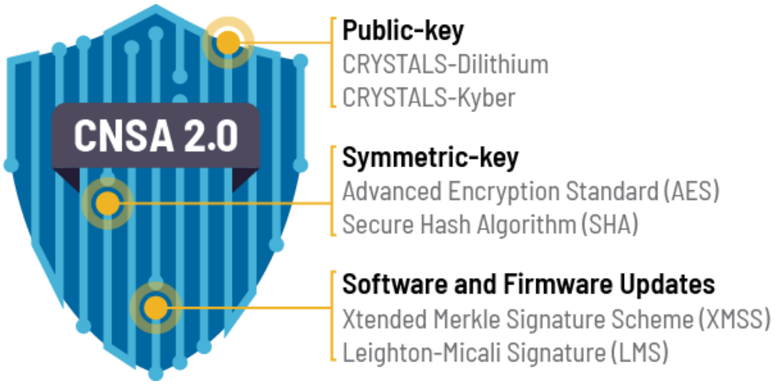
Announcing the Commercial National Security Algorithm Suite 2.0

Executive summary


CNSA 2.0
Public-key
CRYSTALS-Dilithium
CRYSTALS-Kyber
Symmetric-key
Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)
Software and Firmware Updates
Xtended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)

The need for protection against a future deployment of a cryptanalytically relevant quantum computer (CRQC) is well documented. That story begins in the mid-1990s when Peter Shor discovered a CRQC would break public-key systems still used today. Continued progress in quantum computing research by academia, industry, and some governments suggests that the vision of quantum computing will ultimately be realized. Hence, now is the time to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms, to assure continued protection of National Security Systems (NSS) and related assets.

This advisory notifies NSS owners, operators, and vendors of future requirements for QR algorithms for NSS. These algorithms (also referred to as post-quantum algorithms) are analyzed as being secure against both classical and quantum computers. They are an update to those in the Commercial National Security Algorithm Suite (referred to as CNSA 1.0, the algorithms currently listed in CNSSP 15, Annex B). NSA will reference this update as CNSA Suite 2.0, and any future updates will modify the version number.

NSA is providing this advisory in accordance with authorities detailed in NSD-42, NSM-8, NSM-10, CNSSP 11, and CNSSP 15. Its direction applies to all NSS use of public cryptographic algorithms (as opposed to algorithms NSA developed), including those on all unclassified and classified NSS. Using any cryptographic algorithms the National Manager did not approve is generally not allowed, and requires a waiver specific to the algorithm, implementation, and use case. In accordance with CNSSP 11, software and hardware providing cryptographic services require National Information Assurance Partnership (NIAP) or NSA validation in addition to meeting the requirements of the appropriate version of CNSA.

Introduction

This advisory includes the following sections:

- Algorithms for software- and firmware-signing. The National Institute of Standards and Technology (NIST) standardized these algorithms some time ago, but using different algorithms for this special use case is new in CNSA 2.0.
- Symmetric-key algorithms. There is only a modest change from CNSA 1.0 in this section that allows a bit more flexibility.
- General-use quantum-resistant public-key algorithms. These are the main public-key algorithms that most applications will require. As they have not completed standardization, this section is forward-looking.
- Timing. Discusses the timing of the transition to CNSA 2.0.
- Enforcement. Summarizes requirements related to enforcing NSS algorithm requirements.
- Additional guidance: RFCs. Provides links to helpful Internet Engineering Task Force Requests for Comment (IETF RFCs) used to implement CNSA 1.0.
- Reference tables. Features two tables that list algorithms for CNSA 2.0 and for CNSA 1.0.

Algorithms for software- and firmware-signing

The reasons for choosing separate algorithms for software- and firmware-signing are three-fold:

- NIST has standardized these algorithms already, while other post-quantum signatures are not yet standardized,
- This signature use-case is more urgent, and
- This selection places algorithms with the most substantial history of cryptanalysis in a use case where their potential performance issues have minimal impact. In particular, this usage coincides well with the requirement for keeping track of state—that is, how many times a given public key was used in signing software or firmware when deploying these signatures.

The algorithms chosen for software- and firmware-signing are those specified in NIST Special Publication 800-208. NSA recommends Leighton-Micali with SHA-256/192, but all NIST SP 800-208 algorithms are approved for this use case. Note that to avoid weakening the security of these signatures, you must meet all the requirements of SP 800-208, including the need to manage state and implement signing in hardware.

NSA encourages vendors to begin adopting NIST SP 800-208 signatures immediately. For more information on requirement timelines, see the Timing section. The following table lists CNSA 2.0 algorithms for software and firmware updates.

Table I: CNSA 2.0 algorithms for software and firmware updates

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

Symmetric-key algorithms

The following table shows the addition of SHA-512 to the list, the only change when compared with CNSA 1.0.

Table II: CNSA 2.0 symmetric-key algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.

General-use quantum-resistant public-key algorithms

NIST recently announced its standardization selections for post-quantum cryptography. Consequently, there are neither final standards nor Federal Information Processing Standard (FIPS)-validated implementations available at this time. NSA is announcing this selection of public-key algorithms to provide future NSS requirements so vendors may begin building toward these requirements, and so acquisition officials and NSS owners and operators will know what the requirements are.

Note that this will effectively deprecate the use of RSA, Diffie-Hellman (DH), and elliptic curve cryptography (ECDH and ECDSA) when mandated. NSA urges NSS owners and operators to pay special attention to these requirements. In the interim, CNSA 1.0 compliance continues to be required. The following section defines transition timelines and the following table lists CNSA 2.0 algorithms:

Table III: CNSA 2.0 quantum-resistant public-key algorithms

Algorithm	Function	Specification	Parameters
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.

Timing

The timing of the transition depends on the proliferation of standards-based implementations. Because different technologies will adopt QR algorithms at different paces, NSA is providing an overall transition end date and the process for determining specific dates going forward.

NSA expects the transition to QR algorithms for NSS to be complete by 2035 in line with NSM-10. NSA urges vendors and NSS owners and operators to make every effort to meet this deadline. Where feasible, NSS owners and operators will be required to prefer CNSA 2.0 algorithms when configuring systems during the transition period. When appropriate, use of CNSA 2.0 algorithms will be mandatory in classes of commercial products within NSS, while reserving the option to allow other algorithms in specialized use cases.

The following is the general method for transitioning to CNSA 2.0 algorithm use:

1 NIAP will release protection profiles specifying that products support CNSA 2.0 algorithms in accordance with NIST and other standards from standards development organizations and the development of standards-compliant cryptographic equipment.

2 All new equipment must meet the protection profile requirements; older equipment must meet the requirement at its next update to remain NIAP compliant.

3 Using CNSA 2.0 algorithms as the preferred configuration option will begin as soon as validated and tested solutions are available.

4 NIAP Protection Profile requirements and NSM-10 technology refresh requirements will determine the removal of legacy algorithm support.

5 At that point, legacy equipment and software not refreshed regularly will require a waiver and a plan to bring it into compliance.

Timing for software signing and firmware signing

For software signing and firmware signing, NSA recommends:

1. Software and firmware signing begin transitioning immediately.
2. New software and firmware use CNSA 2.0 signing algorithms by 2025.
3. Transitioning deployed software and firmware not CNSA 1.0 compliant to CNSA 2.0-compliant algorithms by 2025.
4. Transitioning all deployed software and firmware to CNSA 2.0-compliant signatures by 2030.

Other requirements for NSS

NSA anticipates the following timetable for implementing other CNSA 2.0 requirements for NSS:

- **Software and firmware signing:** begin transitioning immediately, support and prefer CNSA 2.0 by 2025, and *exclusively* use CNSA 2.0 by 2030.
- **Web browsers/servers and cloud services:** support and prefer CNSA 2.0 by 2025, and *exclusively*[1] use CNSA 2.0 by 2033.
- **Traditional networking equipment (e.g., virtual private networks, routers):** support and prefer CNSA 2.0 by 2026, and *exclusively* use CNSA 2.0 by 2030.
- **Operating systems:** support and prefer CNSA 2.0 by 2027, and *exclusively* use CNSA 2.0 by 2033.
- **Niche equipment (e.g., constrained devices, large public-key infrastructure systems):** support and prefer CNSA 2.0 by 2030, and *exclusively* use CNSA 2.0 by 2033.
- **Custom applications and legacy equipment:** update or replace by 2033.

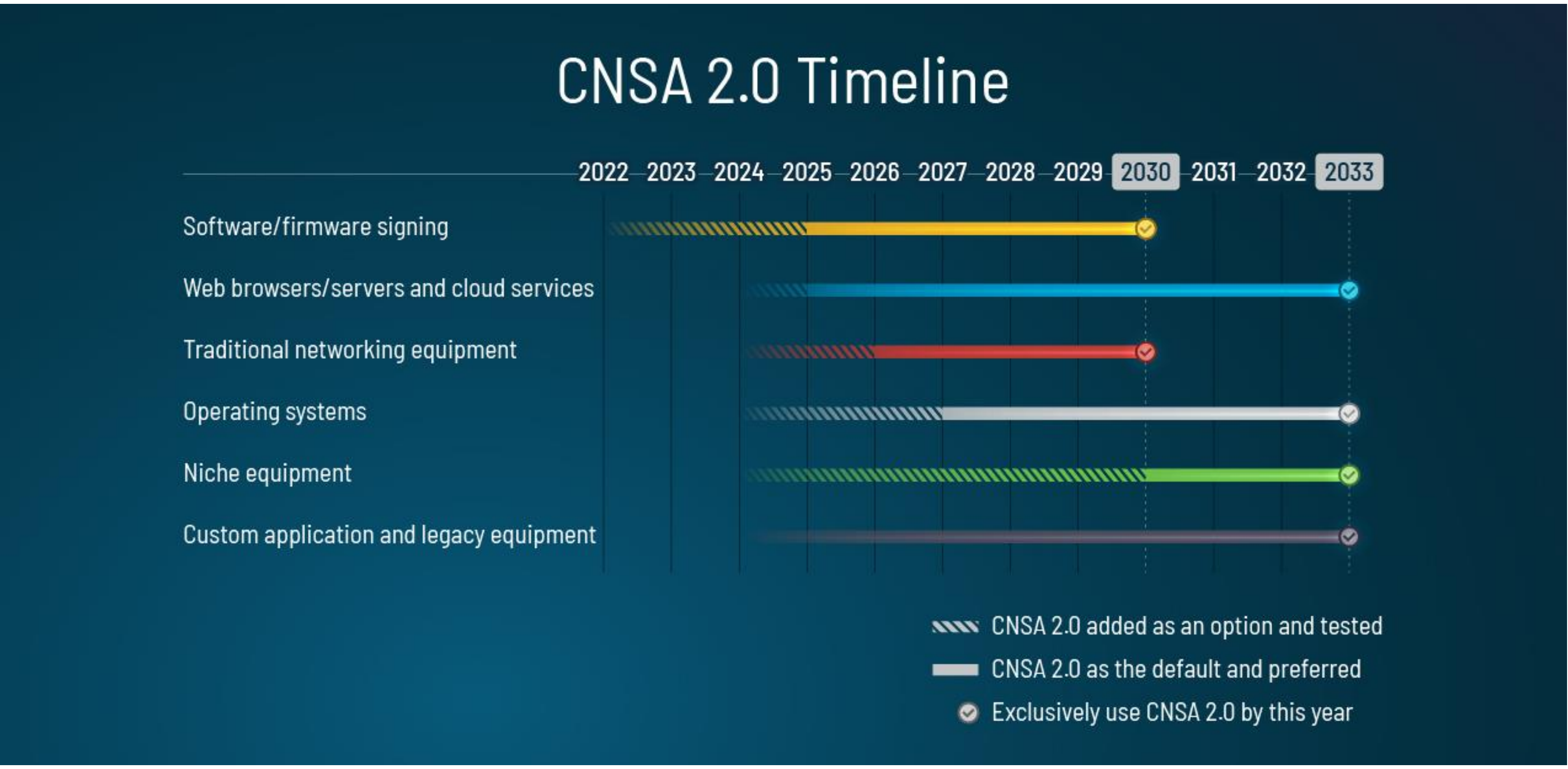


Figure 1: Transition timeline

[1] Even though hybrid solutions may be allowed or required due to protocol standards, product availability, or interoperability requirements, CNSA 2.0 algorithms will become mandatory to select at the given date, and selecting CNSA 1.0 algorithms alone will no longer be approved.

Enforcement

NSS owners and operators must report on their progress in updating to CNSA 1.0 and CNSA 2.0 as part of their responsibilities under NSM-8 and NSM-10. Approving Officials (AOs) should measure compliance as part of the Risk Management Framework (RMF) process when assessing Security Control 12 (SC-12). Furthermore, AOs will need to verify compliance with CNSA 2.0 for software- and firmware-signing on their systems. NSS should **not** be assessed against “FIPS-validated” in the RMF process; instead, solutions must be NSA-approved. In applications where a commercial product is accepted, NSA generally approves products that comply with CNSSP 11 (i.e., are NIAP-validated against an approved protection profile), as long as they are configured correctly in accordance with CNSSP 15 and other specific directions or guidance.

Additional guidance: RFCs

The following documents specify how to configure solutions to comply with CNSA requirements. These include:

- RFC 8603 "Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile" https://datatracker.ietf.org/doc/html/rfc8603
- RFC 8755 "Using Commercial National Security Algorithm Suite Algorithms in Secure/Multipurpose Internet Mail Extensions" https://datatracker.ietf.org/doc/rfc8755/
- RFC 8756 "Commercial National Security Algorithm (CNSA) Suite Profile of Certificate Management over CMS" https://datatracker.ietf.org/doc/rfc8756/
- RFC 9151 "Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3" https://datatracker.ietf.org/doc/rfc9151/
- RFC 9206 "Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec)" https://datatracker.ietf.org/doc/rfc9206/
- RFC 9212 "Commercial National Security Algorithm (CNSA) Suite Cryptography for Secure Shell (SSH)" https://datatracker.ietf.org/doc/rfc9212/

These documents currently apply to CNSA 1.0. NSA will release updated guidance as the standardization process progresses.

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed to further NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats and vulnerabilities to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Inquiries and Feedback: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov

Appendix: Reference tables

The following two tables list the algorithms for CNSA 2.0 and for CNSA 1.0, respectively. CNSA 1.0 is the current standard while CNSA 2.0 is the future one. NSA recommends adopting the CNSA 2.0 software- and firmware-signing algorithms now.

Table IV: CNSA 2.0 algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

Table V: CNSA 1.0 algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm for key establishment	NIST SP 800-56A	Use Curve P-384 for all classification levels.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm for digital signatures	FIPS PUB 186-4	Use Curve P-384 for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 for all classification levels.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm for key establishment	IETF RFC 3526	Minimum 3072-bit modulus for all classification levels
RSA	Asymmetric algorithm for key establishment	FIPS SP 800-56B	Minimum 3072-bit modulus for all classification levels
RSA	Asymmetric algorithm for digital signatures	FIPS PUB 186-4	Minimum 3072-bit modulus for all classification levels.