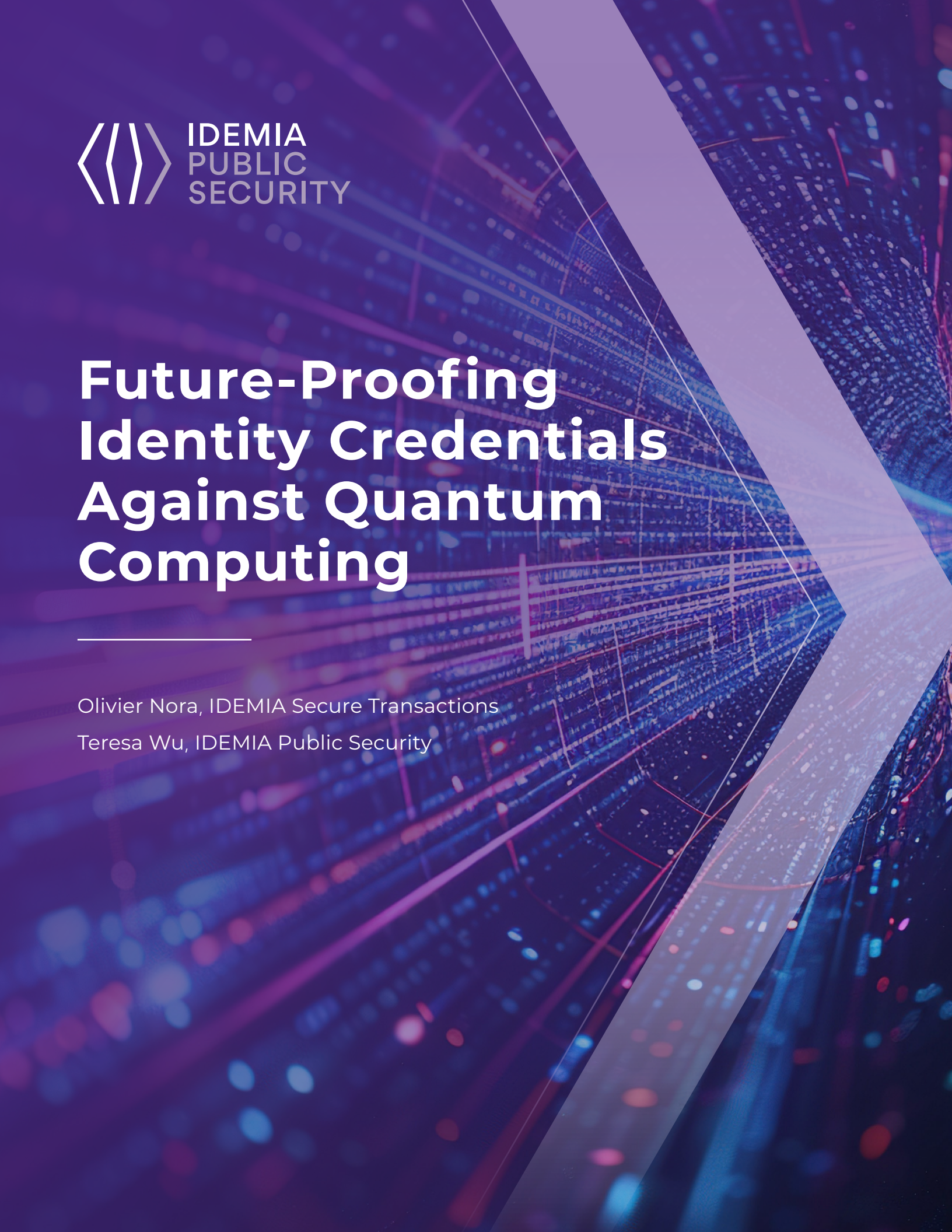


Future-Proofing Identity Credentials Against Quantum Computing

Olivier Nora, IDEMIA Secure Transactions

Teresa Wu, IDEMIA Public Security

1 Quantum Computing: A Game-Changer for Cybersecurity

1.1 A Threat to the Very Foundation of Cybersecurity

With its ability to exploit the principles of quantum mechanics, quantum computing is paving the way for groundbreaking advancements in computational power. While the potential benefits are immense, its emergence introduces severe risks that could fundamentally disrupt cybersecurity.

One of the most significant threats posed by quantum computing is its ability to crack public key cryptography systems—which form the backbone of digital security. These systems are used to authenticate software, secure communications, protect data, and ensure the integrity of connected devices. Without these protections, encrypted information can be deciphered, malware can proliferate, and critical systems can fall victim to malicious attacks.

The accessibility of quantum-based attacks amplifies the urgency of the threat. A hostile actor would only need a single session on a quantum computing platform to unlock secret keys, making it easier than ever to compromise systems using conventional hacking techniques. With access to quantum computing, hostile actors could access, destroy or modify classified government documents or citizen data, or deploy ransomware in critical public infrastructure systems.

1.2 Time for New Cryptographic Algorithms

To address this threat, the solution is to switch out vulnerable cryptographic algorithms for new ones that are based on mathematical problems that quantum computers cannot solve faster. This is the objective of the project led by the National Institute of Standards and Technology (NIST)[1] to select secure and efficient quantum-safe cryptographic algorithms for standardization worldwide.

There are two types of quantum-safe cryptographic algorithms: those which allow the exchange of secret keys between two parties, and those that make it possible to digitally sign a document.

To date, the NIST has selected the first five algorithms for standardization (three for signature and two for key exchange) and is planning to select additional standards (signature) in future. This illustrates the complexity of the new landscape: no single post-quantum algorithm fits all needs, so multiple strategies have been identified to address diverse use cases, and to mitigate the risk of a major vulnerability being discovered.

[1] NIST Post-Quantum Cryptography project – https://csrc.nist.gov/projects/post-quantum-cryptography

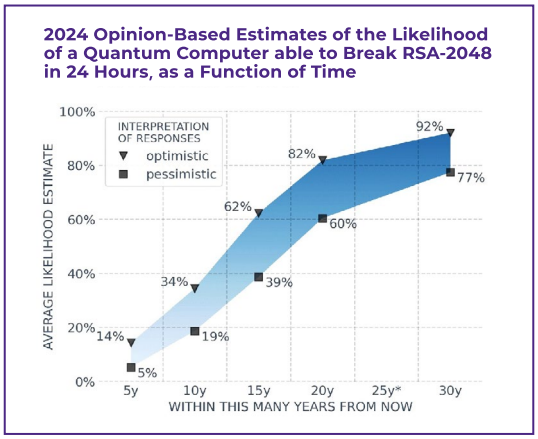
1.3 A Matter of Urgency

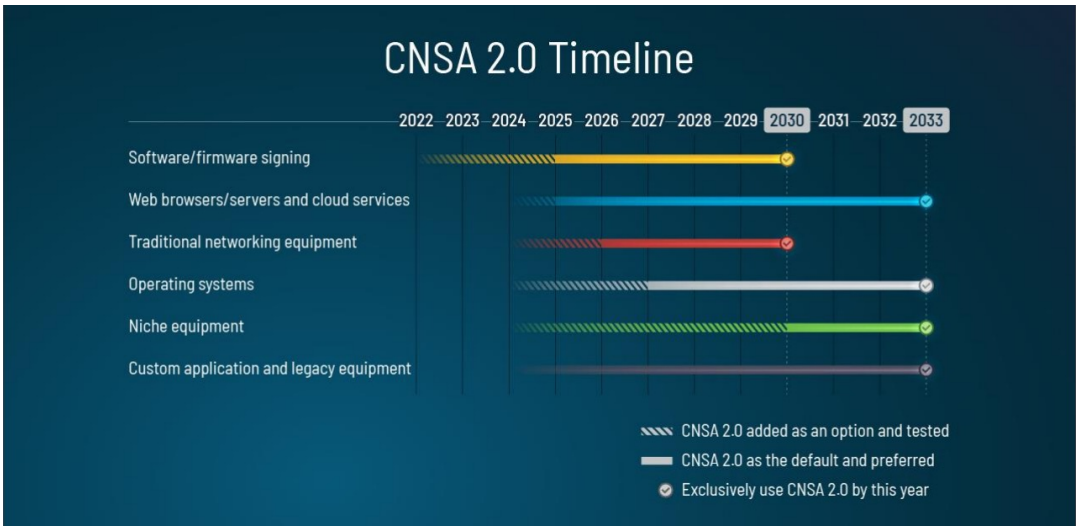
According to the Quantum Threat Timeline Report 2024, experts estimate there is a 19 to 34% probability that a quantum computer capable of breaking current cryptography will exist in 10 years. These forecasts are in line with the roadmaps of major companies and startups in the field. In response to these risks, security agencies worldwide are taking steps to mandate migration by 2030-2035.

In the U.S., the National Security Agency has issued a Cybersecurity Advisory announcing the Commercial National Security Algorithm Suite 2.0. In it, it lays out the expectation that the transition to post-quantum cryptographic algorithms be finalized in 2030-2033.

Through documents like NIST Interagency Report (IR) 8547 titled, "Transition to Post-Quantum Cryptography Standards" (currently in Initial Public Draft), NIST has established the overarching timeline for phasing out all quantum-vulnerable public-key cryptography across the federal agencies. This timeline provides two critical hard deadlines:

- **By the end of 2030:** All cryptographic algorithms providing 112 bits of security strength will be formally deprecated. By this date, agencies must have transitioned away from these algorithms for nearly all use cases.
- **By the end of 2035:** All currently used public-key algorithms that are vulnerable to a Cryptographically Relevant Quantum Computer (CRQC)[2] —including all forms of RSA, ECDSA, and Diffie-Hellman (DH)—will be disallowed for federal use, regardless of their security strength. This final deadline aligns with the primary goal set forth in NSM-10, and represents the target for completing the government-wide migration.





[2] A cryptographically relevant quantum computer (CRQC) is a quantum computer capable of breaking current asymmetric cryptography.

1.4 Crypto-Agility is the Ultimate Goal

As we move toward a quantum-resilient future, crypto-agility is not just about using post-quantum algorithms; the cybersecurity infrastructure needs to be set up to support crypto-agility. THIS is the real problem to solve for. It refers to the ability to rapidly and remotely update or replace cryptographic algorithms in deployed systems, ensuring adaptability as threats evolve and standards shift.

Post-quantum algorithms are very young, and the level of confidence in these algorithms is not as high as for current cryptography. Although they are safe against the latest in quantum computing by design, they could be challenged using traditional means, such as side-channel attacks, fault injection, or even algorithmic breakthroughs.

Early experiences with RSA in the 1980s and 1990s showed that real-world deployment required many adjustments to ensure security. Quantum-safe algorithms will certainly follow the same learning curve and need to be maintained in a timely manner to protect against new vulnerabilities.

NIST CSWP 39 (2nd Public Draft), titled "Considerations for Achieving Cryptographic Agility: Strategies and Practices" highlights the principles of crypto-agility, and states that crypto-agility will help organizations proactively address emerging threats, technological advances, system weaknesses, and evolving business requirements, standards, regulations, and mandates.

Crypto-agility is needed:

- To migrate from classic cybersecurity to quantum-safe cybersecurity;
- To deploy countermeasures against newly-disclosed vulnerabilities in a timely manner;
- To change algorithms and protocols in the event of a major vulnerability discovered that would disqualify one or more quantum-safe algorithms.

When applied directly to existing products, this adaptability provides significant added value in terms of efficiency, cost-effectiveness, and compliance with regulatory changes, while ensuring business continuity.

For example, IDEMIA Secure Transactions (IST), a division of IDEMIA Group, was the first company to provide technical crypto-agility solutions to enable long-term state-of-the-art security for both embedded chip products and digital solutions, capitalizing on more flexible and efficient methods for addressing security flaws.

2〉 Future-Proofing Identity Credentials Against the Quantum Threat

2.1 How Can Organizations Prepare?

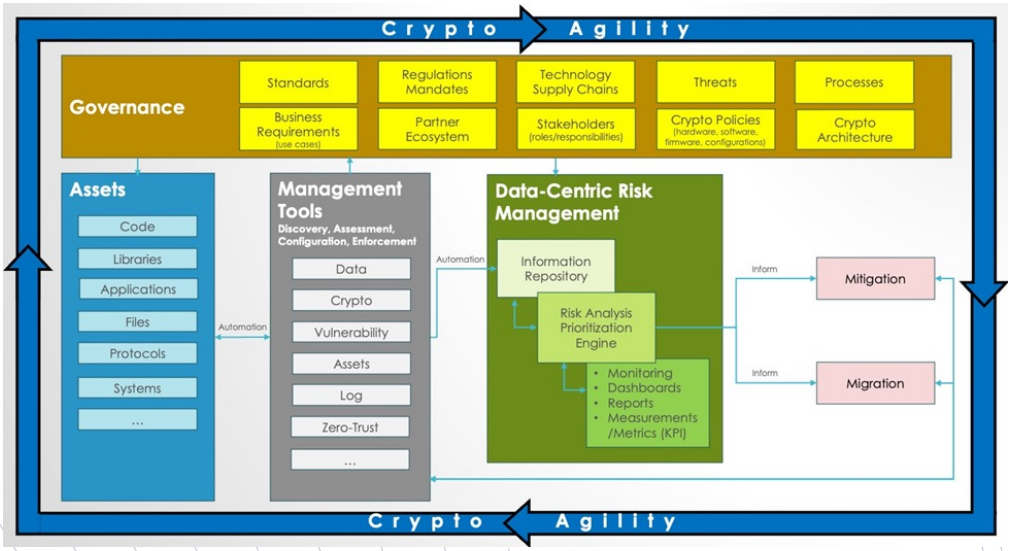
In a factsheet Quantum Readiness: Migration to Post-Quantum Cryptography (Aug. 17, 2023) compiled by CISA, NSA, and NIST, several steps are outlined for post-quantum readiness. These include:

- Establishing a post-quantum readiness roadmap;
- Preparing a cryptographic inventory (all cryptographic algorithms currently in use);
- Engaging with cryptography vendors on the topic of post-quantum computing;
- Establishing the responsibilities of technology vendors.

NIST CSWP 39 (Considerations for Achieving Cryptographic Agility: Strategies and Practices) highlights the organizational steps toward cryptographic agility:

- Integrate crypto-agility into the organization's existing governance function;
- Take inventory of the use of cryptography for data protection across the organization by adopting an asset-centric approach;
- Identify gaps in enterprise management tools for managing assets, configurations, vulnerabilities, and logs;
- Based on the data collected in the previous steps, develop a prioritized list of assets for migration;
- Implement the strategy and actions based on the prioritization list.

The document summarizes its crypto-agility framework as follows:



2.2 Quantum Threat, ICAM Systems (Identity, Credential, and Access Management), PIV Cards

CISA identifies National Critical Function (NCF) 35 (“Provide Identity Management and Associated Trust Support Services') as a crucial enabler for quantum-safe migration across all other NCFs. This is further highlighted in the Homeland Security Operational Analysis Center (HSOAC) Research report, Preparing for Post-Quantum Critical Infrastructure Assessments of Quantum Computing Vulnerabilities of National Critical Functions.

The urgency for government agencies to prepare for quantum migration stems from the fact that ICAM systems are heavily reliant on vulnerable cryptography to secure access to critical resources in government agencies.

Using quantum computing, a malicious actor could duplicate PIV cards or FIDO tokens, or forge fake ones, or compromise the security flow between the ICAM system and business applications.

Such breaches would severely impact identity proofing, user authentication, account recovery, and decentralized identity by undermining the root of trust. Furthermore, compromised access management would eliminate trusted authorities, session authentication, equipment access and authentication control, physical access control, and digital signatures.

2.3 Crypto-Agility and Quantum-Safe Migration for ICAM

Identity, Credential and Access Management (ICAM) systems are critical systems that rely on both physical and digital solutions.

On the physical side, hardware tokens such as PIV cards or FIDO dongles allow the authentication of a person and protect the credentials used by that person to sign a document or access a system. These devices are based on a secure element, a secure, resource-constrained crypto processor.

To be quantum-safe, these secure elements need to evolve, increasing their hardware capabilities (processing power, memory, hardware accelerators), and including a crypto-agile software design following CNSA 2.0 guidance for firmware updates. Next-generation secure elements are coming to market, and may now be included in quantum-ready devices: devices that will be able to migrate to quantum-safe protocols as soon as these are standardized.

On the digital side, the quantum-safe protocols that will be used by the various buildings blocks of the ICAM system—Identity Management, Credential Management, and Access Management—are far from finalized, and the protocols used with PIV Cards (FIPS 201) or FIDO authenticators (FIDO2) have not yet evolved to a quantum-safe version.

Yet, given the timeline required to face up to the nascent quantum threat, it is vital that we anticipate these future standards and start implementing crypto-agile, quantum-ready solutions so that we can respond to nascent standards and be ready to migrate as soon as this is mandated. Crypto-agility will also support the ongoing maintenance of quantum-safe cryptography as the new algorithms are rolled out on a large scale.

2.4 Implementing an End-to-End Crypto-Agility Proof of Concept

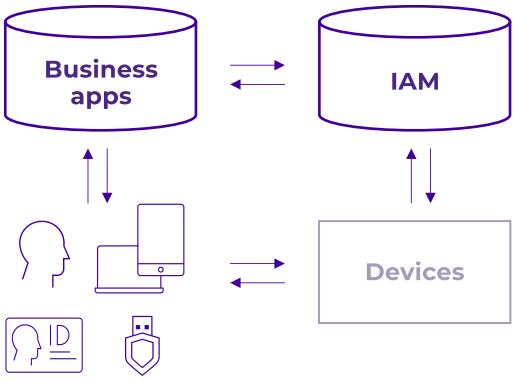
To achieve crypto-agility, two considerations are crucial:

First, procure quantum-ready hardware tokens (PIV cards, FIDO tokens). These are devices which can run post-quantum cryptographic algorithms, are crypto-agile, and can be remotely managed.

For example, at MWC 2025 in Barcelona, IDEMIA Secure Transactions demonstrated a crypto-agile, quantum-ready industrial equipment using a secure element for crypto-agility, and remote management services for cryptographic updates.

The equipment demonstrated the crypto-agility of a mutually authenticated TLS communication, switching from current cryptography to NIST-standardized post-quantum cryptography.

Second, understand the crypto-agility management services that will be required



and the automation necessary to synchronize distribution of new algorithms, generate and distribute new keys and certificates, and phase out vulnerable cryptographic assets.

The first step towards implementing this crypto-agility for PIV and/or FIDO hardware tokens is to run a proof of concept in a sand box environment, implementing end-to-end use cases and demonstrating crypto-agility.

Conclusion

Quantum computing represents both a technological breakthrough and a profound cybersecurity challenge. Its ability to compromise asymmetric public-key cryptography threatens the very foundation of digital trust, making proactive measures essential. As outlined in this paper, the transition to post-quantum cryptography is not merely a matter of adopting new algorithms - it requires a holistic approach centered on **crypto-agility.** Organizations must prepare for a dynamic environment where standards evolve, vulnerabilities emerge, and rapid adaptation becomes critical.

The urgency is clear: government mandates and industry roadmaps anticipate migration by 2030-2035, underscoring the need for immediate planning. This includes inventorying cryptographic assets, engaging vendors, and deploying quantum-ready hardware and software solutions. Furthermore, identity and access management systems - core to securing critical infrastructure - must integrate quantum-safe protocols and crypto-agile architectures to maintain trust and resilience.

Ultimately, future-proofing identity credentials against quantum threats demands collaboration across industry, government, and technology providers. By embracing crypto-agility and investing in quantum-ready solutions today, organizations can ensure continuity, compliance, and security in a post-quantum world.

Further Reading

- Quantum-ready cryptographic libraries
- Certified cryptographic algorithms supporting both classical and post-quantum use cases.
- Quantum-ready cryptographic libraries | IDEMIA
- Migration to Post-Quantum Cryptography. NIST, National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
- MPQC two-page fact sheet: https://www.nccoe.nist.gov/sites/default/files/2023-08/mpqc-fact-sheet.pdf

For more information, contact us at **info@ps-idemia.com** or **na.idemia.com/contact-us**