



The Quantum-Ready Trust Stack

Securing Europe's Identity Infrastructure for the Post-Quantum Era

Europe is building digital identity infrastructure designed to last decades. The cryptographic foundations supporting it may not.

As quantum timelines accelerate, the gap between deployment and security is narrowing and the decisions made now will determine whether trust holds, or fails, at scale.

MAY 2026

thequantumspace.org



**Launch, protect, and monetize your software with
a ready-to-use, secure licensing infrastructure.**

- Built-in software protection against reverse engineering
- Preconfigured licensing models aligned with your business
- Centralized control of licenses, users, and entitlements
- Self-service access for customers and partners
- Secure, scalable cloud operation

**Accelerate time-to-market.
Stay in control of your digital IP.**

Find out more!



THE QUANTUM SPACE

TQS Executive Intelligence

The Quantum-Ready Trust Stack

*Securing Europe's Identity Infrastructure for the
Post-Quantum Era*

PUBLISHED: MAY 2026

The Quantum Space | thequantumspace.org

Trusted Steps. Quantum Leaps.

About This Report

The Quantum-Ready Trust Stack is a executive intelligence report produced by The Quantum Space (TQS), an independent media and research platform dedicated to digital trust, post-quantum security, and the evolving regulatory architecture of the European digital economy.

This whitepaper synthesises original TQS research, analysis from the TQS Innovating Trust podcast series, and the findings published across our content library (including the whitepapers Identities at Scale, Sovereign by Design, and Physics as the New Firewall) with new research and analysis developed specifically for this report.

It is intended for senior technology and security leaders, digital identity programme managers, policy teams, and enterprise architects operating in or alongside European digital infrastructure. It does not assume prior expertise in quantum physics or advanced cryptography, though it does assume a working familiarity with digital trust systems, public-key infrastructure (PKI), and the European regulatory landscape.

The central argument is straightforward: Europe is simultaneously deploying the world's most ambitious digital identity infrastructure and racing against a cryptographic deadline. The European Digital Identity Wallet (EUDI Wallet) is being built to last decades. So is the quantum threat that could undermine it. Getting the cryptographic foundation right now, not later is the defining technical decision of Europe's digital decade.

Table of Contents

About This Report2

Table of Contents3

Executive Summary. 6

Chapter 1: *Digital Identity Has Entered Its Industrial Phase*8

 1.1 From Policy Concept to Production System..... 8

 1.2 What Industrial-Phase Identity Actually Means..... 8

 1.3 The Scale of the Deployment 9

 1.4 How European Countries Are Approaching Implementation 9

 1.5 Identity as Critical Infrastructure 10

Chapter 2: *The Trust Stack – A Framework for the Quantum Age*11

 2.1 Introducing the TQS Trust Stack..... 11

 2.2 The Five Layers and Their Quantum Exposure..... 11

 2.3 The Trust Stack Under Quantum Pressure: A Summary View 13

 2.4 Why the Trust Stack Matters for Migration Strategy..... 14

Chapter 3: *How Quantum Computing Threatens Identity Infrastructure* 15

 3.1 The Cryptographic Foundation of Digital Identity..... 15

 3.2 What Shor's Algorithm Changes 15

 3.3 The Harvest Now, Decrypt Later Threat 16

 3.4 The Timeline Problem 16

 3.5 Identity-Specific Vulnerabilities 17

Chapter 4: *The EUDI Wallet Under Quantum Scrutiny* 18

 4.1 Architecture of the EUDI Wallet 18

 4.2 The Cryptographic Stack at Risk..... 19

 4.3 The Certification Complexity Challenge 19

 4.4 Secure Elements vs HSMs: Different Quantum Migration Paths 20

 4.5 Quantum Threat to Selective Disclosure 20

Chapter 5: *Post-Quantum Cryptography – What the Standards Actually Require*21

 5.1 The NIST PQC Standardisation Programme 21

 5.2 The European Dimension: ETSI and ENISA..... 21

 5.3 Hybrid Cryptography as a Transition Strategy 22

 5.4 Performance and Constraint Considerations..... 22

 5.5 Cryptographic Agility as a Design Principle 23

Chapter 6: <i>The Regulatory Landscape</i>	24
6.1 The EU's Regulatory Architecture for Digital Trust	24
6.2 eIDAS 2.0 — The Identity Foundation.....	24
6.3 The Cyber Resilience Act — Security by Design	25
6.4 NIS2 — Cybersecurity Governance and Quantum Risk.....	25
6.5 DORA — Financial Sector Resilience and Quantum	25
6.6 The AI Act — Intersection with Identity Integrity	26
Chapter 7: <i>National Readiness — How Europe's Member States Are Preparing</i>	27
7.1 The Uneven Landscape of European PQC Readiness.....	27
7.2 The Leading Group: High Technical Maturity.....	27
<i>Germany</i>	27
<i>France</i>	27
<i>The Netherlands</i>	28
7.3 The Middle Group: Active Preparation	28
<i>Estonia</i>	28
<i>Austria and Scandinavia</i>	28
7.4 Areas Requiring Accelerated Progress	28
7.5 The Cross-Border Trust Chain Risk.....	29
Chapter 8: <i>Migration Pathways — A Practical Roadmap</i>	30
8.1 The Migration Framework	30
8.2 Phase 1: Discover — Cryptographic Inventory.....	30
8.3 Phase 2: Plan — Risk Prioritisation and Architecture.....	31
8.4 Phase 3: Transition — Staged Migration.....	32
8.5 Phase 4: Operate — Quantum-Safe Operations	32
Chapter 9: <i>The Geopolitical Dimension</i>	33
9.1 Identity Infrastructure as Strategic Asset.....	33
9.2 The Cryptographic Sovereignty Gap	33
9.3 The Geopolitics of Quantum Computing Access.....	34
9.4 The EUDI Wallet as Geopolitical Instrument.....	34
9.5 International Standards and Alignment.....	35
Conclusion & Recommendations: <i>The Strategic Imperative</i>	36
Recommendations for Identity Programme Managers	37
Recommendations for Regulators and Policymakers	37
Recommendations for Technology Leaders and CISOs.....	38
Appendix A: <i>Glossary of Key Terms</i>	39

Appendix B: *Regulatory Timeline Reference*..... 40

Appendix C: *NIST PQC Standards Summary* 41

About The Quantum Space42

Executive Summary.

Europe is building the most consequential digital identity infrastructure in its history. By 2027, every EU member state will be required to offer citizens a European Digital Identity Wallet — a cryptographically secured container for passports, driving licences, health records, banking authorisations, and university credentials. By 2030, major private-sector service providers will be obliged to accept it.

This is not a pilot. It is a continental infrastructure programme, and it will need to remain trusted not just for years, but for decades. At the same time, a different countdown is running.

Quantum computing capabilities are advancing at pace. The Global Risk Institute estimates a 50 percent probability that quantum computers capable of breaking current public-key cryptography will exist by 2035. The US National Institute of Standards and Technology (NIST) finalised its first post-quantum cryptography (PQC) standards in 2024.

The European Commission has issued a Coordinated Implementation Roadmap requiring national crypto-migration strategies by 2026, migration of high-risk systems by 2030, and medium-risk systems by 2035.

The problem is not that Europe lacks ambition on digital identity. The problem is that the cryptographic foundations currently planned for the EUDI Wallet were not designed for the quantum age.

RSA and Elliptic Curve Cryptography (ECC); the algorithms underpinning nearly every element of today's identity trust architecture, will be rendered obsolete by a cryptographically relevant quantum computer (CRQC). And credentials issued today may still need to be verified in 2040.

This report examines the collision of these two realities. It argues that:

- Digital identity has entered its industrial phase — moving from pilots and policy debates to production infrastructure at national scale.
- The quantum threat to that infrastructure is not theoretical — harvest-now-decrypt-later attacks are already creating risk for long-lived credentials.
- The EUDI Wallet's current cryptographic architecture requires a structured migration pathway to post-quantum algorithms before widespread deployment.
- The EU's regulatory stack — eIDAS 2.0, the Cyber Resilience Act, NIS2, DORA, and the AI Act — provides a coherent framework for managing this transition, but only if organisations understand how these regulations interact.
- Composite cryptography, deploying classical and post-quantum algorithms in parallel, offers a practical near-term transition path.

- The geopolitical stakes are high: European digital sovereignty depends not just on hosting data within EU borders, but on controlling the cryptographic infrastructure that protects it.

The core finding

The decision to deploy quantum-safe cryptography in European digital identity infrastructure is not a future choice. It is a present obligation. Credentials being issued today may be verified — or attacked — in 2040. The cryptographic decisions made in 2026 will determine whether Europe's identity infrastructure is trustworthy across its entire operational lifetime.

Chapter 1: *Digital Identity Has Entered Its Industrial Phase*

For most of the past decade, digital identity in Europe existed primarily as a policy ambition. The original eIDAS regulation of 2014 established a legal framework for cross-border electronic identification and trust services, but adoption was fragmented and largely confined to government-to-citizen services within individual member states. Interoperability across borders remained limited. Private-sector engagement was minimal.

1.1 *From Policy Concept to Production System*

By 2026, that era has ended. The revised eIDAS 2.0 regulation — officially the EU Digital Identity Framework — has transformed digital identity from an optional public-sector convenience into a mandatory infrastructure programme. The European Digital Identity Wallet is no longer a speculative concept. It is entering production across multiple member states simultaneously, with real citizens, real credentials, and real legal effect.

This shift — from policy to production — is what defines the industrial phase of digital identity. As TQS analysis has described, identity is now being manufactured, issued, verified, revoked, and audited at scale. The processes and institutions that once managed identity informally or through paper-based systems are being replaced by cryptographic infrastructure with the same engineering rigour and resilience expectations that we apply to financial payment networks or power grid management.

1.2 *What Industrial-Phase Identity Actually Means*

The term 'industrial phase' is deliberate and precise. It captures something important about the transition underway.

In the pre-industrial phase of digital identity, trust was primarily institutional. You trusted a bank or a government agency to verify who they were interacting with. The technology was secondary — a convenience layer on top of existing human processes and institutional relationships. Failures were handled through those same human processes: phone calls, branch visits, manual review.

In the industrial phase, trust is cryptographic. The EUDI Wallet does not ask you to trust a government department or a private company to tell you that a credential is valid. It asks you to trust a mathematical proof. That proof is generated and verified by standardised algorithms running on certified hardware. There is no human in the loop at the point of verification. The system either works or it does not — and at scale, the difference between those two outcomes affects millions of people.

This is not a critique of the approach. Cryptographic trust is more reliable, more privacy-preserving, and more resistant to corruption than institutional trust. But it comes with a different category of risk. Institutional systems can be patched with policy decisions.

Cryptographic systems can only be patched by changing the mathematics. And once credentials are widely deployed and embedded in legal processes, payment systems, and cross-border services, changing the underlying mathematics becomes extraordinarily complex.

1.3 The Scale of the Deployment

To understand the magnitude of what is being built, consider the deployment targets established under eIDAS 2.0:

- Every EU member state must offer citizens a digital identity wallet by 2026.
- Major online platforms, banks, transport providers, and healthcare systems must accept EUDI Wallets by 2027.
- The wallet must support a minimum set of verified credentials including national identification, driving licence, and academic qualifications.
- Cross-border recognition of EUDI Wallet credentials must be available across all member states.

The European Commission estimates that approximately 450 million EU citizens will eventually be eligible to use the wallet. Even conservative adoption projections suggest hundreds of millions of credential presentations per year within the first few years of full deployment.

This is a scale of operation that places the EUDI Wallet in the same category as SWIFT, the European payments infrastructure, or the DNS system — critical infrastructure whose failure would cascade across economies and societies. It demands engineering to the same standards.

1.4 How European Countries Are Approaching Implementation

One of the most revealing aspects of the EUDI Wallet programme is the diversity of national implementation approaches. Different European countries are bringing different architectural philosophies, institutional legacies, and risk appetites to the same regulatory objective.

Nordic countries — particularly Finland, Sweden, and Estonia — are pursuing architecture-first models that build on existing mature national digital identity infrastructure. Estonia's X-Road system, for example, already provides a distributed data exchange layer that can be extended to support wallet credential exchange. These countries tend to favour strong cryptographic assurance, decentralised credential storage, and minimal data sharing beyond what is strictly necessary for a transaction.

Central European countries with highly centralised civil registry systems — including Germany, Austria, and the Netherlands — are approaching the wallet as an extension of existing state identity infrastructure. These models tend to rely on centralised certificate authorities and government-issued secure elements, which offer high assurance but also create single points of failure and potential geopolitical dependency on hardware suppliers.

Southern European countries and newer EU members are generally pursuing more market-driven frameworks that involve significant private-sector participation. These models offer faster deployment timelines but raise additional questions about governance, interoperability, and the long-term management of trust anchors.

The diversity of approaches is not inherently a problem — eIDAS 2.0 intentionally allows architectural flexibility within a common trust framework. But it does mean that the quantum-readiness of the EUDI Wallet ecosystem will vary significantly by country, and that cross-border interoperability will depend on the weakest cryptographic link in the chain.

The rapid expansion of pilot programmes and national implementations should not be interpreted as evidence of quantum readiness. Increased deployment activity demonstrates momentum, but it does not resolve underlying challenges in certification, cryptographic migration, hardware dependency, or cross-border interoperability.

The transition to industrial-scale identity infrastructure is underway, but its long-term trustworthiness remains contingent on decisions that have yet to be fully implemented.

1.5 Identity as Critical Infrastructure

Perhaps the most significant implication of the industrial phase is the reclassification of digital identity as critical infrastructure. This is not merely a rhetorical point. Once identity becomes industrial infrastructure, it also becomes a target.

Critical infrastructure has specific properties that distinguish it from ordinary technology systems. It is deeply embedded in the functioning of society; its failure causes cascading effects across healthcare, finance, transport, and governance. It is difficult to replace quickly because it has no equivalent alternative. It is attractive to sophisticated adversaries because attacking it produces systemic effects disproportionate to the effort involved.

Digital identity, at industrial scale, meets all of these criteria. A successful attack on the cryptographic foundations of the EUDI Wallet — whether through a direct cryptographic break or through a harvest-now-decrypt-later strategy — would not merely compromise individual privacy. It would undermine the legal validity of millions of transactions, the integrity of cross-border services, and the trust that European citizens place in their governments and digital institutions.

Building infrastructure of this importance on a cryptographic foundation that is known to have a finite operational lifetime, and that finite lifetime may be shorter than the deployment lifetime of the infrastructure, is a risk that requires immediate strategic attention.

Chapter 2: *The Trust Stack – A Framework for the Quantum Age*

Understanding how the quantum threat interacts with digital identity infrastructure requires a conceptual framework that can map the complexity of modern digital trust systems. The Quantum Space Trust Stack provides that framework.

2.1 *Introducing the TQS Trust Stack*

The Trust Stack is a layered model of how digital systems establish, maintain, and lose trust. It identifies five layers — Ownership, Responsibility, Control, Participation, and Time — each of which represents a distinct domain of trust governance. Each layer has its own regulatory instruments, technical mechanisms, and failure modes.

The value of the Trust Stack as an analytical tool is that it makes the relationships between layers visible. Quantum computing does not attack just one layer of this architecture. It attacks the foundations of every layer simultaneously — because every layer ultimately depends on cryptography to enforce its security properties.

2.2 *The Five Layers and Their Quantum Exposure*

Layer 1: Ownership — Infrastructure and Technology Sovereignty

The Ownership layer addresses who controls the hardware, software, platforms, and data infrastructure that underpin digital systems. In the European context, this layer is governed primarily by the Cyber Resilience Act, the EU Chips Act, and the Data Act.

The quantum threat to this layer is structural. Europe's digital infrastructure is built on semiconductors, secure elements, and hardware security modules that implement classical cryptographic algorithms at the hardware level. Migrating to post-quantum cryptography requires not just software updates but, in many cases, hardware replacement or recertification.

The EU Chips Act's ambition to build European semiconductor capability becomes even more strategically important in a post-quantum world where the ability to manufacture and certify quantum-safe hardware components is a dimension of national security.

Layer 2: Responsibility — Cybersecurity and Operational Resilience

The Responsibility layer deals with accountability for digital security failures. NIS2 and DORA define who is legally responsible when infrastructure is compromised, and what obligations they carry for incident response and recovery.

The quantum threat here is temporal. NIS2 and DORA were written for the current threat landscape. They define incident reporting obligations and risk management requirements

based on classical attack vectors. As quantum capabilities emerge, both regulatory frameworks will need to be interpreted — and potentially updated — to address quantum-specific risks, including harvest-now-decrypt-later attacks that may not be discoverable until years after the initial data capture.

Layer 3: Control — AI and Automated Decision-Making

The Control layer governs algorithmic systems — their deployment, oversight, and accountability. The EU AI Act is the primary regulatory instrument here, alongside GDPR provisions on automated decision-making.

The quantum threat to this layer is indirect but potentially significant. AI systems used in identity verification — facial recognition, document authentication, behavioural analytics — rely on cryptographic infrastructure for their own integrity and for the security of their training data and model weights. A post-quantum adversary capable of compromising the cryptographic layer could manipulate AI systems in ways that are difficult to detect.

Layer 4: Participation — Digital Identity and Access

The Participation layer is where the quantum threat is most immediately visible. eIDAS 2.0, the EUDI Wallet framework, and the EU Anti-Money Laundering regulations all depend on cryptographic mechanisms — digital signatures, verifiable credentials, selective disclosure proofs — that are vulnerable to quantum attack.

This is the layer where the industrial-phase identity infrastructure described in Chapter 1 sits. And it is the layer where the consequences of cryptographic failure are most direct: credentials that cannot be trusted, identities that cannot be verified, transactions that cannot be legally validated.

Layer 5: Time — Cryptography and Long-Term Trust

The Time layer is the most fundamental, and the most directly threatened by quantum computing. It asks: how long does digital trust last? Cryptography provides the mechanisms — digital signatures, timestamps, certificate chains — that allow transactions, credentials, and documents to remain verifiable over years or decades.

This is precisely the layer where post-quantum cryptography must operate. The question is not whether current cryptographic algorithms will eventually be broken by quantum computers. The question is when — and whether the credentials and transactions being signed today will still need to be verified after that break occurs.

The trust stack is not being shaped by regulation alone. Judicial systems are increasingly asserting influence over how digital systems are designed, operated, and held accountable. Recent legal actions have demonstrated a shift away from evaluating individual transactions or user-generated content, and toward examining the behaviour of systems themselves — how they are constructed, how they guide interaction, and how outcomes are produced at scale.

This introduces a new form of enforcement that operates after deployment but directly impacts system architecture. In this environment, trust cannot be treated as a static property established at design time. It must be continuously demonstrable, with clear lines

of accountability across ownership, control, and operation. The trust stack provides the structure through which that accountability can be understood and implemented.

The post-quantum transition sits within a broader structural shift in how digital trust is defined and enforced. Trust is no longer a property that can be established at design time and assumed to persist. It is increasingly expected to be demonstrable in operation — through verifiable system behaviour, auditable outcomes, and cryptographic integrity that can withstand retrospective scrutiny.

For identity infrastructure, this changes the requirement. It is not sufficient for a system to have been secure at the point of deployment. It must remain provably trustworthy over time, including in environments where verification may occur years after the original transaction. In the quantum context, this elevates cryptographic resilience from a design consideration to an ongoing operational obligation.

2.3 The Trust Stack Under Quantum Pressure: A Summary View

Trust Stack Layer	Primary Focus	Key Regulations	Quantum Exposure
Ownership	Hardware & infrastructure sovereignty	CRA, Chips Act, Data Act	Hardware PQC migration required
Responsibility	Cybersecurity accountability	NIS2, DORA	Harvest-now risk, retroactive liability
Control	AI & algorithmic governance	AI Act, GDPR	Indirect — via cryptographic integrity
Participation	Digital identity & access	eIDAS 2.0, AML	Direct — credential and signature validity
Time	Cryptography & long-term trust	eIDAS Trust Services, ETSI, PQC	Existential — algorithm obsolescence

2.4 Why the Trust Stack Matters for Migration Strategy

The Trust Stack framework reveals something crucial about post-quantum migration that is often missed in purely technical discussions: migration cannot be managed layer by layer. The layers are interdependent. Migrating the Time layer — replacing classical cryptographic algorithms with post-quantum alternatives — will have cascading effects on every other layer.

Certificate authorities that anchor the Ownership layer will need to reissue certificates using post-quantum algorithms. Incident response obligations in the Responsibility layer will need to account for quantum-era attack scenarios. Digital identity credentials in the Participation layer will need to be reissued or cryptographically upgraded. And the legal frameworks that give weight to electronic signatures across all layers will need to evolve to recognise post-quantum signature standards.

This interdependence is both a challenge and an opportunity. It means that post-quantum migration cannot be delegated to a single team or department. But it also means that organisations that approach migration strategically, using the Trust Stack as a map, can identify dependencies, prioritise work, and avoid the duplication and inconsistency that result from uncoordinated point solutions.

The post-quantum transition is not only a technical replacement of algorithms. It sits within a broader shift in digital trust, in which systems are increasingly expected to demonstrate how trust is maintained in operation, not simply declare that trust was designed in at the outset. For identity infrastructure, that means cryptographic resilience, certificate validity, auditability, and verification paths must remain observable and defensible over time. In the quantum era, trust is not a static property of architecture. It is an operational condition that must continue to be evidenced.

Chapter 3: *How Quantum Computing Threatens Identity Infrastructure*

To understand the quantum threat to digital identity, it is necessary to understand what cryptography actually does in a digital identity system. At its core, digital identity infrastructure relies on three cryptographic capabilities: confidentiality (keeping data private), integrity (ensuring data has not been tampered with), and authentication (proving that a message, credential, or transaction comes from who it claims to come from).

3.1 *The Cryptographic Foundation of Digital Identity*

All three of these capabilities, in current digital identity systems, ultimately depend on the computational difficulty of certain mathematical problems — specifically, factoring large integers and computing discrete logarithms in finite groups. These are the mathematical foundations of RSA, DSA, and Elliptic Curve Cryptography (ECC), which collectively underpin virtually all current public-key infrastructure.

The reason these algorithms are secure is simple: no classical computer can solve these mathematical problems in a reasonable amount of time for large enough key sizes. A modern classical computer would take longer than the age of the universe to factor a 2048-bit RSA key. This computational intractability is what makes current identity systems trustworthy.

3.2 *What Shor's Algorithm Changes*

In 1994, mathematician Peter Shor published an algorithm that could, in principle, factor large integers and compute discrete logarithms efficiently on a quantum computer. Shor's algorithm does not make these problems easier in an incremental way. It makes them easy in a categorical sense: a quantum computer running Shor's algorithm can break RSA-2048 in hours rather than millennia.

The implication for digital identity is direct and severe. Every credential currently secured with RSA or ECC; every digital signature, every certificate in a trust chain and every public key used to authenticate a wallet holder, becomes vulnerable to forgery by an adversary with access to a sufficiently powerful quantum computer.

For symmetric encryption algorithms and hash functions, the situation is different but not benign. Grover's algorithm provides a quadratic speedup for searching, effectively halving the security level of symmetric keys. AES-128, which provides 128-bit classical security, would provide only approximately 64-bit quantum security. The practical response — doubling key sizes — is manageable, but it is not automatic. Systems need to be updated.

3.3 The Harvest Now, Decrypt Later Threat

Perhaps the most strategically alarming aspect of the quantum threat to digital identity is not the immediate decryption of current systems. It is the harvest-now-decrypt-later (HNDL) strategy. As TQS has documented extensively, sophisticated adversaries (including state-level intelligence operations) are believed to be intercepting and archiving encrypted data today, with the intention of decrypting it once quantum capabilities mature.

For financial transactions or short-lived communications, the HNDL threat may be manageable. Data that will have no value in ten years is not worth harvesting. But digital identity credentials are different. They are designed to be long-lived. A passport or driving licence credential issued today may be valid for ten years. A qualified electronic signature on a legal document may need to be verifiable for thirty years or more. A verifiable credential in a medical record or educational transcript may be referenced throughout a person's lifetime.

This means that the HNDL threat to digital identity is not merely theoretical — it is active.

Credential presentations, signature operations, and authentication events happening today are generating data that adversaries may be archiving for future quantum decryption. The question is not whether this data will eventually be vulnerable. The question is whether the identity infrastructure will have been migrated to post-quantum algorithms before the decryption becomes possible.

3.4 The Timeline Problem

Estimating when a cryptographically relevant quantum computer (CRQC) will exist is inherently uncertain. But the range of credible expert opinion is narrower than many assume. A 2023 report from the Global Risk Institute estimated a 50 percent probability of a CRQC by 2033, and a 17 percent probability by 2026.

IBM's quantum computing roadmap and Google's published progress toward fault-tolerant quantum computing suggest that the engineering challenges, while formidable, are being systematically addressed.

The European Commission's Coordinated Implementation Roadmap takes a deliberately conservative approach, planning as if a CRQC could arrive within the decade. This is appropriate risk management for critical infrastructure. If the timeline proves longer, the cost of early migration is wasted preparation. If the timeline proves shorter, the cost of late migration is the collapse of critical national infrastructure.

For digital identity planners, the relevant question is not when a CRQC will exist. It is how long it takes to migrate a major digital identity infrastructure to post-quantum cryptography. The evidence from analogous technology transitions — the migration from SHA-1 to SHA-2, the transition from TLS 1.0 to TLS 1.2 — suggests that large-scale cryptographic migrations take between five and fifteen years, depending on the complexity of the legacy environment. For the EUDI Wallet ecosystem, that clock has already started.

3.5 Identity-Specific Vulnerabilities

While the quantum threat affects all cryptographic systems, digital identity infrastructure has specific characteristics that make it particularly vulnerable:

- Long credential lifetimes. Unlike TLS certificates that expire after months, identity credentials may be valid for years or decades. Every year of delay in PQC migration extends the window of vulnerability.
- Legal status of signatures. Qualified electronic signatures under eIDAS 2.0 have legal equivalence to handwritten signatures. A successful quantum attack that compromises the cryptographic basis of past signatures does not merely create a security problem — it creates a legal problem of potentially enormous scale.
- Hardware dependencies. The WSCD and WSCA components of the EUDI Wallet are hardware-rooted. Post-quantum migration may require hardware replacement, not just software updates, in hundreds of millions of devices.
- Cross-border trust chains. The EUDI Wallet requires mutual recognition of credentials across 27 member states. A cross-border trust chain is only as secure as its weakest link — meaning that a single member state's failure to migrate to post-quantum algorithms could compromise the integrity of the entire European identity ecosystem.
- Selective disclosure mechanisms. Zero-knowledge proof systems used for selective disclosure in the EUDI Wallet — allowing users to prove an attribute without revealing their full credential — rely on cryptographic constructions that also need post-quantum variants.

Chapter 4: *The EUDI Wallet Under Quantum Scrutiny*

The European Digital Identity Wallet is not a single application, but a layered system of hardware, software, and trust services. That complexity defines both its resilience and its exposure. As quantum risk is introduced, each layer of the architecture becomes a potential point of failure. This chapter examines how the wallet is built, where the cryptographic dependencies sit, and why migrating it is as much a certification and systems challenge as it is a technical one.

4.1 *Architecture of the EUDI Wallet*

The European Digital Identity Wallet is not a single application. It is an ecosystem specification — a set of technical and regulatory requirements that define how a compliant wallet must behave, without mandating a single implementation. This architectural flexibility is both a strength and a challenge for quantum migration.

At its core, the wallet security model rests on two components identified in the Architecture and Reference Framework (ARF) developed by the EU Commission's expert group:

1. **The Wallet Secure Cryptographic Device (WSCD)** is the tamper-resistant hardware anchor. It can take the form of a secure chip embedded in a smartphone (an eSIM or embedded secure element), an external hardware device such as a smart card or hardware token, or a cloud-based Hardware Security Module (HSM). The WSCD stores private keys and performs cryptographic operations in a protected environment that cannot be accessed by other software on the device.
2. **The Wallet Secure Cryptographic Application (WSCA)** is the software layer that implements the wallet's security policies and manages interactions with the WSCD. The WSCA enforces rules about when credentials can be presented, what user verification is required, and how transactions are logged.

Together, the WSCD and WSCA form a cryptographic safe. Their integrity guarantees — issuing, presenting, and verifying credentials without possibility of forgery or unauthorised duplication — are entirely dependent on the strength of the underlying cryptographic algorithms.

4.2 *The Cryptographic Stack at Risk*

The EUDI Wallet ARF specifies the use of standard cryptographic algorithms for credential issuance and presentation. The current specifications rely heavily on:

- ECDSA (Elliptic Curve Digital Signature Algorithm) for credential signatures and wallet attestations.
- X.509 certificates with RSA or EC keys for establishing trust chains between issuers, wallets, and relying parties.
- AES-GCM for symmetric encryption of stored credentials.
- SHA-256 and SHA-384 for hash functions in credential integrity verification.

Of these, ECDSA and RSA-based X.509 certificates are directly vulnerable to Shor's algorithm. AES-GCM remains secure against quantum attack if key sizes are doubled (AES-256 is the appropriate choice). SHA-256 provides reduced but still adequate security against Grover's algorithm for most purposes.

The practical implication is that the entire credential issuance and verification chain — from issuer signature through wallet attestation to relying party verification — requires migration to post-quantum algorithms before the CRQC threshold is reached.

4.3 *The Certification Complexity Challenge*

One of the most underappreciated barriers to quantum migration in the EUDI Wallet ecosystem is the complexity of the certification regime. Achieving Level of Assurance High (LoA High) — the minimum baseline for EUDI Wallet compliance — requires certification of the entire wallet system, not merely its individual components.

As TQS analysis has documented, this creates a unique dilemma. Each component of the wallet system comes from different actors with distinct life cycles: handset manufacturers, chip vendors, telecom operators, operating system providers, and cloud service providers. ENISA is expected to introduce EU-wide certification for WSCD and WSCA components only after 2026. Until then, member states must rely on national certification regimes that may have different standards and timelines.

Introducing post-quantum algorithms into this certification landscape is not simply a matter of updating code. It requires re-certification of WSCD components — a process that may take years and that depends on the availability of certified post-quantum implementations from hardware vendors. This is one of the most concrete reasons why PQC migration planning must begin now, rather than waiting for regulatory mandates.

4.4 *Secure Elements vs HSMs: Different Quantum Migration Paths*

The choice between secure element-based and HSM-based WSCD implementations has direct implications for quantum migration strategy. As TQS has analysed, each approach presents different constraints.

Secure elements — embedded chips in smartphones — offer sovereign offline control and are already present in hundreds of millions of devices. However, their cryptographic capabilities are determined by the chip vendor and cannot typically be upgraded via software alone. Migrating a secure element to post-quantum algorithms requires either new hardware (a new chip) or a new device. For a deployment at the scale of the EUDI Wallet, this could mean hardware replacement cycles affecting hundreds of millions of devices across Europe.

Cloud-based HSMs offer greater flexibility. Post-quantum algorithm libraries can be updated in software, and HSM vendors have generally been faster to implement NIST-approved PQC algorithms. However, HSMs introduce cloud dependency, cannot function offline, and create potential concentration risk if large numbers of wallets rely on a small number of HSM providers.

Hybrid architectures that combine both approaches — using secure elements for offline credential storage and HSMs for online signing operations — are emerging as a pragmatic solution. But hybrid architectures also double the migration complexity, requiring post-quantum support in both layers simultaneously.

4.5 *Quantum Threat to Selective Disclosure*

One of the most privacy-preserving features of the EUDI Wallet is selective disclosure — the ability to present a single attribute from a credential (for example, proving you are over 18 without revealing your date of birth) without exposing the rest of the credential. This capability relies on cryptographic constructions, including SD-JWT and mdoc/ISO 18013-5 formats, that use ECDSA signatures and Merkle tree constructions.

Post-quantum variants of these selective disclosure mechanisms exist — including lattice-based signature schemes that support similar functionality — but they are not yet standardised for use in the EUDI Wallet ecosystem. This represents a gap that needs to be addressed in parallel with the migration of the core signing algorithms. An EUDI Wallet that has migrated its credential signatures to ML-DSA but still relies on classical ECDSA for selective disclosure proofs is not quantum-safe.

Chapter 5: *Post-Quantum Cryptography — What the Standards Actually Require*

The question is no longer whether post-quantum cryptography will be required, but how it will be implemented in systems that are already being deployed. With NIST standards finalised and European guidance evolving, organisations must now translate theory into architecture. This chapter cuts through the abstraction to examine what the standards actually demand, where they create friction, and how they reshape the design of identity infrastructure.

5.1 *The NIST PQC Standardisation Programme*

The most authoritative source of post-quantum cryptography standards for the global technology industry is the US National Institute of Standards and Technology (NIST). After a multi-year evaluation process that began in 2016, NIST published its first three post-quantum cryptography standards in August 2024:

- FIPS 203 — ML-KEM (Module-Lattice-Based Key Encapsulation Mechanism). This is the primary standard for post-quantum key exchange — replacing the Diffie-Hellman and EC Diffie-Hellman protocols used to establish shared secrets in TLS and other protocols.
- FIPS 204 — ML-DSA (Module-Lattice-Based Digital Signature Algorithm). This is the primary standard for post-quantum digital signatures — replacing ECDSA and RSA signatures in certificate chains, credential signatures, and other trust-bearing operations.
- FIPS 205 — SLH-DSA (Stateless Hash-Based Digital Signature Algorithm). This is a conservative backup signature algorithm based on hash functions rather than lattice mathematics, providing a defence-in-depth option in case vulnerabilities are discovered in lattice-based schemes.

A fourth standard, FN-DSA (based on FALCON), is expected to be published as FIPS 206 and provides more compact signatures suitable for constrained environments such as secure elements.

5.2 *The European Dimension: ETSI and ENISA*

For European organisations operating under eIDAS 2.0, NIST standards are a necessary reference but not a sufficient one. European digital identity infrastructure must also comply with standards developed by ETSI and with guidance published by ENISA. ETSI's post-quantum cryptography work programme has produced technical reports on PQC algorithm selection (ETSI TR 103 616) and on the migration of existing cryptographic protocols to post-quantum alternatives. ETSI is also actively working on standards for hybrid certificates — X.509 certificate extensions that combine classical and post-quantum public keys in a single certificate, enabling a transition period during which both classical and post-quantum verifiers can validate the same credential.

ENISA has published guidance on the quantum threat landscape and on cryptographic agility as a migration strategy. ENISA's framework for post-quantum migration emphasises the importance of cryptographic inventory — systematically cataloguing all uses of classical cryptography within an organisation — as the first step in any migration programme. Without a comprehensive inventory, organisations cannot know where migration is needed or how to prioritise the work.

5.3 Hybrid Cryptography as a Transition Strategy

One of the most practically important developments in post-quantum standards is the emergence of hybrid cryptography as an official transition strategy. Hybrid cryptography combines a classical algorithm (such as ECDSA or X25519) with a post-quantum algorithm (such as ML-DSA or ML-KEM) in a way that provides security as long as at least one of the two algorithms remains unbroken.

The rationale for hybrid approaches is twofold. First, they provide backwards compatibility. A hybrid certificate can be verified by a classical verifier that ignores the post-quantum components, and by a post-quantum verifier that validates both. This allows migration to proceed gradually, without a hard cutover that would break interoperability with non-migrated systems.

Second, hybrid approaches provide defence in depth against potential vulnerabilities in the new post-quantum algorithms. Post-quantum algorithms are relatively young. Despite extensive academic scrutiny, it is possible that vulnerabilities will be discovered in lattice-based or other PQC constructions after widespread deployment. A hybrid approach ensures that such a discovery does not immediately compromise systems that have already migrated.

As TQS research has argued, for digital identity systems, composite cryptographic approaches offer a pragmatic transition path that preserves compatibility while introducing quantum resilience — not as a permanent state, but as a migration bridge.

5.4 Performance and Constraint Considerations

A common concern about post-quantum algorithms — particularly lattice-based schemes — is their performance characteristics compared to classical algorithms. The concern is legitimate and needs to be addressed honestly.

ML-DSA signatures are significantly larger than ECDSA signatures. An ML-DSA-65 signature (the mid-security-level variant) is approximately 3.3 kilobytes, compared to 64 bytes for an ECDSA P-256 signature. ML-KEM key encapsulation involves larger public keys and ciphertexts than ECDH. These size increases have implications for protocols, storage requirements, and bandwidth, particularly in constrained environments. For the EUDI Wallet, the most critical constraint is the WSCD hardware. Secure elements have limited computational capacity and storage. Not all current secure elements support the cryptographic operations required by ML-DSA or ML-KEM. This is one of the primary reasons why hardware migration planning is essential — and why it needs to be incorporated into procurement and device lifecycle decisions now.

Algorithm	Type	Key/Signature Size	Security Level	Quantum Safe?
RSA-2048	Signature / Key Exchange	256 bytes (key), ~256 bytes (sig)	Classical ~112 bit	No
ECDSA P-256	Signature	64 bytes (sig), 64 bytes (pub key)	Classical ~128 bit	No
X25519	Key Exchange	32 bytes	Classical ~128 bit	No
ML-DSA-65 (FIPS 204)	Signature	~3,293 bytes (sig)	~128 bit quantum	Yes
ML-KEM-768 (FIPS 203)	Key Encapsulation	~1,184 bytes (pub key)	~128 bit quantum	Yes
SLH-DSA-128s (FIPS 205)	Signature	~7,856 bytes (sig)	~128 bit quantum	Yes (conservative)

5.5 Cryptographic Agility as a Design Principle

The most important architectural lesson from the PQC standardisation process is the value of cryptographic agility. A cryptographically agile system is one designed so that cryptographic algorithms can be replaced without requiring a complete system redesign.

Many legacy systems — including legacy PKI infrastructure — are not cryptographically agile. The algorithm is baked into the hardware, the certificate format, or the protocol in ways that make substitution extremely difficult. This is why the SHA-1 to SHA-2 migration took so long in some domains, even though the technical solution was well understood.

A critical but often underestimated dimension of cryptographic agility is certificate lifecycle management. Post-quantum migration is not limited to replacing algorithms. It requires full visibility and control over how certificates are issued, distributed, validated, rotated, and revoked across complex trust chains.

In identity infrastructure, where certificates underpin credential issuance, wallet attestation, and cross-border verification, poor lifecycle management can delay migration even when post-quantum algorithms are available. Organisations must therefore treat certificate inventory, trust anchor mapping, verifier compatibility, and reissuance strategy as first-order concerns in any quantum-readiness programme.

For the EUDI Wallet and associated identity infrastructure, cryptographic agility should be a design requirement, not an afterthought. Systems should be designed with clearly abstracted cryptographic layers, algorithm negotiation capabilities, and documented procedures for algorithm replacement. This will not eliminate the complexity of future migrations — but it will make them manageable within acceptable timescales.

Chapter 6: *The Regulatory Landscape*

Post-quantum migration is not being driven by standards alone. It is being shaped by a regulatory architecture that increasingly defines how digital systems must be secured, operated, and held accountable. eIDAS 2.0, the Cyber Resilience Act, NIS2, DORA, and the AI Act do not address quantum risk in isolation, but together they establish a trajectory that organisations cannot ignore. This chapter examines how these frameworks intersect — and how they collectively turn quantum-readiness from a technical choice into a compliance reality.

6.1 *The EU's Regulatory Architecture for Digital Trust*

One of the defining features of Europe's approach to digital technology is the comprehensiveness of its regulatory architecture. Rather than addressing individual technologies or sectors in isolation, the EU has constructed an interlocking framework of regulations that collectively govern the entire digital economy. For organisations working in digital identity and post-quantum security, understanding how these regulations interact is as important as understanding the technical standards.

The TQS Trust Stack framework maps the major EU regulations onto five layers of digital trust governance. This section examines each regulation's relationship to quantum-readiness and identifies where regulatory obligations create both constraints and opportunities for PQC migration.

6.2 *eIDAS 2.0 — The Identity Foundation*

eIDAS 2.0 (Regulation EU 2024/1183) is the primary regulatory instrument for digital identity in Europe. It establishes the legal framework for the EUDI Wallet, defines the levels of assurance for digital identity systems, and creates the trust service framework that governs qualified electronic signatures, seals, and timestamps.

From a quantum-readiness perspective, eIDAS 2.0 presents both a mandate and a gap. The regulation mandates Level of Assurance High for EUDI Wallets, which implies cryptographic security sufficient to resist state-level adversaries. A CRQC is precisely such an adversary. Yet the implementing acts and technical specifications currently define security requirements in terms of current cryptographic standards, not post-quantum alternatives.

The implementing acts that govern EUDI Wallet specifications are, however, living documents. The Architecture and Reference Framework is updated regularly, and the Commission has signalled that post-quantum requirements will be incorporated as the relevant standards mature. For identity providers and wallet implementers, this means that PQC migration is not just a security best practice — it is a compliance trajectory.

6.3 *The Cyber Resilience Act — Security by Design*

The Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for all connected hardware and software products sold in the EU market. Products must be secure by design, vulnerabilities must be managed throughout the product lifecycle, and security updates must be made available for a defined period.

The CRA's implications for quantum readiness are significant. Hardware products that embed cryptographic capabilities — including secure elements, HSMs, and IoT devices — must be designed with security measures adequate to withstand current and anticipated threats. A secure element designed and sold in 2026 may remain in use until 2036 or beyond. The CRA's lifecycle security requirement creates a strong argument for including post-quantum algorithm support in new hardware designs, even where post-quantum requirements are not yet mandated by separate regulations.

The CRA's vulnerability management obligations also apply to cryptographic weaknesses. When post-quantum algorithms become mandatory — as is increasingly likely given the trajectory of NIST and ETSI standardisation — manufacturers who have not designed their products for cryptographic agility may find themselves in violation of CRA obligations.

6.4 *NIS2 — Cybersecurity Governance and Quantum Risk*

The NIS2 Directive (Directive EU 2022/2555) establishes cybersecurity obligations for a wide range of critical and important entities, including digital identity providers, trust service providers, financial infrastructure, and healthcare systems. Its most significant innovation is elevating cybersecurity to a board-level responsibility with direct legal consequences for senior management.

NIS2's risk management obligations require covered entities to implement measures appropriate to the risks they face. As quantum computing capabilities develop and as regulatory expectations evolve, the argument that post-quantum readiness is not required by current risk management standards will become increasingly difficult to sustain. ENISA, which plays a significant role in defining the technical reference for NIS2 implementation, has published guidance on quantum threats that is beginning to shape regulatory expectations.

6.5 *DORA — Financial Sector Resilience and Quantum*

The Digital Operational Resilience Act (DORA) applies to financial entities and their ICT service providers, imposing ICT risk management, incident reporting, resilience testing, and third-party risk management obligations. Financial infrastructure is among the most quantum-sensitive sectors: SWIFT transactions, interbank payments, and digital asset custody all rely on PKI that is vulnerable to Shor's algorithm.

DORA's resilience testing requirements — including threat-led penetration testing (TLPT) for significant financial institutions — will increasingly need to incorporate quantum threat scenarios. The harvest-now-decrypt-later threat is particularly acute in the financial sector,

where long-term confidentiality obligations and extended data retention requirements create extended windows of vulnerability. Financial institutions preparing DORA-compliant risk management frameworks should explicitly assess their quantum exposure and their timeline for PQC migration.

6.6 The AI Act — Intersection with Identity Integrity

The EU AI Act establishes a risk-based regulatory framework for artificial intelligence systems. High-risk AI systems — including those used in biometric identification and digital identity verification — face stringent requirements for accuracy, transparency, human oversight, and technical robustness.

The intersection of the AI Act and post-quantum security is subtle but increasingly important. AI systems used in identity verification rely on cryptographic infrastructure for their own integrity: model weights, training data, and audit logs are protected by digital signatures and encrypted storage. In a post-quantum world, the integrity of AI systems depends on the quantum-safety of the cryptography that protects them. The AI Act's robustness requirements should therefore be interpreted to include resilience against quantum-capable adversaries.

Regulation	Primary Quantum Relevance	Key Obligation	Migration Timeline Pressure
eIDAS 2.0	Identity credential cryptography	LoA High for EUDI Wallet; PQC in implementing acts trajectory	High — wallet deployment now
Cyber Resilience Act	Hardware PQC capability	Security by design; lifecycle vulnerability management	High — new hardware designs now
NIS2	Critical infrastructure resilience	Risk management proportionate to threats	Medium — ENISA guidance evolving
DORA	Financial data confidentiality	ICT risk management; resilience testing	High — HNDL risk immediate
AI Act	AI system integrity	Technical robustness for high-risk AI	Medium — interpretation evolving
GDPR	Personal data protection	Appropriate technical measures	Medium — enforcement guidance pending

Chapter 7: *National Readiness — How Europe's Member States Are Preparing*

Europe's post-quantum transition is not happening at a single speed. While the regulatory framework is shared, readiness is fragmented — shaped by national capabilities, legacy infrastructure, and differing approaches to identity architecture. This uneven landscape creates a structural risk: a cross-border system that is only as secure as its weakest implementation. This chapter examines where Europe stands today, and why coordination matters as much as capability.

7.1 The Uneven Landscape of European PQC Readiness

The European Commission's Coordinated Implementation Roadmap sets common targets for PQC migration across all member states. But the starting points from which each country is approaching that roadmap vary enormously. Understanding this variation is essential for any organisation that operates across borders — because cross-border digital identity trust chains are only as quantum-safe as their least-prepared participant.

7.2 The Leading Group: High Technical Maturity

Germany

Germany's Federal Office for Information Security (BSI) is among the most technically advanced national cybersecurity agencies in Europe on quantum security. The BSI has published detailed guidance on post-quantum migration, maintains a list of recommended quantum-safe algorithms, and has updated its Technical Guidelines for cryptographic key recommendations (TR-02102) to include PQC algorithms. Germany's digital identity programme (the national eID system) is being developed with explicit requirements for cryptographic agility.

France

The French National Agency for Information Systems Security (ANSSI) has published a comprehensive quantum security roadmap and participated actively in ETSI's PQC standardisation work. France is one of the few European countries to have explicitly mandated the use of hybrid classical/PQC algorithms in certain government systems; an approach that provides immediate quantum protection while maintaining backwards compatibility.

The Netherlands

The Netherlands' National Cyber Security Centre (NCSC-NL) published a detailed post-quantum cryptography migration guide in 2023, covering inventory methodology, algorithm selection, and implementation planning. The Netherlands is also notable for its active participation in quantum network research, including the EuroQCI quantum communication infrastructure initiative.

7.3 The Middle Group: Active Preparation

Estonia

Estonia's mature digital identity infrastructure — the X-Road data exchange layer and the national eID card system — provides a strong foundation for quantum migration. Estonia is actively engaged in European quantum security initiatives and has technical capacity to migrate its core identity systems to post-quantum algorithms. However, the full quantum-readiness of all components of the Estonian digital identity ecosystem has not yet been publicly assessed.

Austria and Scandinavia

Austria's A-Trust and the Nordic countries' BankID systems represent well-governed identity infrastructure with active engagement on quantum security. Nordic countries benefit from strong institutional relationships between government, research, and industry that are conducive to rapid coordinated migration. However, as with Estonia, comprehensive public quantum readiness assessments are not yet available for all components.

7.4 Areas Requiring Accelerated Progress

Several European member states face significant challenges in meeting the 2030 high-risk migration deadline. These challenges are not primarily technical — they reflect resource constraints, institutional fragmentation, and the complexity of legacy systems that were not designed for cryptographic agility.

Key areas of concern include:

- Countries whose national digital identity infrastructure relies on older smart card technology with embedded classical algorithms that cannot be upgraded without hardware replacement.
- Countries where digital identity services are provided by multiple competing private providers with different technical architectures and no coordinated migration governance.
- Countries where the policy and regulatory framework for quantum migration has not yet been developed at the national level, leaving individual organisations without authoritative guidance.

The European Commission, ENISA, and the European Cybersecurity Competence Centre (ECCC) are all providing support for member states in this group. But the scale of the challenge — and the 2030 deadline for high-risk systems — means that significantly accelerated progress is needed in the next two to three years.

7.5 The Cross-Border Trust Chain Risk

The diversity of national quantum readiness creates a specific risk for the EUDI Wallet ecosystem: the cross-border trust chain risk. When a citizen from Country A uses their EUDI Wallet to access a service in Country B, the verification process relies on a trust chain that extends from the citizen's wallet through the national trust anchor of Country A, through the European trust registry, to the service provider in Country B.

If Country A has migrated its national trust anchor to post-quantum algorithms but Country B's verification infrastructure has not been updated to validate post-quantum signatures, the cross-border verification will fail. Conversely, if Country A's wallet still uses classical ECDSA signatures and a CRQC becomes available, the entire cross-border trust chain is compromised regardless of Country B's migration status.

Managing this cross-border dependency requires coordinated migration governance at the European level — not just national plans. The European Commission and ENISA will need to establish clear interoperability requirements, minimum quantum-readiness baselines, and a coordinated migration timeline that prevents the weakest national implementation from becoming the vulnerability that compromises the entire ecosystem.

Chapter 8: *Migration Pathways — A Practical Roadmap*

The post-quantum transition will not happen all at once. It will be staged, uneven, and constrained by the realities of existing systems, certification cycles, and operational risk. For organisations responsible for identity infrastructure, the question is not whether to migrate, but how to do so without breaking what already works. This chapter sets out a practical migration framework, translating strategy into a sequence of decisions and actions.

8.1 *The Migration Framework*

Post-quantum migration for digital identity infrastructure is not a single project. It is a programme of interlocking changes that must be planned and sequenced carefully to maintain operational continuity while progressively eliminating quantum vulnerabilities. This chapter provides a practical framework for organisations approaching this challenge.

The migration framework presented here is structured around four phases: Discover, Plan, Transition, and Operate. These phases are sequential at the programme level but may run in parallel for different components of a complex identity ecosystem.

8.2 *Phase 1: Discover — Cryptographic Inventory*

The single most important first step in any PQC migration programme is a comprehensive cryptographic inventory. An organisation cannot migrate what it does not know it has.

A cryptographic inventory should document:

- All cryptographic algorithms in use — including their specific implementations, key sizes, and operational contexts.
- All certificates — their issuing authority, expiry dates, key algorithms, and the systems that depend on them.
- All trust anchors — root certificates, intermediate CA certificates, and their distribution across systems.
- All hardware cryptographic components — secure elements, HSMs, smart cards, and TPMs — and their algorithm support capabilities.
- All data with long-lived confidentiality requirements — data that must remain confidential beyond the anticipated CRQC horizon.
- All signatures with long-lived validity requirements — signatures that must remain verifiable beyond the anticipated CRQC horizon.

Automated cryptographic discovery tools are available from several vendors and can significantly accelerate the inventory process for large organisations. However, automated tools typically cannot discover all uses of cryptography — particularly custom implementations, embedded system cryptography, and cryptography in legacy applications. Manual review of high-risk systems should complement automated discovery.

8.3 Phase 2: Plan — Risk Prioritisation and Architecture

Based on the cryptographic inventory, organisations should classify their cryptographic assets by quantum risk level. The classification should consider two dimensions: the sensitivity of the data or operation protected by the cryptographic asset, and the time horizon over which protection is required.

High-priority assets for quantum migration are those where both dimensions are high — sensitive, long-lived data or operations. For a digital identity organisation, these typically include: qualified electronic signatures and their underlying signing keys; long-lived credential certificates and trust anchor certificates; historical credential presentation logs if these are stored in a form that could reveal sensitive personal data; and authentication tokens with long validity periods.

The planning phase should also resolve key architectural decisions:

- Hybrid vs. full migration: For most organisations, a hybrid approach — deploying classical and post-quantum algorithms in parallel — is the appropriate near-term strategy. This preserves interoperability with non-migrated systems while introducing quantum protection for new operations.
- Algorithm selection: For European digital identity systems, ML-DSA (FIPS 204) for signatures and ML-KEM (FIPS 768) for key exchange are the primary algorithm choices. SLH-DSA provides a conservative backup option for the most sensitive signing operations.
- Hardware assessment: Determine which hardware components can support post-quantum algorithms in software and which require hardware replacement or upgrade. Incorporate PQC hardware requirements into procurement planning for all new hardware purchases.

8.4 Phase 3: Transition — Staged Migration

The transition phase implements the migration plan in a staged sequence that minimises operational risk. The recommended staging order for digital identity infrastructure is:

Stage	Components	Timeline	Key Actions
1 — Root CAs	Root certificate authorities	2025–2026	Issue new root certs with ML-DSA and hybrid classical/PQC signatures
2 — Intermediate CAs	Intermediate & issuing CAs	2026–2027	Migrate issuing CAs; issue hybrid subordinate certificates
3 — Credential Issuance	Issuer signing keys & credential formats	2027–2028	Implement ML-DSA signing for new credential issuance; update SD-JWT and mdoc formats
4 — Wallet Attestation	WSCA/WSCD attestation	2027–2029	Update WSCA to support PQC wallet attestation; procure PQC-capable WSCD hardware
5 — Verifier Infrastructure	Relying party verification	2028–2030	Update verifier systems to validate ML-DSA signatures; retire classical-only verification paths
6 — Legacy Transition	Existing credential base	2029–2032	Managed re-issuance of existing credentials with PQC signatures; sunset classical credential types

8.5 Phase 4: Operate — Quantum-Safe Operations

The final phase is not a destination but an operational posture. Post-migration, organisations must maintain quantum-safe operations through continuous monitoring, proactive algorithm management, and preparation for further cryptographic transitions that will inevitably occur as the field evolves.

Key operational practices for quantum-safe identity systems include:

- Continuous cryptographic monitoring: Automated monitoring of all cryptographic assets to detect the use of deprecated algorithms, expired certificates, and configuration drift.
- Algorithm agility testing: Regular exercises to verify that cryptographic algorithms can be replaced within defined timeframes without disrupting services.
- Quantum threat intelligence: Monitoring of advances in quantum computing capabilities and of any vulnerabilities discovered in post-quantum algorithms, with defined processes for rapid response.
- Regulatory compliance tracking: Active monitoring of updates to eIDAS implementing acts, ETSI standards, and ENISA guidance that may require further cryptographic changes.

Chapter 9: *The Geopolitical Dimension*

The post-quantum transition is not happening in a neutral environment. It is unfolding within a landscape defined by geopolitical competition, supply chain dependency, and uneven access to advanced technologies. For Europe, the question is not only how to secure identity infrastructure, but who ultimately controls the systems and components on which that security depends. This chapter examines the geopolitical dimension of quantum readiness, and why sovereignty in cryptography is inseparable from sovereignty in infrastructure.

9.1 *Identity Infrastructure as Strategic Asset*

Digital identity infrastructure is not merely a technical system. It is a geopolitical asset. A nation that controls its own identity infrastructure — that can issue, verify, revoke, and audit identity credentials without dependence on foreign hardware, algorithms, or cloud services — possesses a dimension of sovereignty that is increasingly recognised as strategically vital.

As TQS research in Sovereign by Design has documented, Europe's digital sovereignty is at risk not merely from external data harvesting, but from the structural dependencies embedded in its technology supply chain. If the underlying hardware, standards, and cryptographic infrastructure remain externally sourced, sovereignty risks becoming an administrative fiction — a policy aspiration ungrounded in technical reality.

9.2 *The Cryptographic Sovereignty Gap*

Europe currently faces a cryptographic sovereignty gap. The post-quantum algorithms standardised by NIST — ML-KEM, ML-DSA, SLH-DSA — were developed primarily by US and European academic researchers and are patent-free, which is significant. But the hardware that implements these algorithms at scale — the secure processors, HSMs, and smart card chips that will anchor the EUDI Wallet ecosystem — is manufactured overwhelmingly by non-European companies.

The EU Chips Act addresses this dependency at the level of semiconductor manufacturing, with targets for European production capacity. But semiconductor manufacturing capability alone does not guarantee cryptographic sovereignty. European-manufactured chips that implement algorithms designed in the United States and whose supply chains depend on East Asian component sourcing are not sovereign in any meaningful sense.

True cryptographic sovereignty requires a deeper alignment: European algorithm expertise, European hardware manufacturing, European certification authority, and European cloud infrastructure — all operating under European legal jurisdiction. The post-quantum transition creates both a challenge and an opportunity in this regard. The transition is a forcing function: it requires hardware and software replacement at continental scale. If that replacement cycle is managed with sovereignty as an explicit design criterion, it can close the gap. If it is managed purely on commercial terms, the gap may widen.

9.3 The Geopolitics of Quantum Computing Access

The development of cryptographically relevant quantum computers is not happening in a geopolitically neutral environment. The leading quantum computing programmes are concentrated in a small number of countries — primarily the United States, China, and to a lesser extent Canada, the UK, and Japan. European quantum computing research is significant but has not yet produced the scale of investment or the deployment of operational quantum systems that these leading programmes represent.

This asymmetry matters for digital identity in two ways. First, the state with the first operational CRQC gains the ability to retrospectively decrypt any previously harvested data encrypted with classical algorithms — including identity credentials, qualified signatures, and authentication records. Second, states with advanced quantum computing capabilities will have significant advantages in quantum-safe cryptography research, potentially discovering vulnerabilities in post-quantum algorithms before they are publicly disclosed.

Europe's response to this asymmetry should be strategic, not reactive. It requires investment in European quantum computing research, active participation in international PQC algorithm evaluation programmes, and the maintenance of European cryptographic expertise that is not dependent on the goodwill of non-European allies.

9.4 The EUDI Wallet as Geopolitical Instrument

The EUDI Wallet is simultaneously a citizen service, a technical standard, and a geopolitical instrument. By establishing a European digital identity standard that is legally recognised across 27 member states and increasingly across partner countries, the EU is asserting its right to define the terms of digital participation in its market — and by extension, the cryptographic standards that underpin that participation.

This geopolitical dimension strengthens the case for quantum-safe design in the EUDI Wallet. A wallet whose cryptographic foundations can be compromised by a state-level quantum adversary is not just a security failure. It is a demonstration that European digital sovereignty can be overridden by a technologically superior adversary — precisely the outcome that the European digital sovereignty agenda is designed to prevent.

Conversely, a EUDI Wallet that has been migrated to quantum-safe cryptography before a CRQC becomes available demonstrates that Europe can manage critical infrastructure transitions proactively, on its own terms, and in advance of external threat. That demonstration matters for the credibility of the broader European digital sovereignty project.

9.5 International Standards and Alignment

Europe cannot — and should not — pursue cryptographic sovereignty in isolation. The global digital economy requires interoperability, and interoperability requires shared standards. European participation in NIST, ETSI, ISO, and IETF standardisation processes is therefore a dimension of sovereignty strategy, not an alternative to it.

The EUDI Wallet's cross-border functionality — the ability of European citizens to use their wallets in third countries and of foreign nationals to interact with European services — depends on standards alignment that extends beyond Europe's borders. A PQC-migrated EUDI Wallet that cannot interoperate with equivalent systems in the United States, United Kingdom, or Japan is a sovereignty success but an interoperability failure.

Managing this tension — between the need for European cryptographic autonomy and the need for global interoperability — is one of the most important strategic challenges of the post-quantum transition. It argues for active European leadership in international standardisation, not withdrawal from it.

Conclusion & Recommendations: *The Strategic Imperative*

The central tension is no longer theoretical. Europe is deploying identity infrastructure designed to operate at continental scale, with operational lifetimes measured in decades. The cryptographic foundations currently underpinning that infrastructure were never designed to persist across that same horizon.

This is not a future risk emerging on the edge of planning cycles. It is a structural condition already embedded in systems being deployed today. Credentials issued now will need to be verified in environments that do not yet exist, against adversaries whose capabilities are still developing. The integrity of those future verifications depends entirely on decisions being made in the present.

The post-quantum transition therefore sits outside the normal cadence of technology upgrade cycles. It cannot be deferred to a later phase of optimisation or treated as an incremental enhancement. Once identity infrastructure reaches industrial scale, the cost and complexity of altering its cryptographic foundations increase non-linearly. At that point, migration becomes constrained not by technical feasibility, but by operational disruption, certification cycles, and cross-border dependency.

The implication is straightforward. Quantum resilience is not a feature to be introduced once systems are stable. It is a condition that must be established while they are still being formed.

What distinguishes the current moment is not uncertainty, but alignment. Post-quantum standards have been defined. Regulatory direction across eIDAS 2.0, the Cyber Resilience Act, NIS2, and DORA is converging. The engineering pathways for migration are understood, even where implementation remains complex. The remaining variable is execution.

This is where the trust stack becomes operational rather than conceptual. Decisions taken at the cryptographic layer propagate upward into identity issuance, system verification, regulatory compliance, and ultimately legal accountability. Trust is no longer established at the point of deployment and assumed to persist. It is expected to remain demonstrable over time, including under retrospective scrutiny.

That shift carries consequences beyond security. As digital identity becomes embedded in legal processes, financial systems, and cross-border services, the ability to validate past transactions acquires evidentiary weight. Systems that cannot sustain that validation over time do not simply degrade—they become contested. In that environment, cryptographic failure does not remain a technical issue. It becomes a question of liability.

The post-quantum transition should therefore be understood as a structural adjustment to how trust is engineered, verified, and enforced. It introduces a requirement that systems remain defensible not only in operation, but in retrospect. For identity infrastructure, this places time—not just security—at the centre of system design.

The window to act remains open, but it is not indefinite. The timelines associated with quantum capability development, regulatory enforcement, and infrastructure deployment

are beginning to converge. Delay does not pause that convergence; it compresses the response window.

The decision facing European organisations is not whether to engage with post-quantum migration. It is whether to do so under controlled conditions, or under pressure.

Recommendations for Identity Programme Managers

Post-quantum migration begins with visibility. A comprehensive cryptographic inventory is not preparatory work; it is the foundation on which every subsequent decision depends. Without a clear view of where cryptography is embedded, how it is used, and how long it must remain valid, migration cannot be prioritised or sequenced with any confidence. Organisations that delay this step will not delay the problem—they will lose control over it.

Procurement decisions taken now will define the constraints of the next decade. Secure elements, HSMS, and identity hardware deployed in the current cycle will remain in operation well into the anticipated quantum threat window. If those components cannot support post-quantum algorithms or be upgraded without replacement, they will introduce structural barriers to migration. Post-quantum capability should therefore be treated as a baseline requirement in all hardware procurement, not a future consideration.

The transition phase should be approached with controlled continuity rather than abrupt replacement. Composite cryptographic models—deploying classical and post-quantum algorithms in parallel—provide a viable path to introduce quantum resilience without disrupting existing verification ecosystems. This is not an end state, but it is a necessary bridge that allows migration to proceed without fragmenting interoperability.

The longest lead-time constraint sits outside software. Certification of wallet components, particularly WSCD hardware, will define the pace at which migration can occur. Engagement with national certification bodies and hardware vendors cannot be deferred until standards are fully mandated. By that point, timelines will already be constrained. Early alignment on certification pathways is the difference between planned migration and enforced delay.

Recommendations for Regulators and Policymakers

Regulatory direction has reached the point where ambiguity becomes a risk in itself. The absence of explicit post-quantum requirements within EUDI Wallet implementing acts does not create flexibility; it creates inconsistency. Incorporating clear migration timelines and minimum algorithm requirements will not accelerate the transition artificially, but it will prevent fragmentation across national implementations.

The cross-border nature of the EUDI Wallet introduces a dependency that cannot be managed at national level alone. Trust chains that extend across member states are only as resilient as their least prepared participant. Establishing minimum post-quantum readiness baselines for cross-border recognition is therefore not a technical refinement—it is a prerequisite for maintaining the integrity of the system as a whole.

The Cyber Resilience Act provides a mechanism to influence the future state of deployed infrastructure, but only if its provisions are interpreted with sufficient forward scope. Cryptographic agility and post-quantum capability should be treated as core security requirements for any product with embedded cryptographic functionality. Without this, hardware entering the market today will become the limiting factor in tomorrow's migration.

The post-quantum transition also exposes a broader structural issue. Cryptographic sovereignty cannot be achieved through standards alone if the hardware, certification capacity, and supply chains remain externally dependent. Coordinated investment across these domains is not an adjunct to the transition; it is part of its execution.

Recommendations for Technology Leaders and CISOs

Under NIS2, quantum risk is not a theoretical concern to be monitored at the margins of security strategy. It sits within the category of foreseeable risk, and therefore within the scope of board-level accountability. Organisations that fail to incorporate post-quantum exposure into their risk frameworks are not deferring action—they are accepting unmanaged liability.

The harvest-now-decrypt-later threat introduces a time asymmetry that traditional risk models do not fully capture. Data and credentials considered secure today may be compromised retrospectively, with consequences that only become visible years later. Identifying which assets carry long-term sensitivity, and prioritising their protection accordingly, is now a core component of risk management.

Resilience testing frameworks must evolve to reflect this shift. For organisations operating under DORA or equivalent regimes, quantum threat scenarios should be incorporated into testing programmes, not as speculative exercises but as boundary conditions for system design. The question is no longer whether systems can withstand current attack models, but whether they remain defensible under future ones.

Finally, quantum readiness cannot be contained within organisational boundaries. Supply chains, cloud providers, and trust service partners form part of the same cryptographic ecosystem. If those dependencies are not aligned with post-quantum migration timelines, they become points of failure that sit outside direct control. Engagement with suppliers on their migration posture is therefore not due diligence—it is risk containment.

Appendix A: *Glossary of Key Terms*

Term	Definition
Cryptographically Relevant Quantum Computer (CRQC)	A quantum computer with sufficient qubits, error correction, and computational capacity to run Shor's algorithm at a scale that breaks current public-key cryptographic systems.
Harvest Now, Decrypt Later (HNDL)	A threat strategy in which adversaries intercept and archive encrypted data today with the intention of decrypting it once quantum computing capabilities become available.
ML-DSA (FIPS 204)	Module-Lattice-Based Digital Signature Algorithm. The primary NIST post-quantum standard for digital signatures, replacing ECDSA and RSA for signature operations.
ML-KEM (FIPS 203)	Module-Lattice-Based Key Encapsulation Mechanism. The primary NIST post-quantum standard for key exchange, replacing Diffie-Hellman and ECDH protocols.
SLH-DSA (FIPS 205)	Stateless Hash-Based Digital Signature Algorithm. A conservative backup PQC signature standard based on hash functions rather than lattices.
Hybrid Cryptography	A cryptographic approach that combines a classical algorithm with a post-quantum algorithm, providing security as long as at least one remains unbroken. Used as a migration strategy.
WSCD	Wallet Secure Cryptographic Device. The tamper-resistant hardware component of the EUDI Wallet that stores private keys and performs cryptographic operations.
WSCA	Wallet Secure Cryptographic Application. The software layer of the EUDI Wallet that implements security policies and manages interactions with the WSCD.
Cryptographic Agility	The property of a system that allows cryptographic algorithms to be replaced without requiring a complete system redesign.
eIDAS 2.0	The revised EU regulation on electronic identification and trust services (EU 2024/1183), which establishes the legal framework for the European Digital Identity Wallet.
EUDI Wallet	European Digital Identity Wallet. A digital application allowing EU citizens to store and present verified identity credentials for use in public and private sector services.
Level of Assurance High (LoA High)	The highest level of assurance defined in eIDAS, required for EUDI Wallet compliance, implying strong identity proofing and highly secure credential management.
Post-Quantum Cryptography (PQC)	Cryptographic algorithms believed to be secure against attacks by both classical and quantum computers. Primarily based on mathematical problems such as lattice problems and hash functions.
Shor's Algorithm	A quantum algorithm published in 1994 that can efficiently factor large integers and compute discrete logarithms, rendering RSA and ECC vulnerable to quantum attack.

Term	Definition
Trust Stack	The TQS layered model of digital trust governance, comprising five layers: Ownership, Responsibility, Control, Participation, and Time.

Appendix B: *Regulatory Timeline Reference*

Date	Event / Milestone
2024 (August)	NIST publishes FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA) — first post-quantum cryptography standards.
2024	eIDAS 2.0 (EU 2024/1183) enters into force, establishing the EUDI Wallet framework.
2026	EU member states must offer EUDI Wallets to all citizens. European Commission Coordinated Implementation Roadmap requires national PQC migration strategies.
2027	Major private-sector service providers (banks, transport, healthcare) must accept EUDI Wallets. ENISA expected to publish EU-wide WSCD/WSCA certification scheme.
2030	European Commission Roadmap target: high-risk systems migrated to post-quantum cryptography.
2033	Global Risk Institute median estimate for 50% probability of a Cryptographically Relevant Quantum Computer.
2035	European Commission Roadmap target: medium-risk systems migrated to post-quantum cryptography.

Appendix C: *NIST PQC Standards Summary*

Standard	Algorithm Family	Primary Use	Key Sizes	Recommended For
FIPS 203	ML-KEM (lattice)	Key encapsulation / key exchange	ML-KEM-512/768/1024	TLS, key establishment, encrypted credential transport
FIPS 204	ML-DSA (lattice)	Digital signatures	ML-DSA-44/65/87	Credential signing, certificate chains, wallet attestation
FIPS 205	SLH-DSA (hash-based)	Digital signatures (conservative)	Multiple parameter sets	High-assurance signing where conservative security is prioritised
FIPS 206 (expected)	FN-DSA / FALCON (lattice)	Compact digital signatures	FALCON-512/1024	Constrained environments including secure elements

Note: All four NIST PQC signature algorithms are patent-free and available for unrestricted use. Hybrid deployments combining ML-DSA with ECDSA P-256 or Ed25519 are recommended for transition periods. ETSI TS 119 312 provides European guidance on algorithm selection for qualified trust service providers.

About The Quantum Space

The Quantum Space (TQS) is an independent research and intelligence platform dedicated to quantum computing, post-quantum cryptography, cybersecurity, and digital sovereignty. Our mission is to equip Europe's decision-makers with actionable, evidence-based insights to anticipate and adapt to the quantum era.

We specialise in sector-specific strategic analysis that bridges the gap between technical depth and boardroom priorities — supporting leaders in technology, defence, finance, and infrastructure with intelligence that is:

- Technically rigorous — grounded in verifiable data, technical standards, and leading-edge research.
- Strategically relevant — framed in the context of sovereignty, resilience, and competitive advantage.
- Forward-looking — identifying not just immediate threats, but the emerging opportunities of quantum technologies.

Our research methodology integrates:

- Primary source analysis — EU directives, national strategies, and industry technical publications.
- Sector engagement — consultation with vendors, regulators, and operators across critical industries.
- Comparative intelligence — mapping Europe's positioning against global competitors in quantum readiness.

TQS operates as an independent voice, committed to transparency and neutrality in its assessments. We work with public-sector agencies seeking to set resilient quantum migration policies and private-sector leaders integrating quantum-safe technologies into mission-critical systems. We also work with industry consortia shaping international standards and collaborative innovation.

<https://thequantumspace.org>

Turn your software into a thriving revenue generator with CodeMeter.

- **Flexible Monetization:** Adaptable licensing models for all market demands
- **Robust IP Protection:** Innovative encryption and integrity protection methods
- **Effortless Compatibility:** Smooth integration into diverse platforms
- **Future-Proof Solutions:** Designed to evolve alongside your business needs

With CodeMeter, your software grows stronger roots and flourishes.

sales@wibu.com
www.wibu.com



Start now and
request your
CodeMeter SDK
wibu.com/sdk





THE QUANTUM SPACE

Trusted Steps. Quantum Leaps.