4th International Workshop on Trends in Digital Identity

Software-assisted analysis of post-quantum cryptography migration for the European Digital Identity Wallet

Salvatore Migliaccio, Paolo Campegiani, Giulio di Clemente
Namirial S.p.A.

Content Overview

1. **Introduction**
2. **EUDI Wallet & Namirial Wallet**
3. **The Quantum Threat & Standardisation**
4. **CBOM-Based Security Assessment**
5. **Conclusions & Future Work**

1 Introduction

What is the EUDI Wallet?

- **The European Digital Identity Wallet (EUDI Wallet)** is a flagship EU initiative under the revised **eIDAS 2.0 regulation** (Reg. 2024/1183), set to become the central digital trust infrastructure of the European Union. By end of 2026, every Member State must provide at least one wallet solution to citizens and residents.

- The Wallet will enable:
  - **Secure Cross-border Authentication**
  - **Electronic signatures**
  - **Presentation of verifiable credentials**

ARF — Architecture & Reference Framework

▶ Common protocols (OpenID4VCI, OpenID4VP) for interoperability across all Member States

▶ MUST/SHOULD normative language — strict security baseline for all implementations

▶ Trust model: issuer authentication, verifier validation, wallet attestation

▶ Privacy principles: selective disclosure, data minimization, user control

▶ Credential formats: SD-JWT VC, ISO mdoc (18013-5), PID, EAA, QEAA

2 EUDI Wallet: Ecosystem Architecture

Wallet Unit — Internal Components

Wallet Instance
The mobile app — manages the credential lifecycle and the user interface.

WSCD
Secure chip where private keys reside. Keys **never leave** the WSCD

WTE & WIA
Cryptographic attestations proving the wallet's authenticity to Relying Parties.

Trust Model & Trusted Lists

Trust is rooted in **X.509 certificates** distributed through national Trusted Lists, aggregated at EU level.

EU Trust Registry
Aggregates Trusted Lists from all 27 Member States

- **National Trusted Lists**
- **Attestation Rulebook Catalogue**

Large Scale Pilots (LSP)

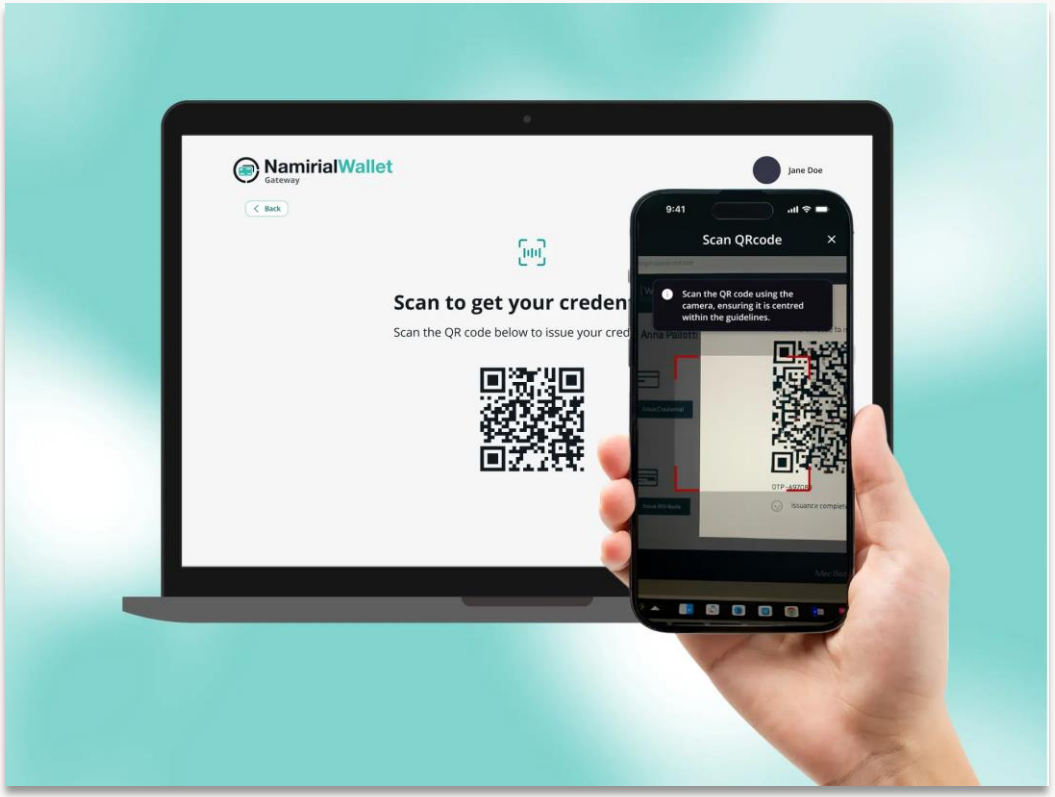
EU-funded projects testing the EUDI ecosystem in real cross-border scenarios

Concluded (2024)
- **POTENTIAL**
- **EWC**
- **NOBID**
- **DC4EU**

Active(2025-now)
- **APTITUDE**
- **WE BUILD**

2 The Namirial Wallet platform

- Issues and manages **PID, EAA, QEAA,** qualified attestations with legal standing across all Member States.
- **Wallet-as-a-Service (WaaS),** SDKs, APIs, and infrastructure for public and private sector integration.
- Supports qualified **electronic signatures (QES)**, KYC onboarding, and cross-border verifiable credentials.



3 The Quantum Threat – Impact on EUDI Wallet Cryptography

- The EUDI Wallet relies on **public-key cryptography** at every layer. A Cryptographically Relevant Quantum Computer (CRQC) running Shor's algorithm would compromise all of it.

Primitive	Used for	Quantum Threat
RSA-2048	Cert. Signatures, WTE/WIA	**Broken with Shor**
ECDSA, P-256	Credential Signing	**Broken with Shor**
ECDH	TLS Key Exchange	**Broken with Shor**
X.509 PKI	Trusted Lists, root CA	**Broken with Shor**
AES-256 / SHA	Symmetric Encryption	**Weakened – Safe with Larger keys**

IF CRYPTOGRAPHY BREAKS — THE CASCADE

CRQC runs Shor's algorithm

↓

Private keys recovered
RSA/ECC keys from certs, WSCD, Trusted Lists

↓

Credential forgery
Attacker creates valid PID, EAA, QEAA — undetectable

↓

Trust chain collapses
Trusted Lists, root CAs, Wallet Trust Evidence — all invalid

↓

EUDI Wallet ecosystem integrity

4 PQC Standardization Landscape

NIST Standardization process 2016 → Now

- **FIPS 203 ML-KEM**
  Key Encapsulation Mechanism based on Module Lattice-Based Learning with Errors (ML-WE), published in August 2024.
- **FIPS 204 ML-DSA**
  Digital Signature Algorithm based on Module Lattice-Based Learning with Errors (ML-WE), formerly known as CRYSTALS-Dilithium
- **FIPS 205 SLH-DSA**
  Hash-Based Digital Signatures based on stateless hash-based problems, formerly known as SPHINCS+
- **FIPS 206 FN-DSA (in development)**
  Compact Signatures, Fast-Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm

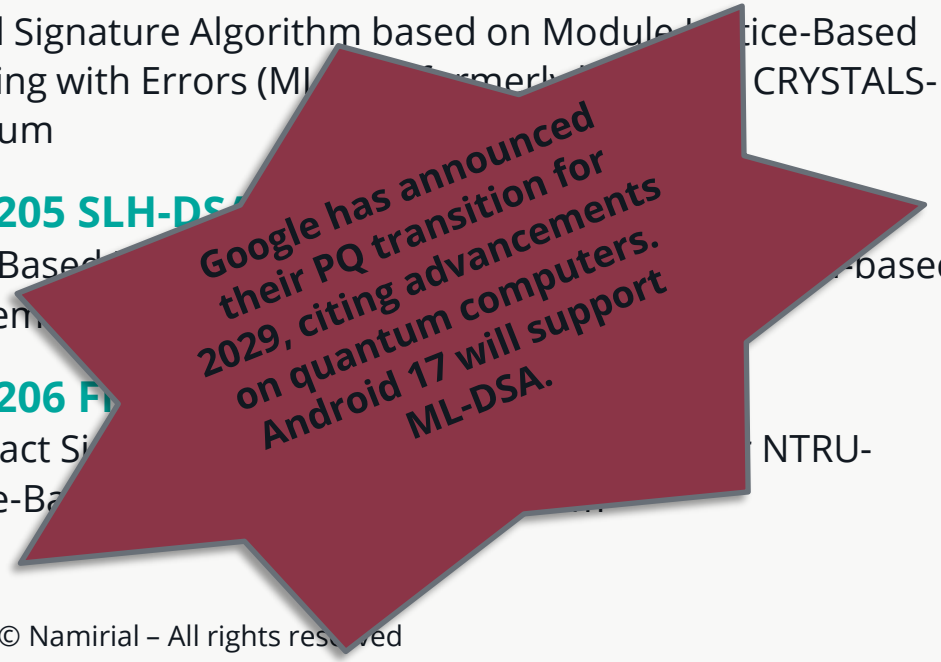
EU Coordinated Implementation Roadmap — June 2025

- **2026**
  National strategies & inventories: All Member States initiate PQC plans. CBOM inventories, stakeholder mapping, pilot projects for high/medium-risk use cases.
- **2030**
  High-risk systems fully transitioned: Critical infrastructure, finance, healthcare, defense. Quantum-vulnerable algorithms not allowed stand-alone. **EUDI Wallet is in this category.**
- **2035**
  Full transition — all systems: Medium-risk use cases complete. Crypto-agility by default. Aligned with NIST IR 8547 deprecation schedule.

4 PQC Standardization Landscape

NIST Standardization process 2016 → Now

- **FIPS 203 ML-KEM**
  Key Encapsulation Mechanism based on Module Lattice-Based Learning with Errors (ML-WE), published in August 2024.
- **FIPS 204 ML-DSA**
  Digital Signature Algorithm based on Module ice-Based Learning with Errors (MI CRYSTALS-Dilithium
- **FIPS 205 SLH-DS**
  Hash-Based -based problem
- **FIPS 206 F**
  Compact Si NTRU-Lattice-Ba



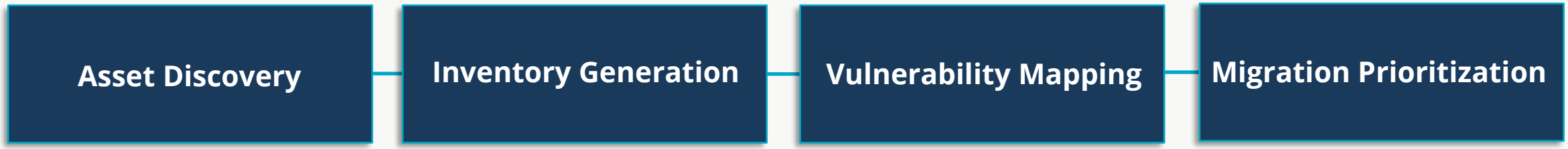
EU Coordinated Implementation Roadmap — June 2025

- **2026**
  National strategies & inventories: All Member States initiate PQC plans. CBOM inventories, stakeholder mapping, pilot projects for high/medium-risk use cases.
- **2030**
  High-risk systems fully transitioned: Critical infrastructure, finance, healthcare, defense. Quantum-vulnerable algorithms not allowed stand-alone. **EUDI Wallet is in this category.**
- **2035**
  Full transition — all systems: Medium-risk use cases complete. Crypto-agility by default. Aligned with NIST IR 8547 deprecation schedule.

5 CBOM-Based Security Assessment

- A **Cryptographic Bill of Materials (CBOM)** is a structured inventory of all cryptographic components used in a system — algorithms, key sizes, libraries, certificates, and protocol usage. It enables systematic discovery of quantum-vulnerable assets and supports migration planning.

CBOM Workflow



WHAT A CBOM CAPTURES

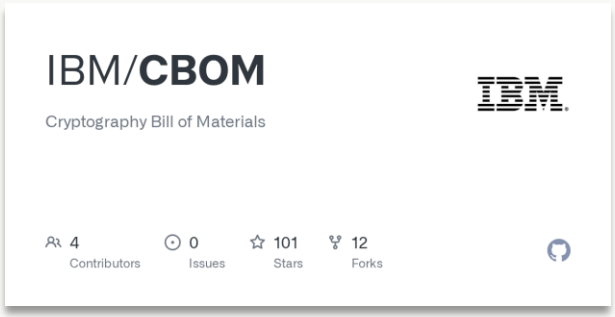
- **Algorithms & parameters** — name, key size, padding scheme (e.g. SHA256-RSA with PKCS#1 v1.5)
- **Certificates & trust anchors** — X.509 profiles, issuer chains, validity periods
- **Cryptographic libraries & versions** — OpenSSL, BouncyCastle and their configurations
- **Protocol-level usage** — TLS version, cipher suites, key exchange mechanisms
- **Keys & secrets** — location, size, exposure risk (e.g. private keys in config paths

5 CBOM Tools – Evaluated in This Work

Selected | Open source

CBOMkit

IBM Research, Now PQC Alliance

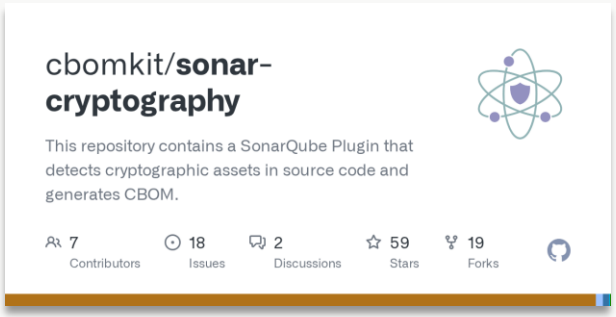


- CycloneDX CBOM output
- No license required
- Reproducible, CI/CD ready
- Limited language coverage

Evaluated | Open source

Sonar Cryptography

IBM · "Hyperion" plugin



- Detects crypto usage in code
- CBOM-compatible export
- Requires SonarQube infrastructure
- Not production-grade for PQC

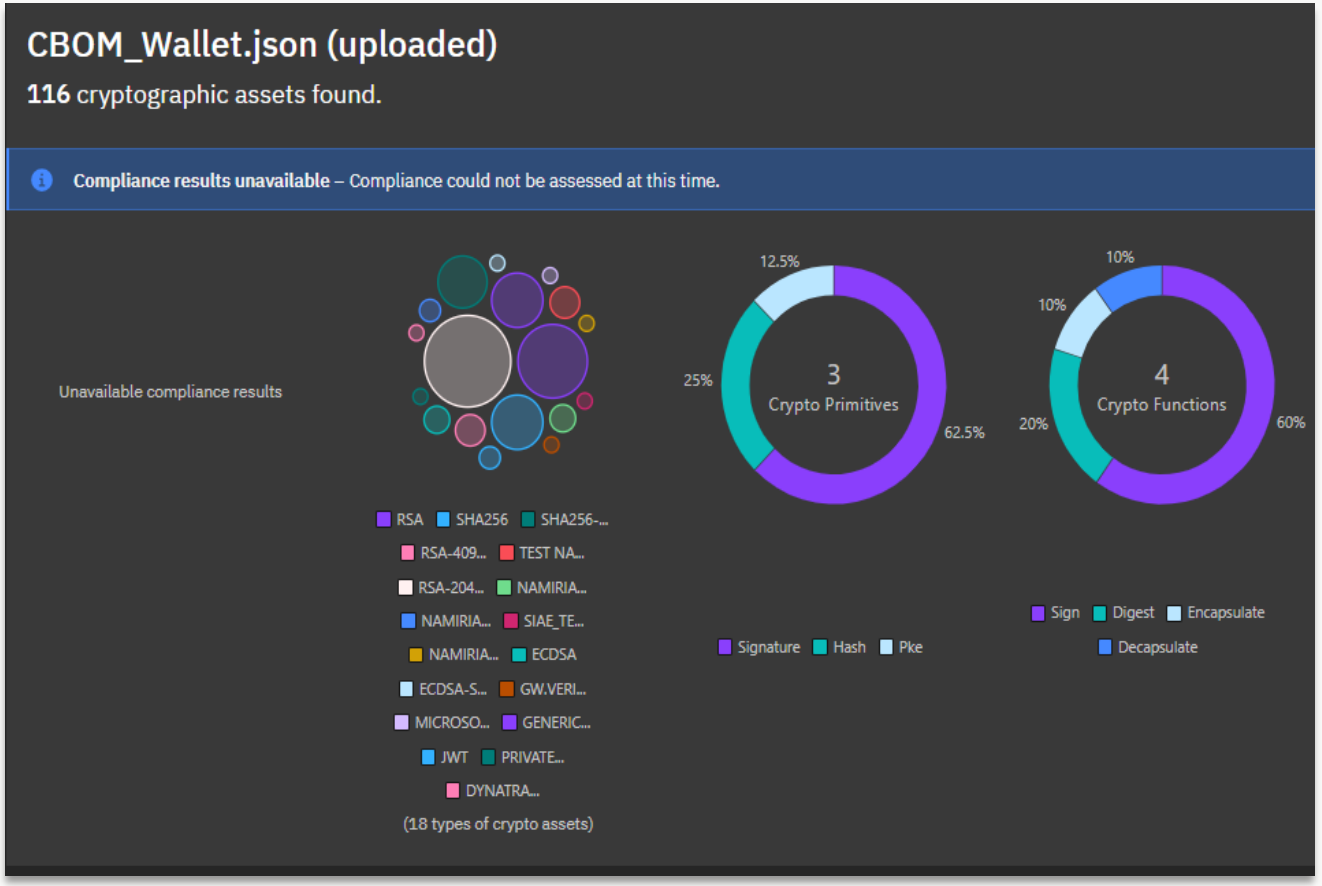
Evaluated | Enterprise

IBM Quantum Safe Explorer

IBM Commercial

- Enterprise-scale discovery
- Risk dashboard & dependency maps
- Proprietary — IBM license required
- Not selected for reproducibility

6 CBOM Results on the Namirial Wallet



Key Findings

- **RSA-dominant signature schemes**
  RSA and RSA-based signatures (e.g., SHA256-RSA with PKCS#1 v1.5 padding) identified in certificate stores and wallet-related artifacts. Directly quantum-vulnerable.
- **Secrets & API**
  Generic API keys and integration endpoints found in the CBOM. Not PQC-specific, but materially affect the overall security posture and correctness of key management practices.
- **Long-lived trust material**
  Certificate properties indicate trust anchors and credentials that remain operational well into the PQC mandatory migration window. Critical under HNDL threat model.

6 CBOM Results on the Namirial Wallet

- Migration complexity assessment: **moderate-to-high**. If such complexity arises in an ecosystem still under active deployment, similar or greater challenges are expected for legacy digital identity systems where cryptography is more deeply embedded.

Category	Count	Notes
Total assets	116	As reported by CBOMkit viewer
Algorithms	48	Signature (30), Hash (12), KEM (6)
Certificates	12	X.509 in config and stores
Crypto material	56	Key material, tokens, secrets

- **Technical challenge**
  Toolchain still evolving, automated PQC compliance assessment not always available.
- **Standards challenge**
  PQC standards (NIST FIPS 203/204/205) are finalized, but their integration into identity protocols is still ongoing and not yet normatively defined.
- **Regulatory challenge**
  eIDAS 2.0, ARF, ENISA guidelines, NIS2, and DORA all impose compliance requirements

7 Conclusion & Future Works

- *Post-quantum migration should be addressed **early** — the wallet will become a long-lived foundation for digital trust in Europe. Greater challenges expected for legacy identity systems where cryptography is more deeply embedded.*

Conclusion

1. **PQC transition overlaps with wallet deployment**
   Cryptographic choices made today may create future technical debt.
2. **Not a simple algorithm swap**
   Trust anchors, credential lifecycles, and validation chains must all be addressed. Standard must be modified
3. **Tooling is still evolving**
   Automated PQC compliance assessment is not yet fully available.

Future Works

1. **Extend CBOM analysis**
   Analyze additional wallet implementations and legacy identity management systems.
2. **Compare cryptographic profiles**
   Identify common patterns and migration hotspots across different wallet solutions
3. **Evaluate hybrid migration strategies**
   Test PQC+classical hybrid approaches in real cross-border interoperability scenarios.
4. **Integration with AI Cybersecurity Agent**
   Adding AI LLMs model for advanced analysis and conformity assessments

7 Call for Collaboration

- We are actively looking for collaborators, research partners, and practitioners to extend this work — across academia, industry, and standardization bodies

TOPICS WE ARE INTERESTED IN:

Post-Quantum Cryptography | **EUDI Wallet**

CBOM & Crypto Agility | **eIDAS 2.0 Compliance**

ML-KEM / ML-DSA | **Digital Trust Infrastructure**

Legacy Identity Migration | **Hybrid PQC Approaches**

AI Tools & ML Models | **Agentic AI**

OUR ROADMAP INCLUDES:

- CBOM analysis of multiple wallet implementations & legacy identity systems
- Evaluation of hybrid PQC migration strategies in cross-border scenarios
- Automated PQC readiness rulesets and compliance tooling

Get in contact!

Salvatore Migliaccio

R&D Engineer

Email: s.migliaccio @namirial.com

