Post-Quantum

Cryptography Conference

How ETSI is Preparing for PQC

Inigo Barreira
ETSI ESI Vice Chair at Sectigo

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

The Standards People

ETSI and Quantum-Safe Cryptography

PKI Consortium PQC Conference – October 2025 Kuala Lumpur

Presented by: **Iñigo Barreira. CA Manager at Sectigo.**

ETSI ESI Vice-chair

SECTIGO

Index

European Union

EU – Quantum Europe Strategy

- The Quantum Europe Strategy aims to make Europe a global leader in quantum by 2030.
- Europe´s strengths
  - Scientific leadership: Nobel prize level of expertise
  - Investments: 11B euros invested by the EU and the MS in the last 5 years
  - Vibrant scosystem: Startups and SMEs
- Main goals
  - Turn scientific discoveries into market–ready applications
  - Enhance Europe´s security and tech sovereignty
  - Maintain Europe´s scientific leadership
- Targeted areas
  - Quantum Europe: R/I, dual-use, skills, quantum ecosystem and infrastructure

EU – Quantum Europe Strategy

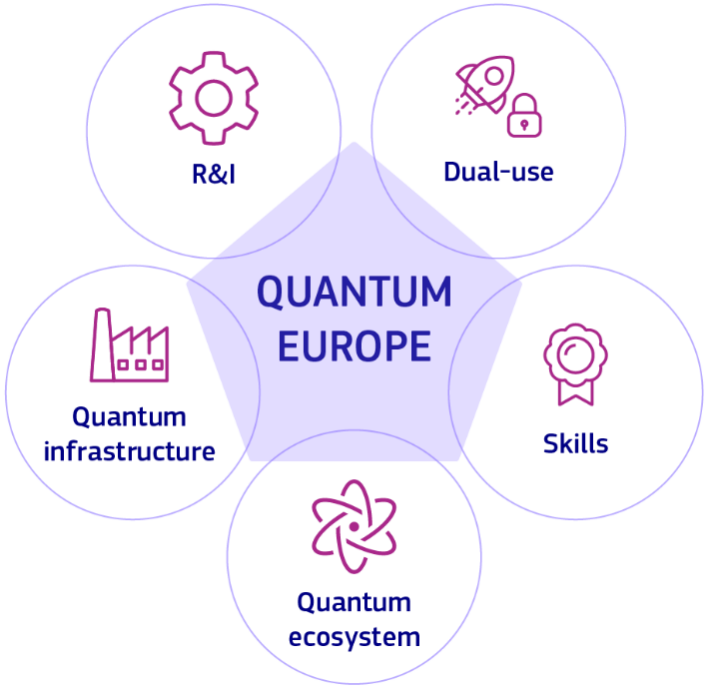
- Quantum Europe Strategy | Shaping Europe's digital future, Published July 2, 2025
- The Strategy focuses on five interconnected (targeted) areas:

- **Research and Innovation**: Consolidating excellence across Europe to lead in quantum science and its industrial transformation
- **Quantum Infrastructures:** Developing scalable, coordinated infrastructure hubs to support production, design, and application development
- **Strengthening the Quantum Ecosystem**: through investments in startups and scaleups, securing supply chains and the industrialisation of quantum technologies
- **Space and Dual-Use Quantum Technologies (Security and Defence)**: Integrating secure, sovereign quantum capabilities into Europe's space, security and defence strategies
- **Quantum Skills:** Building a diverse, world-class workforce through coordinated education, training, and talent mobility across the EU

EU – Quantum Europe Strategy

- This strategy sets a clear course:

- Build a quantum-safe communication Network by 2030
  - Expanding International cooperation
  - Delivering a european roadmap for quantum standards by 2026



EU – Quantum Europe Strategy. General approach

- Quantum technologies flagship launched on 2018
  - As per the Quantum manifesto launched in 2016
  - 1B euros investment over 10 years
- Quantum Computing
  - Part of the European High Performance Computer Joint Undertaking (EuroHPC JU)
  - In 2022 six sites selected to have European quantum computers (Czechia, Germany, Spain, Italy, France and Poland)
  - first step towards the deployment of a European quantum computing infrastructure, which will be accessible to European users from science and industry via the cloud on a non-commercial basis
- The European Quantum Communication Infrastructure (EuroQCI) initiative
  - In 2019, All EUMS signed the EuroQCI declaration with the help of the ESA to develop a quantum communication infrastructure
- Quantum sensing
  - Quantum sensors offer greatly improved performance and accuracy compared with their classical equivalents
  - The EU Commission is investing in pan-European quantum sensing infrastructures that will link these sensors

EU – Quantum Europe Strategy → Projects

- Transition to post-quantum Public Key Infrastructures Strengthening the cybersecurity ecosystem (DIGITAL-ECCC-2025-DEPLOY-CYBER-08)
  - Opening-close: June-October 2025
  - Expected outcome:
    - New combiners ensuring that cryptographic schemes provide at least 128-bit security against quantum adversaries.
    - New and/or improved open-source libraries for certificate requests, issuance, validation, revocation and (privacy-friendly) certificate transparency.
    - Test and evaluation of uses of X.509 certificates other than their core uses.
    - Tests and evaluation of alternatives to X.509 certificates.
  - Objective
    - The overarching aim of this call is to tackle the challenges of an effective integration of PQC algorithms in Public Key Infrastructures (PKIs), which offers efficient migration strategies and strong business continuity guarantees.

EU – Quantum Europe Strategy → Projects

- Scope
  - Proposals should address functions such as key establishment, digital signatures, and secure communication protocols that require careful adaptation with post-quantum counterparts to ensure resilience against threats posed by quantum-capable adversaries.
  - Proposals should safeguard compatibility with existing legacy systems. To achieve this, a transition to PKIs that support both pre-quantum and post-quantum cryptography should be addressed.
  - The proposed systems should be able to seamlessly interact with legacy systems by disabling the post-quantum component as needed while preventing downgrade attacks.
  - Relying solely on PQC solutions in this intermediate transition phase could introduce security risks given that the security analysis of the cryptosystems and of their implementations is not as mature as for their pre-quantum counterparts. Proposals should therefore use combinations of PQC solutions and established pre-quantum solutions, making sure to provide strongest-link security, meaning that the system remains secure as long as at least one of the components of the combination is secure.
  - For certificates for protocols that support negotiation, such as X.509 certificates for the Transport Layer (TLS), the use of post-quantum key exchange has already been demonstrated and can be implemented in a decentralised manner.

EU – Quantum Europe Strategy → Projects

- Activities
  - Identification of requirements necessary to implement hybrid certificates.
  - Development of novel protocols for Automatic Certificate Management and revocation, and of novel protocols for (privacy-friendly) certificate-transparency. Support to standardisation activities.
  - The proposed systems should be able to seamlessly interact with legacy systems by disabling the post-quantum component as needed while preventing downgrade attacks.

➢ Participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, this topic is subject to Article 12(5) of Regulation (EU) 2021/694.

- The PQC part has a budget of € 15M

EU – Quantum Europe Strategy → Projects

- Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/HORIZON-CL3-2025-02-CS-ECCC-06
- Opening-close: June-November 2025
- POst-quantum SEcure dIgital iDentities for EurOpean solutioNs (POSEIDON) https://cordis.europa.eu/project/id/101225797
- Opening-close: October 2025 - September 2028
  - POSEIDON will focus on providing robust and reliable solutions in digital identity management applications, given the critical importance of protecting citizens and businesses against the rising threats of identity-centric cyberattacks
  - POSEIDON will address the provision of crypto-agile, PQC-ready identity tools in a moment where new applications are being introduced for pan-European digital identity aligning with EU advancements and security policy like NIS2, CRA, CSA, etc

EU – Quantum Europe Strategy. Regulation NIS2 (2022/2555)

- PQC migration is covered under NIS2 directive
  - Article 21(2)(h)
    - Entities must establish policies and procedures on the use of cryptography → this includes crypto-agility by addressing the obsolescence and the ability to migrate to new standards with new cryptography
- Implementing Act (CIR 2024/2690)
  - Mandates a cryptographic policy based on crypto-agility
  - Follow ENISA guidelines
  - Explicit reference to PQC migration
- EU PQC Roadmap. Milestones
  - 2026: Cryptographic Risk Assessments
  - 2030: Migration of assets based on criticality
  - 2035: Everything has to be migrated

ENISA

ENISA

- Quantum technologies have been around and discussed over years
  - First publication on QKD goes back to 2009
  - In 2022, published Post-Quantum Cryptography: Anticipating threats and preparing the future which was a continuation of the report published a year ago about current state and quantum mitigation
  - In 2024 report on the state of cybersecurity in the European Union, the Post-Quantum Cryptography has been marked an emerging technology, along with AI, indicating its importance
- EUCC Guidelines on Cryptography
  - SOG-IS replacement
  - EUCC is the EU Cybersecurity Certification. ENISA is driving it
  - https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en
    - Version 2 released on May 2025 which added the PQC mechanisms

ENISA

- European Cybersecurity Certification Group Sub-group on Cryptography
  - This document is primarily addressed to developers and evaluators. Its purpose is to specify which cryptographic mechanisms are recognised agreed, i.e., ready to be accepted by all national cybersecurity certification authorities (NCCAs).
  - New section 1.4 for post-quantum cryptography
  - Recommends the Rolling out of post-quantum secure cryptography in hybrid mode alongside with classic cryptography
    - This approach provides assurance against the quantum threat as well as assurance against security issues that might affect the newer standardized post-quantum mechanisms.
  - In addition to the deployment of hybrid solutions for asymmetric mechanisms, it is also recommended, as a complementary mitigating action, to adapt the parameter lengths of symmetric mechanisms, e.g., key and hash lengths.
- Suggestions
  - Block ciphers: it is recommended not to use block ciphers with key size smaller than 192 bits.
  - Hash functions: it is recommended to not use hash functions with output length smaller than 384 bits
  - MAC schemes: it is recommended not to use MAC schemes with key size smaller than 192 bits.
  - Key combiners: A key combiner mechanism can be used to implement so-called hybrid key establishment mechanisms, e.g. combining a post-quantum KEM and a classical KEM based on ECDH.
  - Asymetric schemes and digital signatures like PKCS#1v1.5 but also references to new ones (FIPS204, 205) not affected by the quantum threat.

ETSI

ETSI work on PQC

ETSI has 2 Technical Committees (TC CYBER and TC ESI) and 1 industry group (ISG) working on PQC matters.

TC CYBER Quantum Safe Cryptography working group (QSC WG) and the Industry Specification Group on Quantum Key Distribution (ISG QKD) are leading the activities while TC ESI is relying on the ECCG

- The Quantum Key Distribution ISG develops common interfaces and specifications for the quantum communications industry to stimulate markets for components, systems, and applications. QKD enables secure key exchange using quantum states, with security based on quantum principles rather than algorithms - prompting the need for industrial standards amid rapid global deployment. In 2023, the ISG launched the First Protection Profile (PP) for the security evaluation of QKD modules (ETSI GS QKD 016), anticipating the need for quantum safe cryptography. The group is currently developing a Protection Profile for Key Processing Modules.

… in TC CYBER QSC WG

ETSI is pioneering in Quantum Key Distribution (QKD) and this is a good example of this vision by recognizing its strategy for advancing secure on standardization on quantum technologies.

- Recent recommendations and specifications from the TC CYBER QSC WG

CYBER; Impact of Quantum Computing on Symmetric Cryptography, TR 103 967 V1.1.1 (2025-01). CYBER; Impact of Quantum Computing on Cryptographic Security Proofs, TR 103 965 V1.1.1 (2024-10).	Analysis
CYBER; A Repeatable Framework for Quantum-Safe Migrations, TR 104 016 V1.1.1 (2024-10). CYBER; Deployment Considerations for Hybrid Schemes, TR 103 966 V1.1.1 (2024-10).	Migration Plans & Recommendations
CYBER; Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies, TS 104 105 V1.1.1 (2025-02). CYBER; Quantum-Safe Hybrid Key Establishment, TS 103 744 V1.2.1 (2025-03).	Standards

… also in TC CYBER

- NWI: Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes
  - Part 1: General.
  - Part 2: ML-KEM.
  - Part 3: ML-DSA.
  - Part 4: SLH-DSA.
- NWI: Cryptographic Agility in Software Quantum-Safe Cryptography Migration.
- Redefined work on migration
  - Quantitative approach (this year) vs management approach (last years)
- Developing a guide to quantum random number generators

… in TC ESI

TC ESI is responsible for Electronic Signatures and Trust Infrastructures standardization within ETSI.

- Policy, security and technical requirements for Trust Service Providers (TSP)
- Trusted Lists

Also supporting the eIDAS Regulation as well as the general requirements of the international community to provide trust and confidence in electronic transactions, specially recently with the supporting services for the new EUDI wallet

- All these activities are supported by the ETSI TS 119 312, Cryptographic suites, which is based on the new ECCG
  - Example: EUDI Wallet, only quantum-safe ZKP (Zero-Knowledge Proof) are to be considered. However, currently, there is no programme for identifying recommended Quantum Safe algorithms for ZKP. See current ETSI TR 119 476 and TR 119 476-1

ETSI TC ESI Standards

Trust services general:
- Conformity Assessment ✓
- Policy & security (NIS2) ✓ (upd)
- Identity proofing ✓

Trust services for:
- Issuing certificates ✓ (upd)
- Time Stamping ✓ (upd)
- Signature creation services ✓ (upd)
- Signature validation services ✓
- Open Banking ✓
- SMIME ✓
- Attribute attestations (new)

- AdES creation & validation ✓(rev)
  - Part 1: procedures
  - Part 2: signature validation report ✓
- Signature policy ✓
  - Part 1: Building blocks ✓
  - Part 2: XML format ✓
  - Part 3: ASN.1 format ✓
  - Part 4: Qualified signatures / ✓ ls ✓ (upd)

CC Protection Profiles ✓
- QSCD - Smart Cards ✓
- HSM used as QSCD ✓
- HSM used by TSPs ✓
- Remote QSCD ✓

✓	Published
(Rev)	Recently revised
(Upd)	Update in progress
(New)	New

319 40x, 461
Trust services general

119 6xx
Trust service status lists

- Trusted list ✓ (rev)
- Using & interpreting trusted list ✓
- Validation policy using trusted list ✓
- General trusted list model and processing (new)

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

Trust services for:
- Registered eDelivery / eMail ✓ (upd)
- Long term preservation ✓

Interop tests

x19 1xx
Signature Creation & Validation

Formats + Interop test:
- XAdES (XML) ✓
- CAdES (CMS) ✓
- PAdES (PDF) ✓ (upd)
- ASiC (containers) ✓ (Rev)
- JAdES (JSON) ✓
- CB-AdES (CBOR) (new)

419 2xx
Signing Devices

119 3xx
Cryptographic suites

- Signature suites ✓(rev)
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime
- Schema for algorithm catalogues (new) ✓

119 0xx
General Framework

- Standards framework ✓ (upd)
- Common definitions ✓
- Guides ✓

ETSI TS 119 312 v1.5.1

Update in progress. Based on ECCG, latest version 2.0

- ECCG suggests hybrid solutions and give advices on quantum threat (e.g., section 5.2)
- To be published by November 2025, v2.1.1

Impact of the quantum threat

The overwhelming majority of ETSI ESI standards are affected by the quantum threat:

- Almost all ETSI ESI standards rely on digital signature techniques.
- Establishing a secure and authenticated communication channel is also a frequent requirement and is especially important for electronic registered delivery services.

Methodology

The methodology adopted by ETSI ESI for the quantum safe migration of its standards is the following:

- Identification of ESI stakeholders
- Classification of the stakeholders based on urgency
- Identification of ESI standards applicable to the stakeholders
- Migration of the standards, with the work priority set based on the classification of stakeholders
  - The migration of the standards is based on the recommendations given in ETSI TR 103 619 V1.1.1.

Migration plan

- **In line with the recommendations given in ETSI TR 103 619, ETSI ESI established an inventory of dependencies for those standards**
- Each dependency was assessed as to whether or not it involved cryptography.
- For each asset which involves cryptography, ETSI ESI identified, when possible, candidate replacement standards and is following the work of the other standardization bodies.
- Once all dependencies have published replacement standards, full Quantum-Safe migration can be undertaken. Before then, ETSI ESI may consider giving recommendations to its stakeholders to begin Quantum-Safe migration in areas where replacement standards are identified.

Stakeholders approach

The first priority stakeholders identified by ETSI ESI were:

- Qualified Trust Service Providers issuing qualified certificates
- Qualified Trust Service Providers providing qualified electronic signatures or seals
- Qualified Trust Service Providers providing qualified electronic registered delivery services
  - Those providers are especially affected by store now decrypt later attacks.
- Those trust services to be used within the EUDI wallet

The second priority stakeholders are all other trust services provided by Qualified Trust Service Providers.

Migration plan

- Specifically, regarding standards on policy and security requirements, ETSI ESI is considering providing requirements for its stakeholders to begin PQC migration, with a recommendation to apply the repeatable framework laid down in ETSI TR 104 016.
  - Publication of ETSI TR 104 016 v.1.1.1 “CYBER; Quantum-Safe Cryptography (QSC);A Repeatable Framework for Quantum-Safe Migrations” (2024-10)

- Timeline for the completion of the PQC migration of all ETSI ESI standard is dependent on the timeline of other standardization bodies to migrate the dependencies on which ESI standards rely on.

Migration plan

- **ETSI ESI identified a first set of standards to undergo Quantum-Safe migration, those standards are EN 319 411-1/2 and the AdES standards EN 319 1x2-1.**
  - The aim is to establish a repeatable approach to migration of its standards, so that the rapporteur of each standard can then implement the changes necessary for the Quantum-Safe migration.
- **In line with the recommendations given in ETSI TR 103 619, ETSI ESI established an inventory of dependencies for those standards**
  - As ETSI considers itself a relying party of other standardization organizations such as W3C, IETF, ITU-T, ISO. It is therefore relying on those organizations to update the standard on which it relies to achieve the migration.

Conclusion

- Require TSPs to begin QSC migration using ETSI TR 104 016 v.1.1.1 as guidance.
  - At the minimum a complete inventory of the cryptographic asset must be required
- Contact other Standards Organizations to enquire about timeline for PQC migrated standards (based on the dependencies identified previously).
- Begin work in AdES standards (at least CAdES and JAdES) to reference current draft signature format dependencies dealing with ML-DSA and SLH-DSA.

EU-ETSI ESI arrangement (EISMEA project) – STF 705

- 2 years (2026-2027)
- Update of +20 current standards
- Development of +20 new standards

Supervisory Bodies

Role of Supervisory Bodies

- Every EU member state has appointed a specific entity/organization as supervisory body as per eIDAS Regulation (910/2014) eIDAS Dashboard
- They are in charge of (Q)TSPs management
- They may add/define/update specific rules, directives, … according to their own requirements
  - The best example is the use of the TS 119 312, which can be superseded by national laws.
- FESA (Forum of European Supervisory Authorities for TSPs) coordinates all SBs
  - FESA URL: Forum of European Supervisory Authorities for trust service providers
  - Members: Membership list

Spanish Supervisory Body

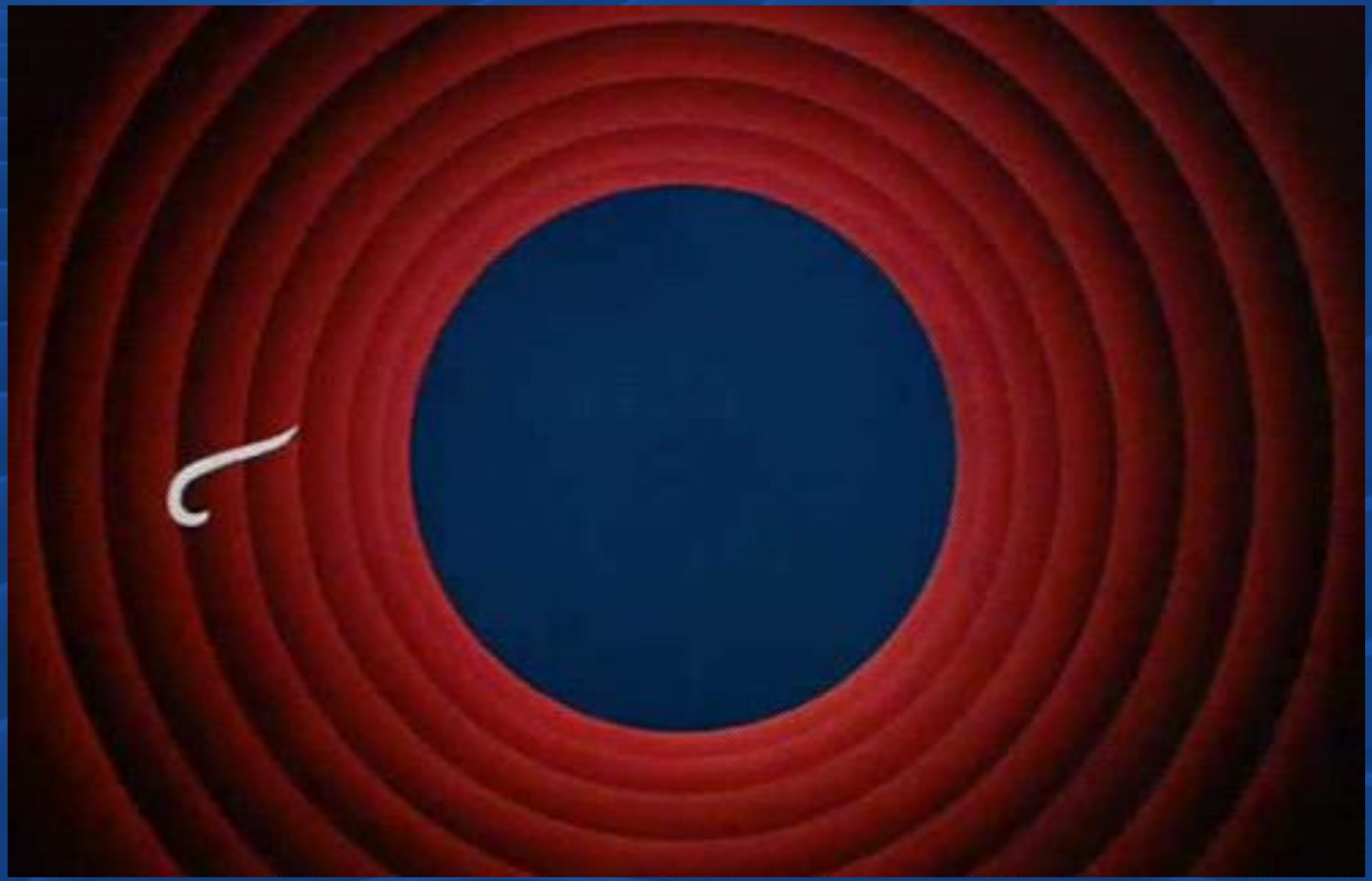
- Ministry of Digital Transformation
- Latest communications
  - Mandatory migration to longer key length RSA keys
  - Transition to Post-Quantum Cryptography (PQC)
    - In compliance with European guidelines and within the framework of the NIS2 Directive, all TSPs must begin the transition to post-quantum cryptography (PQC) algorithms.
    - This transition is essential to ensure the resilience of trusted services against threats arising from quantum computing.

Transition to PQC

To facilitate this transition, a Roadmap coordinated by the NIS2 PQC Working Group has been published, establishing phases, priorities, and technical recommendations. It is strongly recommended to consult and implement it:

- Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (EU PQC Workstream v1.1, published on June 2025)
  - Milestones: 2026, 2030 and 2035

- Additionally, in Spain as example, the Spanish CCN recommendations for a secure post-quantum transition must be taken into account, which will be updated shortly.
  - CCN-TEC 009



SECTIGO®