Post-Quantum

Cryptography Conference

# ETSI ESI and Quantum-Safe Cryptography

ETSI ESI (Electronic Signatures and Trust Infrastructures) develops policies, security, and technical requirements for Trust Service Providers (TSPs), including certification authorities, time-stamping authorities, and providers of remote signature creation, validation, registered e-delivery, and long-term data preservation services. ETSI ESI also maintains Trusted Lists, which enhance confidence in digital certificates and services by indicating TSP compliance with recognized approval schemes. This presentation will explore how developments in Quantum-Safe Cryptography (QSC) and Post-Quantum Cryptography (PQC) affect ETSI ESI standards. It will highlight areas where changes from other standards development organizations (SDOs) may influence ETSI ESI work, discuss potential impacts on existing frameworks, and provide an estimated timeline for adoption by consumers and organizations.


**Iñigo Barreira**
CA Manager at Sectigo


SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

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



PKI Consortium

# ETSI TC ESI and Quantum-Safe Cryptography

## PKI Consortium PQC Conference – January 2025


Presented by:

Iñigo Barreira – Sectigo

Jean-Emmanuel Perez – Nowina Solutions

# Index

ETSI

TC ESI

Standards

Quantum Threat

- Methodology
- Stakeholders
- Migration plan

Conclusions

- Example

# Bringing people together at ETSI …

ETSI is an Independent, non-profit organization

More than 900 member organizations worldwide

Drawn from over 60 countries and on five continents

30+ years track record of technical excellence in the ICT sector

Strong community of experts and innovators

Diverse community: SMEs, micro-enterprises, large companies, research entities, academia, government and public bodies, societal stakeholders

Large and small member organizations

Organized in several technical groups (ETSI - Committees for ICT standardization work)

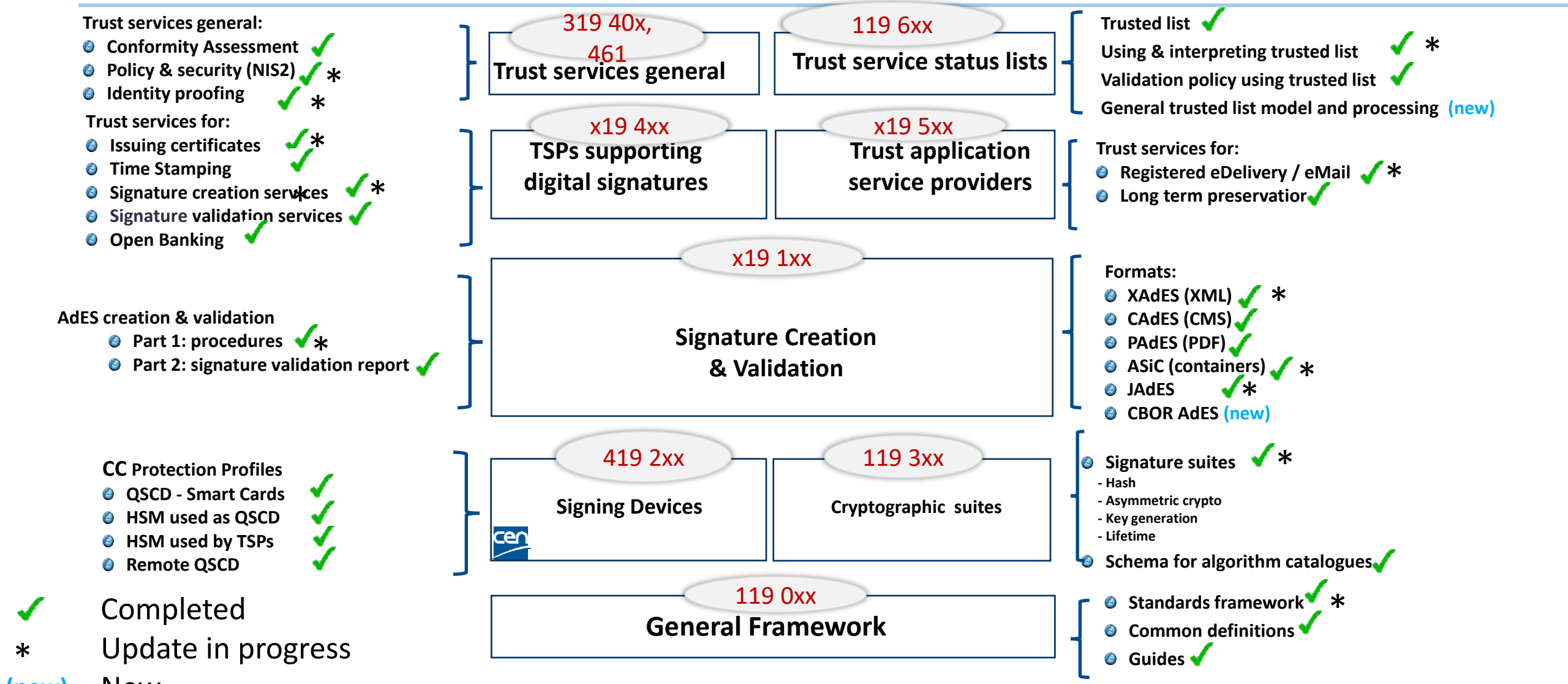
# … in TC ESI

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

- Policy, security and technical requirements for Trust Service Providers (TSP)
  - Certification Authorities (CA)
  - TimeStamp Authorities (TSA)
  - (Remote) Signature creation and validation
  - (Long-term) preservation
  - E-Delivery
- 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

# TC ESI Standards

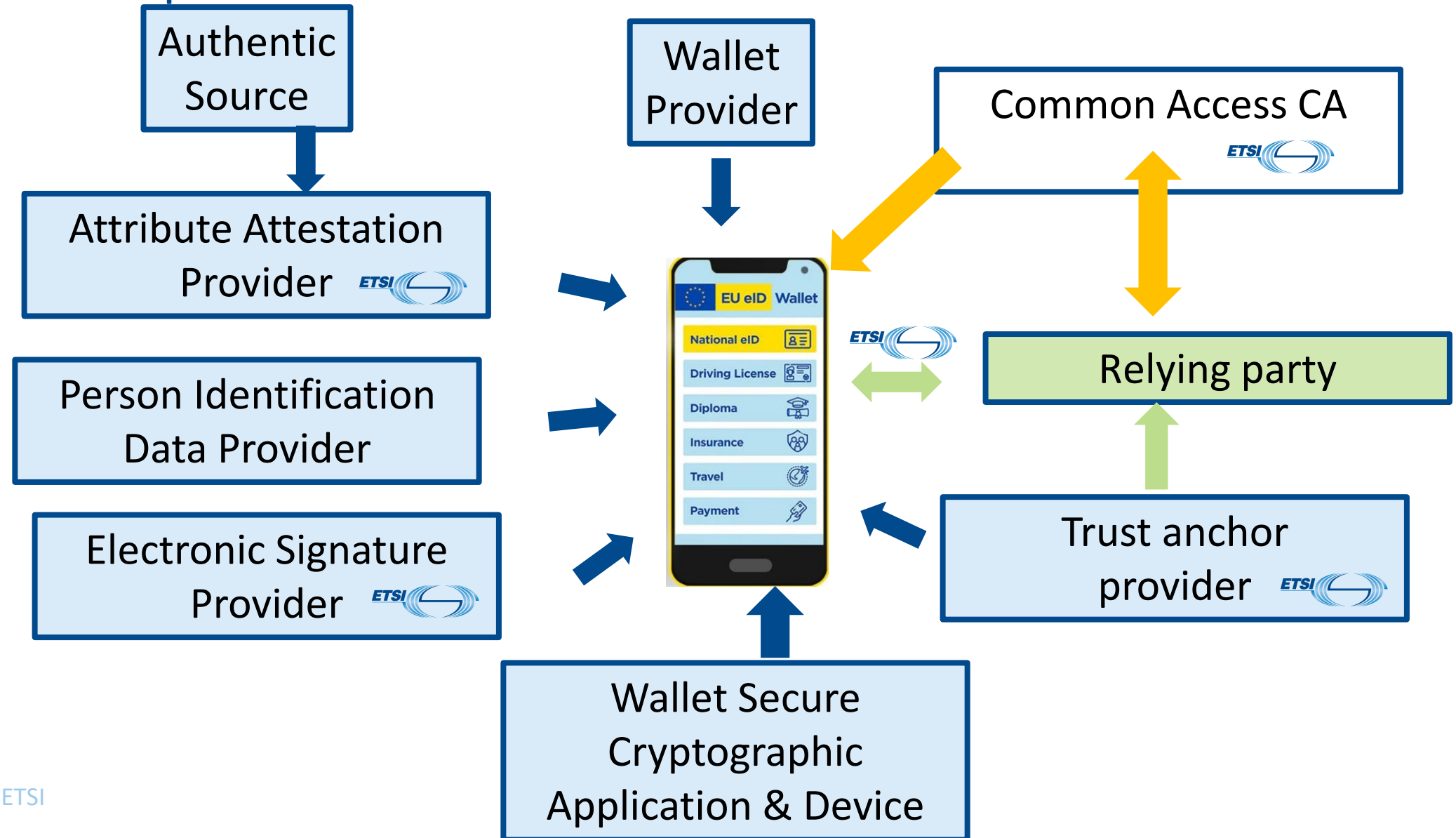



✓ Completed

* Update in progress

(new) New

# Main components and Interfaces for EUDI Wallet



# Standards

General Framework: It describes the general structure for digital signature standardization

- TR 119 000: Framework for standardization of signatures
- TR 119 001: Definitions and abbreviations

Trust Service Providers

**Policy and Security:** EN 319 401: General policy and security requirements for TSPs

**Conformity Assessment:** EN 319 403-1: Requirements for CABs assessing TSPs

**Identity Proofing:** TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects

# Standards

Trust Services Providers supporting digital signatures

## Certificates

- EN 319 411-1 and EN 319 411-2: Policy and security requirements for TSPs issuing certificates: general requirements (part 1) and issuing EU qualified certificates (part 2)
- EN 319 412-x: Certificate profiles

## Timestamps

- EN 319 421: Policy and security requirements for TSPs issuing electronic time-stamps
- EN 319 422: Time stamp protocol and profile

## Attestation of attributes

- TS 119 470 and 119 471

# Standards

## Trust Application Service providers

### eDelivery

- Registered Delivery Service
  - EN 319 521: Policy and Security Requirements for Electronic Registered Delivery Service Providers
  - EN 319 522-x: Registered Electronic Delivery Services
- Registered Email Service
  - EN 319 531: Policy and Security Requirements for Electronic Registered Email Service Providers
  - EN 319 532-x: Registered Electronic Mail (REM) Services

### Preservation

- TS 119 511: Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- TS 119 512: Protocols for trust service providers providing long-term data preservation services

# Standards

Signatures: Creation and validation

AdES creation and validation

- EN 319 102-1: Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation

Formats

- EN 319 122-x: CAdES, EN 319 132-x: XAdES, EN 319 142-x: PAdES, EN 319 162-x: ASiC,
- TS 119 182-x: JAdES

Cryptographic suites (Based on SOG-IS)

- TS 119 312: Cryptographic suites (aka “Algo Paper”)

# 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
  - This urgency classification relied on the very simple "X + Y + T > Z“ equation outlined in ETSI EG 203 310.
- 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.

# Methodology

ETSI TR 103 619:

- Staged approach to QSC migration
  - Stage 1: Inventory compilation
    - Risk, data, cryptographic assessment
    - Infrastructure and suppliers inventory
  - Stage 2: Preparation of the migration plan
    - Issues
    - Key and trust management
    - Business process
  - Stage 3: Execution of the migration plan
    - Migration and mitigation management

# Stakeholders approach

The first priority stakeholders identified by ETSI ESI were:

- Qualified Trust Service Providers issuing qualified certificates
  - The relying parties of such providers are especially susceptible to have with long-lived/monolithic infrastructure with means they should begin their QS migration as soon as possible.
- 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

- **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 QS migration can be undertaken. Before then, ETSI ESI may consider giving recommendations to its stakeholders to begin QS migration in areas where replacement standards are identified.

# Migration plan

- Specifically, regarding standards on policy and security requirements, ETSI ESI is considering providing requirements for its stakeholders to begin QSC 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 QSC 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 QS 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 QS 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.

# Migration plan

## NIST

- FIPS-203 Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) Standard (2024-08-13)
- FIPS-204 Module-Lattice-Based Digital Signature (ML-DSA) Standard (2024-08-13)
- FIPS-205 Stateless Hash-Based Digital Signature (SLH-DSA) Standard (2024-08-13)
- NIST IR 8547 Transition to Post-Quantum Cryptography Standards (Initial Public Draft), published November 12, 2024 Comments Due: January 10, 2025

## IETF

- RFC 9629 "Using Key Encapsulation Mechanism (KEM) Algorithms in the Cryptographic Message Syntax (CMS)"
- draft-ietf-tls-hybrid-design-11 "Hybrid key exchange in TLS 1.3" seems ready for adoption
- draft-ietf-lamps-dilithium-certificates-05 "Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA"
- draft-ietf-lamps-x509-slhdsa-03 "Internet X.509 Public Key Infrastructure: Algorithm Identifiers for SLH-DSA"
- draft-ietf-lamps-kyber-certificates-06 "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)"

# Migration plan

- IETF
  - draft-ietf-lamps-cms-ml-dsa-01 “Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)”
  - draft-ietf-lamps-cms-sphincs-plus-17 “Use of the SLH-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)”
  - draft-ietf-lamps-pq-composite-kem-05 “Composite ML-KEM for use in X.509 Public Key Infrastructure and CMS”
  - draft-ietf-cose-dilithium-04 “ML-DSA for JOSE and COSE”
  - draft-ietf-cose-sphincs-plus-05 “SLH-DSA for JOSE and COSE”
  - draft-ietf-cose-hpke-09 “Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)”
  - draft-ietf-cose-hpke-09 “Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)”
  - draft-bonnell-lamps-chameleon-certs-05 “A Mechanism for Encoding Differences in Paired Certificates”
  - draft-ietf-pquip-hybrid-signature-spectrums-04 “Hybrid signature spectrums”

# 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 QSC 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.
- Require support for RFC 9629 (at least for ERDS TSPs)

# EUDI Wallet and Selective Disclosures based on ZKP

Regulation (EU) 2024/1183 introduced the concept of the European Digital Identity Wallets for which there are 2 important points

1- EUDI Wallet infrastructure depends on digital signatures (e.g., signed credential and credential presentation)

2- ZKP and selective disclosure

- A key tenet of this EUDI Wallet is the ability of the user to selectively disclose the personal data / credentials / attributes held in that wallet.
- Selective disclosure can be achieved through various means which include carefully designed formats and cryptography (ZKP)
- ETSI ESI published a technical report providing an analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes: ETSI TR 119 476.
- In general, ZKP offers more flexibility and possibilities regarding selective disclosure compared to format-driven approaches.
- Considering the quantum threat, only quantum-safe ZKP should be considered
- However, currently, there are no programme for identifying recommended QS algorithms for ZKP.

# Further information

Information on available standards and current activities:
https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

ETSI standards: available for free download
http://www.etsi.org/standards-search

CEN standards: available through National Standards Organisations

Updates on standardisation:
https://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1