Cryptography in a Post-Quantum World

How organizations can safeguard against the looming quantum threat and prevent today's encrypted data from being tomorrow's biggest vulnerability

Abstract: Quantum computers are not yet able to crack encryption keys, but "Q-Day" is likely to arrive in the coming years. In the meantime, there's the risk of harvest now, decrypt later (HDNL). In preparation, the US government and various standards bodies are actively pursuing solutions for post-quantum cryptography (PQC). This paper sets out several core concepts that one needs to know to navigate the process of preparing for PQC, with an emphasis on steps you can take today to help ensure a secure future.

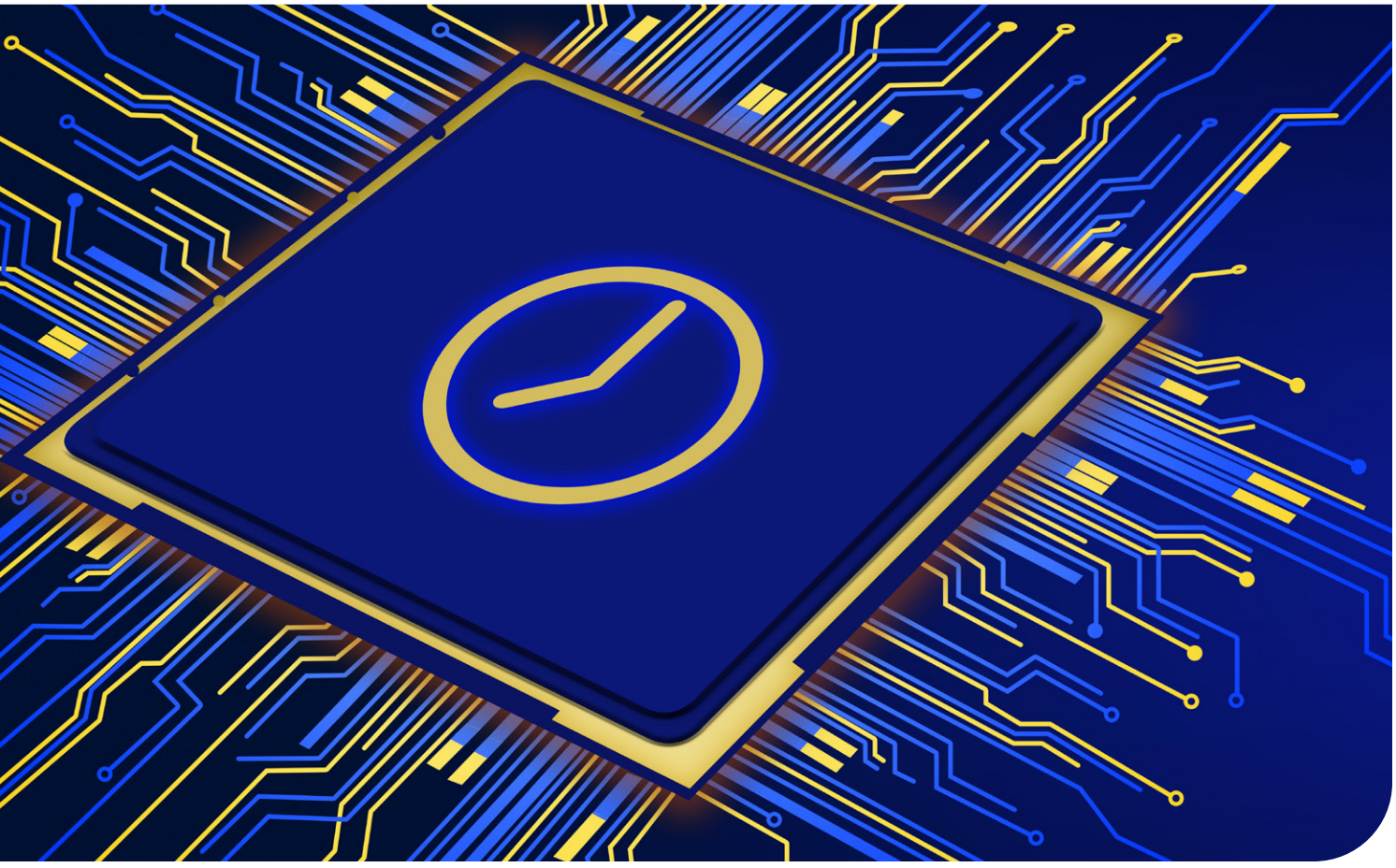
Contents

Introduction

Cryptanalytically relevant quantum computing (CRQC) is a quantum computer capable of breaking all public-key cryptography systems in operation today. This existential threat to data security known as “Q-Day” has not yet arrived as current quantum computers are not nearly powerful enough. However, many experts believe it’s just a matter of time before CRQCs become a reality.

Governments and forward-thinking organizations are already preparing for post-quantum cryptography (PQC). They are actively following guidelines for the quantum-resistant algorithms, such as those recently released by the US National Institute of Standards and Technology (NIST). It’s a complicated topic to be sure.

This paper sets out several core concepts to help you better understand and navigate the process as you prepare for PQC, with an emphasis on network infrastructure, which is not typically the focus of dialogues around quantum security



The Quantum Threat: Q-Day and Harvest Now, Decrypt Later

Quantum computers use the principles of quantum mechanics to solve complex problems that are well beyond the capabilities of today's classical computers. Instead of conventional bits representing either 0 or 1, quantum computers are based on qubits, subatomic particles that can be both 0 and 1 simultaneously, enabling them to process an incredible amount of information at once.

It is not necessary to understand the underlying science to grasp the potential significance and threat of quantum computing. When you use a computer or network device, you expect it to be trustworthy and operate as expected, without malware or other unauthorized changes. Cisco pushes to meet these expectations through its Trustworthy Solutions, an integrated set of policies, processes, and technologies to help ensure code running on Cisco hardware is authentic and unmodified, with unique device identity and validation of all levels of software, establishing a chain of trust for the entire system. Much of this relies on state-of-the-art cryptography, such as RSA-2048, which is considered invulnerable against brute force attacks using today's classical computers. Unfortunately, a cryptanalytically relevant quantum computer (CRQC), when it becomes viable, could crack RSA-2048 in a matter of minutes.

Quantum computing at this level of power does not exist and may still be years away. When the moment arrives, however, Q-Day will be a cybersecurity disaster for organizations that did not prepare for this eventuality. There is an additional and more immediate concern: the possibility that malicious actors could exfiltrate your encrypted data today, then use quantum computers to decrypt that data when CRQC becomes viable in the future. This is known as "harvest now, decrypt later" (HNDL). Given the prevalence of large-scale data breaches by foreign governments, it's not difficult to imagine the risk exposure inherent in HNDL.

Government and Standards Bodies Respond to the Threat

The US government recognizes the seriousness of the quantum threat and the potential risks to national security inherent in Q-Day and HNDL. The Biden administration issued an Executive Order (EO) and National Security Memorandum (NSM) in 2022 to address the problem. The NSM directed the National Institute of Standards (NIST) to "publish new quantum-resistant cryptographic standards that can protect against these future attacks."

This process, which involved contributions from numerous scientists and institutions worldwide, culminated in the publication of three quantum-safe encryption algorithms in 2024. These algorithms are part of new quantum-resistant Federal Information Processing (FIPS) standards.

The National Security Agency (NSA), working in parallel, issued a requirement that all companies and government agencies working with National Security Systems (NSS) implement accepted quantum-safe encryption by 2030, with preferred availability in 2026 for network devices. The NSA specified the methods for realizing this goal in its Commercial National Security Algorithm (CNSA) version two (CNSA 2.0), which the agency published in 2022.

Technically speaking, the NIST and NSA standards only apply to entities that need to be FIPS compliant or work on NSS. However, for practical reasons, many organizations in both the private and public sector are pursuing the adoption of these standards, even if they are not mandated. Financial institutions, for example, feel an urgent need to be quantum safe, even if the government hasn't yet required it of them.

The NIST Algorithms

NIST, which had been working on standardizing PQC countermeasures for six years prior to the EO and NSM, has settled on three post-quantum encryption algorithms in two distinct categories: general encryption and digital signatures.

- **The CRYSTALS-Kyber** algorithm (renamed ML-KEM by NIST) is for general encryption, e.g., for securing websites. CRYSTALS-Kyber is a "lattice-based" Key Encapsulation Mechanism (KEM) which uses highly complex mathematical structured lattice equations to create patterns of encryption that cannot be broken, even by a quantum computer. NIST selected CRYSTALS-Kyber partly due to its use of relatively small keys that can be easily exchanged. CRYSTALS-Kyber also operates at high speed, which is advantageous for most workloads.
- **CRYSTALS-Dilithium and SPHINCS+** are for digital signatures, e.g., used to verify identities. CRYSTALS-Dilithium algorithm was renamed ML-DSA by NIST, standing for Module-Lattice-Based Digital Signature Algorithm. Based on early reactions to the NIST publication, it is probable that the lattice-based CRYSTALS-Dilithium will emerge as the predominant standard. SPHINCS+, renamed SLH-SSA by NIST, uses hashes to create a quantum safe mode of encryption.

These three algorithms are now part of FIPS encryption standards for PQC. FIPS 203, which is seen as the general standard for PQC, is based on ML-KEM. FIPS 204, which is for protecting digital signatures, uses ML-DSA. FIPS 205, also for digital signatures, uses SPHINCS+ or Stateless Hash-Based Digital Signature Algorithm (SLH-DSA).

The Impact and Timeline of CNSA 2.0

The NSA's CNSA 2.0 defines the PQC algorithms and timeline requirements for products used in NSS. There's a lot to CNSA 2.0. For the sake of simplicity, be aware that CNSA 2.0 requires algorithms that cover:

- **Signatures for firmware and software:** Leighton-Micali Signatures (LMS) and Extended Merkle Signature System (XMSS), which are stateful and hash-based. CNSA 2.0 now also allows ML-DSA-87 for this purpose.
- **Signatures for identity and authentication**, i.e., general purpose: ML-DSA-87, which is the level 5 security parameter set for ML-DSA.
- **Bulk encryption/decryption:** AES-256
- **General system-wide hashing:** Secure hash algorithm (SHA)-384 or SHA-512 for hashing functions.

CNSA 2.0 specifies a timeline for adoption. The year 2030 is the "must have" date, but the NSA has said that it prefers for NSS to be protected perhaps as soon as 2027. As the chart below shows, PQC image signing and verification have a preferred adoption date of 2025. For network devices, it's 2026.

	Preferred date of adoption	Required date of adoption
PQC image signing and verification	CY 2025	CY 2030
Network Devices	CY 2026	CY 2030

Challenges to Implementation

Industry consensus is favorable toward the new NIST PQC standards and CNSA 2.0. Stakeholders recognize that these algorithms represent the best countermeasures against the quantum threat. Challenges are apparent, however, most notably regarding the implementation timeframe. FIPS certification, for instance, can take up to two years or more. If an organization is concerned about HNDL, that's a long time to wait. Similarly, with the rigorous testing envisioned for the new algorithms, adoption could be quite slow, compared with the urgency of mitigating HNDL risks as quickly as possible.

Emerging Solutions and Best Practices for PQC

Solutions and best practices for PQC are emerging as the details and timelines of mandated standards have become clear. They offer an approach to quantum safe encryption that addresses the risks inherent in waiting for FIPS certification as well as testing and adoption of the NIST standards.

In the near term, deal with the transport layer– One best practice is to establish a priority for PQC implementation based on risk. Given the HNDL threat, it makes sense to move as quickly as possible to protect the most sensitive data first. In practical terms, this means combining legacy cryptographic methods with alternate quantum-safe methods for provisioning bulk encryption keys (see *Protecting Yourself Today*). Migrate to PQC-based solutions once they become available (see *Protecting Yourself Tomorrow*).

Then, implement quantum safe computing in hardware–It will take longer to deploy quantum-resistant modes of encryption in network hardware, such as secure boot, authenticated firmware updates, and device identity. While many Cisco devices already include critical quantum-safe protections (such as LDWM for Secure Boot), no hardware exists today that is compliant with CNSA 2.0 algorithms. It is, therefore, recommended that organizations consider including quantum-safe hardware into their product refresh cycles as they become available.

Protecting Yourself Today

Networks provide foundational protection from bad actors by using secure transport protocols (e.g., IPsec, MACsec, and TLS). These protocols use symmetric cryptography algorithms to encrypt and decrypt information. Symmetric cryptography is quantum safe if the keys used are of sufficient size and quality (such as with AES-256). Unfortunately, asymmetric cryptography is used to establish these keys and quantum computers are well-suited to breaking asymmetric key pairs. Therefore, organizations should assess the risk and impact of a harvest now, decrypt later attacks and begin work to protect their most sensitive data.

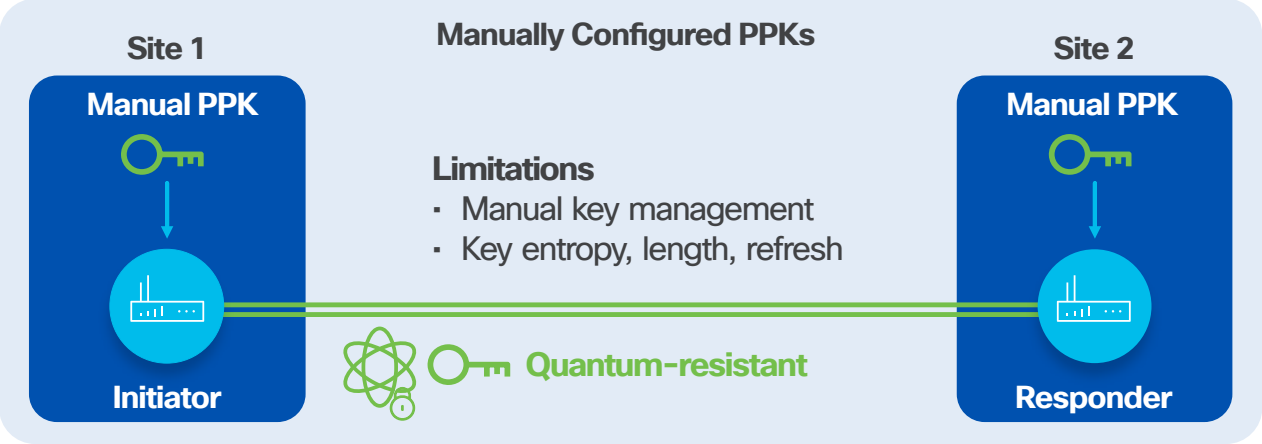
One solution is to use an alternative method for obtaining the keys used to encrypt/decrypt data—one that doesn't rely on asymmetric cryptography. There are three methods for accomplishing this today:

- Manually pre-provisioned keys
- Quantum Key Distribution (QKD) systems
- Integrated Key Management Services (KMS)

Each of these methods produce Postquantum Pre-shared Keys (PPK) to ensure that currently encrypted traffic is safe against an HNDL attack.

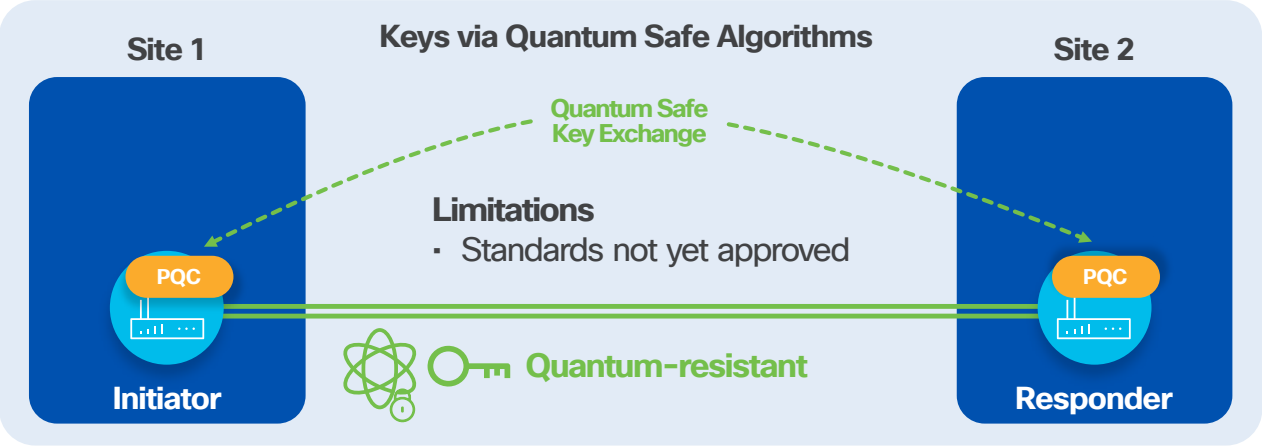
Manually pre-provisioned keys

Here, an operator or network management system configures network devices with a quantum-safe key using existing technology. Simplicity and speed of deployment are two advantages of this approach. However, relying on manual processes can lead to "key entropy" and potentially risk key exposure.



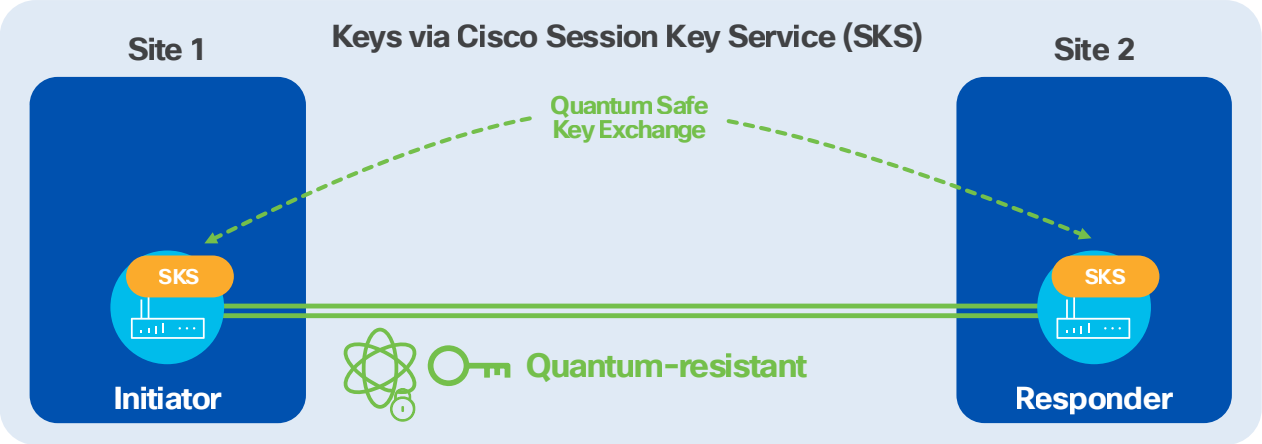
Quantum Key Distribution (QKD) systems

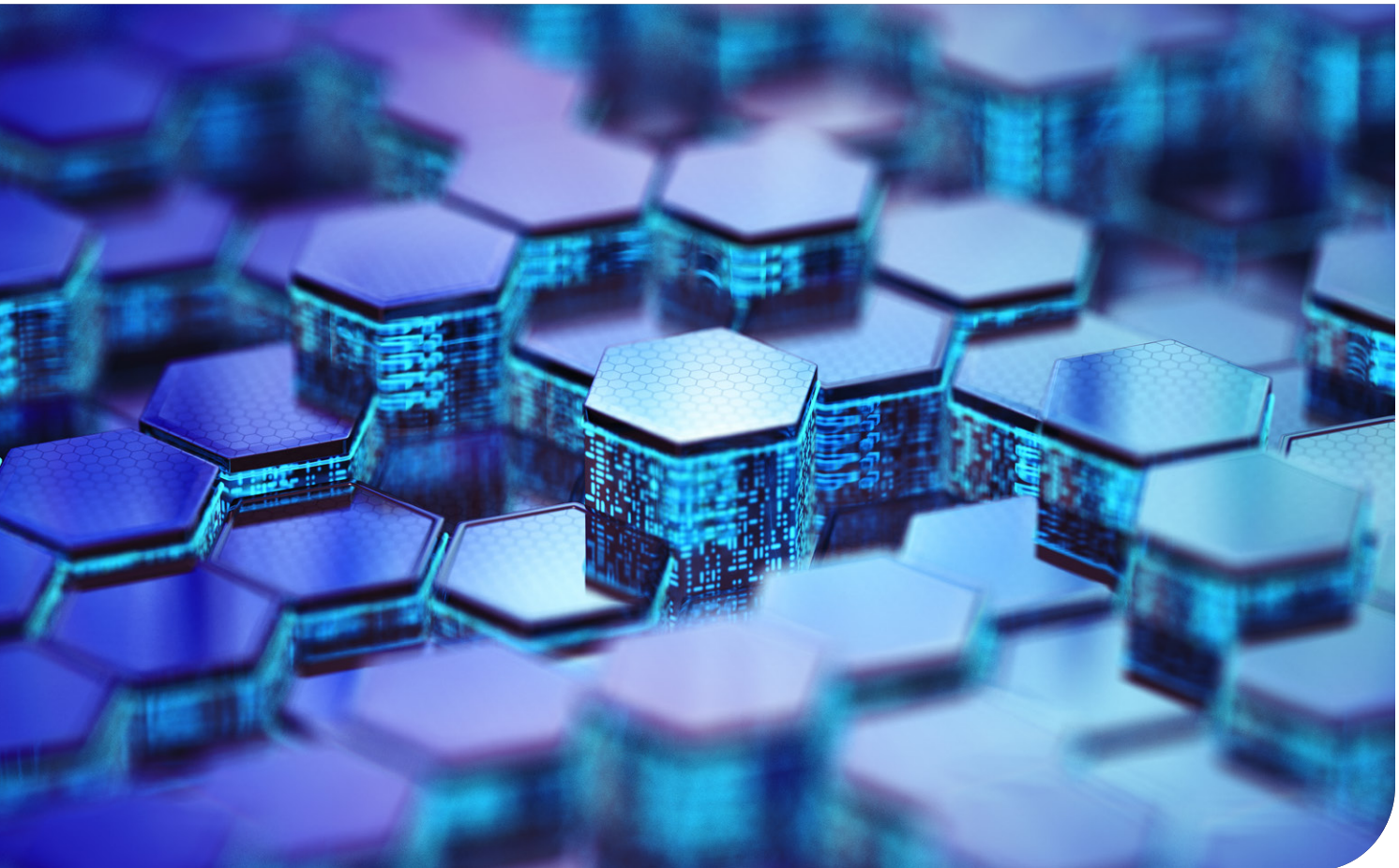
QKD uses an external key management system to create quantum-safe keys. Network devices can request keys on demand through the Secure Key Integration Protocol (SKIP) API. While a QKD infrastructure includes added expense and complexity, there are numerous QKD offerings available in the market.



Integrated Key Management Services (KMS)

As the name suggests, KMS is a service integrated in the network device itself that provides quantum-safe keys on demand. While no additional infrastructure is required, there are a limited number of KMS-enabled products on the market. The Cisco KMS offering is called Session Key Service (SKS).





Protecting Yourself Tomorrow

PQC-based solutions using multiple (hybrid) or native (single) key exchange methods are being developed now, with many solutions becoming available in 2025.

To ensure continued security in the face of the quantum risk, traditional cryptographic protocols such as Internet Security Protocol (IPsec), Transport Layer Security (TLS), and Secure Shell (SSH) are evolving to incorporate PQC algorithms—a critical adaptation to help protect against HNDL attacks sooner rather than later.

- **Internet Security Protocol (IPsec)**—The Internet Key Exchange version 2 (IKEv2) tunneling protocol, which is based on IPsec, establishes a secure connection between devices using multiple keys. Specific IKEv2 standards include RFC 9730, which enables multiple key exchanges, RFC 9242, the Intermediate Exchange, which uses IKEv2 for transmission of the large amounts of data, and the draft post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2, which defines profiles for using ML-KEM with RFCs 9370/9242.
- **Transport Layer Security (TLS)**—The draft Hybrid key exchange standard in TLS 1.3 simultaneously uses multiple key exchange algorithms to ensure quantum-safe encryption even if all but one of the component algorithms are broken.
- **Secure Shell (SSH)**—The draft Post-quantum Hybrid Key Exchange standard in SSH uses Elliptic Curve and ML-KEM schemes as key exchange methods with the goal of creating a discrete algorithm problem that is computationally impossible for hackers to crack, even using quantum computers.

Multiple key exchange is required for IPsec and many in the industry, including Google, currently support it for TLS. Beyond the issue of interoperability with these vendors, Cisco and other industry leaders believe it prudent, at least initially, to use multiple key exchanges for transport protocols for the following reasons:

1. While the PQC algorithms are believed to be solid, the software implementations and associated protocols are new. Even though they will be well tested, new vulnerabilities are typically uncovered over time. By using multiple (or hybrid) key exchanges, you will have fallback protection with the legacy key exchange in the event there is an issue with the PQC implementation.
2. Many organizations require products used in their environment be FIPS certified, however, as stated earlier, the current average time to complete FIPS certification of the PQC algorithms is two years or more. A hybrid approach using a FIPS-certified legacy crypto algorithm for the initial key eliminates this delay.

Conclusion

While no one truly knows when Q-Day will arrive, organizations are advised to assess their risk and, if needed, prioritize quantum-safe measures to mitigate the immediate threat of harvest now, decrypt later (HNDL) attacks. Solutions exist today that provide this protection while the security sector waits for PQC-based solutions to become available. To begin, it's essential to protect your most sensitive data by implementing hybrid cryptographic transport protocol solutions that combine legacy encryption with quantum-resistant algorithms. This allows for quicker FIPS-certified deployment while maintaining security in the event that future vulnerabilities are discovered in the new PQC algorithm.

Additionally, organizations should evaluate and invest in quantum-safe hardware and consider including it in their product refresh cycles as they become available. Evolving standards here include unique device identity certificates. Industry availability for PQC-capable hardware components such as CPUs and TPMs is also evolving. By acting swiftly and strategically, companies can safeguard against both current and future quantum computing threats.

You can learn more about Cisco post-quantum cryptography capabilities on the Cisco Trust Center