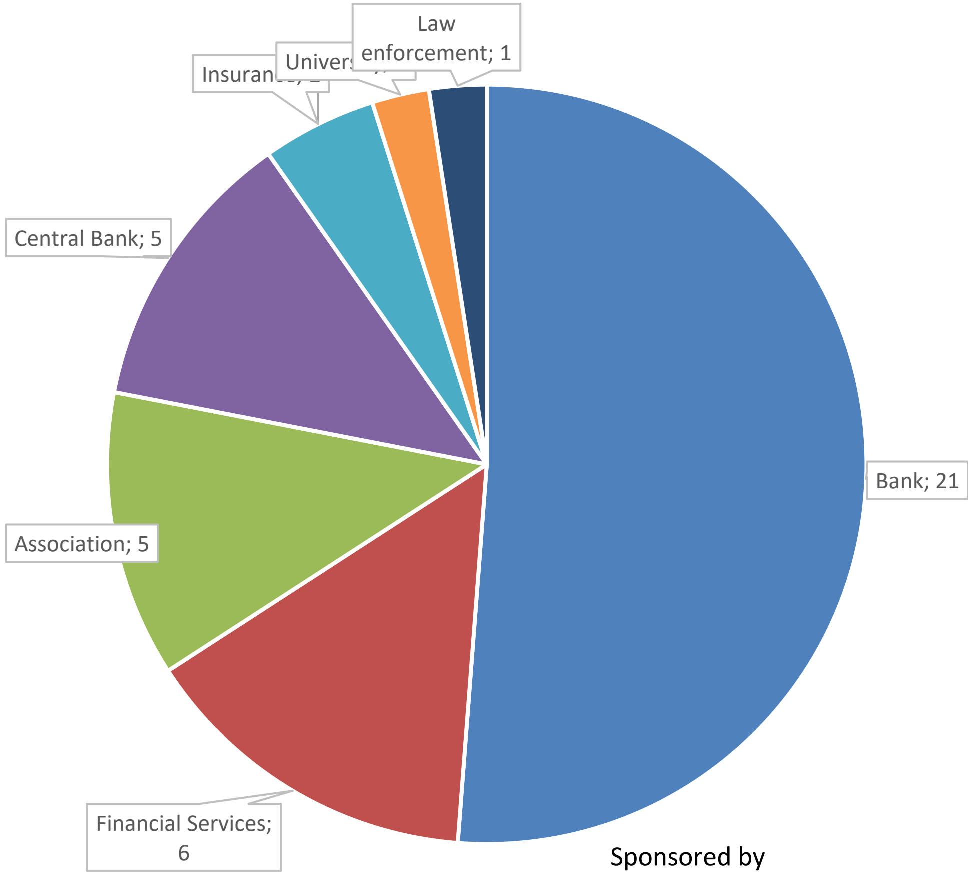
- Design principle
- Adapt to ANY future threats to cryptography
- Minimal disruption to business

Good old exit plans, no more set and forget in cryptography

https://www.fsisac.com/pqc-crypto-agility

Europol Quantum Safe Financial Forum

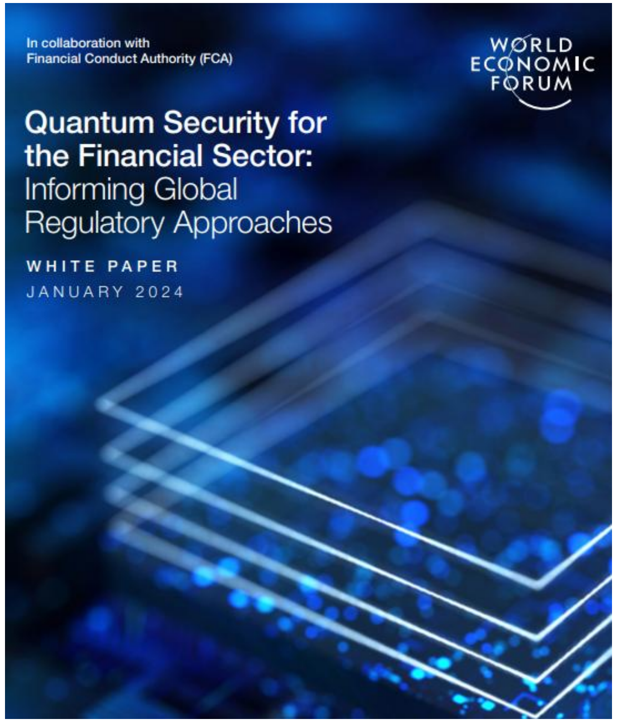
Quantum Safe Financial Forum members
(Total as of Dec. 18th 2024, 41 members)



Sponsored by

EUROPOL

Other position statements in 2024

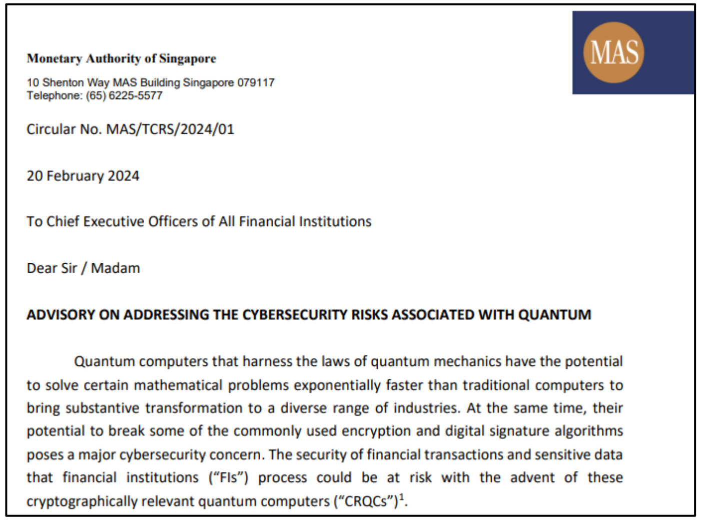


In collaboration with
Financial Conduct Authority (FCA)

WORLD ECONOMIC FORUM

Quantum Security for the Financial Sector: Informing Global Regulatory Approaches

WHITE PAPER
JANUARY 2024



Monetary Authority of Singapore

10 Shenton Way MAS Building Singapore 079117
Telephone: (65) 6225-5577

MAS

Circular No. MAS/TCRS/2024/01

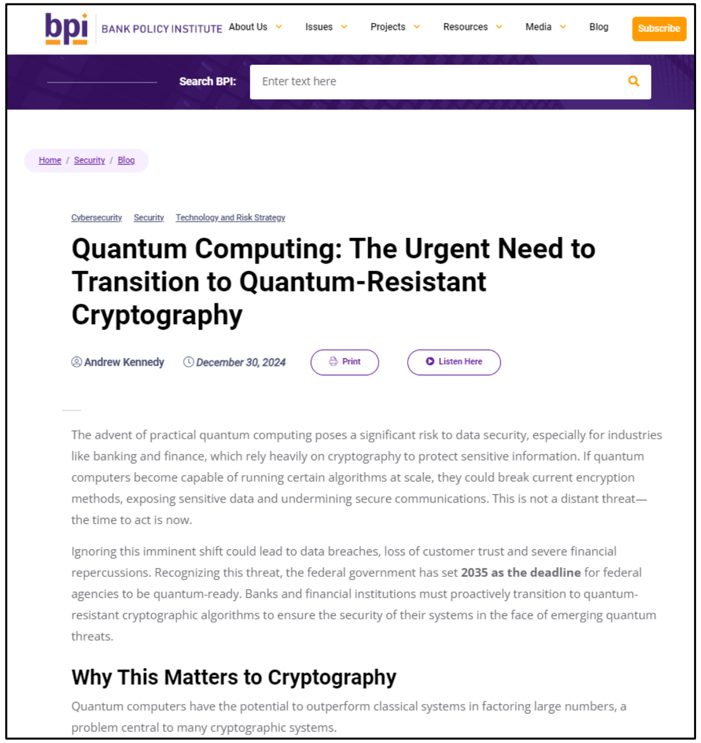
20 February 2024

To Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

ADVISORY ON ADDRESSING THE CYBERSECURITY RISKS ASSOCIATED WITH QUANTUM

Quantum computers that harness the laws of quantum mechanics have the potential to solve certain mathematical problems exponentially faster than traditional computers to bring substantive transformation to a diverse range of industries. At the same time, their potential to break some of the commonly used encryption and digital signature algorithms poses a major cybersecurity concern. The security of financial transactions and sensitive data that financial institutions ("FIs") process could be at risk with the advent of these cryptographically relevant quantum computers ("CRQCs")[1].



Cybersecurity Security Technology and Risk Strategy

Quantum Computing: The Urgent Need to Transition to Quantum-Resistant Cryptography

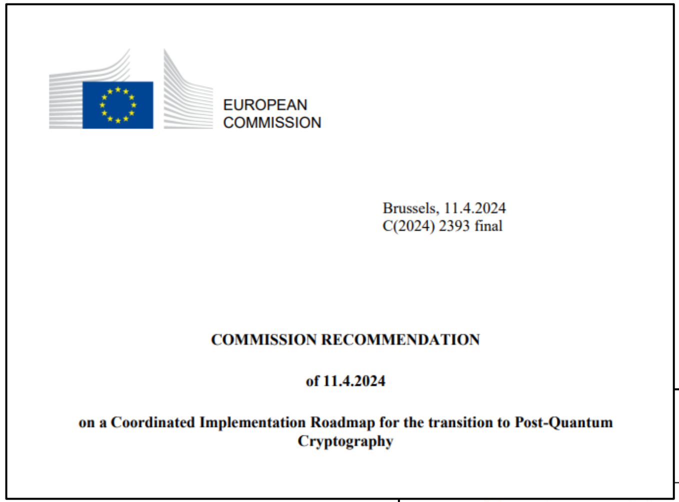
Andrew Kennedy December 30, 2024

The advent of practical quantum computing poses a significant risk to data security, especially for industries like banking and finance, which rely heavily on cryptography to protect sensitive information. If quantum computers become capable of running certain algorithms at scale, they could break current encryption methods, exposing sensitive data and undermining secure communications. This is not a distant threat—the time to act is now.

Ignoring this imminent shift could lead to data breaches, loss of customer trust and severe financial repercussions. Recognizing this threat, the federal government has set **2035 as the deadline** for federal agencies to be quantum-ready. Banks and financial institutions must proactively transition to quantum-resistant cryptographic algorithms to ensure the security of their systems in the face of emerging quantum threats.

Why This Matters to Cryptography

Quantum computers have the potential to outperform classical systems in factoring large numbers, a problem central to many cryptographic systems.



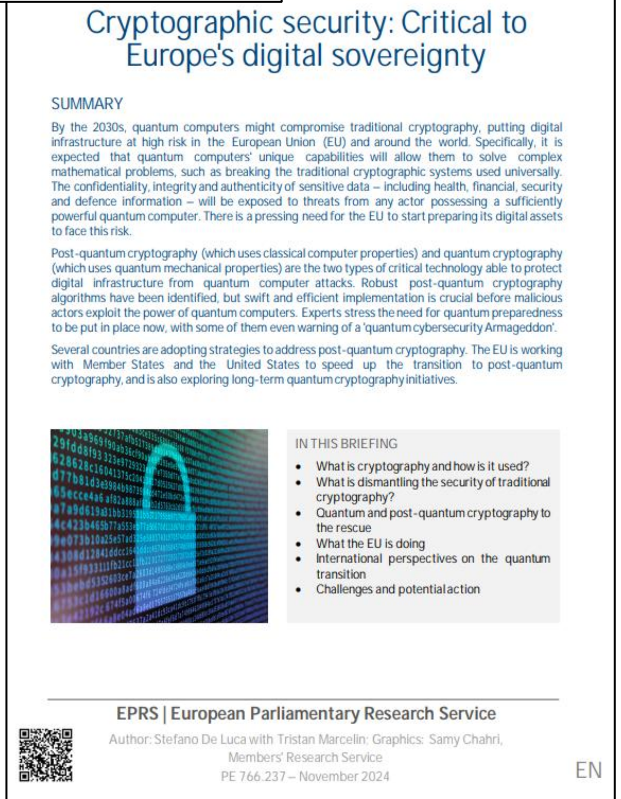
EUROPEAN
COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography



European Parliament

Cryptographic security: Critical to Europe's digital sovereignty

SUMMARY

By the 2030s, quantum computers might compromise traditional cryptography, putting digital infrastructure at high risk in the European Union (EU) and around the world. Specifically, it is expected that quantum computers' unique capabilities will allow them to solve complex mathematical problems, such as breaking the traditional cryptographic systems used universally. The confidentiality, integrity and authenticity of sensitive data – including health, financial, security and defence information – will be exposed to threats from any actor possessing a sufficiently powerful quantum computer. There is a pressing need for the EU to start preparing its digital assets to face this risk.

Post-quantum cryptography (which uses classical computer properties) and quantum cryptography (which uses quantum mechanical properties) are the two types of critical technology able to protect digital infrastructure from quantum computer attacks. Robust post-quantum cryptography algorithms have been identified, but swift and efficient implementation is crucial before malicious actors exploit the power of quantum computers. Experts stress the need for quantum preparedness to be put in place now, with some of them even warning of a 'quantum cybersecurity Armageddon'.

Several countries are adopting strategies to address post-quantum cryptography. The EU is working with Member States and the United States to speed up the transition to post-quantum cryptography, and is also exploring long-term quantum cryptography initiatives.

IN THIS BRIEFING

- What is cryptography and how is it used?
- What is dismantling the security of traditional cryptography?
- Quantum and post-quantum cryptography to the rescue
- What the EU is doing
- International perspectives on the quantum transition
- Challenges and potential action

EPRS | European Parliamentary Research Service

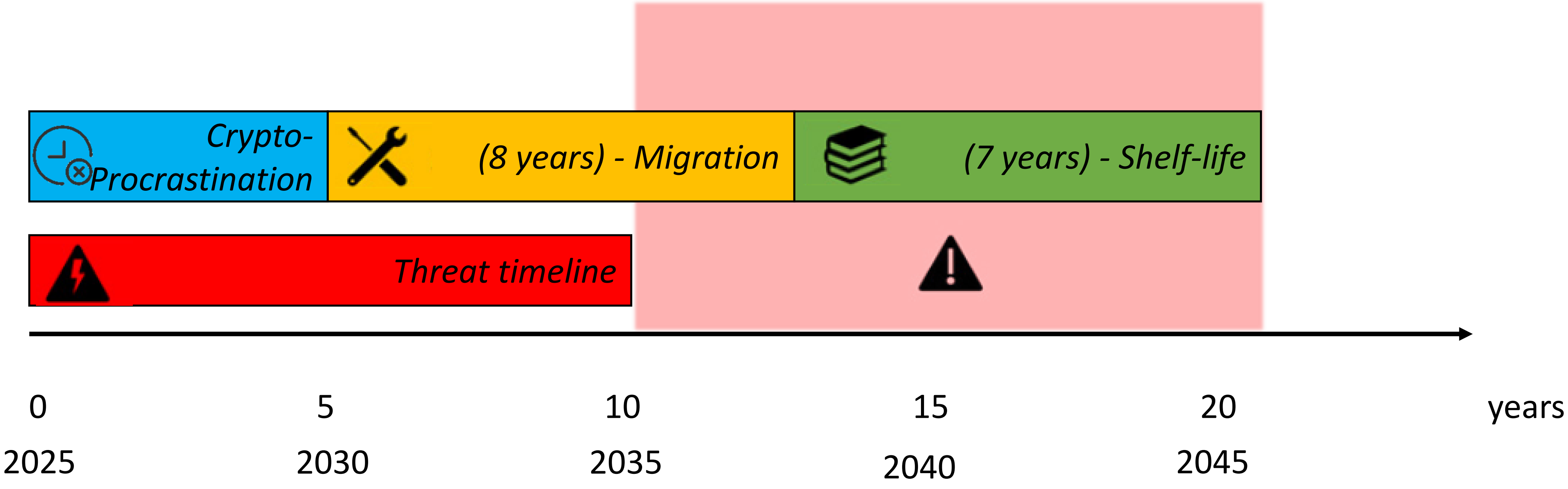
Author: Stefano De Luca with Tristan Marcelin; Graphics: Samy Chahri,
Members' Research Service
PE 766.237 – November 2024

EN

I understand the threat, but I can’t engage the organization
We still fight with obsolete software, let alone cryptography
We have little expertise on cryptography

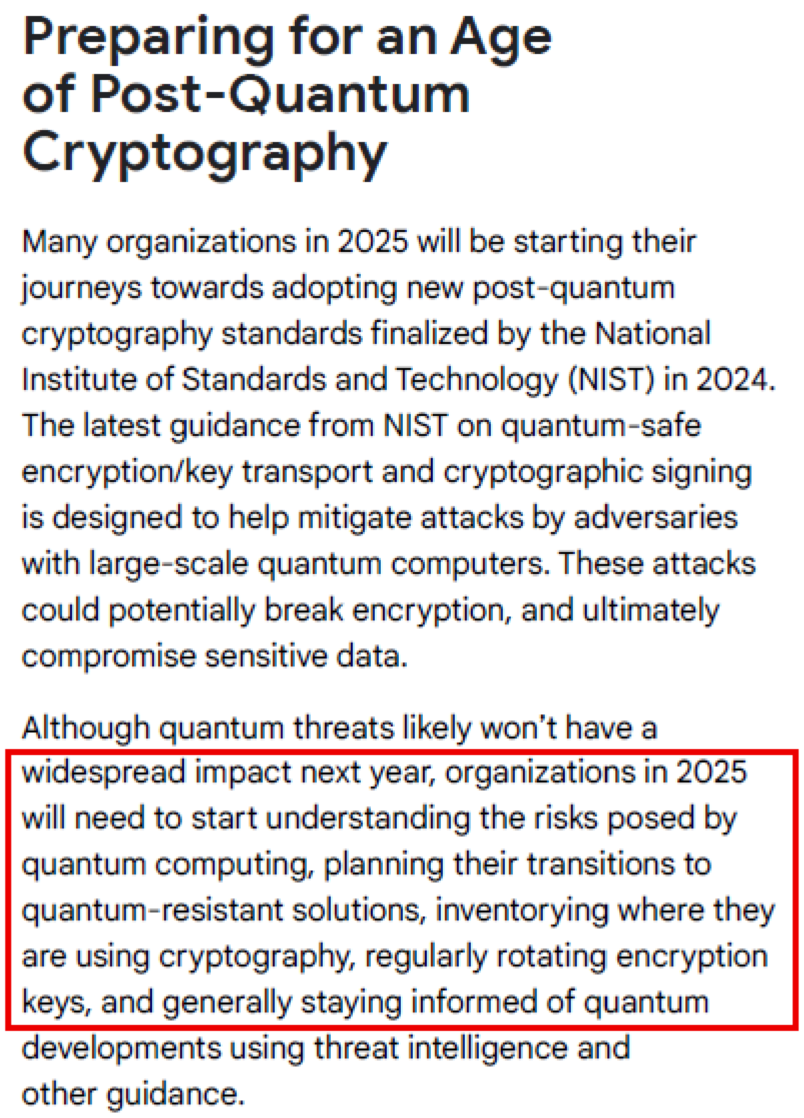
Image generated with Bing

Augmented Mosca’s theorem



Cybersecurity Forecast 2025

Google Cloud Security



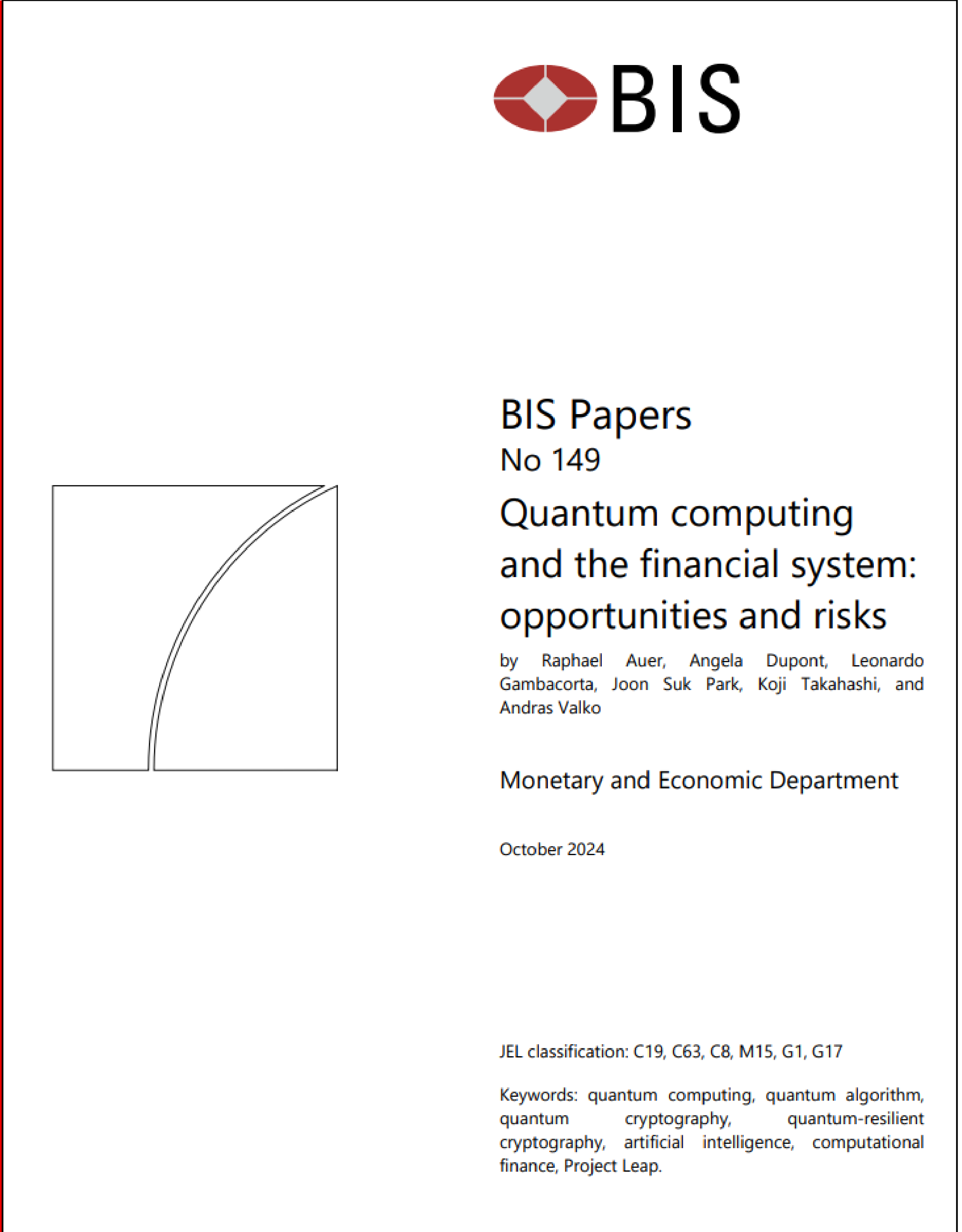
Preparing for an Age of Post-Quantum Cryptography

Many organizations in 2025 will be starting their journeys towards adopting new post-quantum cryptography standards finalized by the National Institute of Standards and Technology (NIST) in 2024. The latest guidance from NIST on quantum-safe encryption/key transport and cryptographic signing is designed to help mitigate attacks by adversaries with large-scale quantum computers. These attacks could potentially break encryption, and ultimately compromise sensitive data.

Although quantum threats likely won’t have a widespread impact next year, organizations in 2025 will need to start understanding the risks posed by quantum computing, planning their transitions to quantum-resistant solutions, inventorying where they are using cryptography, regularly rotating encryption keys, and generally staying informed of quantum developments using threat intelligence and other guidance.

- Understand
- Plan
- Inventory
- Rotate keys
- Stay informed

https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025



BIS

BIS Papers
No 149

Quantum computing and the financial system: opportunities and risks

by Raphael Auer, Angela Dupont, Leonardo Gambacorta, Joon Suk Park, Koji Takahashi, and Andras Valko

Monetary and Economic Department

October 2024

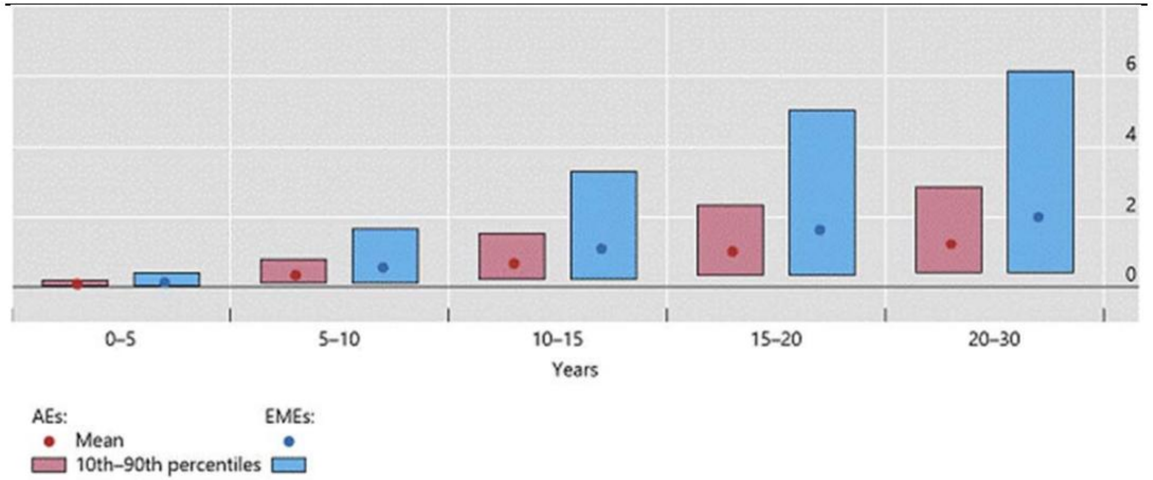
JEL classification: C19, C63, C8, M15, G1, G17

Keywords: quantum computing, quantum algorithm, quantum cryptography, quantum-resilient cryptography, artificial intelligence, computational finance, Project Leap.

Projected economic losses from a systemically relevant cyber attack enabled by quantum computing[1]

As a percentage of GDP

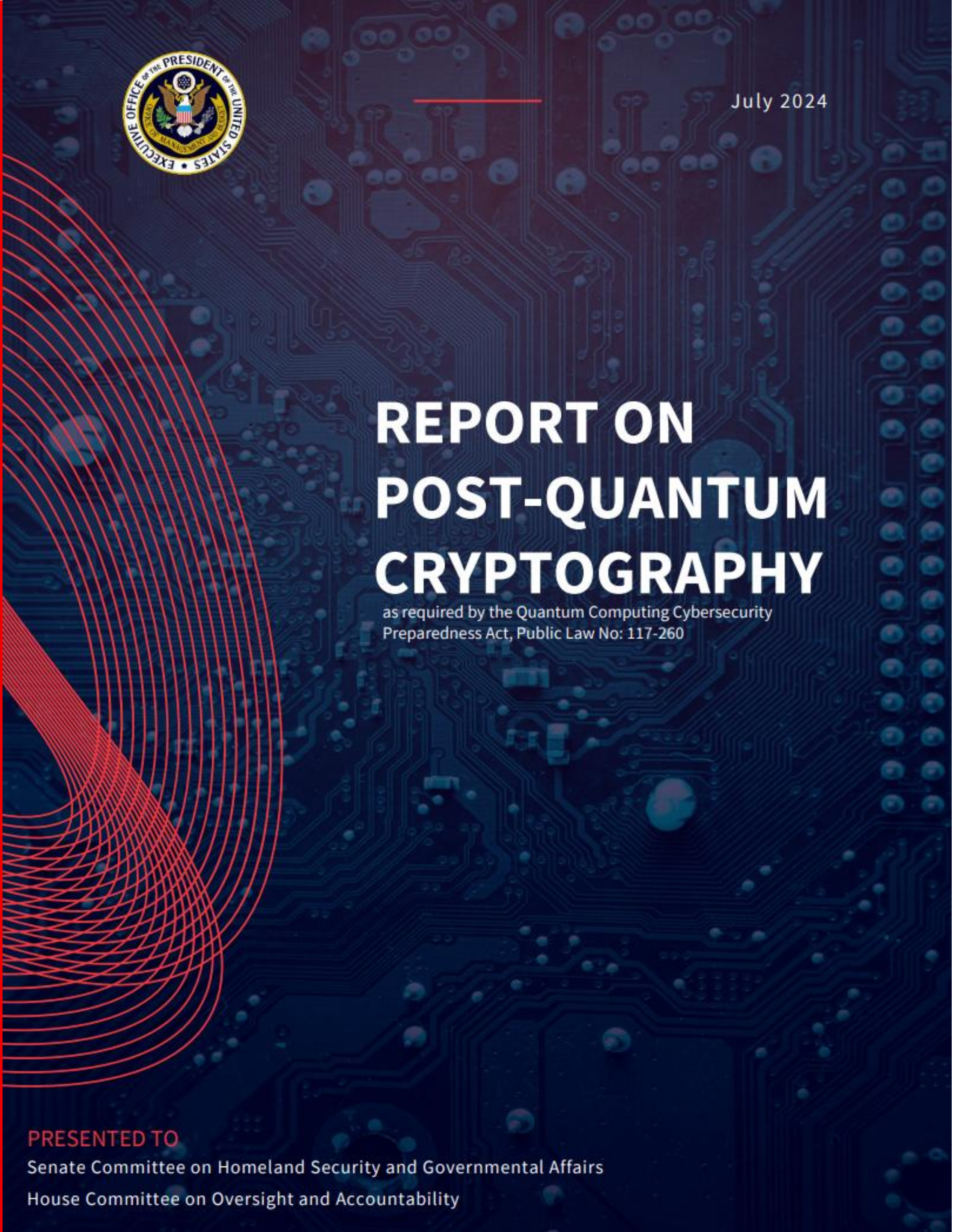
Graph 11



[1] The expected losses are derived by multiplying the magnitude of potential losses with the probability of quantum computing breaching RSA-2048 encryption within 24 hours over various time horizons. The estimation of loss size is based on a survey question directed to central banks, asking, "In your opinion, what is the maximum loss in % of annual GDP that a systemically relevant cyber-attack on traditional financial institutions could cause?" This query was posed to a sample comprising seven advanced economies (AEs) and 11 emerging market economies (EMEs). The probability estimates are obtained from a professional survey of field experts. The x-axis represents the projection horizon in years.

Sources: Survey on Doerr et al (2022); Mosca and Piani (2023)

https://www.bis.org/publ/bppdf/bispap149.htm

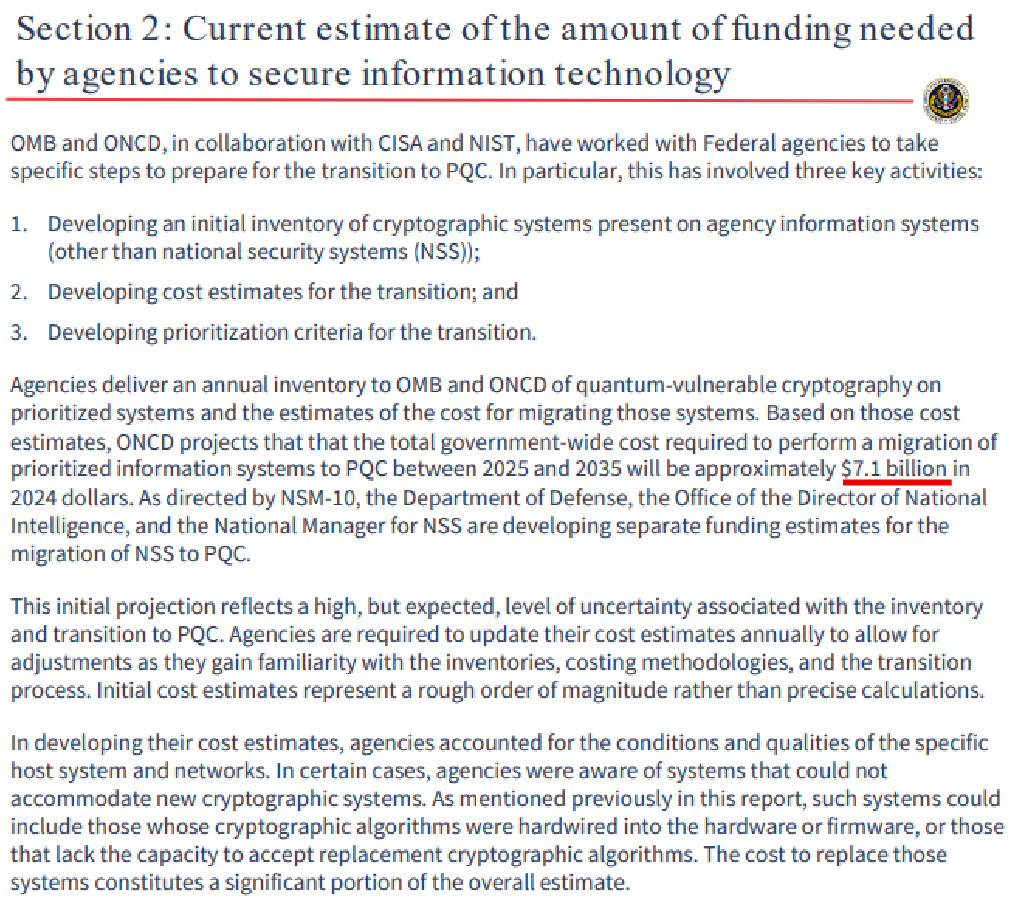


July 2024

REPORT ON POST-QUANTUM CRYPTOGRAPHY

as required by the Quantum Computing Cybersecurity Preparedness Act, Public Law No: 117-260

PRESENTED TO
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Oversight and Accountability



Section 2: Current estimate of the amount of funding needed by agencies to secure information technology

OMB and ONCD, in collaboration with CISA and NIST, have worked with Federal agencies to take specific steps to prepare for the transition to PQC. In particular, this has involved three key activities:

1. Developing an initial inventory of cryptographic systems present on agency information systems (other than national security systems (NSS));
2. Developing cost estimates for the transition; and
3. Developing prioritization criteria for the transition.

Agencies deliver an annual inventory to OMB and ONCD of quantum-vulnerable cryptography on prioritized systems and the estimates of the cost for migrating those systems. Based on those cost estimates, 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. As directed by NSM-10, the Department of Defense, the Office of the Director of National Intelligence, and the National Manager for NSS are developing separate funding estimates for the migration of NSS to PQC.

This initial projection reflects a high, but expected, level of uncertainty associated with the inventory and transition to PQC. Agencies are required to update their cost estimates annually to allow for adjustments as they gain familiarity with the inventories, costing methodologies, and the transition process. Initial cost estimates represent a rough order of magnitude rather than precise calculations.

In developing their cost estimates, agencies accounted for the conditions and qualities of the specific host system and networks. In certain cases, agencies were aware of systems that could not accommodate new cryptographic systems. As mentioned previously in this report, such systems could include those whose cryptographic algorithms were hardwired into the hardware or firmware, or those that lack the capacity to accept replacement cryptographic algorithms. The cost to replace those systems constitutes a significant portion of the overall estimate.

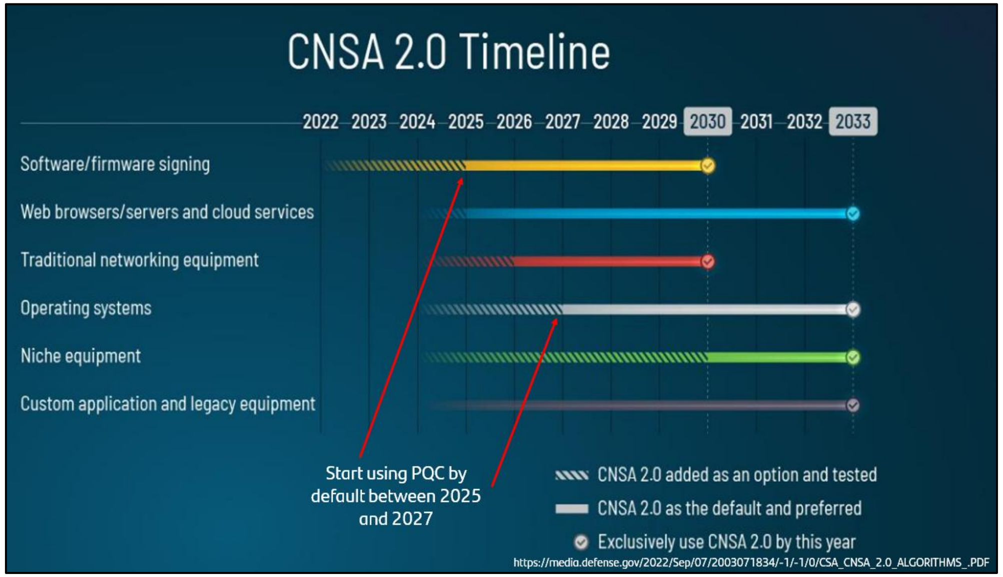
Estimated to be 1% of the yearly IT budget over 10 years

https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

Active regulations

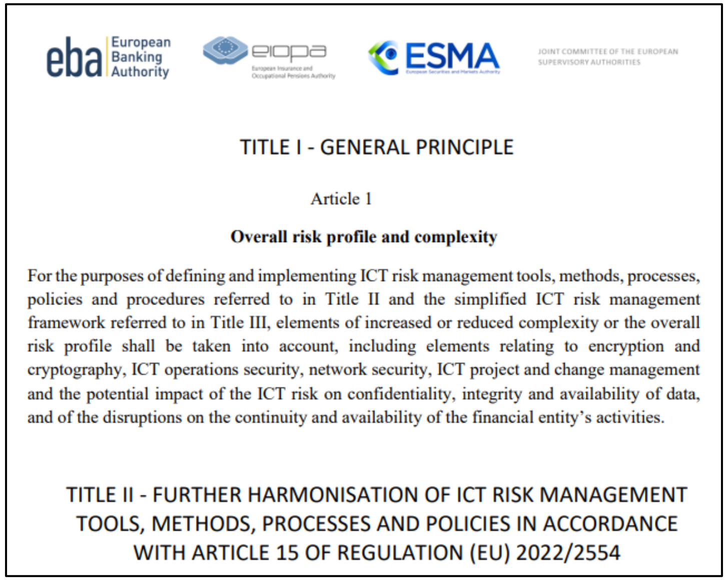
Block›chain

USA government



https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

EU DORA



eba European Banking Authority — eiopa European Insurance and Occupational Pensions Authority — ESMA European Securities and Markets Authority — JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

TITLE I - GENERAL PRINCIPLE

Article 1

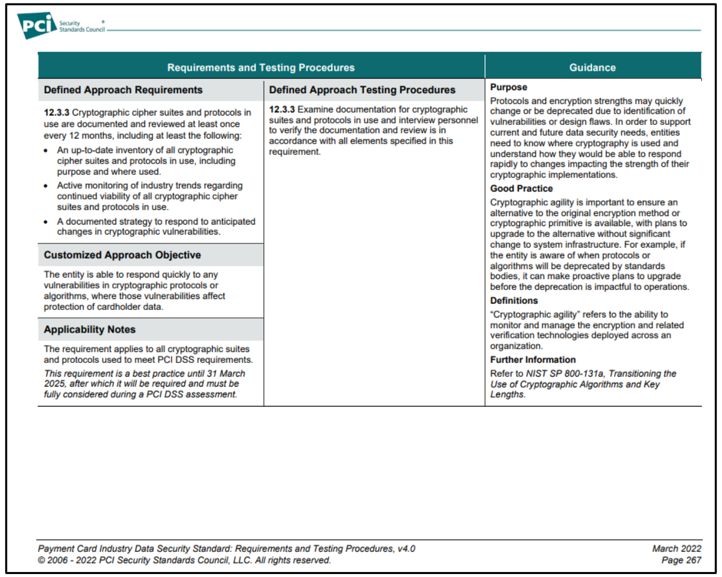
Overall risk profile and complexity

For the purposes of defining and implementing ICT risk management tools, methods, processes, policies and procedures referred to in Title II and the simplified ICT risk management framework referred to in Title III, elements of increased or reduced complexity or the overall risk profile shall be taken into account, including elements relating to encryption and cryptography, ICT operations security, network security, ICT project and change management and the potential impact of the ICT risk on confidentiality, integrity and availability of data, and of the disruptions on the continuity and availability of the financial entity's activities.

TITLE II - FURTHER HARMONISATION OF ICT RISK MANAGEMENT TOOLS, METHODS, PROCESSES AND POLICIES IN ACCORDANCE WITH ARTICLE 15 OF REGULATION (EU) 2022/2554

January 17th, 2025

PCI DSS



PCI Security Standards Council®

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations. **Good Practice** Cryptographic agility is important to ensure an alternative to the original encryption method or cryptographic primitive is available, with plans to upgrade to the alternative without significant change to system infrastructure. For example, if the entity is aware of when protocols or algorithms will be deprecated by standards bodies, it can make proactive plans to upgrade before the deprecation is impactful to operations. **Definitions** "Cryptographic agility" refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization. **Further Information** Refer to *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths*.
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	**12.3.3** Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.		
Applicability Notes		
The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0 *March 2022*
© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved. *Page 267*

April 1st, 2025

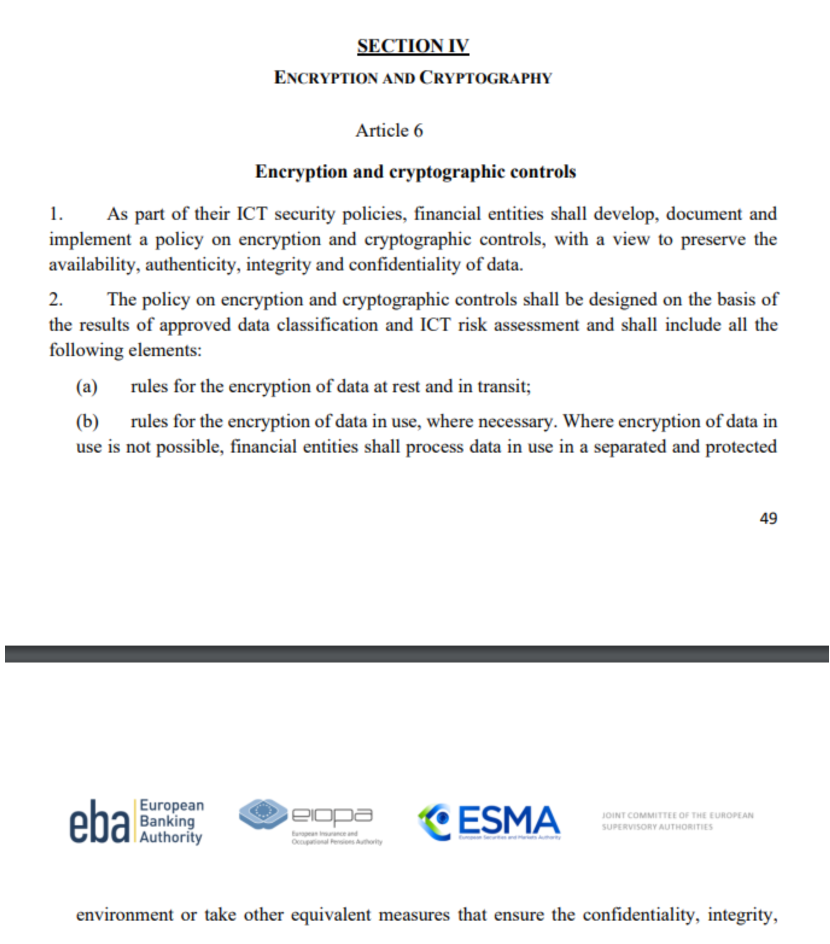
Santander

https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-_Final_report_on_draft_RTS_on_ICT_Risk_Management_Framework_and_on_simplified_ICT_Risk_Management_Framework.pdf
https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

DORA requirements – Art. 6

Block›chain

The draft Regulatory Technical Standard for ICT risk management contains a whole section for encryption and cryptography.



SECTION IV

ENCRYPTION AND CRYPTOGRAPHY

Article 6

Encryption and cryptographic controls

1. As part of their ICT security policies, financial entities shall develop, document and implement a policy on encryption and cryptographic controls, with a view to preserve the availability, authenticity, integrity and confidentiality of data.

2. The policy on encryption and cryptographic controls shall be designed on the basis of the results of approved data classification and ICT risk assessment and shall include all the following elements:

(a) rules for the encryption of data at rest and in transit;

(b) rules for the encryption of data in use, where necessary. Where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected

49

environment or take other equivalent measures that ensure the confidentiality, integrity,

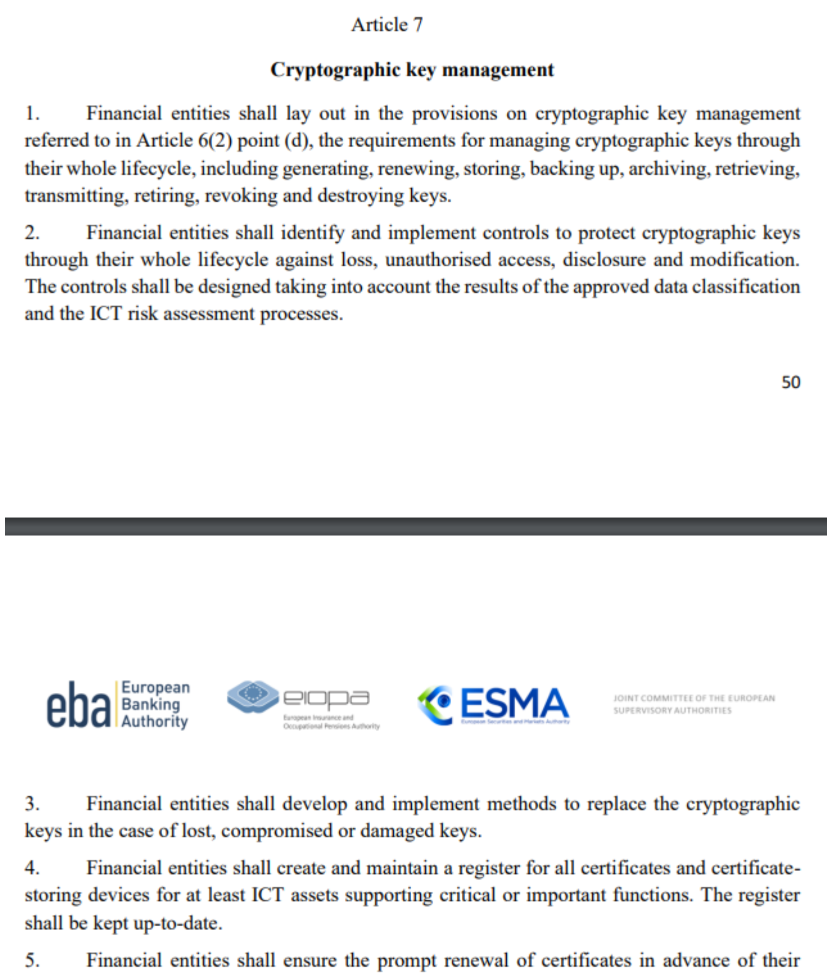
Requirement	Actions
Financial entities shall develop, document and implement a policy on encryption and cryptographic controls. The policy shall be designed on the basis of the results of approved data classification and risk assessment. It shall include rules defining when to encrypt data and for key lifecycle management. (Art. 6.1 and 2)	• Organizations must **verify and update their cryptography and data security policies**
Financial entities shall include in the policy on encryption and cryptographic controls criteria to select cryptographic techniques and use practices taking into account leading practices and standards. Where reliable techniques cannot be met, it shall adopt mitigation and monitoring measures to ensure resiliency against cyber threats. (Art. 6.3)	• The cryptography policies must specify valid algorithms based on standards. • Non-compliant use cases must be mitigated. • **This requires use case and technical inventories**
Financial entities shall include provisions to update or change the cryptographic technology to ensure they remain resilient against cyber threats. Where the financial entity cannot update or change the cryptographic technology, it shall adopt mitigation and monitoring measures to ensure they remain resilient against cyber threats. (Art. 6.4)	• **Crypto-agility**
Financial entities shall include a requirement in the policy controls to record the adoption of mitigation and monitoring measures adopted in accordance with paragraphs 3 and 4 and to provide a reasoned explanation for doing so. (Art. 6.5)	• **Monitoring of cryptography use cases and algorithms**

Santander

Enforcement date: January 17th, 2025

DORA requirements – Art. 7

The draft Regulatory Technical Standard for ICT risk management contains a whole section for encryption and cryptography.



Article 7

Cryptographic key management

1. Financial entities shall lay out in the provisions on cryptographic key management referred to in Article 6(2) point (d), the requirements for managing cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys.

2. Financial entities shall identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure and modification. The controls shall be designed taking into account the results of the approved data classification and the ICT risk assessment processes.

50

3. Financial entities shall develop and implement methods to replace the cryptographic keys in the case of lost, compromised or damaged keys.

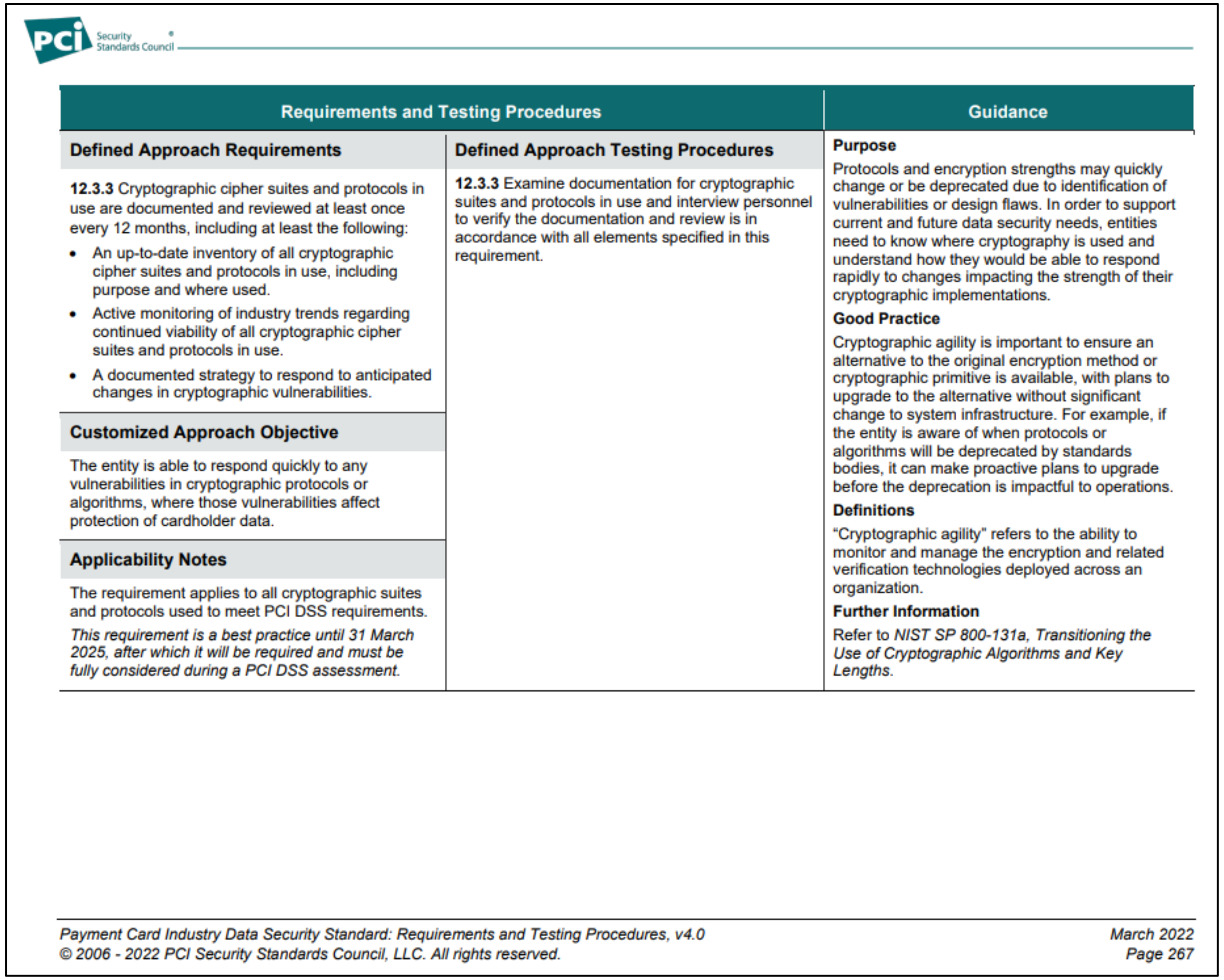
4. Financial entities shall create and maintain a register for all certificates and certificate-storing devices for at least ICT assets supporting critical or important functions. The register shall be kept up-to-date.

5. Financial entities shall ensure the prompt renewal of certificates in advance of their

Requirement	Actions
Financial entities shall define the requirements for managing cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys. (Art. 7.1)	• Policies must **include key lifecycle management**
Financial entities shall implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorized access, disclosure and modification, and implement methods to replace the cryptographic keys in the case of lost, compromised or damaged keys. (Art. 7.2 and 3)	• **Key lifecycle must be monitored and ready to tackle security events**
Financial entities shall create and maintain a register for all certificates and certificate storing devices for at least ICT assets supporting critical or important functions. (Art. 7.4)	• **Certificates and certificate storing devices inventory**
Certificates must be renewed before expiration. (Art. 7.5)	• **Certificate Lifecycle Management and Monitoring**

Enforcement date: January 17th, 2025

PCI-DSS requirements



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations. **Good Practice** Cryptographic agility is important to ensure an alternative to the original encryption method or cryptographic primitive is available, with plans to upgrade to the alternative without significant change to system infrastructure. For example, if the entity is aware of when protocols or algorithms will be deprecated by standards bodies, it can make proactive plans to upgrade before the deprecation is impactful to operations. **Definitions** "Cryptographic agility" refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization. **Further Information** Refer to *NIST SP 800-131a, Transitioning the Use of Cryptographic Algorithms and Key Lengths.*
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	**12.3.3** Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.	
Customized Approach Objective		
The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.		
Applicability Notes		
The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		

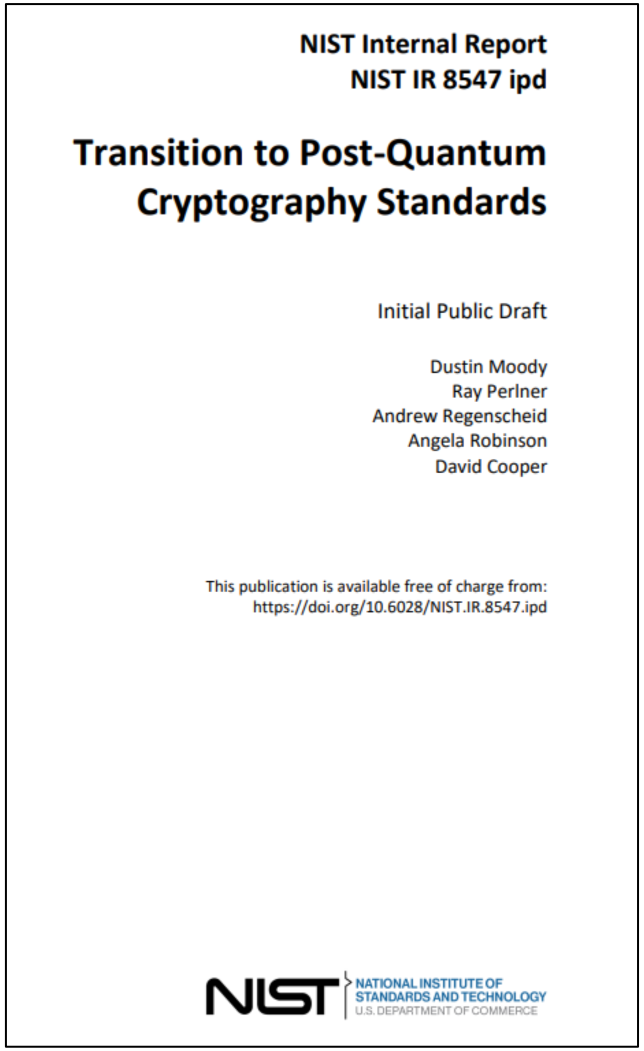
Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0 *March 2022*
© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved. *Page 267*

Requirement	Actions
Strong cryptography requested throughout the standard	• Organizations must **verify and update their cryptography and data security policies**
Methods to mitigate attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. (Req. 6.2.4)	• Organizations must include cryptography controls in their **QA and security audit processes**
• Up-to-date inventory of all cryptographic cipher suites and protocols in use • Active monitoring of industry trends regarding continued viability of all cryptographic • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities (Req. 12.3.3)	• **Cryptographic inventories** • **Crypto-agility**

Enforcement date: April 1st 2025

Block›chain

End of Life for Vulnerable Cryptography



NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

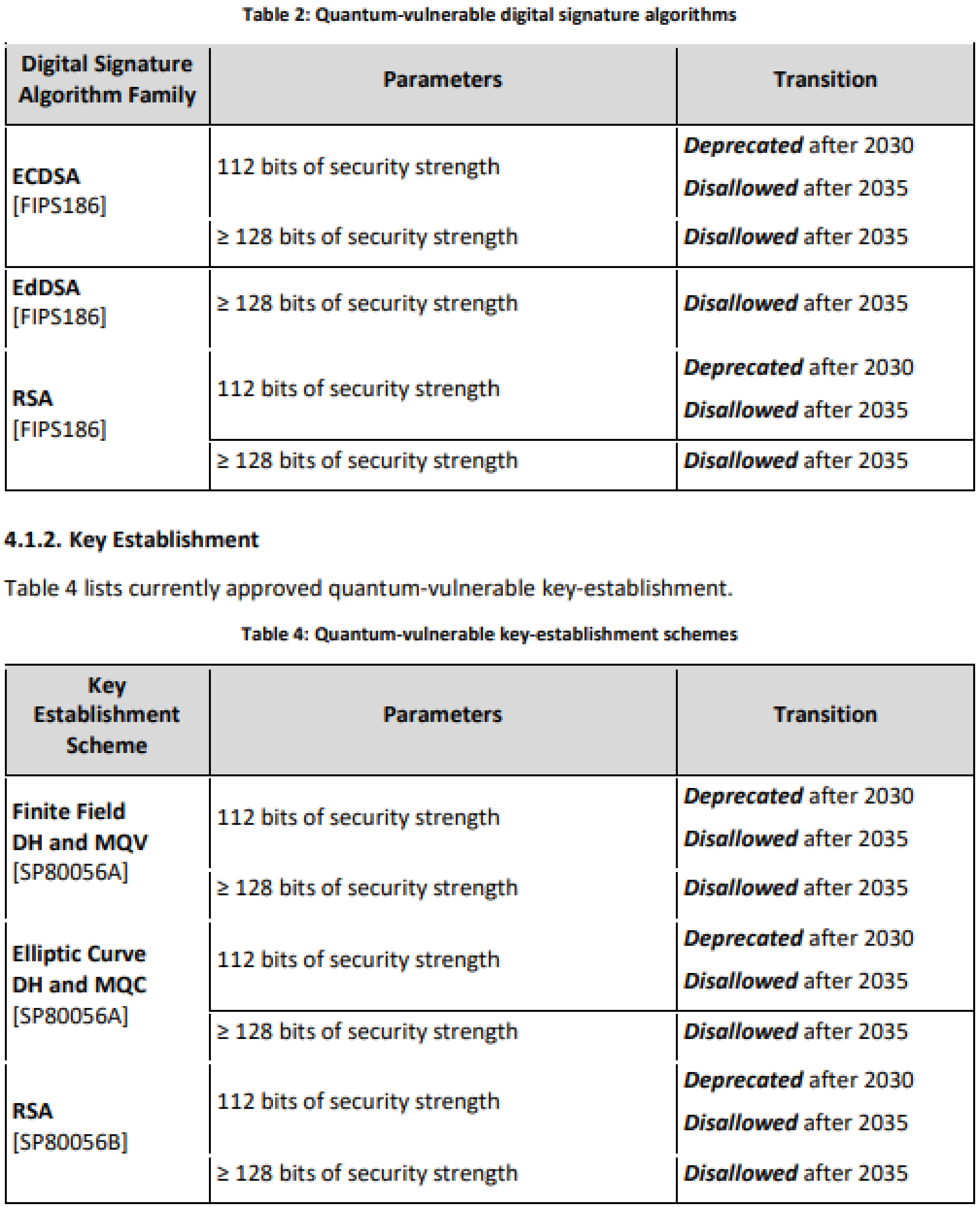


Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

4.1.2. Key Establishment

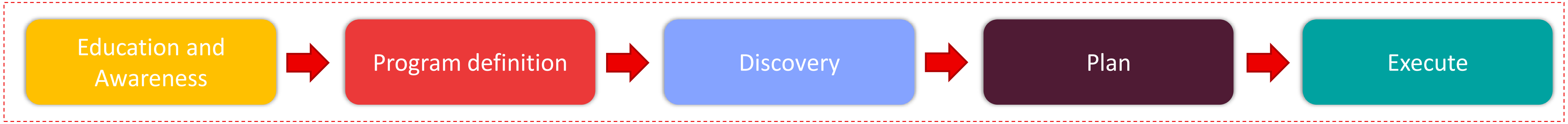
Table 4 lists currently approved quantum-vulnerable key-establishment.

Table 4: Quantum-vulnerable key-establishment schemes

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

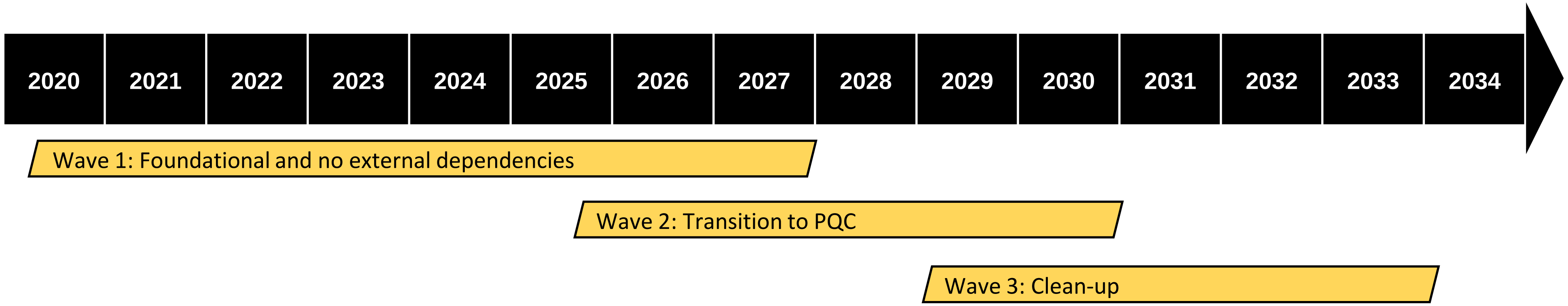
Santander

Roadmap to Quantum-Readiness



Our **long-term timeline** considers three main waves:

- **Wave 1 Foundational activities and those without external dependencies** (No-Regret Actions)
- **Wave 2 Transition to PQC**
- **Wave 3 Clean-up**



Wave 1: Foundational and No-Dependencies Activities

Main goals “No-Regret Actions”

The talent and practices challenge

Update cryptographic capabilities

- **Identify and upskill global cryptographic talent**
- **Establish a mature cryptography management framework. Update cryptography-related policies**
- **Understand future implications of PQC**

The inventory and scattered knowledge challenge

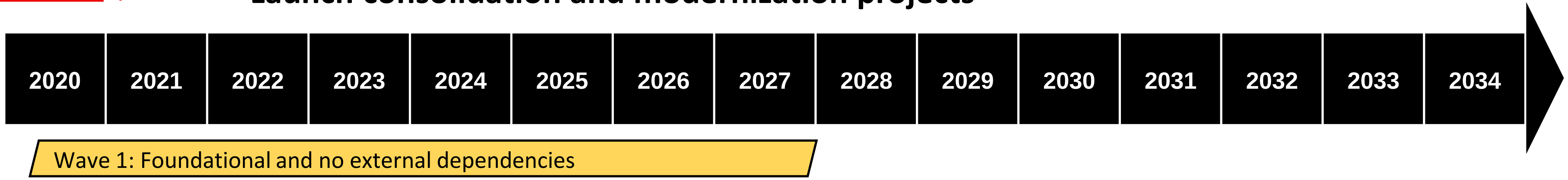
Understand our cryptographic landscape

- **Identify and inventory cryptographic use cases and assets**
- **Assess existing practices, stakeholders and associated roadmaps**
- **Upgrade current practices to a homogeneous and mature standard**

Optimizing future transition projects

Prepare the TO-BE

- **Identify best solutions and expertise for the different use cases**
- **Identify gaps vs expected future features and dependencies. Focus on legacies needing refactor**
- **Launch consolidation and modernization projects**



Wave 2: Transition to PQC

Main goals “Adapting to the new standards”

Timeline based on risk drivers

Priority-based, gradual transition

- Perform risk, dependency and impact assessments for the different use cases
- Design gradual transition plans with coexistence of classical and PQ cryptography (Hybrid)
- Establish a priority-based execution roadmap

Protect the future

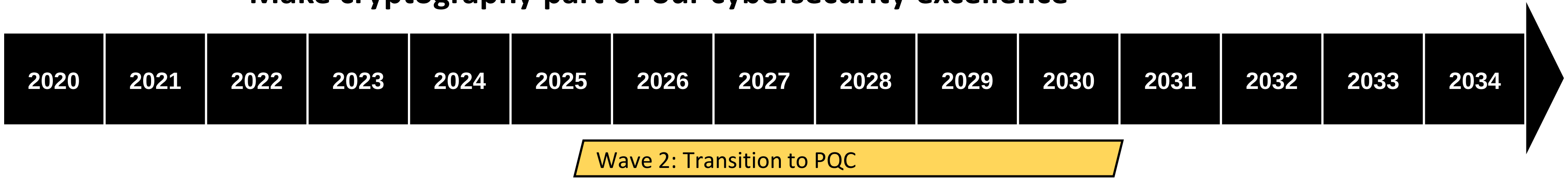
Implement crypto-agility

- Implement cryptography usage monitorization and control
- Introduce automation features in cryptography usage
- Establish exit plans while transitioning to PQC

Lead the challenge

Demonstrate a strong cybersecurity cryptographic leadership

- Have a clear and open transition roadmap
- Execute the transition in a simple and global manner
- Make cryptography part of our cybersecurity excellence



Wave 3: Clean-up

Main goals

“Decommissioning obsolete cryptography”

Ensure completeness

Understand legacy use cases of classical cryptography

- **Identify remaining classical cryptography**
- **Assess dependencies not discovered in previous waves**

Enter PQC only

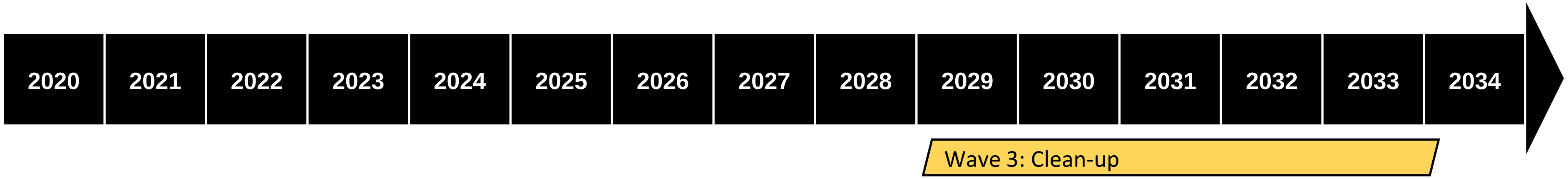
Decommission classical cryptography

- **Eliminate classical cryptography configurations**
- **Mitigate or refactor remaining dependencies**

Mature BAU management

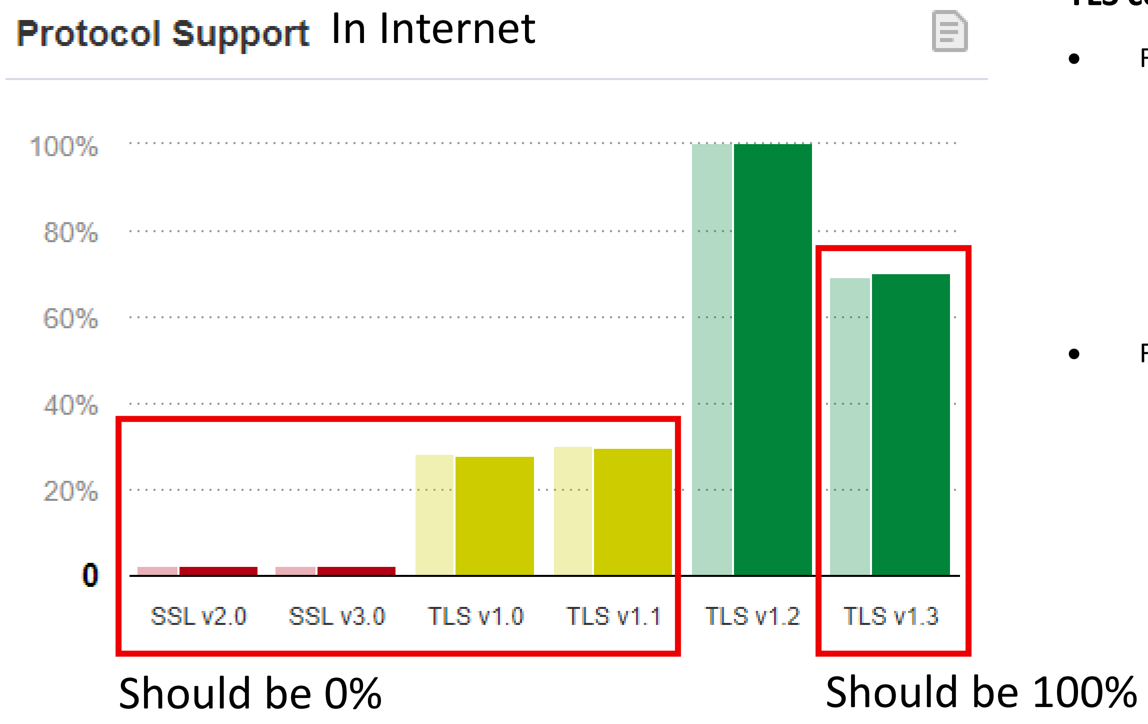
Make crypto-agility practical

- **Update our cryptography management framework**
- **Exercise practical crypto-agility to ensure we are ready for future challenges**


2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034

Wave 3: Clean-up

TLS Evolution



TLS compliance model

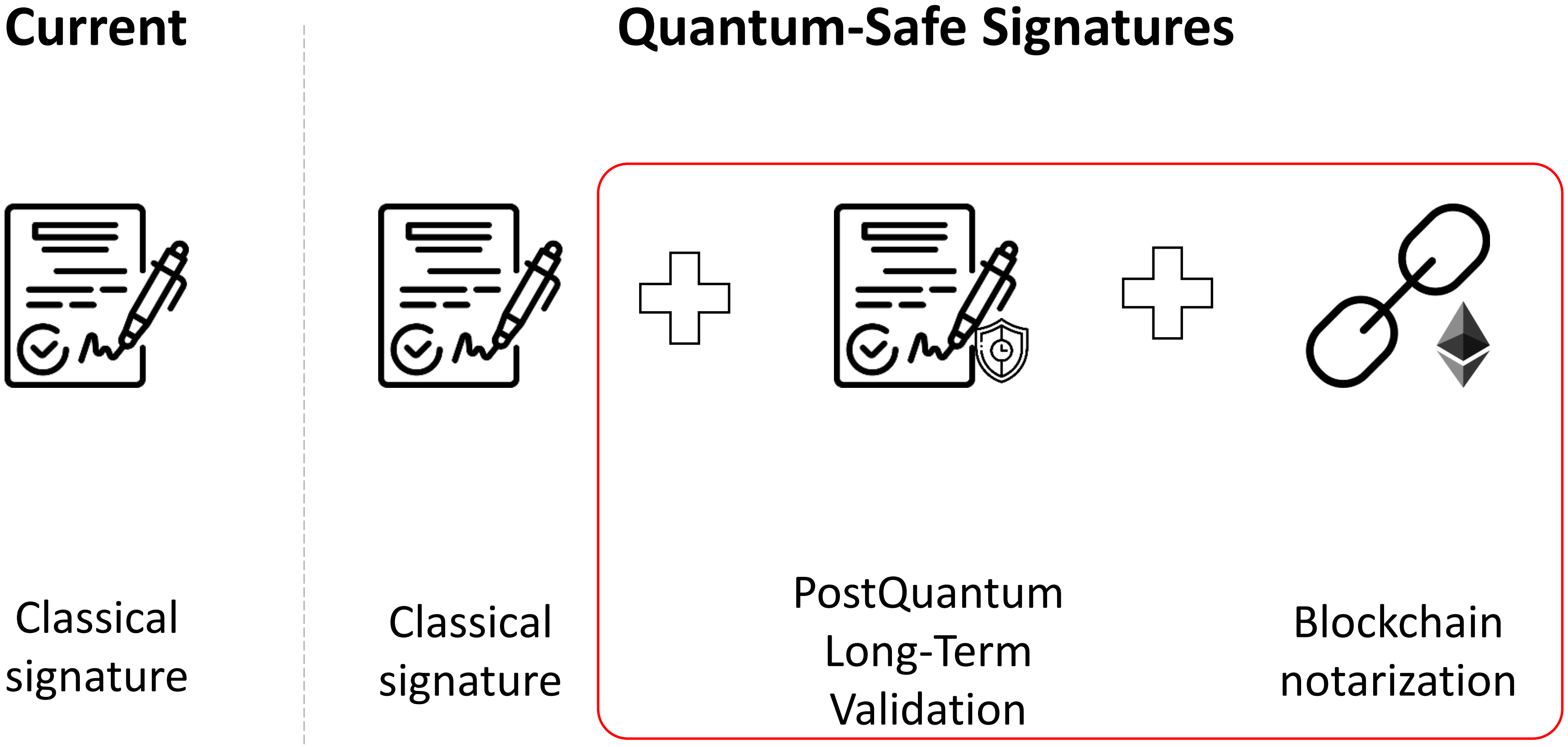
- For **TLS VERSION COMPLIANCE**, number of TLS services exposing:
  - *Compliant* configurations, all of them *Safe*.
  - *Non-compliant* configurations, which can be:
    - *Safe but obsolete*: If they support TLSv1.2 only.
    - *Forbidden*: If they support any version lower than TLSv1.2.
- For **CIPHERSUITE COMPLIANCE**, number of TLS services exposing:
  - *Compliant* configurations, all of them *Safe*.
  - *Non-compliant* configurations, which can be:
    - *Safe:* All configured ciphersuites are *Compliant* and *Safe* but the configuration does not follow the format specified in our recommendation.
    - *Weak*: If they support non-compliant, but not forbidden ciphersuites.
    - *Forbidden*: If they support any forbidden ciphersuite.

Visibility of 9000 Apache instances globally already by adapting existing tools!

Santander

https://www.ssllabs.com/ssl-pulse/

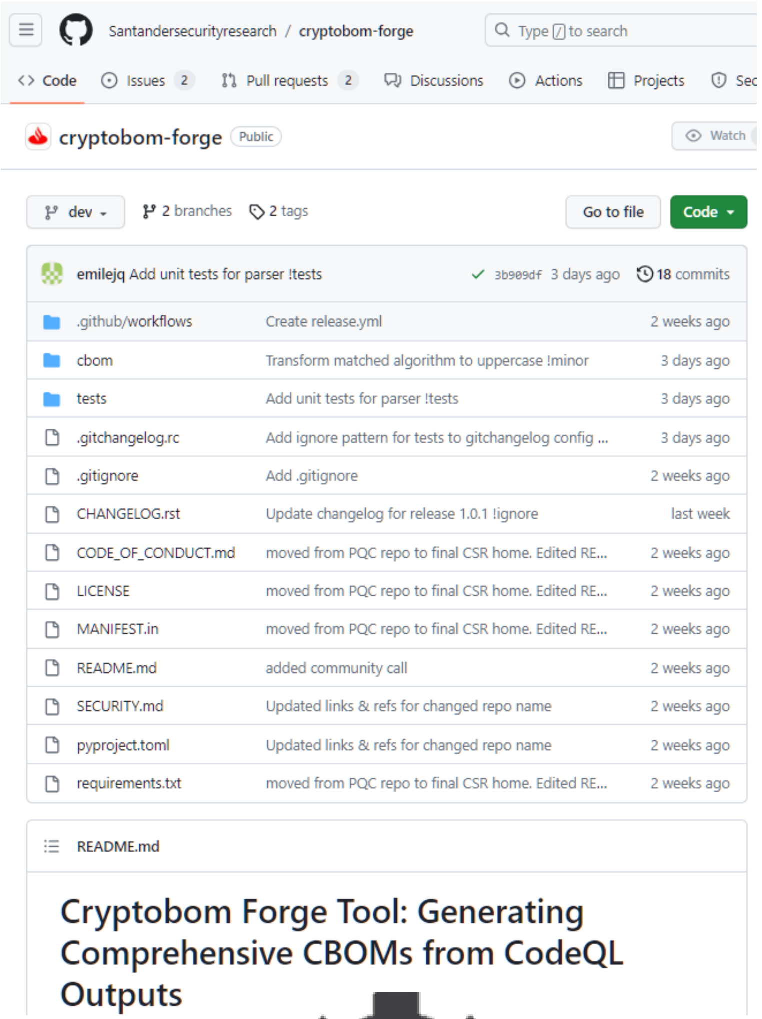
Quantum-safe Document Signatures



Provides a quantum-safe, independent and immutable proof of existence of the signatures when the algorithms were secure

Opensource Cryptography Bill of Materials

Block<>chain



cryptobom-forge

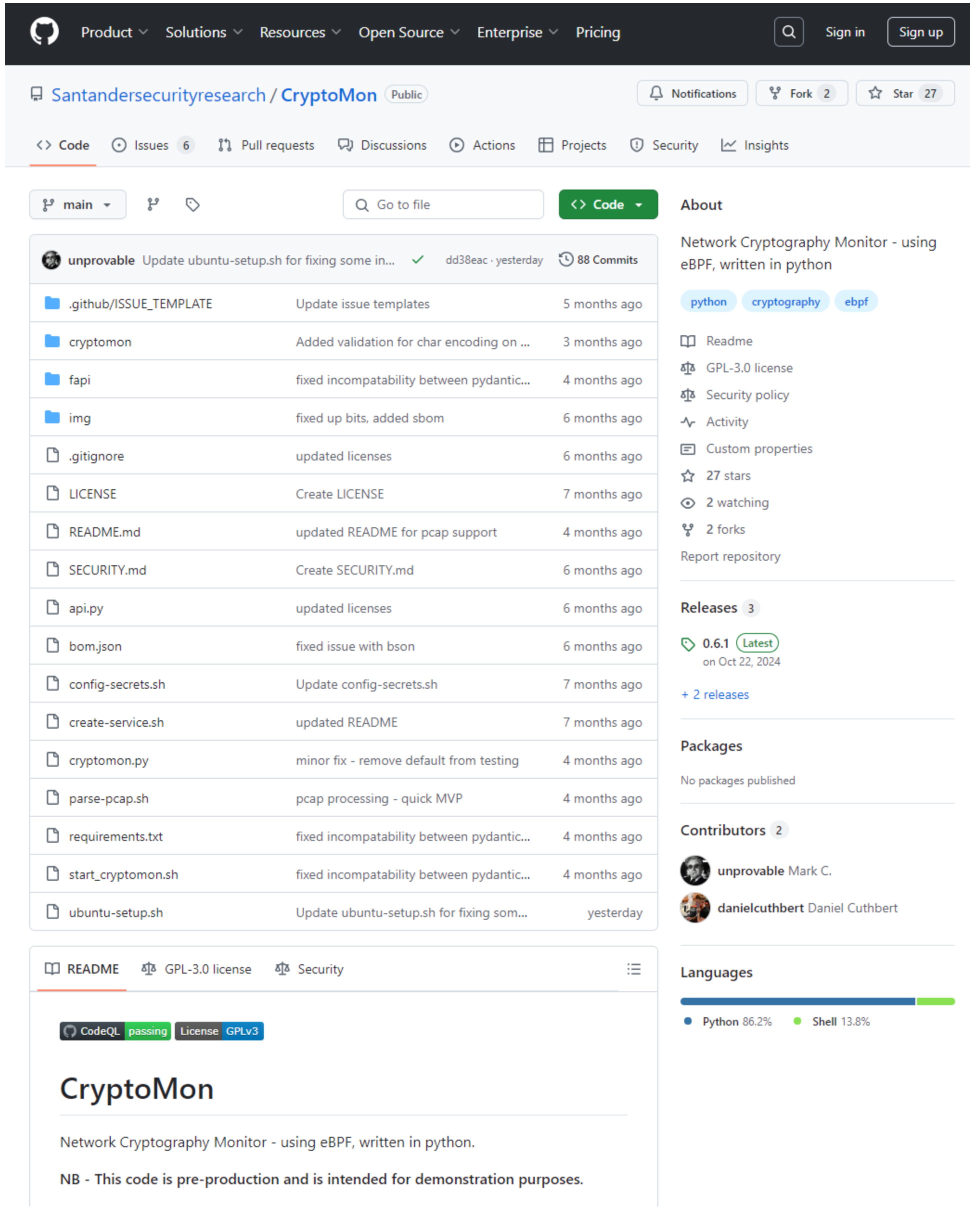
2 branches 2 tags

emilejq Add unit tests for parser !tests ✓ 3b909df 3 days ago 18 commits

.github/workflows	Create release.yml	2 weeks ago
cbom	Transform matched algorithm to uppercase !minor	3 days ago
tests	Add unit tests for parser !tests	3 days ago
.gitchangelog.rc	Add ignore pattern for tests to gitchangelog config ...	3 days ago
.gitignore	Add .gitignore	2 weeks ago
CHANGELOG.rst	Update changelog for release 1.0.1 !ignore	last week
CODE_OF_CONDUCT.md	moved from PQC repo to final CSR home. Edited RE...	2 weeks ago
LICENSE	moved from PQC repo to final CSR home. Edited RE...	2 weeks ago
MANIFEST.in	moved from PQC repo to final CSR home. Edited RE...	2 weeks ago
README.md	added community call	2 weeks ago
SECURITY.md	Updated links & refs for changed repo name	2 weeks ago
pyproject.toml	Updated links & refs for changed repo name	2 weeks ago
requirements.txt	moved from PQC repo to final CSR home. Edited RE...	2 weeks ago

README.md

Cryptobom Forge Tool: Generating Comprehensive CBOMs from CodeQL Outputs



Santandersecurityresearch / CryptoMon

unprovable Update ubuntu-setup.sh for fixing some in... ✓ dd38eac · yesterday 88 Commits

.github/ISSUE_TEMPLATE	Update issue templates	5 months ago
cryptomon	Added validation for char encoding on ...	3 months ago
fapi	fixed incompatability between pydantic...	4 months ago
img	fixed up bits, added sbom	6 months ago
.gitignore	updated licenses	6 months ago
LICENSE	Create LICENSE	7 months ago
README.md	updated README for pcap support	4 months ago
SECURITY.md	Create SECURITY.md	6 months ago
api.py	updated licenses	6 months ago
bom.json	fixed issue with bson	6 months ago
config-secrets.sh	Update config-secrets.sh	7 months ago
create-service.sh	updated README	7 months ago
cryptomon.py	minor fix - remove default from testing	4 months ago
parse-pcap.sh	pcap processing - quick MVP	4 months ago
requirements.txt	fixed incompatability between pydantic...	4 months ago
start_cryptomon.sh	fixed incompatability between pydantic...	4 months ago
ubuntu-setup.sh	Update ubuntu-setup.sh for fixing som...	yesterday

About

Network Cryptography Monitor - using eBPF, written in python

python cryptography ebpf

Readme

GPL-3.0 license

Security policy

Activity

Custom properties

27 stars

2 watching

2 forks

Report repository

Releases 3

0.6.1 Latest on Oct 22, 2024

+ 2 releases

Packages

No packages published

Contributors 2

unprovable Mark C.

danielcuthbert Daniel Cuthbert

Languages

● Python 86.2% ● Shell 13.8%

CryptoMon

Network Cryptography Monitor - using eBPF, written in python.

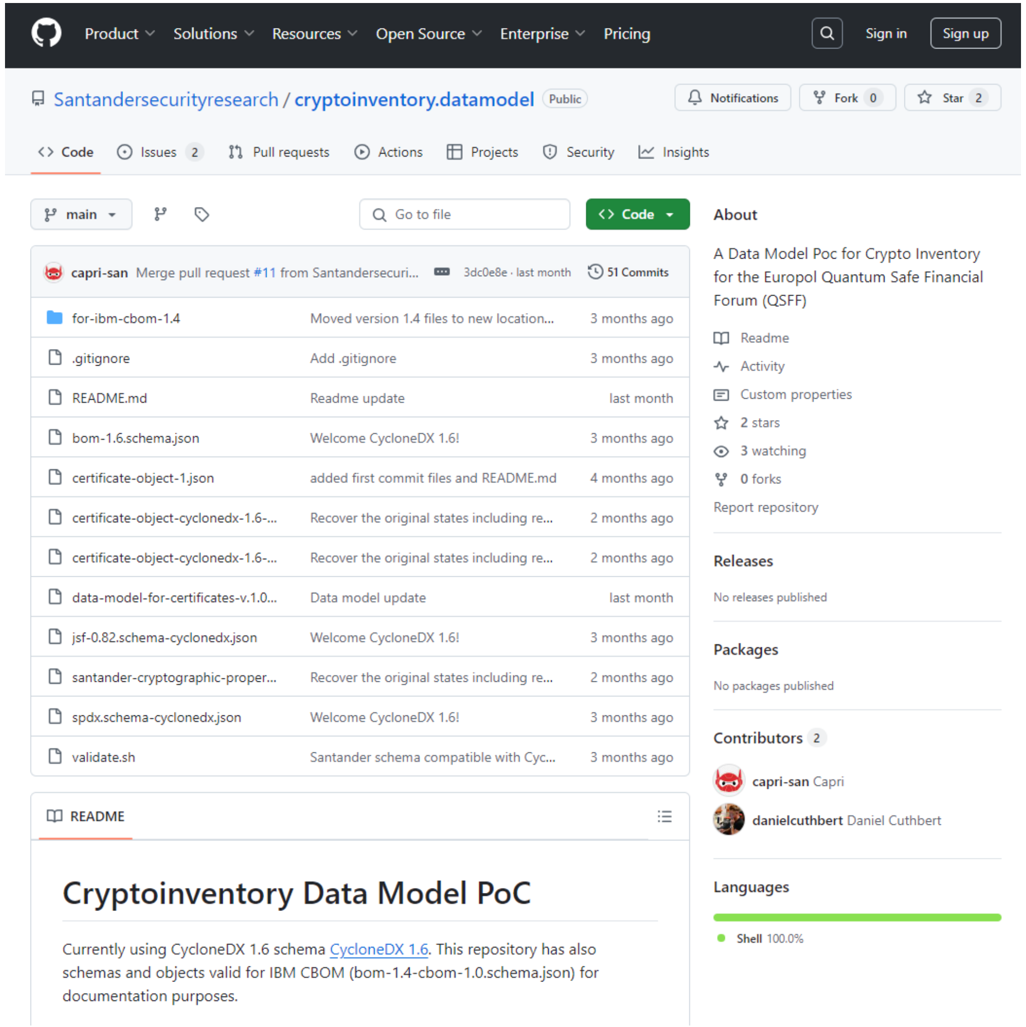
NB - This code is pre-production and is intended for demonstration purposes.

Santander

https://github.com/Santandersecurityresearch/

Block<>chain

Certificate Inventory in CMDB



Santandersecurityresearch / cryptoinventory.datamodel Public

Notifications | Fork 0 | Star 2

Code | Issues 2 | Pull requests | Actions | Projects | Security | Insights

main | Go to file | Code

capri-san Merge pull request #11 from Santandersecuri... 3dc0e8e · last month 51 Commits

for-ibm-cbom-1.4	Moved version 1.4 files to new location...	3 months ago
.gitignore	Add .gitignore	3 months ago
README.md	Readme update	last month
bom-1.6.schema.json	Welcome CycloneDX 1.6!	3 months ago
certificate-object-1.json	added first commit files and README.md	4 months ago
certificate-object-cyclonedx-1.6-...	Recover the original states including re...	2 months ago
certificate-object-cyclonedx-1.6-...	Recover the original states including re...	2 months ago
data-model-for-certificates-v.1.0...	Data model update	last month
jsf-0.82.schema-cyclonedx.json	Welcome CycloneDX 1.6!	3 months ago
santander-cryptographic-proper...	Recover the original states including re...	2 months ago
spdx.schema-cyclonedx.json	Welcome CycloneDX 1.6!	3 months ago
validate.sh	Santander schema compatible with Cyc...	3 months ago

README

Cryptoinventory Data Model PoC

Currently using CycloneDX 1.6 schema CycloneDX 1.6. This repository has also schemas and objects valid for IBM CBOM (bom-1.4-cbom-1.0.schema.json) for documentation purposes.

About

A Data Model Poc for Crypto Inventory for the Europol Quantum Safe Financial Forum (QSFF)

Readme
Activity
Custom properties
2 stars
3 watching
0 forks
Report repository

Releases

No releases published

Packages

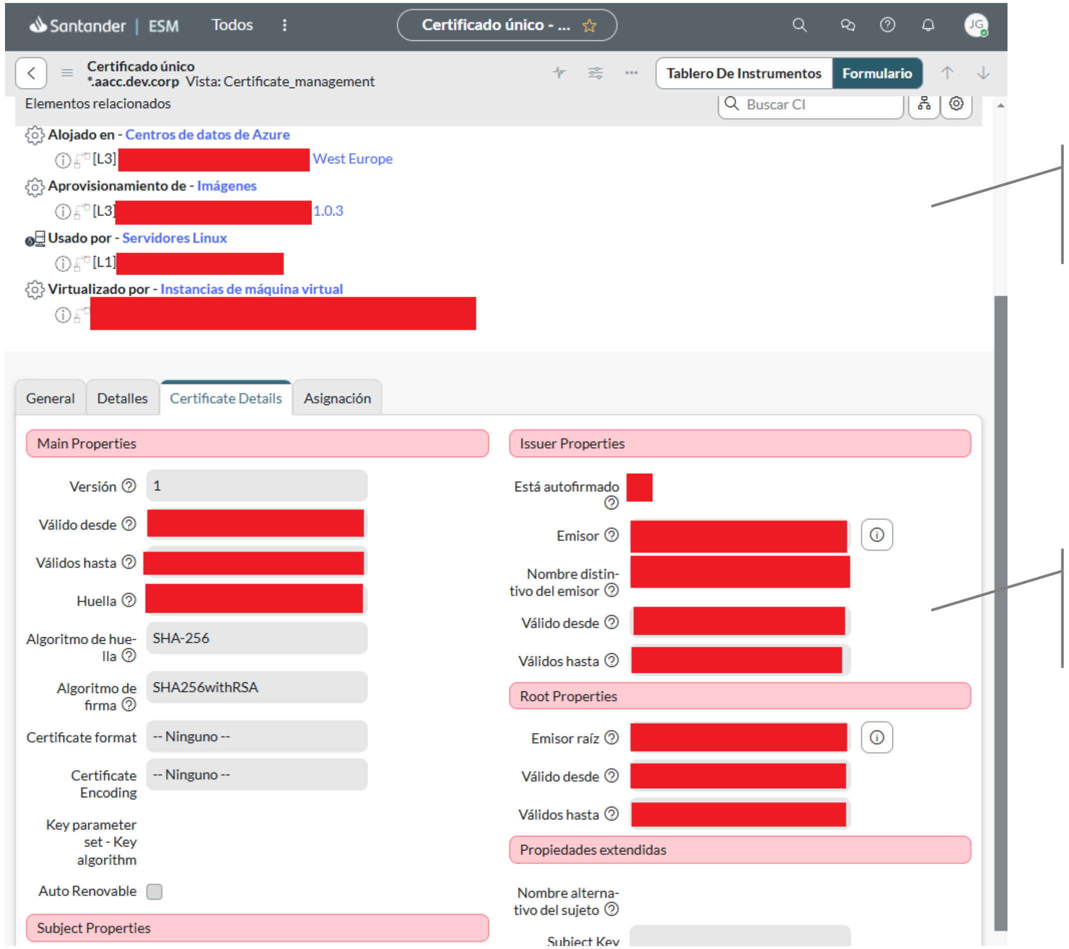
No packages published

Contributors 2

capri-san Capri
danielcuthbert Daniel Cuthbert

Languages

Shell 100.0%



Certificado único
*.aacc.dev.corp Vista: Certificate_management

Elementos relacionados

Alojado en - Centros de datos de Azure
[L3] [redacted] West Europe

Aprovisionamiento de - Imágenes
[L3] [redacted] 1.0.3

Usado por - Servidores Linux
[L1] [redacted]

Virtualizado por - Instancias de máquina virtual
[redacted]

General | Detalles | Certificate Details | Asignación

Main Properties

Versión	1
Válido desde	[redacted]
Válidos hasta	[redacted]
Huella	[redacted]
Algoritmo de huella	SHA-256
Algoritmo de firma	SHA256withRSA
Certificate format	-- Ninguno --
Certificate Encoding	-- Ninguno --
Key parameter set - Key algorithm	
Auto Renovable	□

Subject Properties

Issuer Properties

Está autofirmado	[redacted]
Emisor	[redacted]
Nombre distintivo del emisor	[redacted]
Válido desde	[redacted]
Válidos hasta	[redacted]

Root Properties

Emisor raíz	[redacted]
Válido desde	[redacted]
Válidos hasta	[redacted]

Propiedades extendidas

Nombre alternativo del sujeto

Subject Key

Certificate locations

Certificate details

Santander

https://github.com/Santandersecurityresearch/cryptoinventory.datamodel

Take aways

Awareness is growing and the finance sector is taking action

The transition is a **current regulatory imperative**, independent from the evolution of quantum computing

A **unified action plan** would be highly beneficial

Wishlist

```
$ httpd --output-cbom
```

```
HKEY_LOCAL_MACHINE\...\IISADMIN\...\cbom
```

Software applications to provide their CBOMs

Standard support of cryptography in CMDBs

Multivendor, multitenant, enterprise scale Key Management Systems

¡Gracias!

Jaime Gómez García

Head of Quantum, Banco Santander | Chair of the Quantum...

Santander