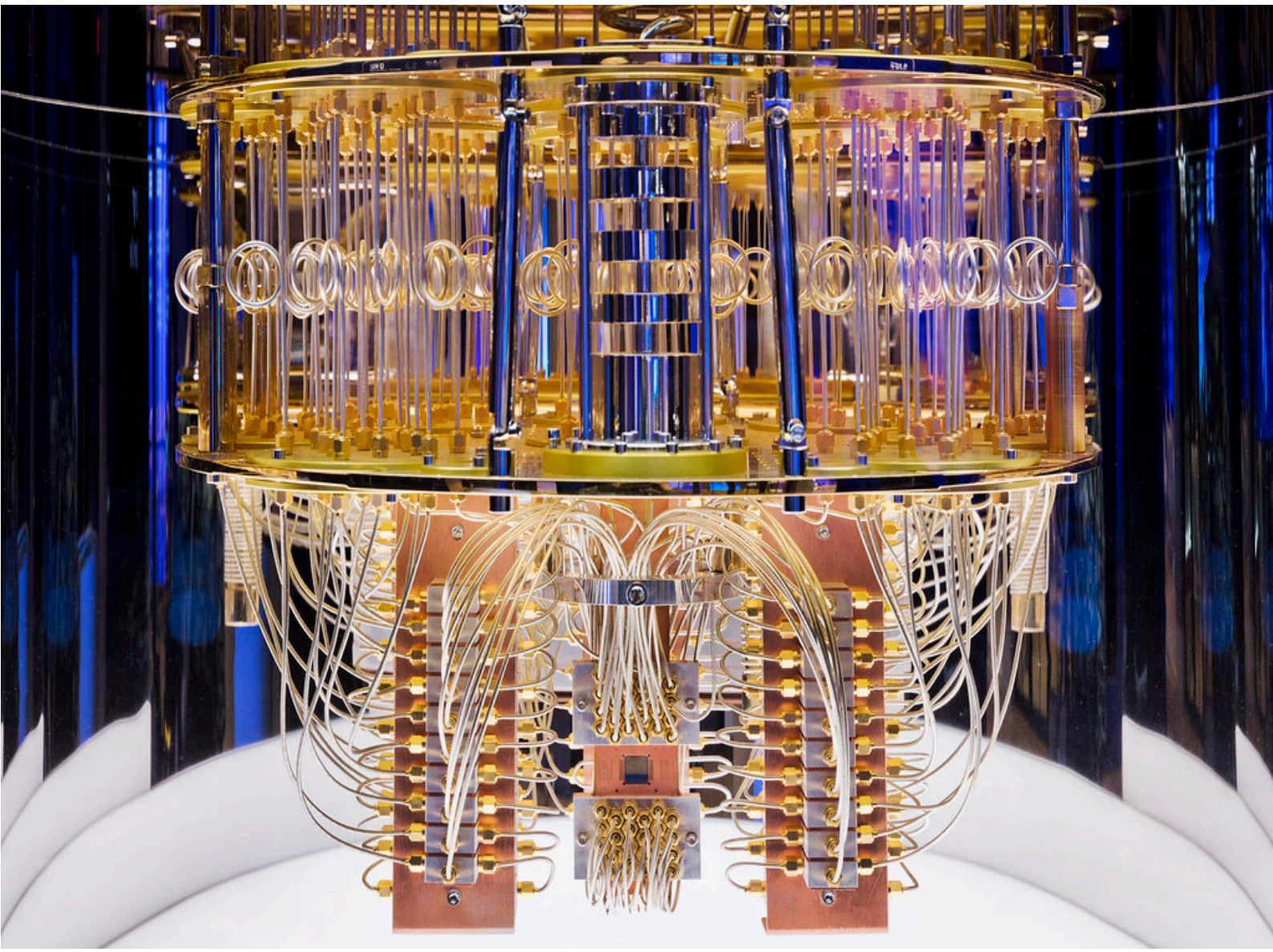
Australia's National
Science Agency

Quantum Safe Transition: Reality, Hurdles and Pathways

Securing the Future of Digital Infrastructure in the Post-Quantum Era

Dongxi Liu, Surya Nepal, Sharif Abuadbba, Jiafan Wang, The Anh Ta, Nazatul Sultan, Shangqi Lai, Sid Chau

28 October 2025



CSIRO Data61

Citation

Dongxi Liu, Surya Nepal, Sharif Abuadbba, Jiafan Wang, The Anh Ta, Nazatul Sultan, Shangqi Lai, Sid Chau (2025) Quantum Safe Transition: Reality, Hurdles, and Pathways. CSIRO, Australia.

Copyright

Important disclaimer

Contents

Executive summary

Quantum computers hold enormous potential to transform scientific discovery and optimise business operations in unprecedented ways. However, alongside these promising opportunities, they also pose significant risks to today's digital infrastructure by breaking public-key cryptographic algorithms that underlie data and communication security. While cryptographically-relevant quantum computers have not been developed, the threat of "harvest now, decrypt later" is real. This makes the transition to post-quantum cryptography urgent, particularly for safeguarding long-term sensitive data. For Australia, proactive preparation is an opportunity to not only safeguard national interests but also shape and adopt global standards in quantum-safe technologies.

Post Quantum Cryptography (PQC) algorithms exhibit distinct performance characteristics, producing longer ciphertexts than the classical ones currently in use. Even with standardised PQC algorithms, migration cannot be achieved through simple drop-in replacements, and the challenges of migration have been recognised and discussed within both research and industry communities. However, the technical solutions for addressing these migration challenges have not been thoroughly analysed.

This technical report identifies eight essential technical domains that must be addressed for a secure and effective PQC transition:

- Guidelines and best practices tailored to Australia's context.
- Cryptographic asset discovery across enterprise systems.
- Cryptographic impact and business risk analysis.
- Trusted transition strategies that minimise new vulnerabilities.
- Hybrid cryptographic approaches during phased migration.
- High-assurance implementations robust against real-world attacks.
- Crypto agility and system modernisation for long-term resilience.
- Rigorous test and validation frameworks to ensure reliability at scale.

Together, these domains provide a roadmap for organisations to prepare, adapt, and modernise their security infrastructure. By investing in discovery, agility, and assurance now, Australia can ensure that sensitive data and critical infrastructure remain secure well into the quantum era. The transition to PQC is not only about defence against a new class of threat — it is an opportunity to modernise digital infrastructure, strengthen trust, and secure Australia's place in a rapidly evolving global cyber landscape.

1 Introduction

Quantum computers are being developed at a steady pace. While this is exciting for science and technology, it also creates a serious problem: the encryption we use today to protect our data will not be secure once powerful quantum computers become available.

Most of our current security systems, like RSA and ECDSA, are based on math problems that quantum computers will be able to solve quickly. This means that in the future, attackers could break into systems that are considered secure today. Even worse, they could already be collecting encrypted data now, planning to decrypt it later when quantum computers are ready. This is called the "**harvest now, decrypt later**" threat.

Governments around the world are starting to act. In the United States, the Senate introduced the National Quantum Cybersecurity Migration Strategy Act in July 2025, which requires government agencies to start testing quantum-safe systems and upgrade at least one critical system by 2027[1]. In Australia, the Australian Signals Directorate (ASD) has announced that older encryption methods will be phased out in high-security systems by 2030 with a 10 years period of vulnerability for critical data until 2040[2]. ASD is also encouraging businesses to start identifying where they use public-key cryptography and create post-quantum cryptography (PQC) as early as 2026[3].

This is not just a government issue. Industries such as telecommunications, defence, healthcare, and energy are particularly at risk. These sectors rely on long-term data protection and secure communication. If they don't prepare early, they may face serious problems, such as data breaches, system failures, or loss of trust. The good news is that international organisations are already working on solutions. In August 2024, the U.S. National Institute of Standards and Technology (NIST) released the first official standards for PQC - publishing FIPS 203, FIPS 204, and FIPS 205[4]. The Internet Engineering Task Force (IETF) is also updating Internet protocols to support quantum-safe encryption. This includes work on hybrid key exchange mechanisms for TLS[5].

However, transitioning to quantum-safe systems cannot be accomplished overnight. It takes time, planning, and a clear understanding of where and how cryptography is used in the existing systems. That's why early preparation is so important. This technical report provides a roadmap for migrating to PQC, focusing on the technical developments needed after PQC algorithms have been standardised as depicted in Figure 1. It explains the areas of concern,

[1] https://postquantum.com/industry-news/quantum-cybersecurity-migration-act/

[2] https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography

[3] https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography

[4] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[5] https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

the challenges, and the existing works to get ready. This technical report also showcases some of CSIRO's research and technical expertise that can support governments and industry in a smooth and secure transition to quantum-safe systems.

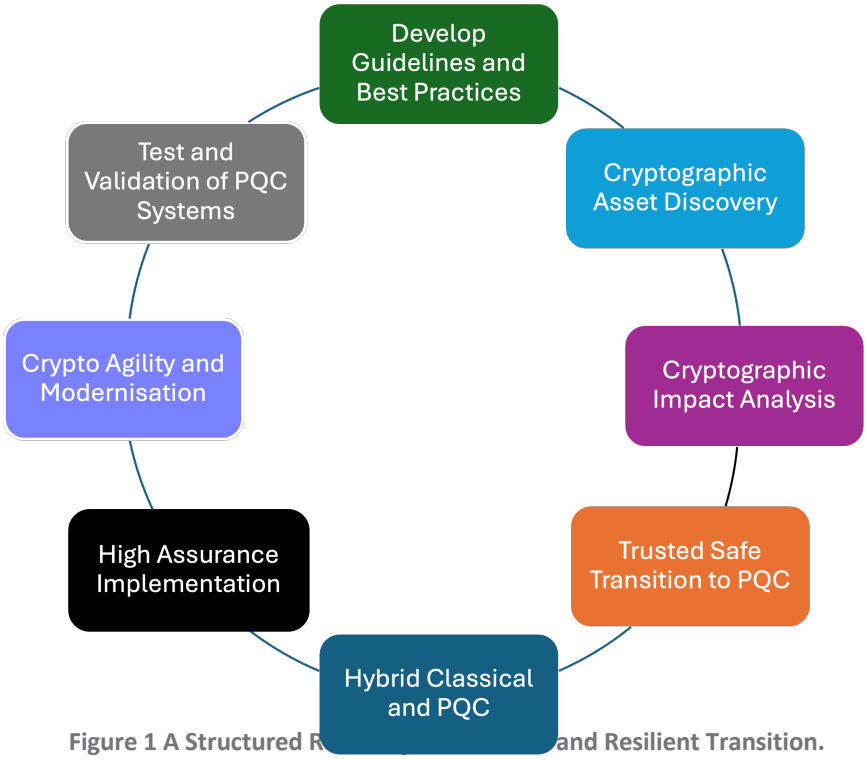


Figure 1 A Structured R and Resilient Transition.

2 Develop Guidelines and Best Practices

The transition to post-quantum cryptography will be large in scale and unprecedented in complexity due to the widespread reliance on cryptographic mechanisms in enterprise information systems. Hence, it is essential to have well-defined transition guidelines that help enterprises navigate the complexity of upgrading to quantum-safe cryptographic systems smoothly and effectively. These guidelines should provide a straightforward framework, along with best practices and clear instructions, for the Australian Government and Industry.

Multiple PQC transition guidelines have been developed worldwide, including reports; for instance, from NIST's project - Migration to Post-Quantum Cryptography[6], the Canadian National Quantum Readiness: Best Practices and Guidelines[7], the EU's Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography[8], and the ASD's Planning for post-quantum cryptography[9].

NIST focuses on specific PQC algorithms like ML-KEM and ML-DSA, but standards for quantum-safe communication are still unresolved, particularly for protocols like TLS. Future standardisation of additional signature algorithms by NIST is possible. Guidelines should encompass PQC applications in such dynamic situations, accommodating various vendors while balancing compatibility, flexibility, and security. The ASD guidelines focus more on the planning stage. These guidelines must be tailored to specific enterprise contexts, considering the diversity of applications, data sensitivity, and local policy requirements[10,11].

It is therefore important for Australia to co-design and develop quantum-safe transition guidelines and best practices in close collaboration with governments, industry, and academia. Furthermore, each organisation should adapt the guidelines to its business contexts. As a national science agency, CSIRO can play a crucial role in this by leveraging its experience in areas like consumer data rights, AI safety, and medical devices. For example, CSIRO Data61 served as an interim standards body to create open technical standards for consumer data sharing and contributed to a TGA guidance document for cybersecurity in medical devices. Additionally, CSIRO helps define AI safety standards and best practices.

---

[6] Dustin Moody et al.: Transition to Post-Quantum Cryptography Standards, https://csrc.nist.gov/pubs/ir/8547/ipd

[7] Canadian National Quantum-Readiness Best Practices and Guidelines, https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf

[8] A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, https https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[9] https://defencescienceinstitute.com/wp-content/uploads/2025/10/Planning-for-post-quantum-cryptography-September-2025.pdf

[10] https://www.oaic.gov.au/privacy/australian-privacy-principles

[11] https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism

3 Cryptographic Asset Discovery

Cryptographic algorithms play a crucial role in securing data, communications, and infrastructure and are omnipresent in today's enterprise systems. However, many organisations lack a clearer visibility and understanding of their cryptographic algorithms, functionalities, and practices across different levels of their IT environment. The aim of cryptographic asset discovery is to address this gap by providing a comprehensive cryptographic inventory that spans the code/binary levels, network cryptography levels, and file system levels.

Cryptographic assets can be scattered across various computing resources within an enterprise, in different forms of access, ranging from black-box systems with only inputs and outputs available to white-box systems where code or files can be accessed. Furthermore, Legacy systems may not be well-documented, and very little can be known about their internal implementation, making it difficult to identify the cryptographic mechanisms used.

Cryptographic asset discovery requires comprehensive knowledge of enterprise digital technologies[12]. The discovery process must be supported by a diverse set of tools capable of analysing cryptographic usage across the entire network and system stack. However, there is currently a gap in both knowledge and skills in finding or developing such tools and effectively applying them to build a complete cryptography inventory. This gap might hinder organisations from undertaking this task on their own, even when engaging with vendors that lack expertise across all aspects of their business systems.

Building cryptographic asset discovery requires research and development capabilities in different aspects of digital technologies, including AI/ML security, cryptography, network protocols, network technology, system security, and program and malware analysis. CSIRO's Data61, as the largest data-driven research organisation in Australia, possesses these capabilities, enabling it to develop and validate tools and technologies that facilitate the discovery of cryptographic assets in compliance with current industry standards and practices. For example, CSIRO has developed AI/ML tools and utilised them to discover cryptographic assets during the transition from ROS to ROS-M for defence applications[13]. The discovery of cryptographic assets may yield additional benefits, such as improving the readiness for broader shifts in cryptographic and data-security requirements under emerging AI workloads.

[12] CycloneDX's Authoritative Guide to CBOM - Implement Cryptography Bill of Materials for Post-Quantum Systems and Applications, https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf

[13] Chandra Thapa, et al.: Transformer-Based Language Models for Software Vulnerability Detection. ACSAC 2022: 481-496

4 Cryptographic Impact and Risk Analysis

PQC is not only a technical upgrade but also a business risk mitigation strategy. Organisations must evaluate how legacy cryptographic dependencies could endanger data integrity, confidentiality, and regulatory compliance under future quantum threats. Many organisations still depend on pre-quantum cryptography (e.g., ECDSA, ECDH), which is vulnerable to quantum attacks. This leaves sensitive data and critical infrastructure exposed to harvest-now-and-decrypt-later attacks.

To enable efficient PQC migration, organisations must assess the business risks of quantum attacks that could expose sensitive data, breach compliance, erode trust, or weaken critical infrastructure. Effective impact analysis aligns security strategy with data lifecycles, operations, and threat models. While the timeline for cryptographically relevant quantum computers remains uncertain—complicating decisions and risking long-lived data—impact analysis helps prioritise assets most vulnerable to quantum threats.

Several assessment frameworks for quantum threats have been proposed, including the crypto agility risk assessment framework[14] and the quantum risk assessment[15]. Since 2021, the Global Risk Institute has published annual reports[16], which include surveys of quantum advancements and forecasts of quantum threats' timelines. However, these assessment frameworks do not place a strong emphasis on the business impacts of quantum attacks.

It is essential for organisations to analyse the business impact of quantum attacks as an earlier step in creating a quantum-safe migration plan that can effectively utilise enterprise resources and protect long-standing, sensitive data, and prioritise migration tasks. The advantage of this approach is that its analysis can cover a wide range, from foundational technologies, quantum algorithms, and cryptography, to AI, data, and business processes, thereby linking it to a migration plan with a technology roadmap. For example, CSIRO has developed an AI tool in collaboration with Google to conduct dependency analysis of open-source software, enabling the impact analysis of newly disclosed vulnerabilities on the software supply chain[17].

---

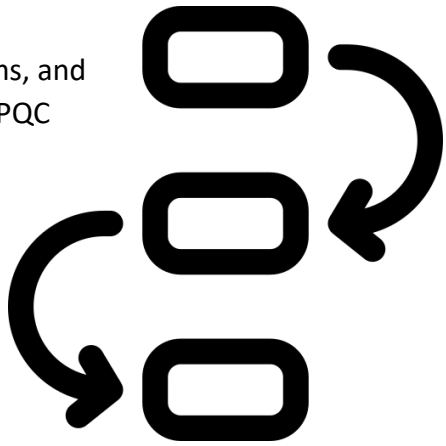
[14] Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi, Vaibhav Garg: CARAF: Crypto Agility Risk Assessment Framework. J. Cybersecur. 7(1) (2021)

[15] Michele Mosca and John Mulholland: A Methodology for Quantum Risk Assessment, https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/

[16] Global Risk Institute: Quantum Threat Timeline, https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

[17] Sajal Halder, et al.: FuncVul: An Effective Function Level Vulnerability Detection Model using LLM and Code Chunk. CoRR abs/2506.19453 (2025)

5 Trusted Transition to PQC



PQC transition must be handled with care across protocols, systems, and applications. Unlike a typical cryptographic upgrade, migrating to PQC introduces new algorithmic structures, key formats, and memory management requirements. Poorly managed transitions may unintentionally introduce vulnerabilities and undermine the purpose of the transition. Manual configurations, inconsistent key handling, and weak documentation are sources of new vulnerabilities from the transition process.

Trusted transition refers to the disciplined and secure migration from classical cryptography to PQC. It involves careful consideration of side-channel resistance, memory safety, and protocol compatibility. To ensure system-wide integrity, the process must incorporate formal verification, consistent coding practices, and continuous validation through static/dynamic analysis. A trusted transition demands disciplined implementation, secure protocol integration, mature tooling, and operational governance. It is challenging to apply such a principle to newly developed PQC algorithms with larger keys and ciphertexts.

ENISA provides general and practical guidance on integrating PQC into modern security protocols[18]. Mechanisms for PQC-integrated protocols, for example, Key Exchange in TLS 1.3[19], have been proposed, addressing negotiation, fallback, and resilience. IBM highlights the operational complexities of the transition and raises concerns about architecture, automation, and governance during the procedure[20]. However, the robustness of the PQC transition needs to be considered for each environment.
It is therefore important to develop the capability for trusted quantum-safe systems. For example, CSIRO has developed the MIKA method that promotes the reuse of existing implementations when incorporating new PQC algorithms[21]. It analyses cryptographic protocols and system implementation, and can provide solutions from infrastructure to applications to minimise the likelihood of introducing new vulnerabilities. To ensure a trusted transition, organisations are encouraged to collaborate with cryptography and cybersecurity domain expert.

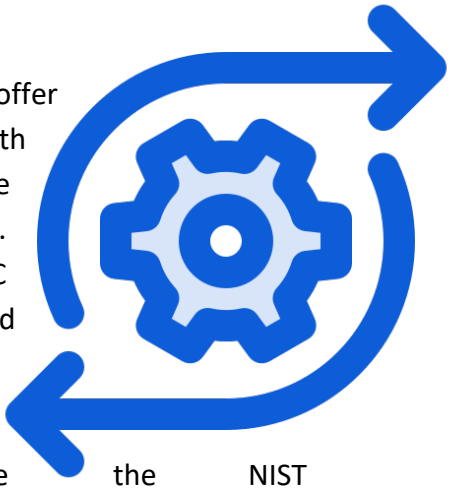
[18] Daniel J. Bernstein, Andreas Hülsing, Tanja Lange: Post-Quantum Cryptography – Integration Study, https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

[19] Douglas Stebila, Scott Fluhrer, Shay Gueron: Hybrid Key Exchange in TLS 1.3, https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

[20] Ray Harishankar, et al.: Crypto-Agility and Quantum-Safe Readiness, https://www.ibm.com/quantum/blog/crypto-agility

[21] R. K. Zhao, et al.:, MIKA: A Minimalist Approach to Hybrid Key Exchange, 21st Annual International Conference on Privacy, Security and Trust (PST 2024).

6 Hybrid Classical and Post-Quantum Cryptography



Hybrid classical and post-quantum cryptography (PQC) schemes offer intermediate solutions during the transition to PQC by employing both classical algorithms and PQC algorithms. It ensures that if one algorithm is compromised, the other may still safeguard the data. Hybrid schemes provide robust solutions for a multi-phased PQC migration process, enabling incremental deployment and interoperability between legacy systems and new PQC components.

The hybrid approach increases system development and configuration complexity and incurs computational overhead. While the NIST supports the hybrid approach as a transitional solution[22] and ASD is neutral on hybrid solutions[23], the National Security Agency (NSA) has raised concerns about its complexity and potential for introducing new vulnerabilities[24,25]. Therefore, hybrid approaches must be adopted with rigorous evaluation and careful system design.

Hybrid approaches have been designed for IKEv2 as an IETF standard for VPN security [26] and for TLS 1.3 in securing Web applications[27]. Hybrid digital signatures are also being incorporated into hardware security modules to strengthen authentication mechanisms[28]. However, these new hybrid approaches have not been widely adopted, and applications may have their specific functional and performance requirements for hybrid approaches.

Hybrid approaches appear to be a suitable path forward, given the maturity of the PQC algorithms and protocols. For example, CSIRO has designed a new hybrid IPSec architecture that minimises code modification to reduce new vulnerabilities and has implemented and evaluated hybrid TLS and hybrid IKEv2 on a physical 5G testbed[29]. This requires expertise in designing hybrid protocols and algorithms, analysing the security, strengths, and weaknesses of hybrid solutions, and providing implementation and evaluation capability.

---

[22] Dustin Moody et al.: Transition to Post-Quantum Cryptography Standards, https://csrc.nist.gov/pubs/ir/8547/ipd

[23] https://defencescienceinstitute.com/wp-content/uploads/2025/10/Planning-for-post-quantum-cryptography-September-2025.pdf

[24] https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[25] https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF

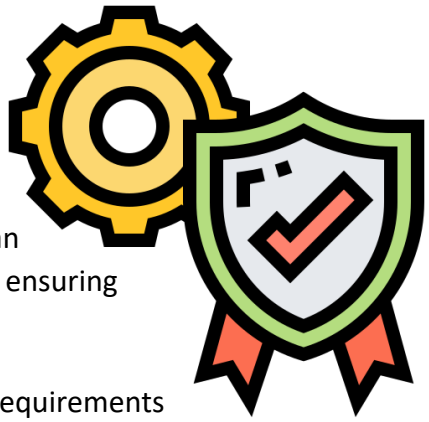
[26] C. Tjhai, et al.: Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2), https://datatracker.ietf.org/doc/rfc9370/

[27] Thom Wiggers, et al.: KEM-based Authentication for TLS 1.3, https://datatracker.ietf.org/doc/draft-celi-wiggers-tls-authkem/

[28] Diana Ghinea, et al.: Hybrid Post-quantum Signatures in Hardware Security Keys. ACNS Workshops 2023: 480-499

[29] Dongxi Liu, et al.: Post-Quantum Cryptography Migration of a Physical 5G Testbed, ACM 2025 Workshop on Quantum-Resistant Cryptography and Security (QRSec 2025).

7 High Assurance Implementation



PQC algorithms approved by NIST are theoretically secure. The practical deployment of PQC algorithms must consider the trust and security of implementations[30]. In particular, high assurance implementation means that the implementation should be robust, reliable, and secure by design in software architecture, so it can resist real-world threats such as side-channel attacks while ensuring compliance with NIST standards and detecting misconfigurations.

Achieving high assurance is challenging due to heterogeneous requirements and constrained resources. Cyber-physical systems often cannot accommodate PQC algorithms with large keys and ciphertexts, creating risks such as buffer overflow. While open-source PQC libraries are valuable for development and testing, they need to be fully evaluated for production. Adapting trusted implementation to new applications could introduce unforeseen vulnerabilities.

NIST-approved PQC algorithms are being implemented in the open-source library liboqs[31] or in formally verified library libcrux[32]. For particular PQC deployment environments, it is desirable that such open-source implementations are analysed, including their formal verification methods, according to a more comprehensive set of principles of high-assurance implementation.

Building sovereign implementation with high assurance is an important step in the quantum-safe transition. To achieve this, CSIRO has implemented quantum-safe protocols on a 5G testbed, with a focus on end-to-end quantum-safe security, and has formally verified the 5G AKA protocol[33]. This requires designing the software architecture for cryptographic systems, following high-assurance development principles, formal verification of protocols, carrying out implementation and evaluations with verifiable properties, and auditing existing implementations.

---

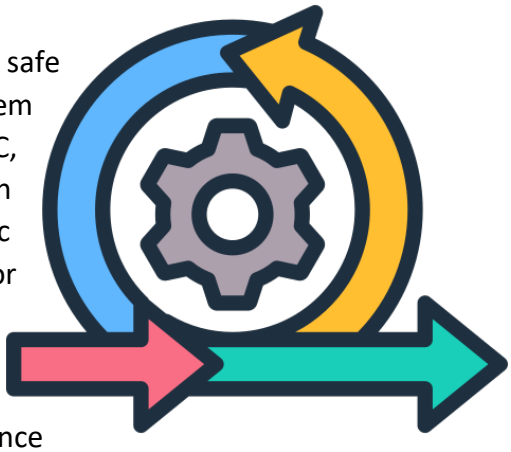
[30] Gorjan Alagic, et al: Recommendations for Key-Encapsulation Mechanisms, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.pdf

[31] https://github.com/open-quantum-safe/liboqs

[32] https://bughunters.google.com/blog/6038863069184000/formally-verified-post-quantum-algorithms

[33] Nazatul Sultan. et al: Active Attack Resilience in 5G: A New Take on Authentication and Key Agreement, 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'25)

8 Crypto Agility and Modernisation



Crypto-agile systems aim for modular and flexible designs to allow safe integration with new PQC components without changing system architecture and implementation. During the transition to PQC, crypto agile systems support dynamic algorithm selection based on operational context, facilitate the addition of new cryptographic primitives, and enable the deprecation or rollback of insecure or problematic algorithms without disrupting core functionality.

A well-established, systematic approach or principles for crypto agility are currently lacking[34,35], presenting the major challenge. Since cryptographic algorithms are rarely upgraded, existing software architectures often lack the modularity, independence, and abstraction needed for cryptographic agility. Designing crypto-agile systems requires carefully balancing competing factors, development efficiency, system performance, ease of configuration, and adaptability.

NIST has proposed strategies for achieving crypto agility[36], outlining the principles of crypto agility for security protocols and applications. It also recommended integrating a cryptographic agility strategic plan into an organisation's existing cybersecurity governance framework. These strategies provide a valuable starting point for planning crypto agility. The utilisation of such strategies must be tailored to the organisation's requirements.

Building crypto agile systems requires comprehensive expertise in cryptographic engineering, system design, and software development. For example, CSIRO has already explored system architectures that combine new protocols for quantum-safe VPNs with minimal modifications[37]. Other features needed in such a system include managing existing cryptographic assets, developing software architecture and protocols to support crypto agility, and defining strategies to modernise cryptographic assets.

[34] David Ott, Kenny Paterson, Dennis Moreau: Where Is the Research on Cryptographic Transition and Agility? Commun. ACM 66(4): 29-32 (2023)

[35] Ray Harishankar, et al.: Crypto-Agility and Quantum-Safe Readiness, https://www.ibm.com/quantum/blog/crypto-agility

[36] Elaine Barker, et al.: Considerations for Achieving Crypto Agility - Strategies and Practices, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.2pd.pdf

[37] R. K. Zhao, et al.:, MIKA: A Minimalist Approach to Hybrid Key Exchange, 21st Annual International Conference on Privacy, Security and Trust (PST 2024).

9 Test and Validation of PQC Systems

Deploying PQC algorithms or PQC-integrated security protocols in real-world applications at scale requires rigorous evaluation to ensure not only theoretical security but also practical reliability and performance. Additionally, validation is necessary to confirm that implementations comply with the PQC algorithm specifications and are properly configured. Test and validation can cover both software and hardware implementation[38]. Regulators should establish clear validation policies, and organisations ensure their PQC systems are properly tested and validated by themselves or vendors.

PQC algorithm can be deployed in diverse scenarios with different protocols like VPN and HTTPS, and resource-constrained IoT. Each scenario may require its own specific evaluation method and environment, which must consider the large PQC keys/ciphertexts and complexity of the hybrid solution[39]. Moreover, PQC lacks mature frameworks for verifying protocol correctness[40] and resistance to SCAs, making rigorous testing essential before deployment.

Several initiatives are actively addressing the practical challenges of PQC test and validation. NIST's CAVP (Cryptographic Algorithm Validation Program) certifies the compliance of the implementation of PQC algorithms. The Open Quantum Safe (OQS) project[41] provides a test framework for benchmarking and integrating PQC algorithms into protocols such as TLS and SSH. These solutions do not ensure reliability and performance from a system perspective. A compliant implementation can still cause a buffer overflow problem due to the use of large ciphertext sizes.

This task demands experience and expertise in designing and testing PQC algorithms and protocols on sophisticated physical testbeds (e.g., 5G testbeds) and the Integration of PQC into protocols such as EDHOC. For example, CSIRO has provided end-to-end cryptographic protocol and system test and evaluation (e.g., critical infrastructure, IoT, embedded systems)[42], formal security verification using tools (e.g., EasyCrypt, ProVerif, and Tamarin)[43], algorithm and protocol compatibility validation[44], standardisation and compliance support.

---

[38] Prasanna Ravi, et al.: Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results. ACM Trans. Embed. Comput. Syst. 23(2): 35:1-35:54 (2024)

[39] Lukas Malina, et al.: On Deploying Quantum-Resistant Cybersecurity in Intelligent Infrastructures. ARES 2023: 131:1-131:10

[40] Yuexi Xu, at al.: Formal Verification Techniques for Post-quantum Cryptography: A Systematic Review. ICECCS 2024: 346-36

[41] https://openquantumsafe.org/

[42] Dongxi Liu, et al.: Post-Quantum Cryptography Migration of a Physical 5G Testbed, ACM 2025 Workshop on Quantum-Resistant Cryptography and Security (QRSec 2025).

[43] Nazatul Sultan. et al: Active Attack Resilience in 5G: A New Take on Authentication and Key Agreement, 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'25)

[44] Sarah Ali Siddiqui, et al.: TELSAFE: Security Gap Quantitative Risk Assessment Framework. CoRR abs/2507.06497 (2025)

10 Conclusion

The transition to post-quantum cryptography is no longer a theoretical concern but an urgent strategic necessity. While quantum computers capable of breaking today's cryptography may not exist yet, the "harvest now, decrypt later" threat is already shaping adversarial behaviour. This technical report has outlined eight critical technical domains—spanning guidelines, asset discovery, risk assessment, trusted migration, hybrid solutions, high-assurance implementation, crypto agility, and testing—that together provide a roadmap for a safe and resilient transition. These domains can be further expanded to meet the needs of large organisations or tailored to the capacities of SMEs.

Success will depend on early preparation, strong collaboration between government, industry, and academia, and investment in sovereign research and development. Transitioning securely requires not just adopting new algorithms, but embedding assurance, agility, and resilience across entire systems. Organisations that act now will be better positioned to safeguard sensitive data and critical infrastructure. Quantum-safe transition is not merely a defensive necessity; it is a chance to modernise digital infrastructure, build trust, and strengthen national resilience in the face of disruptive technological change.

As Australia's national science agency and innovation catalyst, CSIRO is solving the greatest challenges through innovative science and technology.

CSIRO. Unlocking a better future for everyone.

Contact us

1300 363 400
+61 3 9545 2176
csiro.au/contact
csiro.au

For further information

D**ata61**
Surya Nepal
+61 2 9272 4256
surya.nepal@csiro.au
csiro.au/Data61