NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper
Computer Security Division
Information Technology Lab

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

November 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

How to Cite this NIST Technical Series Publication
Moody D, Perlner R, Regenscheid A, Robinson A, Cooper D (2024) Transition to Post-Quantum Cryptography Standards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8547 ipd. https://doi.org/10.6028/NIST.IR.8547.ipd

Author ORCID iDs
David Cooper: 0009-0001-2410-5830
Dustin Moody: 0000-0002-4868-6684
Ray Perlner: 0000-0001-8793-2238
Andrew Regenscheid: 0000-0002-3930-527X
Angela Robinson: 0000-0002-1209-0379

Public Comment Period
November 12, 2024 – January 10, 2025

Submit Comments
pqc-transition@nist.gov
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8547/ipd, including related content, potential updates, and document history.

Abstract

This report describes NIST's expected approach to transitioning from quantum-vulnerable cryptographic algorithms to post-quantum digital signature algorithms and key-establishment schemes. It identifies existing quantum-vulnerable cryptographic standards and the quantum-resistant standards to which information technology products and services will need to transition. It is intended to foster engagement with industry, standards organizations, and relevant agencies to facilitate and accelerate the adoption of post-quantum cryptography.

Keywords

cryptography; post-quantum cryptography; public key cryptography; quantum computing.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: pqc-transition@nist.gov

Table of Contents

List of Tables

1. Introduction

Cryptographic algorithms are vital for safeguarding confidential electronic information from unauthorized access. For decades, these algorithms have proved strong enough to defend against attacks using conventional computers that attempt to defeat cryptography. However, future quantum computing may be able to break these algorithms, rendering data and information vulnerable. Countering this future quantum capability requires new cryptographic methods that can protect data from both current conventional computers and the quantum computers of tomorrow. These methods are referred to as *post-quantum cryptography* (PQC).

In response, NIST has released three PQC standards to start the next and significantly large stage of working on the transition to post-quantum cryptography: the Module-Lattice-Based Key-Encapsulation Mechanism [FIPS203], the Module-Lattice-Based Digital Signature Algorithm [FIPS204], and the Stateless Hash-Based Signature Algorithm [FIPS205]. Historically, the journey from algorithm standardization to full integration into information systems can take 10 to 20 years. This timeline reflects the complexity of companies building the algorithms into products and services, procuring those products and services, and integrating those products and services into technology infrastructures.

Even though the transition to post-quantum cryptography is starting before a cryptographically relevant quantum computer has been built, there is a pressing threat. Encrypted data remains at risk because of the “harvest now, decrypt later” threat in which adversaries collect encrypted data now with the goal of decrypting it once quantum technology matures. Since sensitive data often retains its value for many years, starting the transition to post-quantum cryptography now is critical to preventing these future breaches. This threat model is one of the main reasons why the transition to post-quantum cryptography is urgent.

1.1. Scope and Purpose

Updating cryptographic technology has occurred many times at different scales, such as increasing key sizes or phasing out insecure hash functions and block ciphers. While the transition to PQC is unprecedented in scale, it benefits from a level of awareness and understanding that previous cryptographic changes did not have. NIST recognizes the complexity of migrating the vast array of systems that currently rely on public-key cryptography and acknowledges that this transition will demand substantial effort across diverse applications and infrastructures with specific requirements and constraints.

This report serves as the initial step in a broader strategy to manage and guide the transition to post-quantum cryptography. This transition will involve the adoption of new PQC algorithms as well as the careful deprecation, controlled legacy use, and eventual removal of quantum-vulnerable algorithms that are currently widespread in technological infrastructures. Public-private engagement will be crucial on the path toward PQC. Additionally, this report continues NIST’s ongoing dialogue with industry, standards organizations, and relevant agencies to develop a clear roadmap and realistic timeline for transitioning to PQC. NIST is committed to

ensuring that this transition is as smooth and coordinated as possible, balancing the urgency of adopting PQC with the need to minimize disruption across critical systems.

1.2. Audience

This document is intended for a broad audience, including federal agencies, technology providers, standards organizations, and Cryptographic Module Validation Program (CMVP) laboratories. These groups play a critical role in preparing for the migration to PQC by developing, implementing, and standardizing the new cryptographic methods necessary to secure information in the era of quantum computing. This document should inform these stakeholder's efforts and timelines for migrating information technology products, services, and infrastructure to PQC.

2. Background

2.1. Cryptographic Standards

Federal Information Processing Standards (FIPS) and the NIST Special Publication (SP) 800-series specify a broad set of cryptographic primitives, algorithms, and schemes, including many public-key cryptosystems that will be deprecated and ultimately disallowed as part of the transition to post-quantum cryptography. This section identifies quantum-vulnerable algorithms in NIST's existing cryptographic standards as well as the post-quantum algorithm standards that have been recently published. Section 4.1 provides the transition plan for the quantum-vulnerable algorithms in these standards.

2.1.1. Digital Signature Algorithms

Digital signature algorithms are used to provide identity authentication, integrity authentication, source authentication, and support for non-repudiation. Digital signature algorithms are used in conjunction with hash functions or eXtendable-Output Functions (XOFs) to sign messages of arbitrary length.

NIST-approved digital signature algorithms were historically specified in FIPS 186 [FIPS186]. The current revision of FIPS 186 specifies the Elliptic Curve Digital Signature Algorithm (ECDSA) and adopts the RSA algorithm specified in RFC 8017 and PKCS 1 (version 1.5 and higher) and the Edwards-Curve Digital Signature Algorithm (EdDSA) specified in RFC 8032. The related SP 800-186 [SP800186] specifies the elliptic curves to be used with ECDSA and the elliptic curve cryptography (ECC) based key establishment schemes in SP 800-56A [SP80056A]. These algorithms are vulnerable to Shor's Algorithm on a cryptographically relevant quantum computer.

FIPS 204 and 205 each specify quantum-resistant digital signature schemes. FIPS 204 specifies the Module-Lattice-Based Digital Signature Algorithm (ML-DSA) [FIPS204], which is derived from the CRYSTALS-Dilithium submission. FIPS 205 specifies the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), which is derived from the SPHINCS+ submission [FIPS205].

SP 800-208, *Recommendation for Stateful Hash-Based Signature Schemes,* specifies two stateful hash-based signature (HBS) schemes — the Leighton-Micali Signature (LMS) system and the eXtended Merkle Signature Scheme (XMSS) — along with their multi-tree variants, the Hierarchical Signature System (HSS) and multi-tree XMSS (XMSS^{MT}) [SP800208]. These schemes are also resistant to attacks by quantum computers. In stateful hash-based signature (HBS) schemes, the HBS private key consists of a large set of one-time signature (OTS) private keys. The security of these schemes relies on the signer to ensure that no individual OTS key is ever used to sign more than one message. Due to this need to maintain state, HBS schemes are not intended for general use.

In the future, NIST intends to develop a FIPS that specifies a digital signature algorithm derived from FALCON as an additional alternative to these standards. In addition, NIST is evaluating other proposed digital signature algorithms for possible standardization through the Additional

Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process [NISTIR8528].

2.1.2. Key Establishment

Key establishment is the means by which keys are generated and provided to the entities that are authorized to use them. Current NIST-approved key-establishment schemes are specified in SP 800-56A, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm-Based Cryptography* [SP80056A], and SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography* [SP80056B].

SP 800-56A specifies key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-Qu-Vanstone (MQV) key establishment schemes.

SP 800-56B specifies key-establishment schemes based on the RSA public key cryptosystem. This publication includes approved methods for both key agreement and key transport.

FIPS 203 specifies a cryptographic scheme called Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), which is derived from the CRYSTALS-KYBER submission. A key-encapsulation mechanism (KEM) is a particular type of key-establishment scheme that can be used to establish a shared secret key between two parties communicating over a public channel. The fourth round of the NIST PQC Standardization process is evaluating additional KEM algorithms, and NIST anticipates selecting one or more alternatives to ML-KEM in the future.

2.1.3. Symmetric Cryptography

Symmetric-key algorithms (sometimes called secret-key algorithms) use a single key to both apply cryptographic protection and to remove or check the protection (i.e., the same key is used for a cryptographic operation and its inverse). For example, the key used to encrypt data (i.e., apply protection) is also used to decrypt the encrypted data (i.e., remove the protection). In the case of encryption, the original data is called the plaintext, while the encrypted form of the data is called the ciphertext. The key must be kept secret if the data is to remain protected. Several classes of symmetric-key algorithms have been approved: those based on block cipher algorithms (e.g., AES) and those based on the use of hash functions (e.g., a keyed-hash message authentication code based on a hash function).

Symmetric-key algorithms are used for:

- Block ciphers
- Hash functions
- Encryption using block cipher modes of operation
- Data authentication using block cipher modes of operation
- Data authentication using key-hash constructions

- Key derivation
- Key wrapping
- Random bit generation

As discussed in Sec. 4.1.3, the existing algorithm standards for symmetric cryptography are less vulnerable to attacks by quantum computers. NIST does not expect to need to transition away from these standards as part of the PQC migration.

2.2. Cryptographic Technologies and Components

Once PQC algorithms have been standardized, applications will need to be modified to make use of them. Many applications include components that are based on standardized protocols and security technologies that will need to be revised to support the use of the PQC algorithms. In addition, applications are built on top of software cryptographic libraries that either provide the implementations of the cryptographic algorithms or provide an interface to hardware cryptographic modules. Any software cryptographic libraries and hardware cryptographic modules used by an application will also need to be revised to support the PQC algorithms. Applications may also rely upon infrastructure components, such as public key infrastructures (PKI), that would need to be updated to support the PQC algorithms before the applications themselves can migrate to using the PQC algorithms.

2.2.1. Network Protocol and Security Technology Standards

Network protocols and security technology standards define the rules for data exchange over networks and ensure secure and reliable communication. Examples include Transport Layer Security (TLS), Secure Shell (SSH), Internet Protocol Security (IPsec), and Cryptographic Message Syntax (CMS).

These protocols and security technologies often rely on classical cryptographic algorithms that are vulnerable to quantum attacks. Updating them to incorporate PQC algorithms is essential to maintaining data confidentiality and integrity. This involves revising protocol specifications to support new key exchange mechanisms and authentication methods that are quantum-resistant. In some cases, this will involve simply assigning an identifier for the new algorithm. In other cases, more significant changes will be required to accommodate the larger sizes of the PQC algorithms or as a result of the new algorithms having different interfaces.

2.2.2. Software Cryptographic Libraries

Software cryptographic libraries are collections of cryptographic algorithms and protocols that are implemented in software to provide essential cryptographic functions to applications. OpenSSL, BoringSSL, Libsodium, and the Java Cryptography Architecture (JCA) are a few examples of cryptographic libraries that are used to provide cryptographic support for applications.

These libraries need to incorporate PQC algorithms that are standardized by bodies like NIST. Updating them ensures that developers have access to quantum-resistant cryptographic functions without implementing complex algorithms themselves. This transition involves adding new algorithms, optimizing their implementations for performance, and ensuring those implementations are secure against side-channel attacks.

2.2.3. Cryptographic Hardware

Cryptographic hardware modules, such as hardware security modules (HSMs) and Trusted Platform Modules (TPMs), provide secure environments for performing cryptographic operations and storing sensitive keys. They are used in various applications, from securing server infrastructure to protecting cryptographic keys on personal devices.

Hardware modules must be upgraded or redesigned to support PQC algorithms, which often have larger key sizes and different computational requirements. This includes updating firmware or hardware to handle new algorithms and ensuring that the modules can perform quantum-resistant cryptographic operations efficiently while maintaining the high security standards expected of these devices.

2.2.4. PKI and Other Infrastructure Components

Public key infrastructure (PKI) systems manage digital certificates and public-private key pairs to enable secure communication and authentication across networks. Other infrastructure components include certification authorities (CAs), registration authorities, key management systems, and directory services.

PKI components must be updated to issue, distribute, and manage certificates that use PQC algorithms and to sign certificates and revocation status information using PQC algorithms. This includes supporting new cryptographic algorithms in certificate issuance processes and modifying validation and revocation mechanisms. Ensuring backward compatibility and interoperability during the transition period is crucial to maintaining trust and security across the network.

2.2.5. IT Applications and Services

IT applications and services encompass a wide array of software and platforms used by organizations, including web applications, databases, communication tools, cloud services, and enterprise software. These applications rely on cryptography for securing data, authenticating users, and ensuring secure transactions.

Applications and services must be modified to support PQC algorithms for encryption, digital signatures, and key exchange. This requires updating the underlying cryptographic implementations, adjusting to changes in key sizes and algorithm performance, and ensuring compatibility with updated protocols and libraries. Developers need to refactor code, conduct extensive testing, and potentially redesign user interfaces to accommodate these changes.

3. Migration Considerations

Even though there are no existing cryptographically relevant quantum computers that currently threaten levels of security, it will take a significant amount of time to transition to new post-quantum algorithms. Past cryptographic migrations have taken over a decade, and this more complex migration will likely take at least that long.

Mosca's theorem emphasizes the urgency of migrating to post-quantum algorithms by introducing a simple but powerful timeline: if "*X*" represents the number of years that data must be kept secure, and "*Y*" is the estimated time needed to complete the transition, then organizations must start transitioning to post-quantum algorithms before $X + Y$ exceeds the expected time Z for a cryptographically relevant quantum computer to be built. This means that even if quantum computers are a decade away, organizations must begin the migration to post-quantum cryptography today to avoid having their encrypted data exposed once quantum computers become operational in the future. This threat, often referred to as "harvest now, decrypt later," underscores the necessity of acting immediately, especially for data with long-term sensitivity, such as government secrets or medical records. Ensuring security today will safeguard it for the future.

3.1. Use Cases

3.1.1. Code Signing

Code signing involves digitally signing executables and software packages to verify the author's identity and ensure that the code has not been tampered with. This process is critical for maintaining trust in software distribution channels and preventing the spread of malicious code.

The devices that install and execute this code need the ability to verify the signatures on the code. In some cases, it is not feasible to update the code that performs the signature verification after the devices have been manufactured. When this is the case, it is important for the devices to be designed to require quantum-resistant signatures on the executables, if there is a risk that the devices will still be in use after cryptographically relevant quantum computers become available.

3.1.2. User and Machine Authentication

User and machine authentication systems verify identities to control access to resources. This often involves cryptographic protocols that use asymmetric algorithms for secure key exchange and authentication, ensuring that only authorized users or devices can access sensitive data or services. Depending on the protocol, authentication may be performed using either a digital signature algorithm or a key-establishment scheme.

Unlike with encryption, where there is a threat of "harvest now, decrypt later," an authentication system remains secure as long as the cryptographic algorithms and keys used to perform the authentication are secure when the authentication is performed. Authentication

systems may continue to use quantum-vulnerable algorithms until quantum computers that are capable of breaking current, quantum-vulnerable algorithms become available, at which point authentication using these algorithms will need to be disabled.

Supporting quantum-resistant algorithms for authentication will require upgrades to both the system performing and accepting the authentication, as well as to any supporting infrastructure, such as a PKI. It may also require obtaining hardware cryptographic tokens that support the quantum-resistant algorithms.

3.1.3. Network Security Protocols

Network security protocols like TLS and virtual private networks secure data transmission over public networks. They use cryptographic techniques to provide confidentiality, integrity, and authentication between communicating parties.

Modern network security protocols tend to use separate asymmetric keys for key establishment and authentication. While long-term keys are used for authentication, key-establishment keys are used for a short period of time, usually for a single key establishment. This provides the property of forward secrecy, where the compromise of a long-term key does not result in the compromise of communication sessions that occurred before the compromise.

As symmetric keys that are established through the key-establishment process are used to provide confidentiality, the “harvest now, decrypt later” threat needs to be considered when determining a migration timeline for the key-establishment scheme. The cryptographic algorithm used for authentication may be transitioned at a different time, and for that the considerations in Sec. 3.1.2 apply.

3.1.4. Email and Document Signing and Encryption

Email and document signing employ digital signatures to verify the authenticity and integrity of electronic communications and documents. Common algorithms like RSA and ECDSA are widely used to create a cryptographic binding between the content and the sender’s identity, ensuring that the message has not been altered and that it originates from a legitimate source.

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for public-key encryption and the signing of MIME data. It provides end-to-end encryption and authentication for email and file exchanges to ensure that only intended recipients can access the content. As with other applications providing data confidentiality, email encryption is subject to “harvest now, decrypt later.”

3.2. PQC-Classical Hybrid Protocols

The migration to post-quantum cryptography may initially include hybrid solutions that incorporate the use of quantum-resistant and quantum-vulnerable algorithms when establishing cryptographic keys or generating digital signatures. These hybrid solutions are typically designed to remain secure if at least one of the component algorithms is secure.

Such hybrid solutions are often utilized as a hedge against a cryptographic or implementation flaw in one of the underlying component algorithms. It may also provide a path for accommodating the use of PQC if sector-specific requirements still require legacy quantum-vulnerable algorithms. However, hybrid solutions add complexity to implementations and architectures, which can increase security risks and costs during the transition to PQC. When used, hybrid solutions are typically expected to be temporary measures that lead to a second transition to cryptographic tools that use only PQC algorithms.

These trade-offs will vary based on the hybrid techniques used, the applications involved, and the vendor and user communities that will develop and deploy them. Implementers and standards organizations that specify cryptographic protocols and technologies need to carefully consider the security, costs, and complexity of hybrid solutions in their environments.

Industry and standards organizations are considering a variety of techniques for hybrid solutions with key-establishment schemes and digital signatures. NIST intends to accommodate the use of hybrid techniques in its cryptographic standards to facilitate the transition to PQC where their use is desired.

Whether hybrid solutions are used or not, quantum-vulnerable and quantum-resistant cryptographic algorithms will be fielded and used alongside each other in many applications and systems during the transition to PQC to facilitate interoperability. For example, many network security protocols support the use of multiple sets of cryptographic algorithms and allow two communicating parties to negotiate which algorithms to use in each session. Similarly, during the transition to PQC, public key infrastructures using quantum-vulnerable digital signature algorithms are expected to be deployed and used alongside those using quantum-resistant algorithms. Such approaches are not considered hybrid solutions if each session only uses a single cryptographic algorithm for key establishment and/or digital signatures.

3.2.1. Hybrid Key-Establishment Techniques

A hybrid key-establishment mode is defined here to be a key establishment scheme that is a combination of two or more components that are themselves cryptographic key-establishment schemes. The hybrid key-establishment scheme becomes a composite of these component schemes.

NIST currently allows a generic composite key-establishment technique described in SP 800-56C [SP80056C]. Assume that the value Z is a shared secret that was generated as specified by SP 800-56A or 800-56B and that a shared secret T is generated or distributed through other schemes. The value $Z' = Z || T$ may then be treated as a shared secret and any of the key derivation methods given in SP 800-56C may be applied to Z' to derive secret keying material.

NIST intends to update SP 800-56C so that the value Z may be generated as specified by any current and future NIST key-establishment standards. This will include SP 800-56A, SP 800-56B, FIPS 203, and any additional post-quantum key-establishment standards. The desired property of hybrid techniques is that derived keys remain secure if at least one of the component schemes is secure. Security properties can be complex, and for composite key establishment

schemes they will need to be analyzed on a case-by-case basis with the requirements of the application in mind. NIST intends to offer guidance on various key combiners in the forthcoming SP 800-227, *Recommendations for Key Encapsulation Mechanisms*.

Additionally, the output of the key-establishment scheme specified in FIPS 203 is a shared secret key which is a shared secret that does not require further key derivation. NIST emphasizes that any shared secret key generated as specified in FIPS 203 may be used as the value Z in the generic composite mode described in SP 800-56C. These same properties will apply to any future FIPS which standardize KEMs.

3.2.2. Hybrid Digital Signature Techniques

Common techniques for hybrid digital signatures involve the use of dual signatures, which consist of two or more signatures on a common message. It may also be known as a hybrid signature or composite signature. The verification of the dual signature requires all of the component signatures to be successfully verified, such as by creating a single logical composite signature from two or more component signature algorithms.

Dual signatures could be used to sign user data (e.g., a document or e-mail) or digital certificates that contain references to user key pairs within a PKI. Existing NIST standards and guidelines accommodate their use provided that at least one component digital signature algorithm is NIST-approved.

NIST leaves the decision to each specific application as to whether it can afford the implementation cost, performance reduction, and engineering complexity (including proper and independent security reviews) of a hybrid mode for key establishment or the use of dual signatures. To assist external parties that desire such a mechanism, NIST will accommodate the use of a hybrid key-establishment mode and dual signatures in FIPS 140 validation when suitably combined with a NIST-approved scheme.

4. Towards a PQC Standards Transition Timeline

NIST's cryptography standards provide comprehensive guidance on a broad spectrum of cryptographic mechanisms that are essential for securing sensitive information across both federal and nonfederal systems. These standards cover fundamental areas that are crucial for ensuring the confidentiality, integrity, and authenticity of data, such as encryption algorithms, digital signatures, hash functions, key establishment, and random number generation. Additionally, NIST's standards define key-management practices and offer frameworks for securely generating, storing, distributing, and destroying cryptographic keys.

Beyond individual algorithms, NIST standards provide guidance on cryptographic protocols that secure communications, such as the TLS protocol, which protects internet data exchanges. They also specify requirements for cryptographic modules through the CMVP to ensure that implementations meet stringent security standards. NIST has also developed PQC standards to safeguard systems against future quantum attacks. Through collaboration with industry, academia, and other stakeholders, NIST continually updates its cryptographic standards to address evolving security threats and technological advances.

National Security Memorandum 10 (NSM-10) establishes the year 2035 as the primary target for completing the migration to PQC across Federal systems [NSM10]:

> "Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a Cryptographically Relevant Quantum Computer (CRQC). To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."

This date reflects the urgency of transitioning to cryptographic methods that can withstand future quantum threats. However, it is important to recognize that migration timelines may vary based on the specific use case or application. Some systems, particularly those with long-term confidentiality needs or more complex cryptographic infrastructures, may require earlier transitions, while others may adopt PQC at a slower pace due to legacy constraints or lower risk profiles. Flexibility in migration planning is essential to balance the urgency of securing critical systems with the practical challenges that different sectors face during this transition. NIST will work to ensure that these varying timelines are acknowledged and supported while maintaining the overall goal of achieving widespread PQC adoption by 2035.

4.1. NIST Cryptographic Algorithm Standards and Guidelines

SP 800-131A [SP800131A] [SP800131A] describes the transitions associated with the use of cryptography by Federal Government agencies to protect controlled unclassified information. The document addresses the use of algorithms and key lengths specified in FIPS and NIST SPs. During the transition to post-quantum cryptography, NIST will revise SP 800-131A with more detailed guidelines and schedules.

The terms "**acceptable,**" "**deprecated,** "**disallowed,**" and "**legacy use**" are used throughout SP 800-131A to indicate the approval status of an algorithm:

- **Acceptable** means that the algorithm and key length/ strength in a FIPS or SP are **approved** for use in accordance with any associated guidance.
- **Deprecated** means that the algorithm and key length/strength may be used, but there is some security risk. The data owner must examine this risk potential and decide whether to continue to use a **deprecated** algorithm or key length.
- **Disallowed** means that the algorithm, key length/strength, parameter set, or scheme is no longer allowed for the stated purpose.
- **Legacy use** means that the algorithm, scheme, or parameter set may only be used to process already protected information (e.g., to decrypt ciphertext data or to verify a digital signature).

Transition schedules are primarily driven by the level of cryptographic protection that a given algorithm and associated parameter set can provide, which is described as a rough measure known as security strength. Historically, the security strength that an algorithm could provide was defined in terms of the amount of work (i.e., the number of operations) that is required to break the algorithm (i.e., an algorithm has *s* bits of security strength if breaking the algorithm requires 2^s operations of some kind, where s = 112, 128, 192, or 256). However, there are significant uncertainties in estimating the security strengths of post-quantum cryptosystems given the difficulty of accurately predicting the performance characteristics of future quantum computers, such as their cost, speed, and memory size.

While NIST guidelines continue to use bit-length security strengths to describe the level of protection offered by an algorithm and parameter set against attacks by classical computers, post-quantum security is described using a collection of broad security categories. Each category is defined by a comparatively easy-to-analyze reference primitive, whose security serves as a floor for a wide variety of metrics that are deemed potentially relevant to practical security. NIST based its classification on the range of security strengths offered by the existing standards in symmetric cryptography. Table 1 provides a summary of these security categories.

Table 1: Post-Quantum Security Categories

Security Category	Attack Type	Example
1	Key search on a block cipher with a 128-bit key	AES-128
2	Collision search on a 256-bit hash function	SHA-256
3	Key search on a block cipher with a 192-bit key	AES-192
4	Collision search on a 384-bit hash function	SHA3-384
5	Key search on a block cipher with a 256-bit key	AES-256

4.1.1. Digital Signatures

Table 2 lists currently approved quantum-vulnerable digital signature algorithm standards.

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

NIST's long-term cryptographic algorithm transition plans are outlined in SP 800-57pt1 (Part 1) [SP80057]. These guidelines had projected that NIST would disallow public-key schemes that provide 112 bits of security on January 1, 2031. However, based on the need to migrate to quantum-resistant algorithms during this timeframe, NIST intends to instead deprecate classical digital signatures at the 112-bit security level. Organizations may continue using these algorithms and parameter sets as they migrate to the post-quantum signatures identified in Table 3.

Table 3. Post-quantum digital signature algorithms

Digital Signature Algorithm Family	Parameter Sets	Security Strength	Security Category
ML-DSA [FIPS204]	ML-DSA-44	128 bits	2
	ML-DSA-65	192 bits	3
	ML-DSA-87	256 bits	5

Digital Signature Algorithm Family	Parameter Sets	Security Strength	Security Category
SLH-DSA [FIPS205]	SLH-DSA-SHA2-128[s/f] SLH-DSA-SHAKE-128[s/f]	128 bits	1
	SLH-DSA-SHA2-192[s/f] SLH-DSA-SHAKE-192[s/f]	192 bits	3
	SLH-DSA-SHA2-256[s/f] SLH-DSA-SHAKE-256[s/f]	256 bits	5
LMS, HSS [SP800208]	With SHA-256/192 With SHAKE256/192	192 bits	3
	With SHA-256 With SHAKE256	256 bits	5
XMSS, XMSS^{MT} [SP800208]	With SHA-256/192 With SHAKE256/192	192 bits	3
	With SHA-256 With SHAKE256	256 bits	5

4.1.2. Key Establishment

Table 4 lists currently approved quantum-vulnerable key-establishment.

Table 4: Quantum-vulnerable key-establishment schemes

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Similar to the transition for digital signature algorithms, NIST intends to instead deprecate rather than fully disallow classical key-establishment schemes at the 112-bit security level. Organizations may continue using these algorithms and parameter sets as they migrate to ML-KEM or other approved quantum-resistant techniques. However, in order to mitigate the risk of "harvest now, decrypt later" attacks on network communications, application-specific guidance, as described in Sec. 4.2, may require or recommend migration to quantum-resistant key establishment schemes before the classical schemes are generally disallowed.

Table 5 lists current quantum-resistant key establishment schemes. At this time, ML-KEM is the only approved post-quantum key-establishment scheme based on public key cryptography. Additional algorithms are still being considered as part of the fourth round of the NIST PQC Standardization process. NIST expects to select one or more alternatives to ML-KEM in the future.

Table 5: Post-quantum key-establishment schemes

Key Establishment Scheme	Parameter Sets	Security Strength	Security Category
ML-KEM [FIPS203]	ML-KEM-512	128 bits	1
	ML-DSA-768	192 bits	3
	ML-DSA-1024	256 bits	5

4.1.3. Symmetric Cryptography

NIST's existing standards in symmetric cryptography — including hash functions, XOFs, block ciphers, KDFs, and DRBGs — are significantly less vulnerable to known quantum attacks than the public-key cryptography standards in SP 800-56A, SP 800-56B, and FIPS 186. In particular, all NIST-approved symmetric primitives that provide at least 128 bits of classical security are believed to meet the requirements of at least Category 1 security within the system of five security strength categories for evaluating parameter sets in the NIST PQC standardization process (see Table 1). NIST has a few symmetric cryptography standards at the 112-bit security level, which will be disallowed in 2030. Applications should move away from these when transitioning to post-quantum cryptography.

Table 6: Block ciphers

Block Cipher	Parameter Sets	Security Strength	Security Category
AES [FIPS197]	AES-128	128 bits	1
	AES-192	192 bits	3
	AES-256	256 bits	5

530

531 **Table 7: Hash functions and XOFs**

Hash/XOF Algorithm Family	Variants	Collision Security Strength	Collision Security Category	Preimage Security Strength	Preimage Security Category
SHA-1 [FIPS180]	SHA-1	80 bits	< 1	160 bits	1
SHA-2 [FIPS180]	SHA-224 SHA-512/224	112 bits	< 1	224 bits	3
	SHA-256 SHA-512/256	128 bits	2	256 bits	5
	SHA-384	192 bits	4	384 bits	5
	SHA-512	256 bits	5	512 bits	5
SHA-3 [FIPS202]	SHA3-224	112 bits	< 1	224 bits	3
	SHA3-256	128 bits	2	256 bits	5
	SHAKE128	128 bits	2	128 bits	2
	SHA3-384	192 bits	4	384 bits	5
	SHA3-512	256 bits	5	512 bits	5
	SHAKE256	256 bits	5	512 bits	5

532

533 ## 4.2. Application-Specific Standards and Guidelines

534 NIST develops and maintains standards and guidelines addressing cryptography used in certain
535 security technologies, protocols, and systems. For example, FIPS 201-3 and its supporting
536 technical guidelines in NIST Special Publications specify the Personal Identity Verification
537 standard, including security and interoperability requirements for PKI-based credentials used to
538 authenticate federal employees and contractors. Other Special Publications provide guidance
539 on the configuration and use of cryptographic technologies, such as NIST SP 800-52 Revision 2
540 on the use of TLS servers and clients. These standards and guidelines are regularly updated to
541 address changes to underlying standards and technologies as well as new threats.

542 Throughout the migration to PQC, NIST will revise its documents to provide more detailed
543 guidelines for deprecating quantum-vulnerable algorithms, tailored to relevant applications.
544 While NIST's cryptographic algorithm standards may continue to specify quantum-vulnerable

techniques until 2035 and generally allow their use, these application-specific standards and guidelines may specify earlier transitions for certain cryptographic algorithms, techniques, and protocols used within these applications. These guidelines will be developed based on the expected impact that a cryptographically relevant quantum computer would have on these applications as well as the level of support for PQC in the relevant standards, products, and services. NIST expects to prioritize the migration to quantum-resistant key-establishment schemes within these updates to protect against "harvest now, decrypt later" attacks, particularly in interactive protocols like TLS and IKE.

NIST will also coordinate with standards-developing organizations and industry to ensure that critical security protocols and technologies are updated to support PQC in a timely manner, recognizing that different application areas will have different risks, security needs, and adoption challenges.

References

[FIPS140] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS180] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

[FIPS186] National Institute of Standards and Technology. Digital signature standard (DSS). (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 186-5. https://doi.org/10.6028/NIST.FIPS.186-5

[FIPS197] National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 197. https://doi.org/10.6028/NIST.FIPS.197

[FIPS198] National Institute of Standards and Technology (2008) The Keyed-Hash Message Authentication Code (HMAC). (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 198-1. https://doi.org/10.6028/NIST.FIPS.198-1

[FIPS202] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 202. https://doi.org/10.6028/NIST.FIPS.202

[FIPS203] National Institute of Standards and Technology (2024) Module-Lattice-Based Key-Encapsulation Mechanism Standard. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 203. https://doi.org/10.6028/NIST.FIPS.203

[FIPS204] National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 204. https://doi.org/10.6028/NIST.FIPS.204

[FIPS205] National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) FIPS 205. https://doi.org/10.6028/NIST.FIPS.205

[NISTIR8528] Alagic G, Bros M, Ciadoux P, Cooper D, Dang Q, Dang T, Kelsey J, Lichtinger J, Liu YK, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Silberg H, Smith-Tone D, Waller N (2024) Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8528.

https://doi.org/10.6028/NIST.IR.8528

[NSM10] Biden J (2022) National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. (The White House, Washington, DC), National Security Memorandum 10, May 4 2022. Available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[SP80056A] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Using Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-56Ar3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[SP80056B] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon Scott (2019) Recommendation for Pair-Wise Key-Establishment Schemes Integer Factorization Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-56Br2. https://doi.org/10.6028/NIST.SP.800-56Br2

[SP80056C] Barker E, Chen L, Davis R (2020) Recommendation for Key-Derivation Methods in Key-Establishment Schemes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-56Cr2. https://doi.org/10.6028/NIST.SP.800-56Cr2

[SP80057] Barker EB, Barker WC (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-57pt1r5. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[SP800131A] Barker E, Roginsky A (2019) Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-131Ar2. https://doi.org/10.6028/NIST.SP.800-131Ar2

[SP800185] Kelsey JM, Chang S-jH, Perlner RA (2016) SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-185. https://doi.org/10.6028/NIST.SP.800-185

[SP800186] Chen L, Moody D, Regenscheid A, Robinson A, Randall K (2023) Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-186. https://doi.org/10.6028/NIST.SP.800-186

[SP800208] Cooper DA, Apon DC, Dang QH, Davidson MS, Dworkin MJ, Miller CA (2020) Recommendation for Stateful Hash-Based Signature Schemes, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-208. https://doi.org/10.6028/NIST.SP.800-208

Appendix A. Glossary

acceptable
Approved for use. An allowed algorithm and key length/strength in a FIPS or SP is approved for use in accordance with any associated guidance.

approved
FIPS-approved and/or NIST-recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST recommendation, 2) adopted in a FIPS or NIST recommendation, or 3) specified in a list of NIST-approved security functions.

asymmetric (cryptography)
Cryptography that uses two separate keys to exchange data — one to encrypt or digitally sign the data and one to decrypt the data or verify the digital signature. Also known as public-key cryptography.

block cipher
An invertible symmetric-key cryptographic algorithm that transforms one block of information at a time using a cryptographic key. The resulting output block is the same length as the input block.

certificate
A set of data that uniquely identifies a public key that has a corresponding private key and an owner that is authorized to use the key pair. The certificate contains the owner's public key and possibly other information and is digitally signed by a certification authority (i.e., a trusted party), thereby binding the public key to the owner.

cryptographic module
The set of hardware, software, and/or firmware that implements approved cryptographic functions (including key generation) that are contained within the cryptographic boundary of the module.

cryptographically relevant quantum computer
A quantum computer which is capable of actually attacking real world cryptographic systems that would be infeasible to attack with a normal computer.

deprecated
The algorithm and key length may be used, but the user must accept some security risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection.

digital certificate
See *certificate*.

digital signature
The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism to verify origin authenticity and data integrity and to enforce signatory non-repudiation.

disallowed
The algorithm or key length is no longer allowed for applying cryptographic protection.

dual signature
A dual signature consists of two (or more) signatures on a common message. It may also be known as a hybrid signature or composite signature.

encryption
The process of transforming plaintext into ciphertext using a cryptographic algorithm and key.

eXtendable-Output Function (XOF)
A function on bit strings in which the output can be extended to any desired length.

forward secrecy
Providing protection against the use of compromised old keys that could be used to attack the newer derived keys still in use for integrity and confidentiality protection.

hash function
A function on bit strings in which the length of the output is fixed. Approved hash functions (such as those specified in FIPS 180 and FIPS 202) are designed to satisfy the following properties:

1. (One-way) It is computationally infeasible to find any input that maps to any new pre-specified output.
2. (Collision-resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

KEM combiner
A function that takes in two or more shared secret keys and returns a combined shared secret key.

key agreement
A (pair-wise) key-establishment procedure where the resultant secret keying material is a function of information contributed by two participants so that no party can predetermine the value of the secret keying material independently from the contributions of the other party. Contrast with key-transport.

key derivation
The process of deriving a key in a non-reversible manner from shared information, some of which is secret.

key encapsulation mechanism (KEM)
A set of three cryptographic algorithms (KeyGen, Encaps, and Decaps) that can be used by two parties to establish a shared secret key over a public channel.

key establishment
A procedure that results in establishing secret keying material that is shared among different parties.

key transport
A (pair-wise) key-establishment procedure whereby one party (the sender) selects a value for the secret keying material and then securely distributes that value to another party (the receiver). Contrast with key agreement.

key wrapping
A method of protecting secret keying material (along with associated integrity information) that provides both confidentiality and integrity protection when using symmetric-key algorithms.

legacy use
The algorithm or key length may be used only to process already protected information (e.g., to decrypt ciphertext data or to verify a digital signature).

message authentication code (MAC)
A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data.

mode of operation
An algorithm for the cryptographic transformation of data that features a symmetric key block cipher.

public key infrastructure (PKI)
A framework that is established to issue, maintain and revoke public key certificates.

public key cryptography
Cryptography that uses two separate keys to exchange data — one to encrypt or digitally sign the data and one to decrypt the data or verify the digital signature. Also known as asymmetric cryptography.

security category
A number associated with the security strength of a post-quantum cryptographic algorithm, as specified by NIST.

security strength
A number associated with the amount of work (i.e., the number of operations) that is required to break a cryptographic algorithm or system.

shared secret
A secret value that has been computed during a key-establishment scheme, is known by both participants, and is used as input to a key-derivation method to produce keying material.

shared secret key
A shared secret that can be used directly as a cryptographic key in symmetric-key cryptography. It does not require additional key derivation. The shared secret key must be kept private and must be destroyed when no longer needed.

symmetric key cryptography
A cryptographic algorithm that uses the same secret key for its operation and, if applicable, for reversing the effects of the operation (e.g., an AES key for encryption and decryption).