3 December 2025

Legal Aspects of Post-Quantum Digital Signatures

Santander Group Legal for Technology, Digital and Data

PQC Migration Conference

Sofía Serrat Vallespín

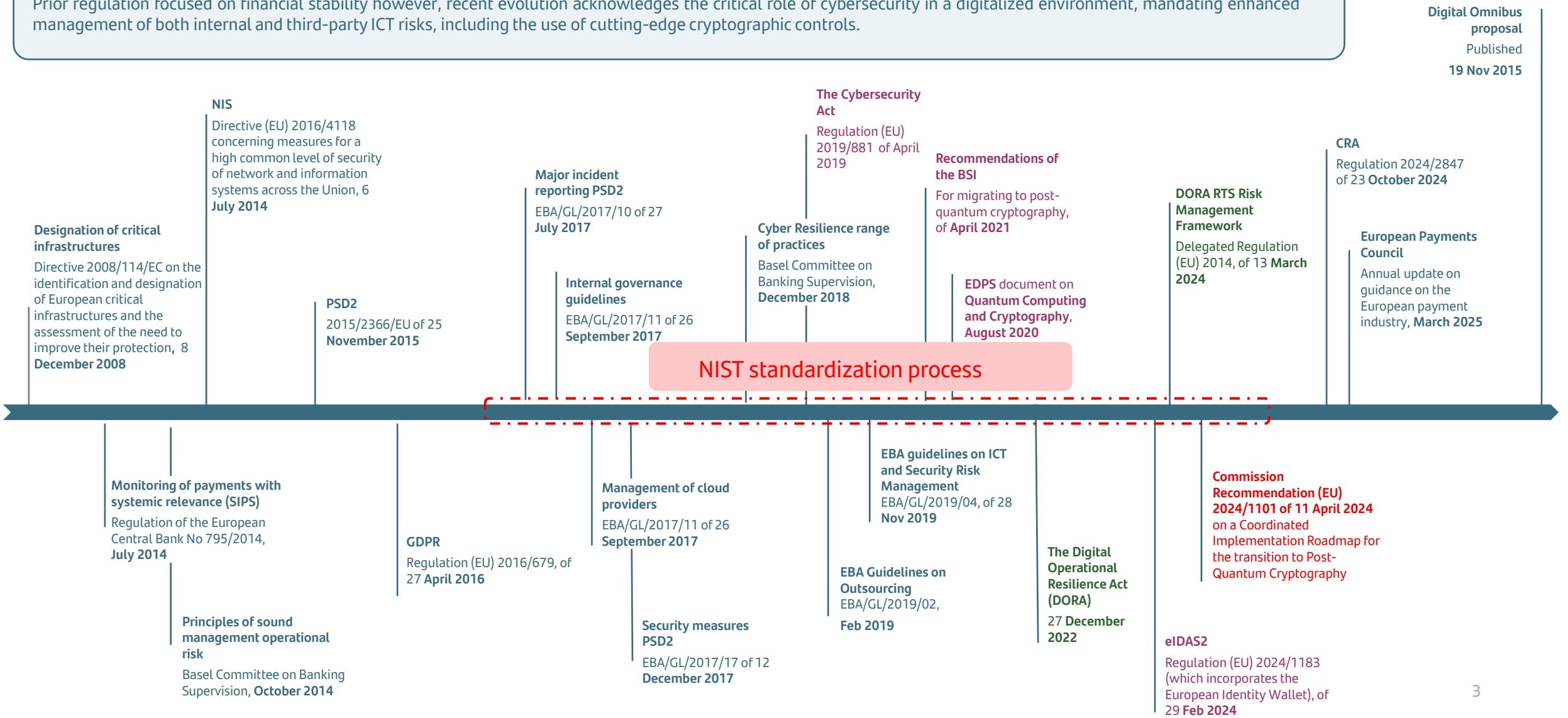
Santander

Introduction

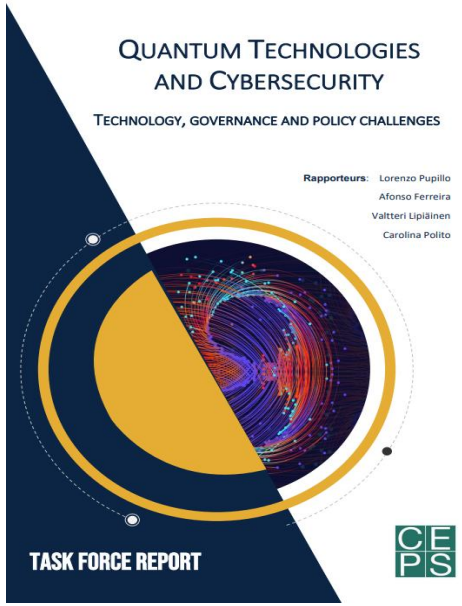
- **The regulatory environment governing cryptographic controls is multi-layered**.
- The EU's legislative trajectory over the last decade shows **a progressive shift from implicit "*state-of-the-art*"** cybersecurity practices **towards more granular** cryptographic controls.
- The world has **become very political and highly influenced by geoeconomics.**
- At the same time, **international bodies are calling for convergence.**
- In November 2025, the **Financial Stability Board urged the G20 to drive consistent reforms and reduce regulatory divergence**, urging coordinated action on several fronts, **including emerging risks.**
- Parallel EU initiatives such as the **Digital Omnibus Proposal** aim to streamline digital regulation.
- The way that this should be affecting the quantum field is in the **international process of cooperation.**

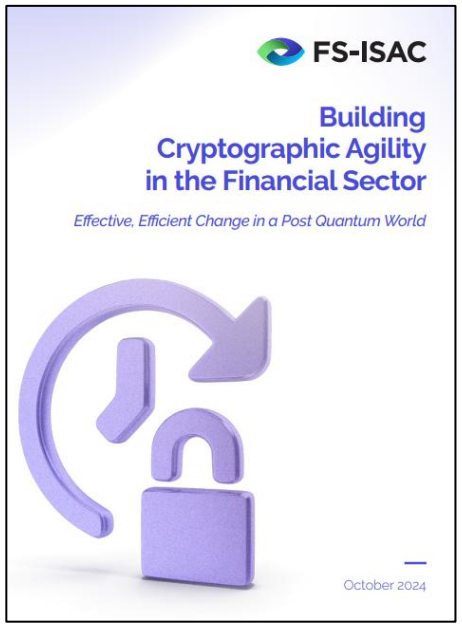
Evolution of the regulation impacting operational risks and resilience in the financial sector

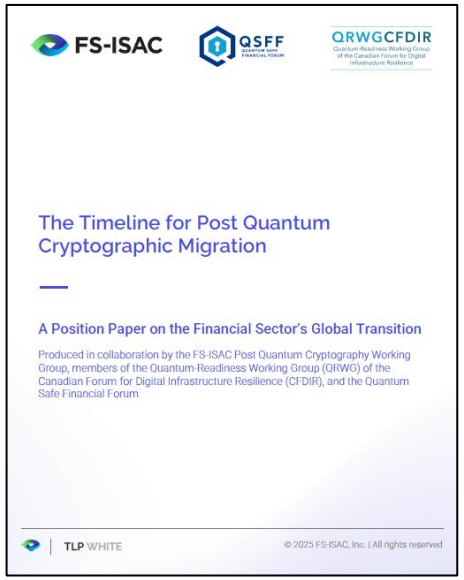
Prior regulation focused on financial stability however, recent evolution acknowledges the critical role of cybersecurity in a digitalized environment, mandating enhanced management of both internal and third-party ICT risks, including the use of cutting-edge cryptographic controls.

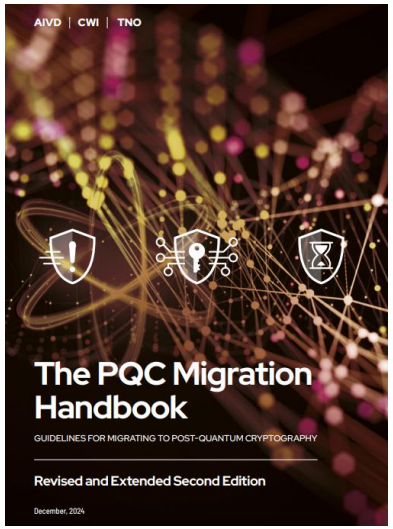


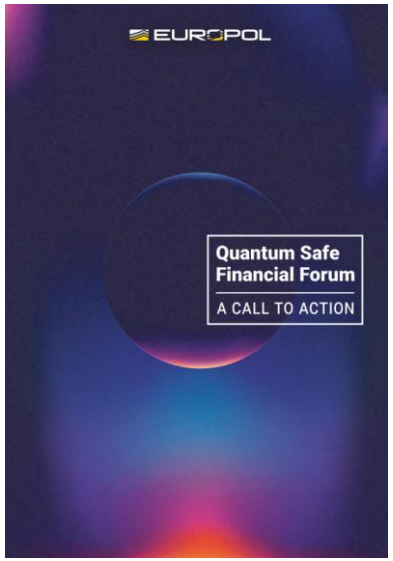
Latest position statements relevant for the financial sector in the EU

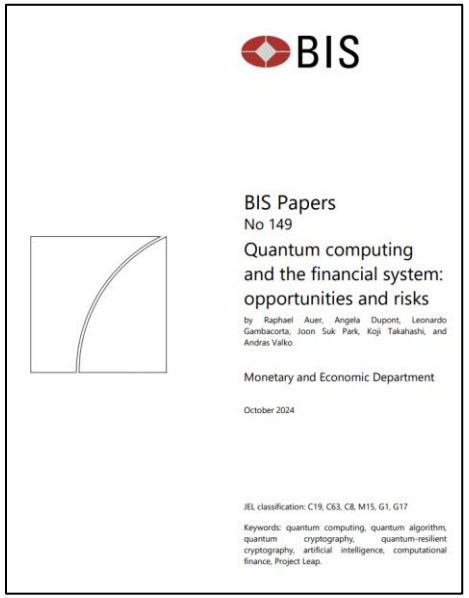


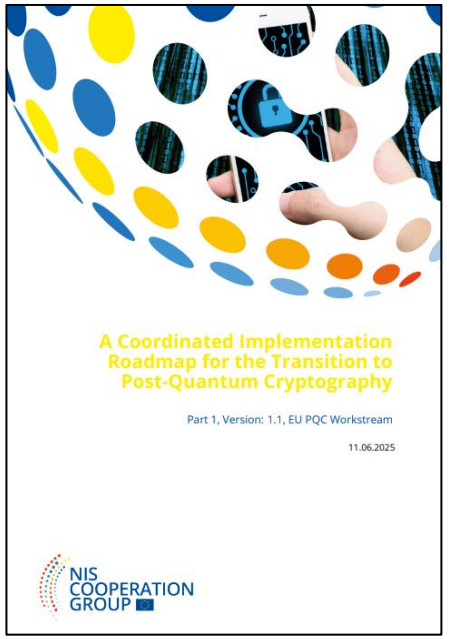












Regulation 2016/679 (GDPR) – Art. 32 security of processing

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

- Under the GDPR, security of processing is not defined through rigid technical prescriptions but through risk-based and state-of-the-art obligations.
- Encryption and pseudonymisation are explicitly cited as examples of such measures.
- Supervisory authorities interpret "*state of the art*" as requiring ***ongoing review of encryption standards.***
- ***Art. 5(f)*** *also refers to the principle of* ***integrity and confidentiality***.

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

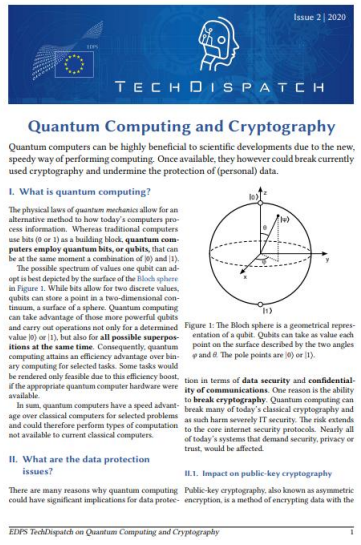
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Organisations should consider for how long they need to guarantee absolute confidentiality of data and protection from retrospective decryption.

For this reason, some organisations may be interested in preparing appropriate risk assessment as well as contingency and migration plans. It refers to the [The German Federal Office for Information Security (2020) has developed initial recommendations for the migration to post-quantum cryptography](#)."


Issue 2 | 2020

TECH DISPATCH

Quantum Computing and Cryptography

Quantum computers can be highly beneficial to scientific developments due to the new, speedy way of performing computing. Once available, they however could break currently used cryptography and undermine the protection of (personal) data.

I. What is quantum computing?

The physical laws of *quantum mechanics* allow for an alternative method to how today's computers process information. Whereas traditional computers use bits (0 or 1) as a building block, **quantum computers employ quantum bits, or qubits**, that can be at the same moment a combination of $|0\rangle$ and $|1\rangle$.

The possible spectrum of values one qubit can adopt is best depicted by the surface of the Bloch sphere in Figure 1. While bits allow for two discrete values, qubits can store a point in a two-dimensional continuum, a surface of a sphere. Quantum computing can take advantage of those more powerful qubits and carry out operations not only for a determined value $|0\rangle$ or $|1\rangle$, but also for **all possible superpositions at the same time**. Consequently, quantum computing attains an efficiency advantage over binary computing for selected tasks. Some tasks would be rendered only feasible due to this efficiency boost, if the appropriate quantum computer hardware were available.

In sum, quantum computers have a speed advantage over classical computers for selected problems and could therefore perform types of computation not available to current classical computers.

Figure 1: The Bloch sphere is a geometrical representation of a qubit. Qubits can take as value each point on the surface described by the two angles φ and θ. The pole points are $|0\rangle$ or $|1\rangle$.

II. What are the data protection issues?

There are many reasons why quantum computing could have significant implications for data protection in terms of **data security** and **confidentiality of communications**. One reason is the ability to **break cryptography**. Quantum computing can break many of today's classical cryptography and as such harm severely IT security. The risk extends to the core internet security protocols. Nearly all of today's systems that demand security, privacy or trust, would be affected.

II.1. Impact on public-key cryptography

Public-key cryptography, also known as asymmetric encryption, is a method of encrypting data with the

Regulation 2016/679 (GDPR) – Art. 35 Data Protection Impact Assessment

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

- A DPIA is required when processing is likely to result in a high risk to individuals.
- To conduct the DPIA, the risk to confidentiality, integrity and availability must be analysed, including the measures you take to mitigate them.
- Cryptography is one of the main safeguards used to mitigate risks to confidentiality and integrity.
- Therefore, a DPIA cannot be complete without assessing cryptographic measures.
- The **EDPB** explicitly identifies encryption, pseudonymization, hashing and key management policies as examples that must be evaluated in DPIAs

New!!* *Data Protection Impact Assessment – Digital Omnibus published Nov 2025

Paragraph 7 would harmonise the lists of processing activities requiring and not requiring data protection impact assessment by providing that a single lists of processing operations which require and do not require a data protection impact assessment be provided at EU level, thereby contributing to the harmonisation of the notion of high risk. The European Data Protection Board would be obliged to prepare proposals for such lists. It would also be obliged to prepare a proposal for a common template and common methodology for conducting data protection impact assessments, which the Commission would be empowered to adopt by means of an implementing act, after reviewing them, as necessary.

Santander

Regulation 2016/679 (GDPR) – Art. 35 Data protection by design and by default

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Design systems so algorithms and keys can be changed without redesigning whole apps.

Agility could be seen as a technical expression of "by design" because it allows "state of the art" controls.

Therefore, isn't cryptographic agility how supervisors call now this same concept?

Directive 2022/2555 (NIS2) – Art. 21

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

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.

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

TECHNICAL IMPLEMENTATION GUIDANCE

On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards **technical and methodological requirements of cybersecurity risk-management measures**

JUNE 2025, VERSION 1.0

ENISA has provided comprehensive guidance on PQC, outlining the five main algorithm families and recommending hybrid implementations and key mixing strategies to mitigate quantum threats even before full standardization is complete.

https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

RTS on ICT Risk Management Framework

Delegated Regulation 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554

Article 6

Encryption and cryptographic controls

1. As part of their ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement a policy on encryption and cryptographic controls.

2. Financial entities shall design the policy on encryption and cryptographic controls referred to in paragraph 1 on the basis of the results of an approved data classification and ICT risk assessment. That policy shall contain rules for all of the following:

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

(b) the encryption of data in use, where necessary;

(c) the encryption of internal network connections and traffic with external parties;

(d) the cryptographic key management referred to in Article 7, laying down rules on the correct use, protection, and lifecycle of cryptographic keys.

For the purposes of point (b), where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment, or take equivalent measures to ensure the confidentiality, integrity, authenticity, and availability of data.

3. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 criteria for the selection of cryptographic techniques and use practices, taking into account leading practices, and standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012, and the classification of relevant ICT assets established in accordance with Article 8(1) of Regulation (EU) 2022/2554. Financial entities that are not able to adhere to the leading practices or standards, or to use the most reliable techniques, shall adopt mitigation and monitoring measures that ensure resilience against cyber threats.

4. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 provisions for updating or changing, where necessary, the cryptographic technology on the basis of developments in cryptanalysis. Those updates or changes shall ensure that the cryptographic technology remains resilient against cyber threats, as required by Article 10(2), point (a). Financial entities that are not able to update or change the cryptographic technology shall adopt mitigation and monitoring measures that ensure resilience against cyber threats.

5. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 a requirement 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.

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

RTS on ICT Risk Management Framework

Delegated Regulation 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554

Article 6

Encryption and cryptographic controls

1. As part of their ICT security policies, procedures, protocols, and tools referred to in Article 9(2) of Regulation (EU) 2022/2554, financial entities shall develop, document, and implement a policy on encryption and cryptographic controls.

2. Financial entities shall design the policy on encryption and cryptographic controls referred to in paragraph 1 on the basis of the results of an approved data classification and ICT risk assessment. That policy shall contain rules for all of the following:

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

(b) the encryption of data in use, where necessary;

(c) the encryption of internal network connections and traffic with external parties;

(d) the cryptographic key management referred to in Article 7, laying down rules on the correct use, protection, and lifecycle of cryptographic keys.

For the purposes of point (b), where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment, or take equivalent measures to ensure the confidentiality, integrity, authenticity, and availability of data.

3. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 criteria for the selection of cryptographic techniques and use practices, taking into account leading practices, and standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012, and the classification of relevant ICT assets established in accordance with Article 8(1) of Regulation (EU) 2022/2554. Financial entities that are not able to adhere to the leading practices or standards, or to use the most reliable techniques, shall adopt mitigation and monitoring measures that ensure resilience against cyber threats.

4. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 provisions for updating or changing, where necessary, the cryptographic technology on the basis of developments in cryptanalysis. Those updates or changes shall ensure that the cryptographic technology remains resilient against cyber threats, as required by Article 10(2), point (a). Financial entities that are not able to update or change the cryptographic technology shall adopt mitigation and monitoring measures that ensure resilience against cyber threats.

5. Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 a requirement 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.

Santander

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**

RTS on ICT Risk Management Framework

Delegated Regulation 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554

Article 7

Cryptographic key management

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

2. Financial entities shall identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure, and modification. Financial entities shall design those controls on the basis of the results of the approved data classification and the ICT risk assessment.

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

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. Financial entities shall keep that register up to date.

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

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**

Santander

RTS on ICT Risk Management Framework

Delegated Regulation 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554

(9) Cryptographic controls can ensure the availability, authenticity, integrity, and confidentiality of data. Financial entities referred to in Title II of this Regulation should therefore identify and implement such controls on the basis of a risk-based approach. To that end, financial entities should encrypt the data concerned at rest, in transit or, where necessary, in use, on the basis of the results of a two-pronged process, namely data classification and a comprehensive ICT risk assessment. Given the complexity of encrypting data in use, financial entities referred to in Title II of this Regulation should encrypt date in use only where that would be appropriate in light of the results of the ICT risk assessment. Financial entities referred to in Title II of this Regulation should, however, be able, where encryption of data in use is not feasible or is too complex, to protect the confidentiality, integrity, and availability of the data concerned th[illegible] other ICT security measures. Given the rapid tech[illegible]logical developments in the field of cryp[illegible]aphic techniques, financial entities referred to in Title II of this Regulation should remain ab[illegible]st of relevant developments in cryptanalysis and consider leading practices and standards. Financial entities referred to in Title [illegible] of this Regulation should hence follow a flexible approach, based on risk mitigation and monitoring, to deal with the dynamic landscape of cryptographic threats, including threats from quantum advancements.

Digital Identity - Regulation (EU) 2024/1183 (eIDAS2)

2024/1183 30.4.202

REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 11 April 2024

amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The Commission Communication of 19 February 2020 entitled 'Shaping Europe's Digital Future' announces a revision of Regulation (EU) No 910/2014 of the European Parliament and of the Council (4) to improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.

(2) In its conclusions of 1-2 October 2020, the European Council called on the Commission to propose the development of a Union-wide framework for secure public electronic identification, including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services.

(3) The Digital Decade Policy Programme 2030, established by Decision (EU) 2022/2481 of the European Parliament and of the Council (5), sets the objectives and digital targets of a Union framework which, by 2030, are intended to

Incorporates the European Digital Identity Wallet, which aims to provide a tool for European citizens to identify and authenticate their identity in a "secure, reliable, user-friendly, convenient, accessible, and harmonized manner across the Union."

Payments represent a significant use case for adopting the eIDAS2 standard, given the obligation to offer customers authentication through the European Digital Identity Wallet as an alternative to Strong Customer Authentication (SCA) for online payments. eIDAS2 is noteworthy as it develops the elements of the European Digital Identity Wallet configuration.

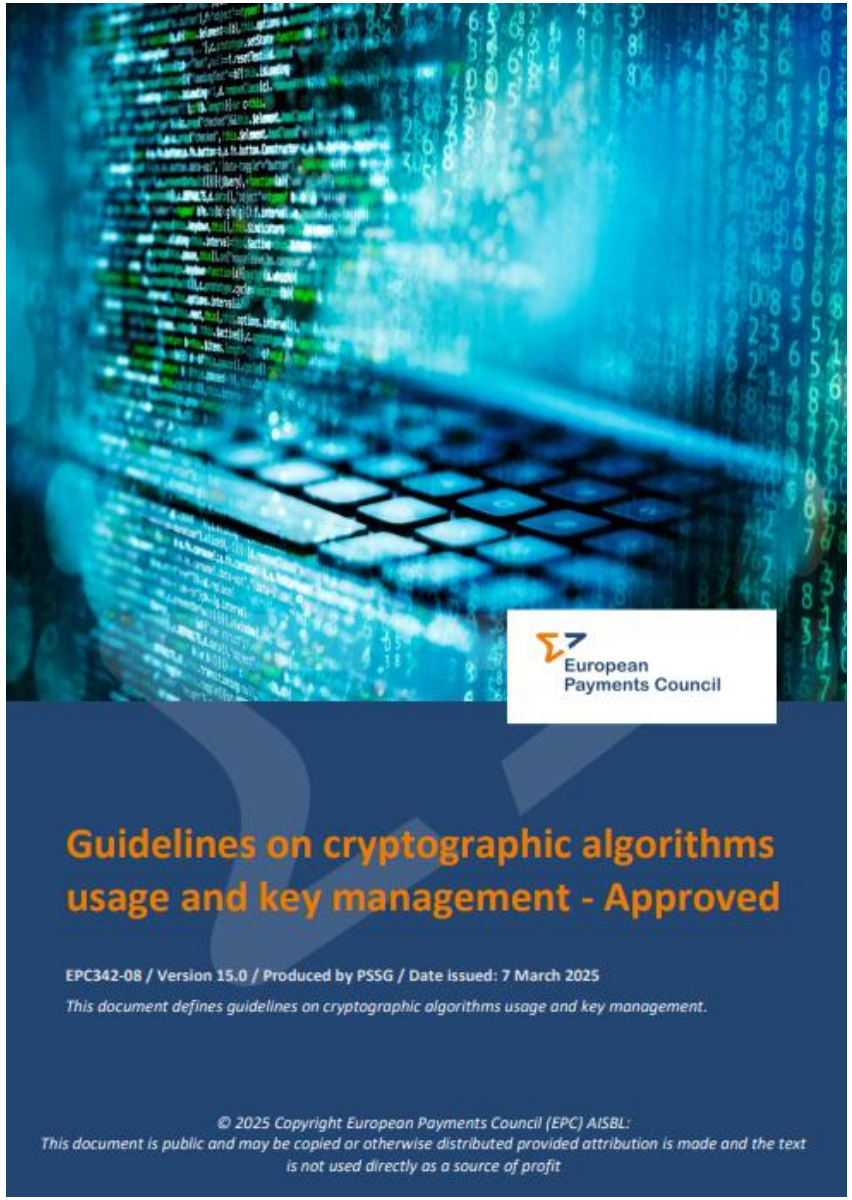
ARF for Digital Identity version 2.6

A Wallet Unit facilitates complying with strong customer authentication (SCA) requirements for electronic payments, ensuring a high level of security and compliance with Article 97 of the PSD2 (and with the future PSD3/PSR).

Note: Whereas the PSD2 speaks about 'strong *customer* authentication', the [European Digital Identity Regulation], Article 5f(2), uses the term strong *user* authentication, and says that Relying Parties in (among others) the banking and financial sector shall accept EUDI Wallet Units to comply with legal requirements regarding strong user authentication. The ARF assumes that this means that Wallet Units must comply with the requirements for SCA in the PSD2.

Commission Delegated Regulation (EU) 2018/389 lays down the requirements for strong customer authentication (SCA), which needs to be complied with when accessing a payment account online and for initiating electronic payments, or carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses. The use of a Wallet Unit for SCA will be in full compliance with those requirements. This implies that the Wallet Unit must enable the User to authenticate payment information, such as amount and payee, originating from a Relying Party, and to return the authenticated data to the Relying Party.

Payments



Electronic banking relies heavily on digital signatures to validate transactions, protect communications, and safeguard the confidentiality and integrity of customer information.

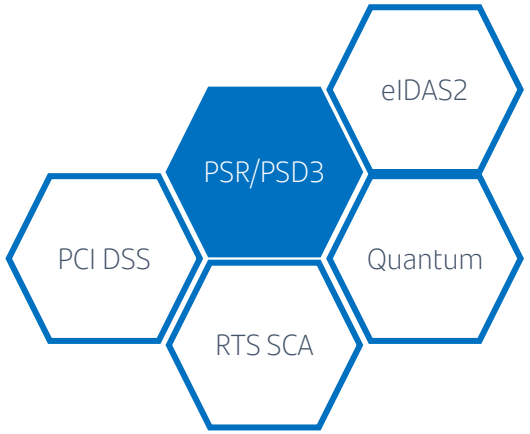
Directive (EU) 2015/2366 of 25 November 2015 (PSD2) introduces the obligation to adopt measures that protect the confidentiality and integrity of users' personalized security credentials. These measures include encryption systems.

In March 2025, the European Payments Council published the annual revision of its Guidelines on Cryptographic Algorithms and Key Management. These guidelines, based on PSD2 and the future PSD3, are intended to guide the European payments industry on **cryptographic algorithms and key-management**.

The guidelines explicitly mention **the quantum threat**, particularly the risks from *"harvest-now, decrypt-later"* attacks, and highlight the significant impact on public-key infrastructures.

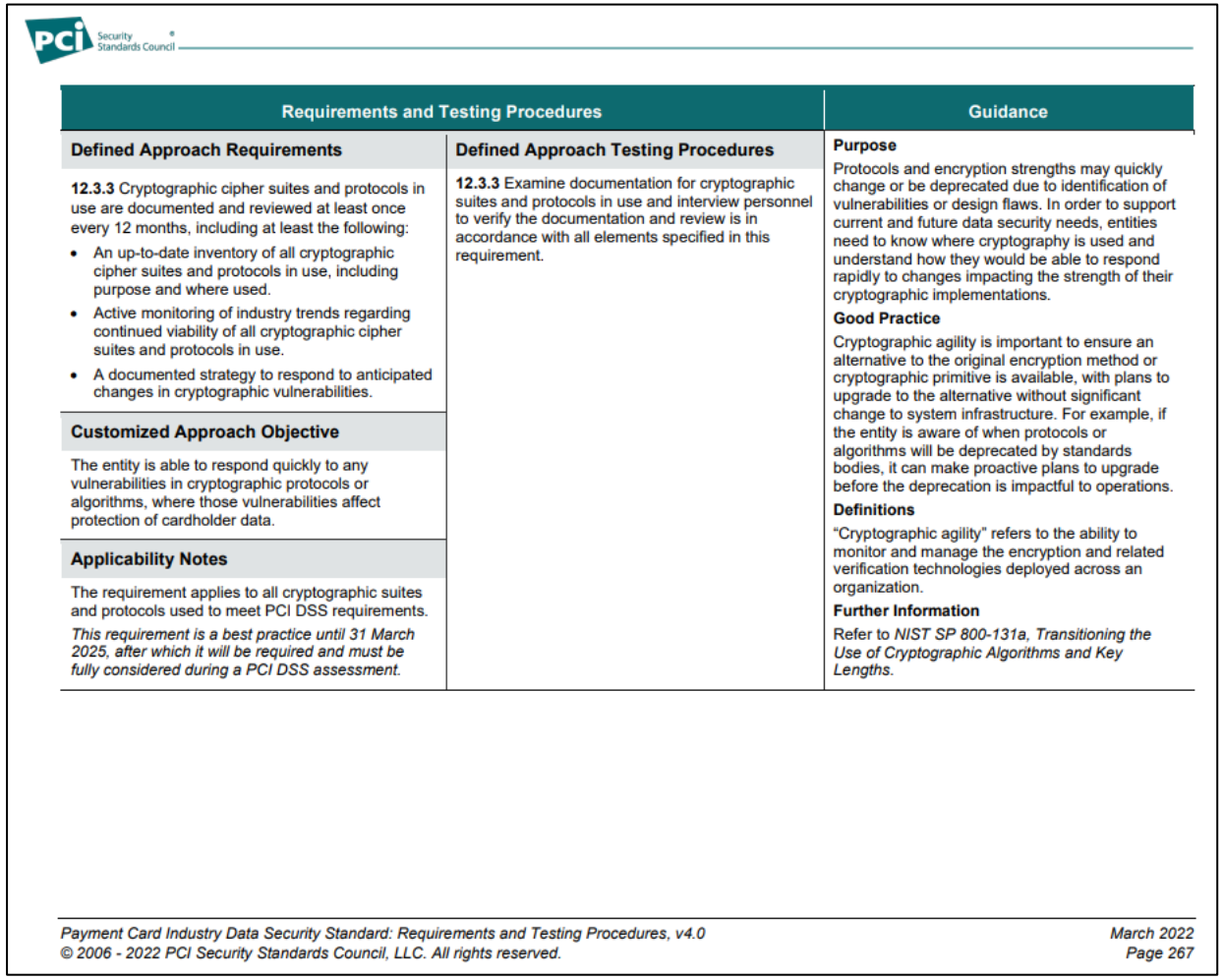
For use cases relying on public-key cryptography, the guidelines emphasize the need to adopt **cryptographic-agility policies** in accordance with recommendations from **NIST and the German Federal Office for Information Security**.

They recommend the deployment of hybrid mechanisms combining classical and post-quantum algorithms as part of a migration and crypto-agility strategy.



14

PCI-DSS requirements

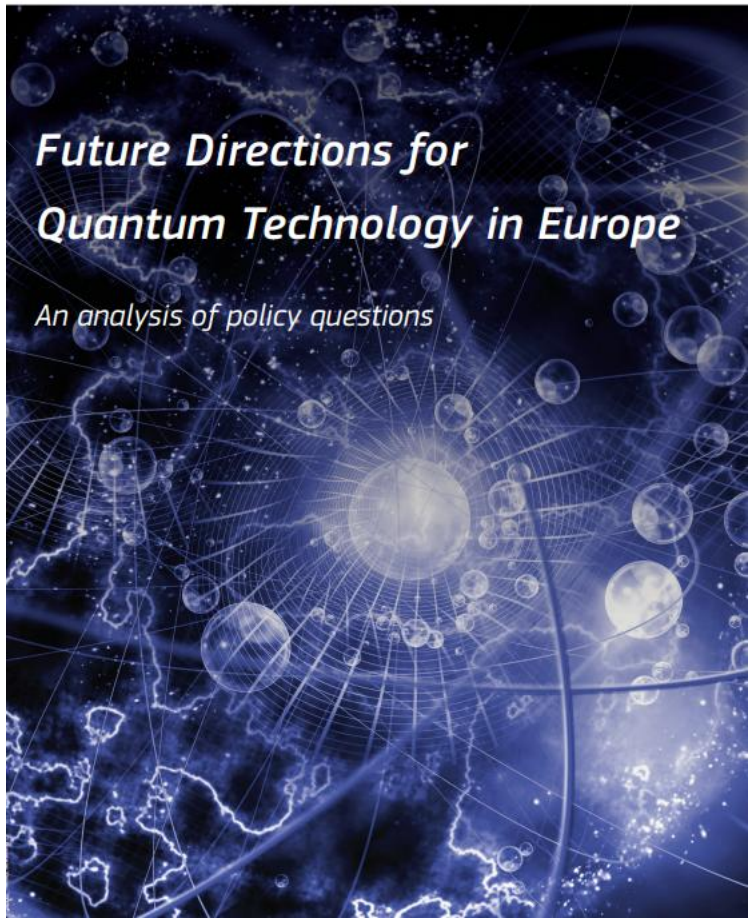


PCI Security Standards Council

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
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.	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.*
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.*		

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**

The Cyber Resilience Act (CRA)



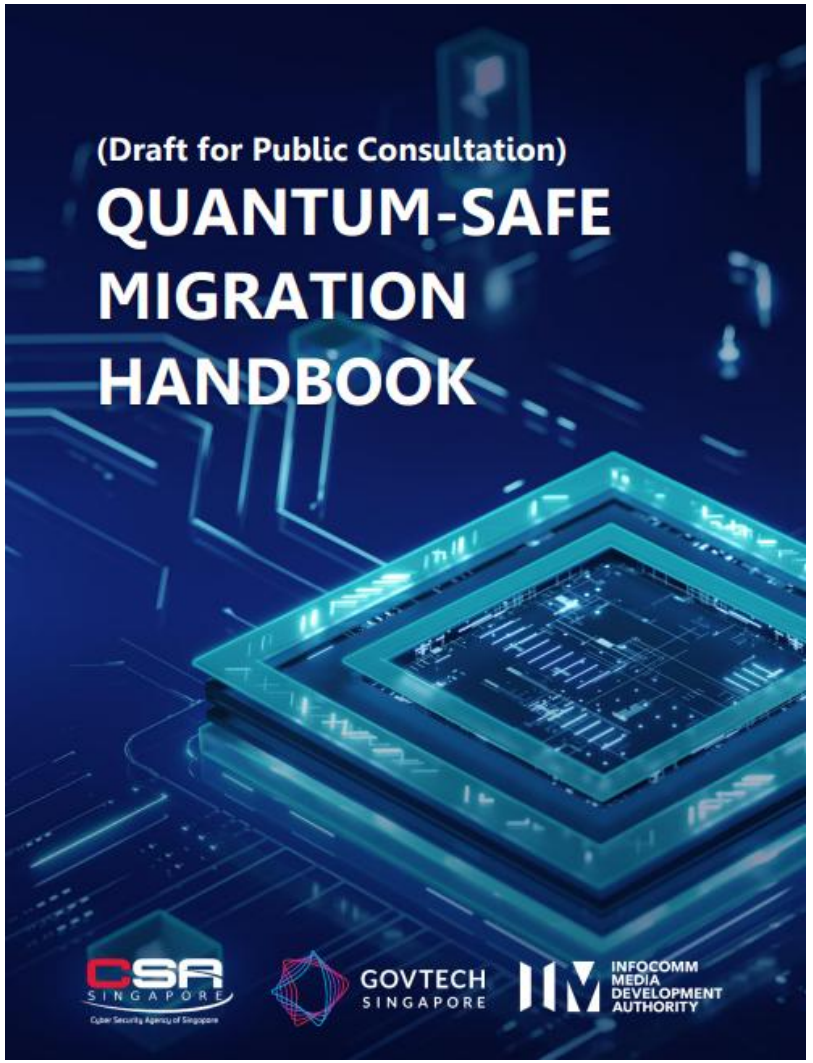
4.2 Legislation, cybersecurity, EUCC certification framework

Quantum communication technology is now at the point where security certification is needed. The regulatory framework addressing certification of ICT products has been rapidly evolving in the past years towards the creation of a digital single market and the enabling of trade within the EU. The EU Cybersecurity Act (Regulation (EU) 2019/881) and Commission Implementing Regulation (EU) 2024/482 establish a harmonised approach to cybersecurity across the EU, under the responsibility of the European Union Agency for Cybersecurity (ENISA). The Act establishes a framework for certifying the security of ICT products, services, and processes, including the European common criteria-based Cybersecurity Certification scheme (EUCC), a voluntary scheme based on the widely recognised ISO / IEC 15408 series standards, known as the Common Criteria. EUCC is the successor to the SOG-IS framework already used across 17 EU Member States. It is the appropriate framework for certification of quantum communication systems.

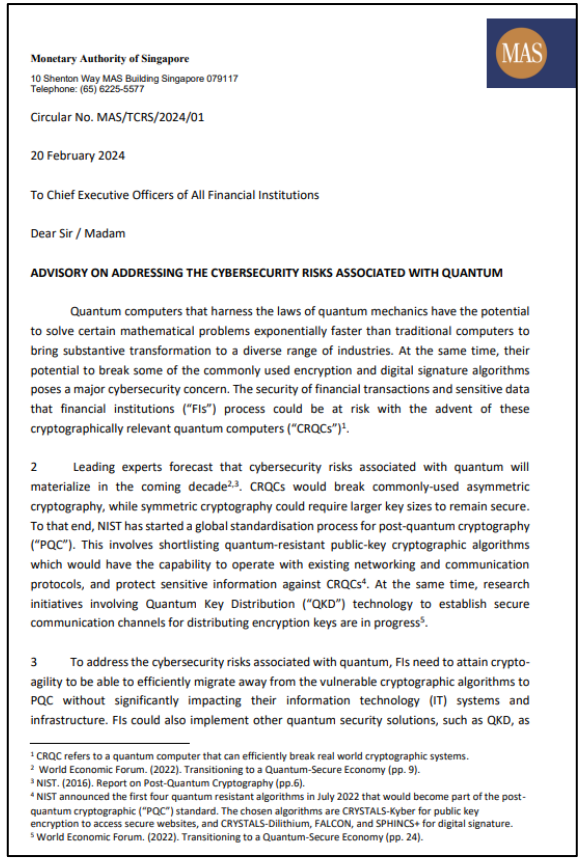
Common criteria evaluation is carried out by a relatively small group of laboratories, denominated Information Technology Security Evaluation Facilities (ITSEFs), officially accredited to conduct evaluations according to ISO / IEC 15408 and Common Evaluation Methodology ISO / IEC 18045. Certificates are issued by a separate group of organisations called Certification Bodies, using the results of tests carried out by ITSEFs.

The standards define a set of stringent criteria against which a product can be evaluated in terms of functional security, security architectures, product development environment, handling identified vulnerabilities in the product, according to Evaluation Assurance Level, EAL1 to EAL7, with higher numbers corresponding to greater rigour. To achieve a particular EAL, a system must meet specific assurance requirements, involving design documentation, analysis, functional or penetration testing. Systems that provide multilevel security, such as those required for QKD, are evaluated at a minimum of EAL4, typically EAL4+, the level foreseen in the ETSI protection profile. This entails an evaluation of whether the device has been methodically designed, tested, and reviewed, plus an advanced methodical vulnerability analysis and verification of the development and support processes.

Other non-EU regulatory approaches – Singapore: a toolkit / handbook approach.



Other non-EU regulatory approaches



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

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

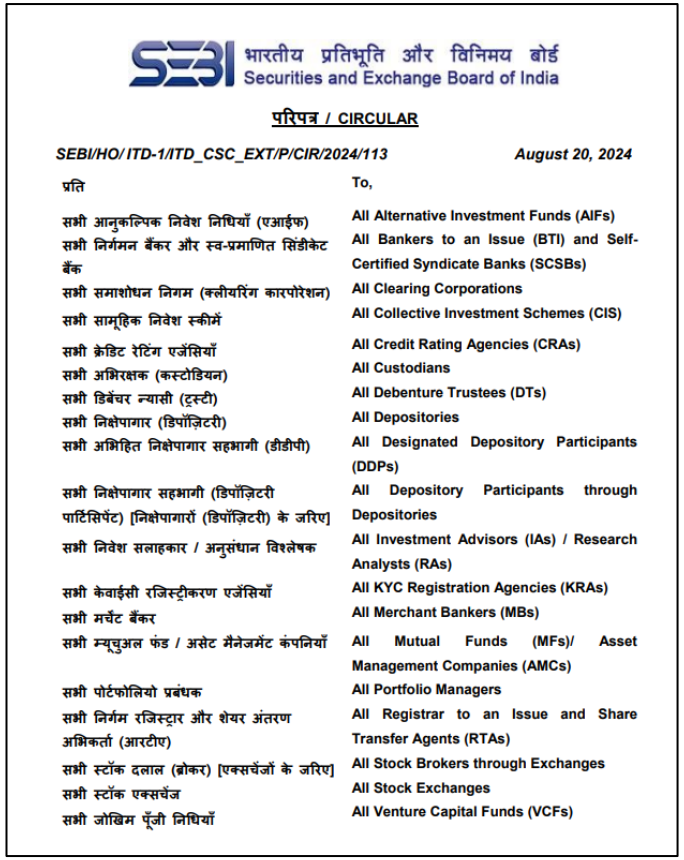
Quantum computers that harness the laws of quantum mechanics have the potential to solve certain mathematical problems exponentially faster than traditional computers to bring substantive transformation to a diverse range of industries. At the same time, their potential to break some of the commonly 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].

2 Leading experts forecast that cybersecurity risks associated with quantum will materialize in the coming decade[2,3]. CRQCs would break commonly-used asymmetric cryptography, while symmetric cryptography could require larger key sizes to remain secure. To that end, NIST has started a global standardisation process for post-quantum cryptography ("PQC"). This involves shortlisting quantum-resistant public-key cryptographic algorithms which would have the capability to operate with existing networking and communication protocols, and protect sensitive information against CRQCs[4]. At the same time, research initiatives involving Quantum Key Distribution ("QKD") technology to establish secure communication channels for distributing encryption keys are in progress[5].

3 To address the cybersecurity risks associated with quantum, FIs need to attain crypto-agility to be able to efficiently migrate away from the vulnerable cryptographic algorithms to PQC without significantly impacting their information technology (IT) systems and infrastructure. FIs could also implement other quantum security solutions, such as QKD, as

[1] CRQC refers to a quantum computer that can efficiently break real world cryptographic systems.
[2] World Economic Forum. (2022). Transitioning to a Quantum-Secure Economy (pp. 9).
[3] NIST. (2016). Report on Post-Quantum Cryptography (pp.6).
[4] NIST announced the first four quantum resistant algorithms in July 2022 that would become part of the post-quantum cryptographic ("PQC") standard. The chosen algorithms are CRYSTALS-Kyber for public key encryption to access secure websites, and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signature.
[5] World Economic Forum. (2022). Transitioning to a Quantum-Secure Economy (pp. 24).

February 2024



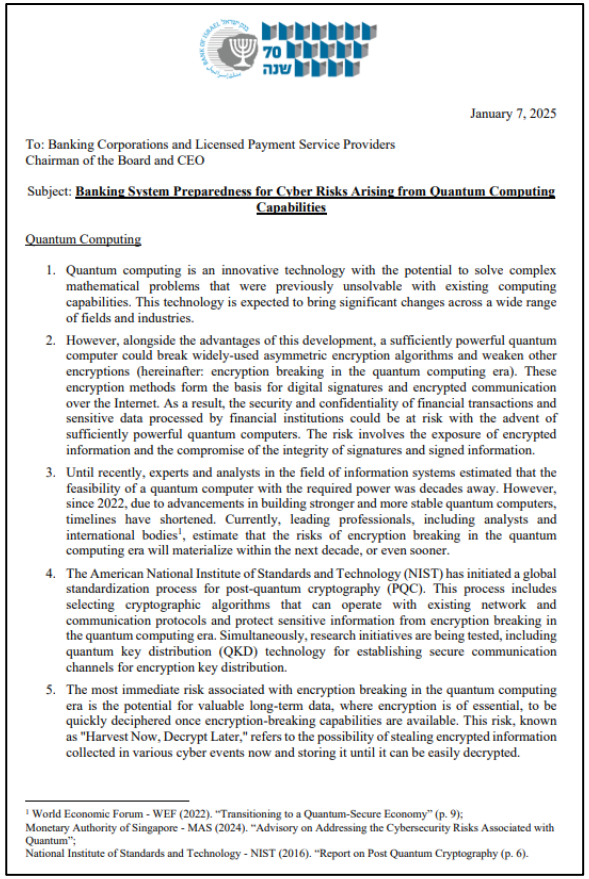
भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

परिपत्र / CIRCULAR

SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113 ***August 20, 2024***

प्रति	To,
सभी आनुकल्पिक निवेश निधियाँ (एआईएफ)	All Alternative Investment Funds (AIFs)
सभी निर्गमन बैंकर और स्व-प्रमाणित सिंडीकेट बैंक	All Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs)
सभी समाशोधन निगम (क्लीयरिंग कारपोरेशन)	All Clearing Corporations
सभी सामूहिक निवेश स्कीमें	All Collective Investment Schemes (CIS)
सभी क्रेडिट रेटिंग एजेंसियाँ	All Credit Rating Agencies (CRAs)
सभी अभिरक्षक (कस्टोडियन)	All Custodians
सभी डिबेंचर न्यासी (ट्रस्टी)	All Debenture Trustees (DTs)
सभी निक्षेपागार (डिपॉज़िटरी)	All Depositories
सभी अभिहित निक्षेपागार सहभागी (डीडीपी)	All Designated Depository Participants (DDPs)
सभी निक्षेपागार सहभागी (डिपॉज़िटरी पार्टिसिपेंट) [निक्षेपागारों (डिपॉज़िटरी) के जरिए]	All Depository Participants through Depositories
सभी निवेश सलाहकार / अनुसंधान विश्लेषक	All Investment Advisors (IAs) / Research Analysts (RAs)
सभी केवाईसी रजिस्ट्रीकरण एजेंसियाँ	All KYC Registration Agencies (KRAs)
सभी मर्चेंट बैंकर	All Merchant Bankers (MBs)
सभी म्यूचुअल फंड / असेट मैनेजमेंट कंपनियाँ	All Mutual Funds (MFs)/ Asset Management Companies (AMCs)
सभी पोर्टफोलियो प्रबंधक	All Portfolio Managers
सभी निर्गम रजिस्ट्रार और शेयर अंतरण अभिकर्ता (आरटीए)	All Registrar to an Issue and Share Transfer Agents (RTAs)
सभी स्टॉक दलाल (ब्रोकर) [एक्सचेंजों के जरिए]	All Stock Brokers through Exchanges
सभी स्टॉक एक्सचेंज	All Stock Exchanges
सभी जोखिम पूँजी निधियाँ	All Venture Capital Funds (VCFs)

August 2024



January 7, 2025

To: Banking Corporations and Licensed Payment Service Providers
Chairman of the Board and CEO

Subject: **Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities**

Quantum Computing

1. Quantum computing is an innovative technology with the potential to solve complex mathematical problems that were previously unsolvable with existing computing capabilities. This technology is expected to bring significant changes across a wide range of fields and industries.
2. However, alongside the advantages of this development, a sufficiently powerful quantum computer could break widely-used asymmetric encryption algorithms and weaken other encryptions (hereinafter: encryption breaking in the quantum computing era). These encryption methods form the basis for digital signatures and encrypted communication over the Internet. As a result, the security and confidentiality of financial transactions and sensitive data processed by financial institutions could be at risk with the advent of sufficiently powerful quantum computers. The risk involves the exposure of encrypted information and the compromise of the integrity of signatures and signed information.
3. Until recently, experts and analysts in the field of information systems estimated that the feasibility of a quantum computer with the required power was decades away. However, since 2022, due to advancements in building stronger and more stable quantum computers, timelines have shortened. Currently, leading professionals, including analysts and international bodies[1], estimate that the risks of encryption breaking in the quantum computing era will materialize within the next decade, or even sooner.
4. The American National Institute of Standards and Technology (NIST) has initiated a global standardization process for post-quantum cryptography (PQC). This process includes selecting cryptographic algorithms that can operate with existing network and communication protocols and protect sensitive information from encryption breaking in the quantum computing era. Simultaneously, research initiatives are being tested, including quantum key distribution (QKD) technology for establishing secure communication channels for encryption key distribution.
5. The most immediate risk associated with encryption breaking in the quantum computing era is the potential for valuable long-term data, where encryption is of essential, to be quickly deciphered once encryption-breaking capabilities are available. This risk, known as "Harvest Now, Decrypt Later," refers to the possibility of stealing encrypted information collected in various cyber events now and storing it until it can be easily decrypted.

[1] World Economic Forum - WEF (2022). "Transitioning to a Quantum-Secure Economy" (p. 9);
Monetary Authority of Singapore - MAS (2024). "Advisory on Addressing the Cybersecurity Risks Associated with Quantum";
National Institute of Standards and Technology - NIST (2016). "Report on Post Quantum Cryptography (p. 6).

January 2025

Concluding remarks

- Together, these laws create an EU-wide cryptographic governance ecosystem. There is no need for additional legislation to be adopted. Existing regulation already requires entities to adopt cryptographic controls in accordance with international standards and explicitly recognize quantum-driven risks. Cryptographic controls must be documented, tested and embedded into governance, with evidence available for supervisory review.

- What remains is securing consistent international alignment, given the interconnected nature of global financial institutions and digital identity frameworks.

- Parallel EU initiatives such as the Digital Omnibus Proposal aim to streamline digital regulation, providing a window for the financial sector to modernize its security architecture in a coordinated manner.

- Next steps could focus on: (i) enhancing cross-border cooperation; and (ii) providing aligned guidance with a "*toolkit approach*".

Legal validity and admissibility of digitally signed documents

Current

Classical signature

Quantum-Safe Signatures

Classical signature

PostQuantum Long-Term Validation

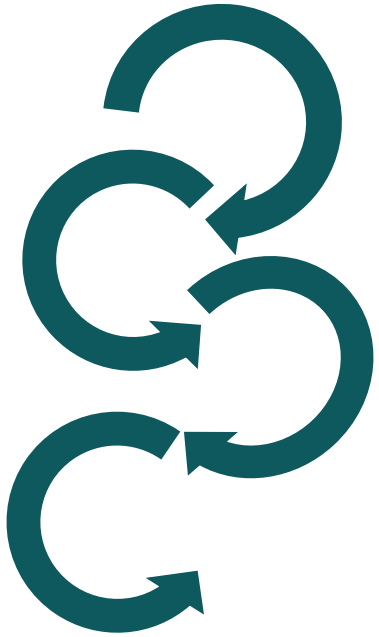
Blockchain notarization

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

Legal validity and admissibility of digitally signed documents

Asymmetric key algorithms, including digital signature schemes are particularly vulnerable to quantum threats. However, they may also present an opportunity, as they allow the renewal or replacement of potentially deprecated signature algorithms.

Timestamping for ensuring the legal validity and preservation of documents signed in a digital environment in the long term, as it demonstrates that the signature existed prior to a potential quantum attack.



If post-quantum algorithms are used in timestamping with long-term validation, the risk of a breach of the integrity of the document, would be mitigated.

Timestamps must be periodically updated, in line with recommendations from international organizations, ensuring the use of state-of-the-art algorithms.

Global ecosystem of regulations and case law, which requires the analysis of the legal criteria in each jurisdiction to configure an interoperable standard for the signature of contractual documents in digital environments, such as electronic banking.

Transitioning to PQC could determine its legal effects and admissibility as evidence in the long term and in various jurisdictions.

Recommended workstreams include:

- Establishing a digital signature standard that is compatible and interoperable across different jurisdictions, featuring an immutable and quantum-resistant long-term validation timestamp.
- Examining existing contractual commitments and related frameworks.
- Evaluating and revising policies, procedures, and tools to guarantee the implementation of PQ algorithms.
- Phasing in digital signature systems as part of a comprehensive Cryptographic Agility approach

Furthermore:

Q&A

Thank You.

Our purpose is to help people and businesses prosper.

Our culture is based on believing that everything we do should be:

Simple Personal Fair

Santander