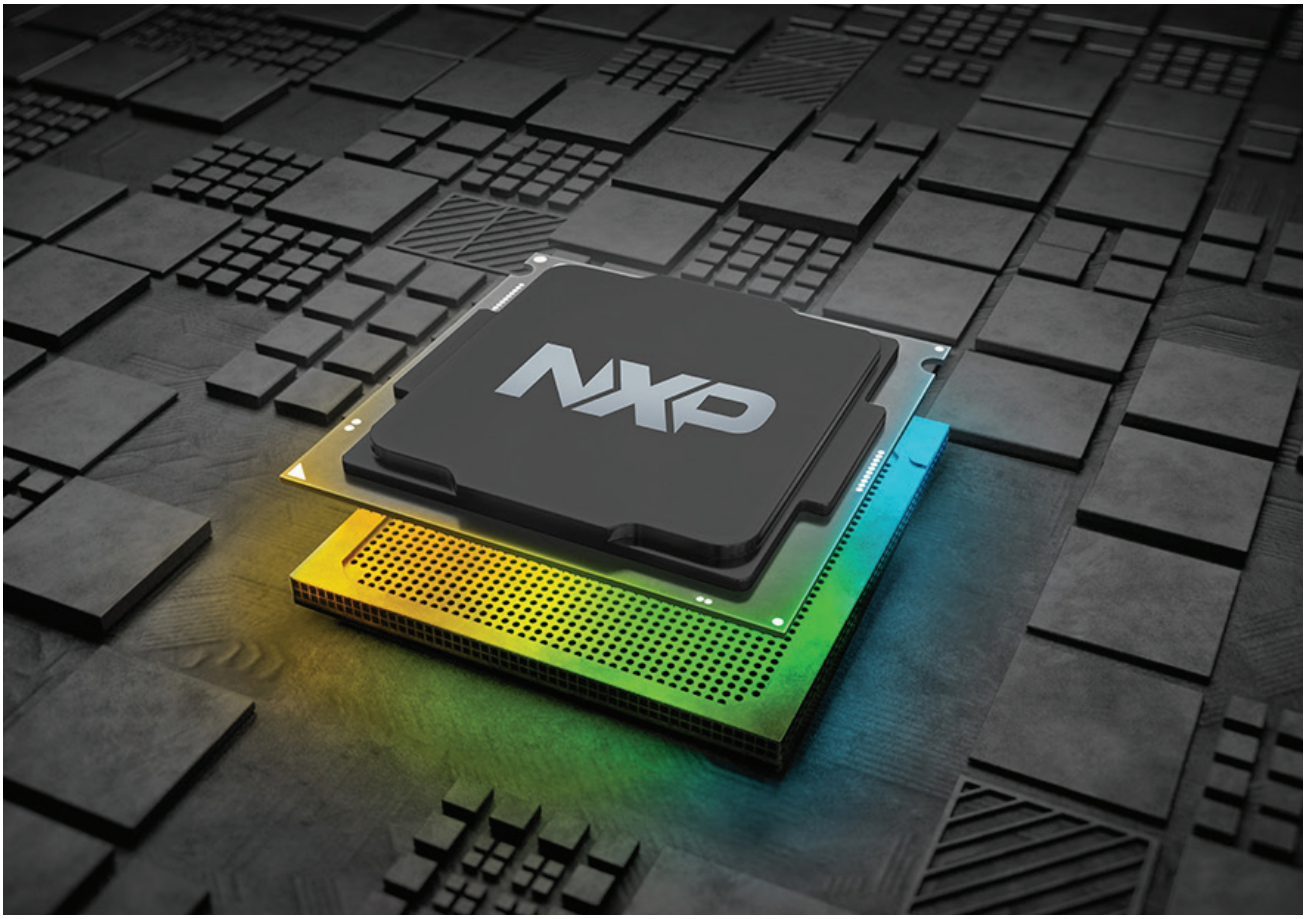
Whitepaper

The future of secure elements: PQC, EUCC and cyber resilience

Managing the multi-dimensional transition to post-quantum cryptography in secure element applications from 2026 to 2030

Mario Stoltz, Mehdi Soumhi, Sarah Esmann, Felipe Fernandez
NXP Semiconductors

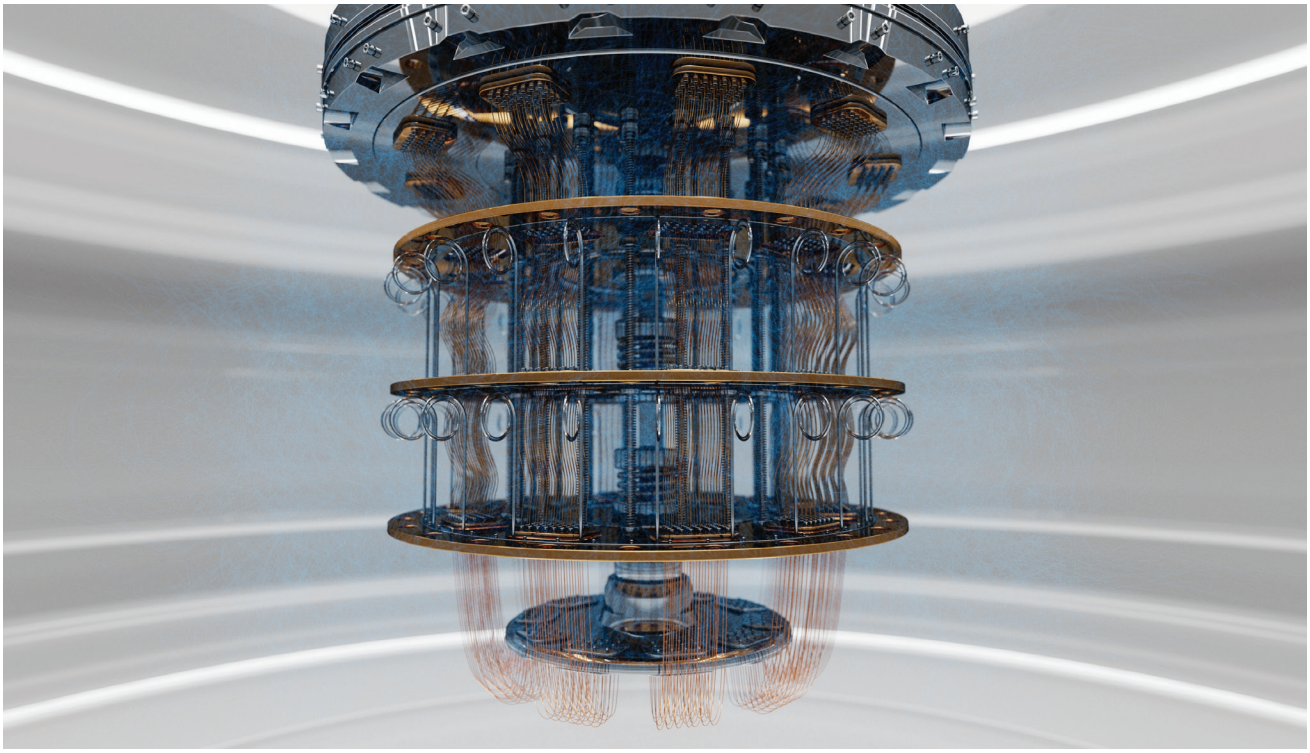


Navigating the transition to next-generation security systems

Secure elements[1] have established themselves as the heart of security applications such as smart cards, tokens and identity documents. However, users of these solutions are facing significant changes in the coming years driven by industry trends and new requirements. These changes include:

- A shift from classical asymmetric/public-key infrastructure (PKI) cryptography to post-quantum cryptography (PQC)
- Changes in security certification requirements
  - Common Criteria version 3.1 (CC v3.1) to Common Criteria version 2022 (CC:2022)
  - SOGIS to the EU Cybersecurity Certification Scheme (EUCC)
- The EU Cyber Resilience Act (CRA) coming into force with new requirements for:
  - risk assessment
  - security assessment or certification
  - security incident management
  - firmware update mechanisms

1 Integrated circuits designed to be used in security and cryptography applications. Also known as secure microcontrollers, embedded secure elements or smart card ICs



The shift to post-quantum cryptography

Many of today's IT security systems use asymmetric cryptography algorithms. These are also referred to as public key infrastructure (PKI) cryptography. However, these algorithms are vulnerable to cryptanalytic attacks via quantum computing. While today's prototype quantum computers are still far from delivering the necessary processing power, it is only a matter of time before such attacks become feasible. The German federal institute for IT security (BSI) publishes a study that estimates cryptographically relevant quantum computers to be available around 2040 or even 2035 (see section 2.10 of the study). Hence, there has been a great deal of effort in cryptography circles to develop post-quantum cryptography (PQC): new algorithms that are secure against quantum attacks. These algorithms are also sometimes described as quantum-resistant, quantum-safe, quantum-proof or quantum-secure.

Delivering cryptography's fastest transition yet

The transition from PKI – as represented by algorithms like RSA and ECC among others – to PQC has already started. For example, Google and Cloudflare have already deployed post-quantum hybrid[2] key agreements (notably X25519 ML-KEM768) across their web servers. Apple is also using PQC protocols to secure iMessage.

2 Hybrid PQC combines a classical cryptographic algorithm (e.g. ECC) with a post-quantum algorithm (e.g. ML-KEM) so that the asset is secured by both. With PQC algorithms not yet considered mature enough to be used alone, the hybrid approach is currently recommended to ensure compatibility with today's infrastructure and continuity of security through the transition period.

From here on, the transition is set to be the fastest and most impactful migration in the history of applied cryptography. For comparison, previous comparable migrations – e.g. from DES to AES and from RSA to ECC – are still rolling out today, decades after the respective newer algorithms were standardized. However, for the migration to PQC, national and regional regulators have set very challenging migration goals for certain applications, requiring the transition to be completed within 5-10 years.

Several things need to happen for a successful migration to PQC.

1. **Establish an agreed set of usable PQC algorithms**
   This step is largely complete, with multiple standards for both symmetric and asymmetric cryptography (e.g. ML-KEM, ML-DSA), with further algorithms expected in the future.
2. **Define PQC protocols**
   By describing the execution of system-level functions using cryptography, protocols explain how to apply an algorithm in a specific application. Examples include how to formally execute a key agreement based on a PQC algorithm.
3. **Update application standards**
   For many applications, regulatory bodies publish specifications that apply to all players in that domain[3]. Once PQC algorithms and protocols for an application are agreed, these specifications must be reviewed and new versions that reference PQC published.
4. **Revise approval processes**
   Methods for compliance testing, security certification and similar processes must be adapted to include PQC and the new versions published.

While this list represents the general sequence of events, the steps do not necessarily need to occur in a strictly sequential manner. There can be parallel timelines, especially between different application areas. However, regulators, industry interest groups and standardization bodies must complete each step for every application affected. Only then will it be possible to submit products for credible compliance testing and type approval – and give customers the confidence to buy PQC solutions, knowing they meet the functional and security requirements of their specific domain.

Change is happening – but standards not yet complete

Various stakeholders have already begun moving on the PQC migration. Standardization and industry specification bodies have started work to discuss and adapt application-level specifications (see Appendix for some examples). But it will still be some time before the updated specifications are published, with each individual application following its own timeline.

In the meantime, some industry players are heavily promoting the prototype use of PQC cryptography. There are also some initial products available claiming Common Criteria security certification and support for PQC. However, in the current authors' view, without published application standards, the value of these products is currently limited to preparing for a smooth migration later or for those willing to rely on proprietary functionality.

[3] E.g. FIDO tokens specified by the FIDO alliance, electronic passports specified by ICAO, trusted platform modules by the Trusted Computing Group, etc.

PQC drives new hardware requirements

Any applied cryptography involves executing complex mathematical algorithms. For classical cryptography, these algorithms are based on the mathematics of large prime numbers.[4]

Manufacturers of secure elements have developed hardware to perform these algorithms efficiently. There is also broad consensus in the security industry and testing community on appropriate countermeasures to harden such accelerators and their operation against commonly accepted threat models.

PQC, however, is based on very different underlying mathematics. Existing crypto accelerators, therefore, cannot execute PQC algorithms effectively. In principle, the algorithms could be run on the microcontroller's CPU – but that would be slow. Moreover, compared to classical cryptography, the mathematical problems in PQC require more memory availability, and keys and cryptographic systems are larger. More memory means larger, more expensive ICs. Not every customer will readily embrace this.

Current ICs are unlikely to be able to run PQC algorithms with acceptable performance or even at all. Therefore, new secure microcontroller platforms with crypto accelerators optimized for PQC algorithms are required and are currently being developed.

Crypto agility is essential for long-term security

Over the last two decades, almost every published cryptography vulnerability was related to a flaw in the implementation rather than the algorithm. Robust implementation design and hardening against relevant attack vectors is critical – especially for IC designs, which cannot be easily corrected after deployment.

Cryptographic implementations must therefore be designed with a clear understanding of the attacks they are expected to resist. This is particularly important in the context of third-party security certification, such as the Common Criteria (CC) evaluation scheme. During evaluation, solutions undergo penetration tests by an independent laboratory. That requires knowledge of the types of attack that are state-of-the-art in the relevant application.

For classical algorithms such as RSA and ECC, there is broad consensus on these attack models and mitigation techniques. This isn't the case yet for PQC, which has a much shorter track record. It is only to be expected that new weaknesses and attack methods will be discovered in the next 5-10 years, and that these could affect some PQC implementations deployed in that time.

Crypto agility and the ability to update cryptographic functionality will be vitally important for any early PQC product generations – and much more so than for previous products. Addressing this involves solving two key challenges:

1. Enabling updates to executable code in a secure element without re-personalization[5]
2. Providing update mechanisms that are practical in real-life situations[6]

[4] The Elliptic Curve Discrete Logarithm Problem for ECC and the Integer Factorization Problem for RSA
[5] E.g. updates do not remove facial portrait or personal electronic signature certificate from eID cards
[6] E.g. updates without internet connection or via smartphone rather than just at a central issuing facility
[7] ICAO Doc 9303 provides specifications for electronic machine-readable travel documents such as ePassports.

Introducing PQC in secure identity applications

Nearly all identity documents issued by national governments rely strongly on standardization. For example, ePassports must be usable globally and are therefore built specifically for interoperability following international specifications[7] released by the International Civil Aviation Organization (ICAO). For national identity documents (eID), countries can, in principle, implement whatever security measures they like. In practice, however, most use standardized protocols for authentication and digital signatures.

Practically all state-of-the-art products for ePassports and national eID are security certified according to the Common Criteria (CC) evaluation and certification scheme. To make products comparable, they are certified according to specific protection profiles (CC PPs), i.e. documents that specify a certain set of security functionality necessary for a given application.

Several countries also have additional national regulations. In Germany, for instance, products for government identification must follow the BSI TR 03110 technical guideline and in France they must comply with the Qualification Renforcée type-approval scheme. National eID solutions for all EU countries need to be compliant with the EU's eIDAS regulation.

Current versions of these specifications refer to particular cryptographic algorithms, configurations and key lengths for specific application protocols. Options for PQC algorithms would need to be added to the relevant specification before PQC solutions could be introduced.

Timeline for PQC adoption in ePassports

For ePassports to adopt PQC, ICAO must first update its Doc 9303. The ICAO new technologies working group (ICAO NTWG) is currently developing options for PQC in ePassports. However, as ICAO is a UN body, a binding decision requires consensus among member states.

Decisions on technical matters such as this are made through the ICAO Technical Advisory Group for the Traveler Identification Program (TRIP TAG), the only body that can vote to formally release a specification. TRIP TAG convenes every two years, the last time being in 2025. It is expected that TRIP TAG will release specifications for passive hybrid PQC signatures in ePassports at its 2027 meeting. Specifications[8] for active PQC functionality in ePassports are very unlikely to be released until TRIP TAG's 2029 meeting at the earliest.

In addition, the relevant Common Criteria protection profile (CC-PP-0068) will also need to be revised or replaced to cover the PQC security protocols adopted by ICAO. Otherwise there can be no robust security certification. In the best-case scenario, this update would be timed to coincide with the release of the ICAO specification. But it could also come later. As a result, it is highly unlikely that any country – even with the best intentions and utmost urgency – would be able to start issuing PQC-enabled ePassports before 2030.

Timeline for PQC adoption in national eID systems

The situation is similar for national eID and comparable products, with changes required to both specifications and protection profiles used in certification. However, as the changes here are at the national or regional level – rather than global – progress could be faster albeit more country-dependent.

Many countries offer eID products with electronic signature functionality to enable online interaction between citizens and public administration typically using standardized cryptographic protocols and algorithms. To be eligible for use in these systems, solutions must be certified against an appropriate protection profile: usually one or more of the series of profiles related to qualified electronic signature creation devices (CC-PP-0059, -0071, -0072, -0075 and -0076).

The first step in enabling the use of PQC in these systems is revising the application-level specifications to incorporate PQC algorithms. Unlike ePassports, this could be done in national or regional specifications such as the EU's eIDAS regulation and the ETSI/CEN specifications that provide its underlying technical detail. As a second step, the relevant protection profiles used for certification would also need to be updated or replaced to include coverage for PQC-based signature protocols. In principle, this could be achieved by 2028 or 2029 – depending on the conditions and urgency of individual nations and the meeting schedules of standardization groups. However, the sheer number of specifications that would need to be updated may make this timeline challenging.

[8] In a 9th or 10th edition of ICAO Doc 9303 or as part of an ICAO technical report on PQC functionality for ePassports

Changes in security certification

Third-party security certification plays a critical role in the market for secure microcontrollers. It gives those purchasing IT solutions independent verification of vendors' claims that a solution is "secure". Specifically, it helps purchasers answer three questions: How secure is it? What is it secure against? Under what conditions?

The security certification landscape is entering a period of transition. Regulatory changes and the shift to new evaluation methodologies will reshape how certificates are issued and interpreted. Ultimately, this should improve harmonization and consistency across markets but could introduce complexity in the short term as the ecosystem adapts.

The situation today: Common Criteria certification

The Common Criteria (CC) is the most important security certification scheme for embedded secure elements and security microcontrollers. Practically every product of this kind is CC certified and new products will only be accepted on the market with a valid CC certificate.

CC certification for security microcontrollers is performed:

- at the IC hardware platform level
- at the operating system (OS) platform level (especially for JavaCard OS)
- at the application level for native OS in specific applications[9]

Unlike some schemes that focus on a product's external behavior (e.g. FIPS 140), CC certification covers everything. Security evaluation must start shortly after product development itself begins and absolutely everything must be open to the evaluators. The evaluation starts with the product developers, security conditions where they work, and their development environment and processes. It then moves on to the product itself, its function as well as all its security features and how they are implemented down to the source code and user documentation. The product then undergoes intensive penetration testing in specialized laboratories.

Once the evaluation is complete, the results are sent to the certifying authority where they are checked for correctness and completeness. Only then will the authority issue and publish a security certificate. These certificates are valid for a limited period and are often subject to regular renewals, maintenance procedures or recertifications after even very small technical changes. There are also strict rules for the hierarchical re-use of evaluation results in other products/components.

[9] E.g. qualified signature creation devices, machine-readable travel documents and various other such products

From national certificates to EUCC: The EU Cybersecurity Act

Today, CC certificates are issued by national authorities. The authorities also accredit one or more laboratories to act as evaluators. This accreditation is specific to certain types of IT solution and application areas, hence not every evaluator in every country is authorized to evaluate all product types.

In principle, then, CC certificates are only valid nationally, which isn't ideal in an international market. In some cases, the certificate may be issued by an authority with a strong enough reputation internationally that the certificate is recognized outside its formal geography of validity. There also exist various mutual recognition schemes that allow CC certificates to be compared (e.g. SOG-IS[10] within Europe and CCRA[11] globally).

Europe is a key region in this context as it is home to many major developers and customers of CC-certified IT security solutions. As such it is at the forefront of efforts to harmonize CC security certification. Adopted in 2019, the EU Cybersecurity Act (EU 2019/881) gave the European Union Agency for Cybersecurity (ENISA)[12] the authority to regulate IT security certification for all member states. This has led to strengthening of the mutual recognition scheme within the EU. As of 2026, CC certificates are still issued by member states' national authorities but are also formally published by (ENISA[13]). Such certificates now use the EU Cybersecurity Certification (EUCC) label.

The transition to CC:2022 and what that means for the ecosystem

When carrying out a CC security evaluation, the accredited laboratory must follow a strict methodology that is standardized by the members of the Common Criteria[14] recognition agreement. This methodology covers how the evaluation is performed and how strengths and weaknesses of the development environment, development process and product should be weighted in the overall result.

That methodology has recently been updated. Until the end of 2025, evaluations followed the CC v3.1 methodology and, from 2026, they should follow the CC:2022 methodology. This will affect how evaluations are performed and how they should be interpreted.

The biggest impact will be on developers of IT solutions, who will need to learn new rules for providing evidence including product and process documentation. However, evaluators and certifying authorities also face changes. All these parties will need to adjust to the new rules. After a brief period of possible disruption, the certification system should be operating smoothly again relatively quickly. But we can expect to see some teething troubles throughout 2026 and into 2027. This could lead to delays as well as some confusion when comparing "old" and "new" certificates.

The EU Cyber Resilience Act and its implications

Any product intended for the European market must adhere to several regulations issued by the European Commission and EU member states. Exactly which regulations apply to a product depends on its intended application. Compliance with the appropriate regulations is indicated by displaying the CE mark on the product.

The Radio Equipment Directive

Since June 2017, any product that emits or meaningfully interacts with radio frequency transmissions needs to comply with the EU's Radio Equipment Directive (RED)[15] to access the EU market. Among its catalog of requirements, the regulations contained several requirements related to IT security. However, its coverage of security was not comprehensive.

[10] www.sogis.eu
[11] commoncriteriaportal.org/ccra/index.cfm
[12] www.enisa.europa.eu/topics/product-security-and-certification
[13] certification.enisa.europa.eu/certificates_en
[14] commoncriteriaportal.org/contact/message/index.cfm
[15] Also known as EU directive 2014/53/EU and later standardized as the EN 18031 series.

What the CRA changes

Regulation (EU) 2024/2847[16], also known as the Cyber Resilience Act (CRA) provides a more complete regulatory framework for IT security. The CRA was officially published in November 2024, and its provisions will come into force over the course of 2026. The Act will be fully in force by December 2027.

The CRA is formulated with "appliances" (i.e. devices that can be brought to market as finished products) in mind. Sub-components and modules that cannot operate independently aren't exempt, but the specifics of the regulation only affect them when they are integrated into a finished product.

The regulation officially covers "products with digital elements". In practice, this means products that "store, transmit or otherwise process data at rest or in transit". In addition, the regulation includes definitions of product categories that can be used to determine if third-party assessment is required and what form that should take.

Specifically, the CRA requires applicable products to:

- protect data confidentiality
- protect data integrity
- perform automated updates of embedded software
- have capabilities for authentication
- perform activity logging
- have capabilities for secure erase and backup

The details of these requirements will be provided in EN standards to be developed by CEN, CENELEC and ETSI.

New requirement for in-field software updates

One of the key requirements that has drawn the most attention in the industry is the need to provide software updates in the field. This is a feature that is already common in some applications but not widely available in others. Under the CRA, any device that communicates, processes data and includes any embedded software (firmware) must be able to update that software in a secure and controlled way.

Consequently, many users of IT security systems now need to answer some crucial questions:

- What do I have to do for the security assessment?
- Do I have to provide updates?
  - If so, how, when and for how long?

This puts extra importance on portfolio management. Previously, manufacturers may have chosen to continue producing older products for an indefinite time. But if the product falls under the scope of the CRA, the manufacturer will remain responsible for actively handling its security and providing firmware updates. This may lead to the manufacturer choosing to actively discontinue some older products.

How the CRA impacts security certification

While it isn't possible to state categorically for all cases yet, products with existing CC certificates will most probably not need additional proof of their cybersecurity properties under the CRA. CC certification will be regarded as sufficient to prove compliance. Note, however, that CC certification does not cover all requirements of the CRA – several other requirements still apply and must be demonstrated.

Preparing for a coordinated transition

Secure identity systems will undergo a period of significant change from 2026 to 2030. The transition to post-quantum cryptography, the evolution of Common Criteria certification including EUCC and CC:2022, and the introduction of the Cyber Resilience Act are unfolding in parallel. These developments are closely interconnected. Changes in cryptographic algorithms influence hardware design and system architecture, which must in turn be reflected in certification approaches and lifecycle requirements.

This has direct implications for secure microcontrollers. Post-quantum cryptography introduces new demands in terms of performance, memory and hardware acceleration. At the same time, the relative immaturity of PQC calls for increased crypto agility and robust update capabilities. With the Cyber Resilience Act extending responsibility across the full product lifecycle, secure update mechanisms and long-term maintenance strategies are becoming essential design elements.

Although progress is being made, many aspects of the ecosystem remain in transition. Application standards, protection profiles and certification methodologies are evolving on different timelines. As a result, organizations cannot rely solely on suppliers to manage this shift. Responsibility remains with those placing products on the market, requiring early planning and active involvement across technology, certification and compliance domains.

Practical steps include assessing current cryptographic usage, evaluating hardware readiness for PQC, reviewing certification strategies and preparing lifecycle management processes in line with regulatory expectations.

Supporting the transformation

NXP is actively supporting this transition. Through engagement in standardization and close collaboration with ecosystem partners, our solutions are aligned with emerging requirements for secure identity applications. Our experts are available to help customers navigate these changes and implement approaches that remain robust in the years ahead.

Resources

- Information about the CRA for NXP customers, including access to helpful application notes
- Information about PQC for NXP customers, including various articles, product announcements, access to documentation

[16] eur-lex.europa.eu/eli/reg/2024/2847/oj

Appendix: Examples of standards bodies active in the PQC migration

Below is a list of initiatives among national and international bodies to prepare application-level standards for post-quantum cryptography.

- **European Union**
  - **November 2024**
    - Declaration from 18 member states on transition to PQC
      - Recommends hybrid solutions
      - Identifies "store now, decrypt later" and long migration periods as key risks
      - Labels PQC transitions as "top priority" and stresses urgency
- **NIST (USA)**
  - PQC algorithm competition and standardization
    - See landing page and PQC migration recommendations
  - **October 2020**
    - NIST SP 800-208 with recommendations for using LMS and XMSS stateful hash-based signature schemes
  - **August 2024**
    - FIPS 203 – ML-KEM (ex Crystals-KYBER)[17]
    - FIPS 204 – ML-DSA (ex Crystals-Dilithium)
    - FIPS 205 – SLH-DSA (ex Sphincs+)[18]
  - **October 2024**
    - Initial public draft of NIST SP 800-131Ar3 details requirements for transition regarding algorithms and key lengths[19]
- **ANSSI (France)**
  - **March 2022**
    - Recommends hybrid protocols as a transition mechanism
    - Indicates that from 2027 security products will only be accepted at the qualification entry stage if they include PQC
  - **2026 (pending)**
    - Expected to publish additional guidance including Référentiel général de sécurité (RGS) to clarify preferred algorithms
- **BSI (Germany)**
  - **August 2025**
    - Study showing viable quantum computers could be available within 10-15 years (2036-2040)
  - **January 2026**
    - BSI TR-02102-1, edition 2026-01 includes recommendations for migrating to PQC and advises against non-quantum-resilient cryptography

This list is not exhaustive. Many other regional or national regulators have mandated national transitions of similar kinds.

[17] NXP cryptographers were among the original co-authors of the KYBER algorithm proposal that became the ML-KEM standard
[18] Additional standards in this series are expected
[19] See particularly table 3 in that document which indicates certain algorithm configurations are no longer allowed for use even today