NSA CYBERSECURITY

Post Quantum Cryptography: A Quintessential Quagmire

MATT DOWNEY, NIAP
1 NOVEMBER 2023

CNSA 2.0 Overview

Motivation for Transition

NSM-8

Goal: Fortify cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.

- All federal agencies must use NSA-approved cryptography to protect NSS.
- NSA must update CNSSP 15: Use of Public Standards for Secure Information Sharing from CNSA 1.0 to CNSA 2.0 algorithms.
- NSA must provide PQ crypto planning.

NSM-10

Goal: Promote US leadership in quantum computing while mitigating risks to vulnerable systems.

- US must develop partnerships, promote collaboration with industry, academia, and overseas allies.
- NSA must provide guidance on quantum-resistant cryptography migration, implementation, and oversight for NSS.
- NSA must release timeline for deprecation of vulnerable cryptography in NSS.

CNSA 2.0 Overview

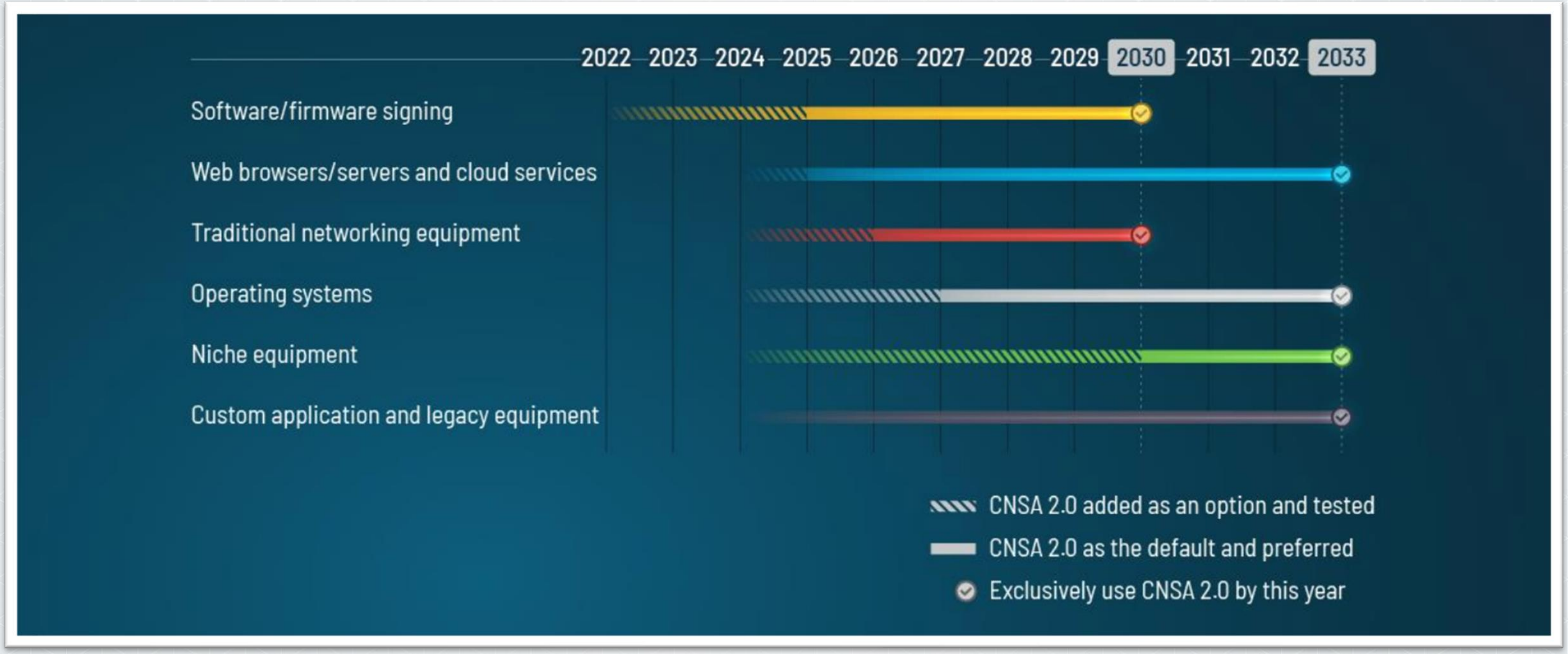
Algorithms

Function	Algorithm	Specification	Use Case	Parameters	CNSA 1.0
Symmetric Key Encryption	AES	FIPS PUB 197	General	AES-256	AES-256
Hash Algorithm	SHA2	FIPS PUB 180-4	General	SHA-384 SHA-512	SHA-384
Digital Signature	Leighton-Micali Signature (LMS)	NIST SP 800-208 RFC 8554	Software and firmware signing	All parameters in SP 800-208*	ECDSA (P-384) RSA (3072 bit min)
Digital Signature	eXtended Merkle Signature Scheme (XMSS)	NIST SP 800-208 RFC 8391	Software and firmware signing	All parameters in SP 800-208*	ECDSA (P-384) RSA (3072 bit min)
Asymmetric Key Establishment	CRYSTALS-Kyber (ML-KEM)	NIST FIPS 203	General	Level V	ECDH (P-384) DH (3072 bit min)
Digital Signature	CRYSTALS-Dilithium (ML-DSA)	NIST FIPS 204	General	Level V	ECDSA (P-384) RSA (3072 bit min)

*All parameters for LMS and XMSS are approved, but use of LMS with parameter SHA-256/192 is preferred.

CNSA 2.0 Overview

Anticipated Timeline



General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes algorithm standard.

1

LMS
- For software and firmware signing
- Standardized by NIST in SP 800-208

2

XMSS
- For software and firmware signing
- Standardized by NIST in SP 800-208

3

CRYSTALS-Kyber (ML-KEM)
- For key establishment
- Draft standard FIPS 203 released by NIST; can expect final standard sometime in 2024
- NIST will publish SP 800-227 on the general properties of KEMs

4

CRYSTALS-Dilithium (ML-DSA)
- For general purpose digital signatures
- Draft standard FIPS 204 released by NIST
- Can expect final standard FIPS 204 sometime in 2024

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes algorithm standard.

The following NIST documents will be updated and/or replaced:

- Federal Information Processing Standard (FIPS) 186-5 Digital Signature Standard
- Special Publication (SP) 800-56A Revision 3 (Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography)
- SP 800-56B Revision 3 (Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.
2. **NIST adds in support for the algorithm to their Cryptographic Algorithm Validation Program.**

General Process for NIAP Implementation of CNSA 2.0

2. NIST adds support for algorithm to CAVP.

> *"All cryptography in the TOE for which NIST provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components must be NIST validated (CAVP and/or CMVP). At minimum an appropriate NIST CAVP certificate is required before a NIAP CC Certificate will be awarded."* (NIAP Policy Letter 5)

NIAP's CAVP Mapping document will need updates to incorporate the new algorithms.

General Process for NIAP Implementation of CNSA 2.0

2. NIST adds support for algorithm to CAVP.

NIST’s Automated Cryptographic Validation Program (ACVP) may expedite this process.

LMS and XMSS may require Cryptographic Module Validation Program (CMVP) validation in addition to CAVP validation.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.
2. NIST adds in support for the algorithm to their Cryptographic Algorithm Validation Program.
3. **NIAP updates the relevant Protection Profiles to include the newly-standardized algorithm as the preferred configuration option.**

General Process for NIAP Implementation of CNSA 2.0

3. NIAP updates PPs to support use of algorithm.

Algorithm-Specific Updates

The algorithm is added in as a selection to all relevant PPs. This is determined by:

- what type of algorithm it is (encryption vs. authentication), and
- whether it is for general use, or approved only for a specific use case (e.g. software and firmware updates for LMS and XMSS).

SFRs, testing activities, application notes, and more may need to be updated to account for additional considerations that arise through use of the algorithm.

Protocol-Specific Updates

SDOs publish new standards documents that update existing standards in order to allow for the use of the new algorithm in a specific protocol standard.

Updates may be made to the CNSA RFC that profiles the protocol in question.

All PPs that use the given protocol need to incorporate updates to align with new SDO documents and CNSA profile.

SFRs, testing activities, threats, assumptions, and more may need to be updated.

In both cases, updates need to be traced through PPs on which revised PPs are dependent (e,g., the dependency a PP-Module has on a base-PP) to ensure consistency throughout updates.

General Process for NIAP Implementation of CNSA 2.0

3. NIAP updates PPs to support use of algorithm.

Example 1: Algorithm-Specific Updates for LMS

- Statefulness property introduces additional requirement for key and signature generation, but not signature verification.
  - Signature generation and verification are currently addressed in a single SFR; need to separate these.
  - Where should key and sig gen requirements be incorporated? (Dedicated Security Component cPP?)
- SP 800-208 prohibits private key export.
  - Non-cryptographic SFRs that address data export may need to be updated.

General Process for NIAP Implementation of CNSA 2.0

3. NIAP updates PPs to support use of algorithm.

Example 2: Protocol-Specific Updates for ML-KEM in IKEv2

General Idea: PQ algorithms have larger public key and ciphertext sizes compared to traditional algorithms. In IKEv2, large sizes cause messages to exceed supported size, requiring fragmentation.

Sequence of Changes:

1. IETF Standards
2. Updates to RFC 9206 CNSA Suite Cryptography for IPsec
3. Updates to Protection Profiles

General Process for NIAP Implementation of CNSA 2.0

3. NIAP updates PPs to support use of algorithm.

Example 2: Protocol-Specific Updates for ML-KEM in IKEv2

IETF Standards to Support:

- **RFC 7383 IKEv2 Message Fragmentation:** This RFC adds a new Notify Payload and updates how authentication is performed.
- **RFC 9242 Intermediate Exchange in IKEv2:** This RFC adds in a new Notify Payload, a new exchange (IKE_INTERMEDIATE), and updates how authentication is performed.
- **RFC 9370 Multiple Key Exchanges in IKEv2:** This RFC adds in a new Notify Payload, changes the name of a Transform Type, changes the supported encryption algorithms, changes how encryption is performed, and changes how authentication is performed.
- **And more!** A standard to specify the use of CRYSTALS-Kyber in IKEv2- an algorithm identifier, the format of the public key, other implementation details.

General Process for NIAP Implementation of CNSA 2.0

3. NIAP updates PPs to support use of algorithm.

Example 2: Protocol-Specific Updates for ML-KEM in IKEv2

Updates to RFC 9206 CNSA Suite Cryptography for Internet Protocol Security (IPsec):

- Incorporate extensions from RFCs on previous slide
- Update IPsec User Interface Suites
- Update security considerations

General Process for NIAP Implementation of CNSA 2.0

3. NIAP updates PPs to support use of algorithm.

Example 2: Protocol-Specific Updates for ML-KEM in IKEv2

Protection Profiles to Be Updated:

- VPN Gateway and VPN Client PP-Modules will need to be updated.
- And their respective base-PPs:
  - VPN Gateway PP-Module uses Network Device PP.
  - VPN Client PP-Module can use General Purpose Operating System PP, Multi-Function Device PP, Application Software PP, and Mobile Device Management PP.
- And PP-Modules that VPN Gateway and VPN Client can be used in conjunction with:
  - Stateful Traffic Filter Firewalls, Intrusion Prevention Systems, Wireless Intrusion Detection/Prevention Systems, Enrolment and Verification, File Encryption Enterprise Management, File Encryption, MDM Agent, Bluetooth, WLAN Client.
- And any other PPs that may include SFRs allowing for IKEv2-based encryption or authentication.

General Process for NIAP Implementation of CNSA 2.0

3. NIAP updates PPs to support use of algorithm.

Example 2: Protocol-Specific Updates for ML-KEM in IKEv2

Examples of PP Updates:

- Add algorithm as selection.
- Ensure SFRs for IKEv2 are able to support simultaneous use of both traditional encryption algorithm and PQ algorithm but that other protocols cannot use traditional encryption algorithm.
- Add testing activities:
  - to assess whether negotiation of algorithms and extensions is successful due to new Notify Payloads and exchanges
  - to ensure modified encryption and authentication processes are securely implemented.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.
2. NIST adds in support for the algorithm to their Cryptographic Algorithm Validation Program.
3. NIAP updates the relevant Protection Profiles to include the newly-standardized algorithm as the preferred configuration option.
4. **New equipment must meet the updated Protection Profile requirements in order to be validated; already validated equipment must meet the updated requirements when it is due for its next update in order to remain compliant.**

General Process for NIAP Implementation of CNSA 2.0

4. Equipment must meet updated PP requirements in order to be validated or remain compliant.

New equipment:

- Equipment that has not yet been validated must meet the updated Protection Profile requirements in order to be validated.

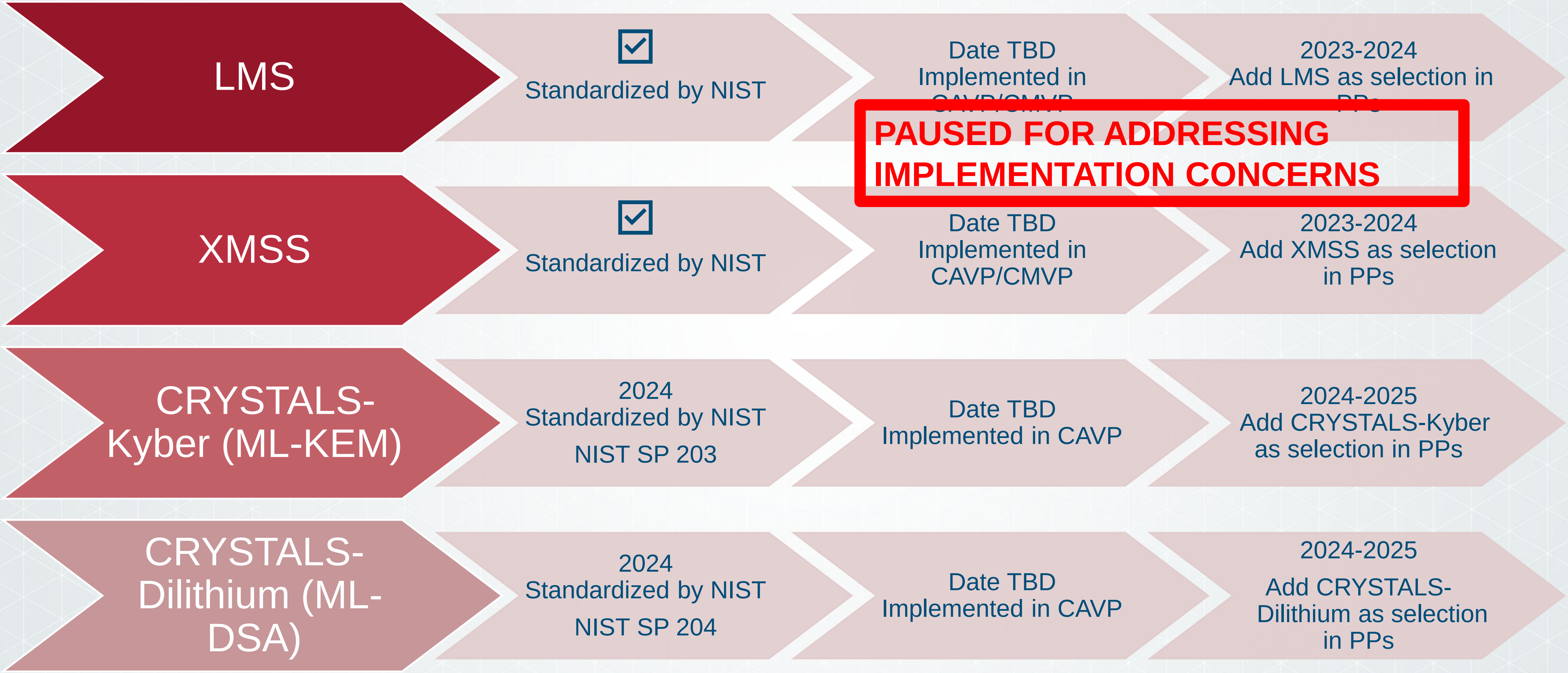
Already validated equipment:

- Equipment that has already been validated must meet the updated Protection Profile requirements when it is due for its next update in order to remain compliant.
- NIAP certifications typically last for two years with the possibility of an additional year.
- Certifications for some technologies may last for up to five years (e.g. Peripheral Sharing Devices).
- For more information on the re-evaluation process, see NIAP-CCEVS Publication 6, Assurance Continuity: Guidance for Maintenance and Re-Evaluation.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.
2. NIST adds in support for the algorithm to their Cryptographic Algorithm Validation Program.
3. NIAP updates the relevant Protection Profiles to include the newly-standardized algorithm as the preferred configuration option.
4. New equipment must meet the updated Protection Profile requirements in order to be validated; already validated equipment must meet the updated requirements when it is due for its next update in order to remain compliant.
5. **After some time, non-CNSA 2.0-approved algorithms will be removed as options from Protection Profiles.**

Predicted Timeline for Adding Algorithms to PPs



LMS	☑ Standardized by NIST	Date TBD Implemented in CAVP/CMVP	2023-2024 Add LMS as selection in PPs
XMSS	☑ Standardized by NIST	Date TBD Implemented in CAVP/CMVP	2023-2024 Add XMSS as selection in PPs
CRYSTALS-Kyber (ML-KEM)	2024 Standardized by NIST NIST SP 203	Date TBD Implemented in CAVP	2024-2025 Add CRYSTALS-Kyber as selection in PPs
CRYSTALS-Dilithium (ML-DSA)	2024 Standardized by NIST NIST SP 204	Date TBD Implemented in CAVP	2024-2025 Add CRYSTALS-Dilithium as selection in PPs

PAUSED FOR ADDRESSING IMPLEMENTATION CONCERNS

NIAP Cryptographic Technical Community

Support Efforts to Update PPs

- Members can provide technical input to the development and maintenance of cryptographic Security Functional Requirements (SFRs).
- TC is focused on incorporating quantum-resistant algorithms from CNSA 2.0 into Protection Profiles.
- First round of updates WAS to enable use of LMS and XMSS stateful hash-based digital signatures for software and firmware signing.
    - Incorporate requirements into Protection Profiles, beginning with Application Software, General Purpose Operating System, and Mobile Device Fundamentals.
    - Make recommendations for collaborative Protection Profiles, beginning with Network Device and Dedicated Security Component.
- Will now focus on removing older algorithms (e.g. SHA-1) and some preliminary work on LMS/XMSS
- Future updates will add support for CRYSTALS-Kyber (ML-KEM) for key establishment, and CRYSTALS-Dilithium (ML-DSA) for digital signatures, and any further LMS/XMSS work once resolution reached..
- The TC is open to all participants.

References

- CNSA Suite 2.0 Cybersecurity Advisory
- CNSA Suite 2.0 FAQ
- NIST SP 800-208
- CNSSP 15
- CAVP Mapping
- NIAP Policy Letter 5
- NIAP-CCEVS Publication 6
- NSM 8
- NSM 10
- Status Report on the 3rd Round of the NIST PQ Cryptography Standardization Process
- NIST DRAFT SP 203, ML-KEM
- NIST DRAFT SP 204, ML-DSA
- RFC 7383, IKEv2 Message Fragmentation
- RFC 9242, Intermediate Exchange in IKEv2
- RFC 9370, Multiple Key Exchanges in IKEv2