National Security Agency | Cybersecurity Information Sheet

The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ

These frequently asked questions (FAQ) and answers are intended to clarify Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) requirements for National Security Systems (NSS) and recommend guidance for the Department of Defense (DoD) and the Defense Industrial Base (DIB). This information may be useful more generally, especially for those who interact with NSS, DoD, or DIB systems.

Sections

Background

Q: To whom are these requirements addressed?

A. These are mainly addressed to the following audiences:

- National Security System (NSS) owners and operators, who need to know the requirements for their systems

- Vendors, who need to know what to implement to meet NSS requirements

NSA is not using these requirements to dictate to any other entity outside of NSS what algorithms they should use, although NSA recognizes that interoperability requirements or other interests may lead to scenarios where these recommendations are used by a larger community.

Q: What is a quantum computer, and how is it different from the computers we use today?

A: In place of ordinary bits used by today's computers, quantum computers use "qubits" that behave in surprising ways, efficiently performing certain mathematical algorithms exponentially faster than a classical computer. Small examples of quantum computers have been built.

Q: What is a "cryptanalytically relevant quantum computer" (CRQC)?

A: Also written as "cryptographically relevant quantum computer," CRQC describes quantum computers that are capable of attacking real world cryptographic systems. Whether the "C" indicates "cryptanalytically" or "cryptographically" is a matter of writer's preference, as the two terms are essentially equivalent in this context. This term distinguishes a CRQC from any other "quantum computer" technologies used in other settings without the performance metrics required to attack real world cryptographic systems.

Q: What is the threat if a CRQC were developed?

A: A CRQC, if built, would be capable of undermining the widely deployed public-key algorithms currently used for asymmetric key exchanges and digital signatures with potentially devastating impact to systems. National security systems (NSS) use public-key cryptography as a critical component to protect the confidentiality, integrity, and authenticity of national security information.

Q: Can I continue to use larger sizes of RSA or ECC to address the threat?

A: No. RSA and Elliptic Curve Cryptography are the main algorithms that need to be replaced to achieve quantum resistance.

Q: What is "quantum-resistant" or "post-quantum" cryptography?

A: "Quantum-resistant" (QR), "quantum-safe," and "post-quantum" (PQ) cryptography are all terms used to describe cryptographic algorithms that can be run on computers today and are believed to be resistant to cryptanalytic attacks from both classical and quantum computers.

Q: What is the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)?

A: CNSA 2.0 is the suite of QR algorithms approved for NSS use. The following table lists the algorithms and their functions, specifications, and parameters.

Table: Commercial National Security Algorithm Suite 2.0

Algorithm	Function	Specification	Parameters
General Purpose Algorithms			
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (previously CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	ML-KEM-1024 for all classification levels.
ML-DSA (previously CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	ML-DSA-87 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.
Algorithms Allowed in Specific Applications			
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. LMS SHA-256/192 is 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.
Secure Hash Algorithm 3 (SHA3)	Algorithm used for computing a condensed representation of information as part of hardware integrity	FIPS PUB 202	SHA3-384 or SHA3-512 allowed for internal hardware functionality only (e.g., boot-up integrity checks)

CNSA 2.0

Q: Where should CNSA 2.0 algorithms be used?

A: CNSA 2.0 algorithms will be required for all products that employ public-standard algorithms in NSS, whether a future design or currently fielded. Any usage of Suite B or CNSA 1.0 algorithms will be required to transition to CNSA 2.0. The Timeframe section of this FAQ and CNSSP 15 provide transition timeframe information. More details will be released on an ongoing basis as industry adjusts to the new technology.

Q: How did NSA choose the CNSA 2.0 algorithms?

A: NSA chose algorithms from among those selected for standardization by the National Institute of Standards and Technology (NIST), the U.S. Government lead for commercial algorithm approval. NSA believes they offer optimal performance for given NSS security requirements.

Q: How strong does NSA believe CNSA 2.0 algorithms are?

A: NSA performed its own analysis of CNSA 2.0 algorithms and considers them appropriate for long-term use in protecting the varied missions of U.S. NSS.

Q: Does NSA intend to produce guidance for CNSA 2.0 similar to the IETF RFCs[1] produced for CNSA 1.0?

A: NSA will provide direction for using CNSA 2.0 algorithms securely in a variety of use cases, and is working with the IETF to produce informational guides to aide with protocol deployment through the RFC series. RFCs detail protocol options in addition to algorithm choices, and NSA expects to provide protocol guidance to ensure smooth and secure operation with CNSA 2.0 algorithms.

Q: For whom is this guidance intended?

A: NSA makes CNSA 2.0 requirements, anticipated timing, and this related FAQ widely available primarily to assist NSS owners and operators in their transition planning, as well as to inform industry and vendors of NSS requirements. This guidance may also be useful to those seeking to interoperate with NSS or those aiming at similar robust security and interoperability requirements.

[1] Internet Engineering Task Force Requests for Comments.

Q: Does CNSA 2.0 apply to fielded equipment?

A: Even NSS that are in current use will need to be upgraded in a timely fashion unless the system received a waiver through the approved process. This is consistent with National Security Memorandums (NSMs) 8[2] and 10[3] as well as CNSSP 11 and CNSSP 15.

Q: What policies should I follow to meet NSS algorithm requirements?

A: High-grade equipment will follow the guidance in CJCSN 6510[4] and CNSSAM 01-07-NSM[5]. Commercial equipment will follow CNSA 1.0 until the transition mandated by CNSSP 15[6], expected to occur sometime between 2025 and 2030, depending on equipment type. In accordance with NSM-10 and CNSSP-11, QR algorithms should be implemented in NSS mission systems as National Information Assurance Partnership (NIAP) validated products or in accordance with other implementation-specific guidance. Typically, this will include, but not be limited to, requiring modules be validated by the NIST Cryptographic Module Validation Program (CMVP).

Q: What is the difference between ML-KEM and CRYSTALS-Kyber or between ML-DSA and CRYSTALS-Dilithium?

A: ML-KEM and ML-DSA are fully specified standards described by NIST in FIPS 203 and 204, respectively. CRYSTALS-Kyber is the name of the proposed algorithm submitted to NIST that eventually became ML-KEM, and similarly CRYSTALS-Dilithium became ML-DSA. In particular, the CRYSTALS algorithms had a variety of versions that were slightly tweaked prior to the publication of the FIPS documents. Once NIST announced the drafting of CRYSTALS-Kyber and CRYSTALS-Dilithium into standards, NSA announced that the standards would be part of CNSA 2.0. NSA clarified the CNSA 2.0 language when the FIPS documents were published. Only ML-KEM and ML-DSA

[2] Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, 19 January 2022.

[3] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 4 May 2022.

[4] Chairman of the Joint Chiefs of Staff Notice 6510, Information Assurance Cryptographic Device Modernization Requirements, August 2019.

[5] Committee on National Security Systems Advisory Memorandum 01-07-NSM, Cryptographic Equipment Modernization Planning, 20 March 2022.

[6] Committee on National Security Systems Policy 15, Use of Public Standards for Secure Information Sharing.

are in CNSA 2.0; any algorithm that is called CRYSTALS-Kyber or CRYSTALS-Dilithium but does not adhere to FIPS 203 or 204 is not CNSA 2.0 compliant.

Q: Where can I learn more about hash-based signatures?

A: Refer to NIST standardized stateful hash-based signatures in NIST SP 800-208[7]. This standard also provides references to other technical documentation on the topic. NSA recommends using Federal Information Processing Standards (FIPS)-validated LMS or XMSS hash-based signatures to protect NSS in the specialized scenarios outlined in the standard—e.g., for firmware signing and software signing. NSA's preferred parameter set is Section 4.2, LMS with SHA-256/192.

Q: Can I use HSS or XMSSMT from NIST SP 800-208?

A: From NIST SP 800-208, NSA has only approved LMS and XMSS for use in NSS. The multi-tree algorithms HSS and XMSSMT are not allowed.

Q: Can I use SLH-DSA (aka SPHINCS+) to sign software?

A: While SLH-DSA is hash-based, it is not part of CNSA and is not approved for any use in NSS.

Q: I'm going to adopt LMS or XMSS for software/firmware validation for NSS. Which components need to be validated, and how? If my hardware security module (HSM) is not FIPS-validated, can I get a waiver?

A: Signature verification is expected to be performed by code that has been validated by NIST's Cryptographic Algorithm Validation Program (CAVP). It is expected that signed code may be received from a variety of sources (signers). If your product is only verifying signatures, CAVP testing is all that is required.

Code sources (signers) that are NSS are required to produce signatures according to NIST SP 800-208, which requires hardware validated by NIST's Cryptographic Module Validation Program (CMVP), or via other NSA guidance. Waivers will not be granted for this.

While some code sources (signers) are not considered NSS themselves and may not be subject to CNSA requirements, they are expected to use code that meets the same

[7] NIST Special Publication 800-208, Recommendation for Stateful Hash-Based Signature Schemes.

development and operational quality as the validated code, that is, code that can pass CAVP testing for use in NSS components.

Note: To avoid weakening the security of these signatures, one should implement signing and state management in hardware, such as an HSM. Backup flows, which may involve transferring keys between modules, must prevent state re-use.

Q: As a commercial vendor, how do I know if my NIST SP 800-208 implementation meets CNSA 2.0?

A: NIAP validates products against its published Protection Profiles, which will start including quantum-resistant signatures consistent with NSA's published transition timelines. For commercial vendors, NSA does not anticipate NIAP Protection Profiles performing signature generation within the Target of Evaluation (TOE) boundary, only signature verification. As signature generation is the component of LMS/XMSS that requires state management, if only signature verification is being performed, only CAVP validation (not CMVP) will be expected to meet CNSA 2.0 for such products.

Q: Why are signatures for software- and firmware-signing listed separately?

A: The reasons for choosing separate algorithms for software- and firmware-signing are as follows:

- NIST standardized the algorithms in NIST SP 800-208 earlier and has CAVP validation available, while other quantum-resistant signatures may not be as easily available for integration;
- This signature use-case is more urgent;
- This selection places hash-based algorithms, with their substantial history of cryptanalysis, in a use case where their well-described potential performance issues have minimal impact. In particular, this usage coincides well with the requirement for keeping track of state—that is, ensuring a given node with its private data is not used more than once in signing software or firmware when deploying these signatures.

Q: Why are firmware signatures more urgent?

A: In many firmware-signing cases the validation algorithm is not easily updated. Thus, firmware-signing algorithms are frequently locked in for the life of a system. Even in systems that are designed for extensibility and cryptographic agility, a quantum-resistant root of trust may be required in the firmware years before the rest of the system upgrades to quantum-resistance. NSA prioritizes this in its timelines to avoid unexpected costs and security issues later in the NSS transition.

Q: Under what circumstances is SHA-3 available for use?

A**:** At a vendor's discretion, for internal components of a hardware system that do not interoperate outside a vendor's environment, SHA3-384 or -512 may also be used as part of a system's integrity-checking process, such as secure boot. This is specifically being allowed in CNSA 2.0 to speed the transition process when vendor-specific internal processes make use of the properties of a cryptographic hash to enable them to transition to the new post-quantum signatures with minimal disruption to their workflow. In order not to be prescriptive in these cases, and due to the particular threat vectors inherent in these processes, NSA is allowing the use of either SHA-384, SHA-512, SHA3-384, or SHA3-512 for these purposes.

Q: Can I use SHA-3 as a hash?

A: No, neither SHA-3 nor SHAKE are approved for use in CNSA 2.0 as a general purpose hash algorithm. While NSA allows any parameter set of LMS, including some that call SHA-3 as a function, NSA has not approved SHA-3 as a general purpose hash algorithm. Its use is strictly limited to those cases where it is prescribed by the standard describing an NSA-approved algorithm, such as LMS within NIST SP 800-208, or for internal hardware system processes as described above.

The SHA-2 selections are sufficient for security, and their ubiquity in the commercial world ensures interoperability. Using SHA-3 or SHAKE outside those narrowly defined applications where it is completely self-contained, such as when called within an algorithm function, significantly increases the interoperability testing burden and breaks many use cases for CNSA 2.0.

Q: Where can I learn more about lattice-based key encapsulation mechanisms (KEMs) and digital signatures?

A: NIST's post-quantum standardization page includes reports from previous rounds of the standardization effort which detail why NIST chose lattice-based cryptography.

These reports include summaries of all the cryptography under consideration and many references.

Q: Why did NSA choose ML-DSA over FN-DSA (aka Falcon)?

A: For NSS, NSA agrees with NIST: ML-DSA is preferred, as FN-DSA seems more susceptible to implementation errors that may affect security. As NIST has prioritized standardizing ML-DSA, FN-DSA is not available yet, and NSA does not anticipate adding it to CNSA 2.0 when it is.

Q: Can I use ML-DSA for firmware or software signing?

A: Yes, however firmware roots of trust are a critical component to upgrade and NSA expects this to be implemented for some long-lived signatures in 2025, before validated ML-DSA is widely available. At this time, validated LMS and XMSS are commercially available. NSA prefers to see this transition begin now (using LMS and XMSS) rather than wait for ML-DSA due to the long timeframes involved in moving from small components and/or early designs to completed products.

Validated ML-DSA is approved for all signing use cases and when it is available it may be the most appropriate choice for some software/firmware signing use cases. For example, when a user’s software signing strategy requires more signatures than can be reasonably used with a single LMS or XMSS key, or in software development environments with a distributed signing system, it would be reasonable to use ML-DSA.

Q: Is HashML-DSA, aka the pre-hash mode of ML-DSA, allowed in CNSA 2.0?

A: Not at the present time. HashML-DSA is a variant on ML-DSA in FIPS 204, which describes a method of compressing a message before signing while intentionally breaking interoperability with ML-DSA to prevent a vulnerability in the case of key re-use. Because HashML-DSA does not offer any functionality not already offered by the CNSA hash functions combined in a standard way with ML-DSA-87, and because standard ML-DSA-87 is expected to be widely supported, NSA anticipates there will be no need for HashML-DSA in NSS. Hence, at this time, HashML-DSA is not allowed. If at a later date protocol usage demands it, NSA will provide specific guidance on its limited usage at that time.

Q: Will NSA add more selections to CNSA in the future?

A: NSA does not currently plan to add future NIST post-quantum standards to CNSA. Circumstances could change in ways not currently foreseen, but adding more algorithms generally makes interoperability more complex (although admittedly less so for algorithms for software and firmware signing).

Q: What if my solution uses hash functions other than SHA-384 or SHA-512?

A: SHA-384 remains approved in the CNSA 2.0, as NSA believes it provides sufficient security for NSS. Designers often prefer to use SHA-512 for performance reasons. This is now supported by CNSA 2.0; however, customers need to be certain that using SHA-512 does not lead to interoperability issues.

Where NSA has approved an algorithm or cryptographic application that incorporates a truncated hash value (e.g., SHA-256/192) or other NIST-approved hash function (e.g., SHA-3) as part of its design, using those hash functions is acceptable within the scope of the algorithm or cryptographic application. Also, use of SHA3-384 and SHA3-512 is allowed in internal hardware processes, but general purpose use of such hash functions is not approved at this time for NSS.

Just as SHA-512 was added to CNSA, NSA may in the future add another NIST algorithm if it achieves ubiquity in a key area of the ecosystem, satisfies NSA’s independent security requirements, and is unlikely to interfere with interoperability.

Q: How is CNSA 2.0 implementation enforced in NSS?

A: Authorizing officials will be reporting regularly on adoption of CNSA 2.0 in accordance with NSM-10. It is important they use the tools and resources available to ensure all systems that use cryptography for security (including software update mechanisms) implement CNSA 2.0 algorithms. The authorizing officials must report any deviations to NSA in accordance with NSM-10 processes.

Q: Can a commercial product be used in my NSS that runs cryptography other than in CNSA 2.0?

A: If a commercial product does not use CNSA 2.0 algorithms, it is not allowed to be used to protect NSS, unless NSA has provided specific written guidance otherwise. CNSA 2.0 relies on NIST standardized algorithms, which have been widely vetted as quantum resistant, and other algorithms should not be employed. Further, CNSSP-11 requires that commercial products used in NSS be NIAP validated, and this validation will generally require CNSA 2.0 compliance.

Q: When should deployment of CNSA 2.0 algorithms in mission systems begin?

A: When validated products become available, they should be deployed in mission systems. NIAP and the Commercial Solutions for Classified (CSfC) program both intend to swiftly update profiles as validation with new products becomes feasible. For systems outside these programs, please refer to CNSSP 15 and future guidance for deprecation schedules of quantum-vulnerable cryptography. Meanwhile, NSA encourages responsible testing in vendor and government research environments now to understand the effects of deployment of the new algorithms on particular systems given the increased sizes used in these algorithms.

Timeframe

Q: What timeframe information can NSA provide for adoption of CNSA 2.0?

A: NSA intends that all NSS will be quantum-resistant by 2035, in accordance with the goal espoused in NSM-10. NSA’s recent update to CNSSP 15 has set several dates to aid in this transition in the commercial space, with the hope of completing much of the transition sooner.

Any NSS currently validated against a NIAP or CSfC profile continues to be approved for the life of that validation, and no requirement to transition will be enforced prior to December 31, 2025. However, any NSS not CNSA 1.0 compliant has six months from the publication date of the updated CNSSP 15 to come into compliance with CNSA 2.0, or 90 days to request a waiver.

CNSSP 15 states that by January 1, 2027, all new acquisitions for NSS will be required to be CNSA 2.0 compliant unless otherwise noted.

By December 31, 2030, all equipment and services that cannot support CNSA 2.0 must be phased out unless otherwise noted, and by December 31, 2031, CNSA 2.0 algorithms are mandated for use unless otherwise noted.

Q: Will I need to transition all my algorithms to CNSA 2.0 at once?

A: As NSS transition to CNSA 2.0 by 2031, NSA expects to have a long period of systems using both CNSA 1.0 and 2.0 in different places. New NSS developments will be required to support CNSA 2.0 algorithms once appropriate standards for the given technology are in place. All appropriate system components should be configured to prefer CNSA 2.0 algorithms. As products mature, those components should be configured to accept only CNSA 2.0 algorithms.

NSA will provide guidance and updated protection profiles as Standard Development Organizations (SDOs) develop the appropriate standards because product lines may develop at different speeds, and not every profile supporting CNSA 2.0 will support it for every cryptographic service offered. CNSA 1.0 algorithms will continue to be used until current solutions can operate in a CNSA 2.0 mode.

Q: What is the timeline for new deployments?

A: NIAP and the CSfC program will update their profiles and requirements in accordance with industry adoption. NSA intends an aggressive timeframe for adoption (see above) and requests industry support. Starting January 1, 2027, NSA expects new deployments to be compliant with CNSA 2.0, unless otherwise explicitly noted in profiles.

Q: What is the timeline for transitioning fielded equipment?

A: As industry adopts CNSA 2.0 algorithms, NSA will require transition of fielded equipment to CNSA 2.0 as well. In some circumstances, this may require a hardware refresh. NSA encourages NSS owners and operators to plan for this.

Cryptographic agility is necessary to accomplish this transition in a timely manner; even equipment purchased before support is mandated should have sufficient memory and processing power when possible to run new algorithms, as well as capacity for future algorithms and protocols so that any future enhancements can be included via a software update.

NSA expects these equipment transitions to be completed by December 31, 2030.

Q: When will IETF RFCs containing guidance on configurations for CNSA 2.0 compliant protocols be available?

A: IETF and other SDOs are independent bodies that are in charge of their own publication schedules. Due to the interest in this guidance beyond standard NSA customers, and to facilitate quantum-resistant deployment more broadly, NSA is working with IETF and other SDOs to produce RFCs and other documentation with the appropriate level of security and implementation analysis. NSA encourages CNSA 2.0 adoption in standards and deployment in vendor products, but it is not a requirement beyond NSS.

CNSSP 15 and NSM 10

Q: What is National Security Memorandum (NSM) 10?

A: National Security Memorandum 10: Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems lays out a variety of tasks for the federal government to undertake with the goal of achieving quantum resistance by 2035, including the creation of quantum-resistant standards and the deprecation of quantum-vulnerable standards. NSA is explicitly called out to provide timely guidance for quantum resistance in NSS, and NSS owners are given annual reporting requirements for quantum-vulnerable systems.

Q: What is CNSSP 15?

A: Committee on National Security Systems Policy 15 (CNSSP 15) specifies commercial cryptographic algorithms for protecting NSS, in conjunction with other CNSS- and NSA-documented processes. Originally, it specified “NSA Suite B” as the required commercial algorithms for protecting NSS, and then it was revised to specify the CNSA 1.0 Suite in CNSSP 15 Annex B. It now includes CNSA 2.0 algorithms as NIST has completed its initial standards from its Post-Quantum Standardization Process. Further details about CNSS are at www.cnss.gov.

Q: What changes are in the CNSSP 15 update?

A: The 2024 update to CNSSP 15 makes three significant changes in order to execute NSM 10 for its users. These are as follows:

1. It updated the list of allowed algorithm standards, which was previously defined as CNSA 1.0, to now require CNSA 2.0. This deprecated all quantum-vulnerable algorithms, added quantum-resistant public key mechanisms, as well as added SHA-512 into general usage and SHA3 into specific applications.

2. It set out dates for the transition from CNSA 1.0 to CNSA 2.0, including adoption dates for new systems, as well as deprecation dates for currently deployed systems.

3. It revoked the previous eight years of waivers to CNSSP 15, which therefore requires modernization of several NSS.

Q: As an NSS owner, when will my quantum-resistant transition be completed with regard to the reporting requirements under NSM 10?

A: As noted in CNSSP 15, as long as any component of an NSS is still not quantum-resistant, there will still be reporting requirements under NSM 10. Hence, while CNSSP 15 allows the use of currently validated profiles that rely on CNSA 1.0, as long as a profile requires any non-CNSA 2.0 algorithm to function securely (such as those in CNSA 1.0) it will be reportable under NSM 10. NSA expects this to continue for many customers through December 31, 2031, when the vast majority of cryptography in an NSS should be quantum resistant.

Q: How does CNSSP 15 relate to CNSSI 1253, NIST SP 800-53, and the RMF process?

A: CNSS Instruction 1253[8] mandates using the Risk Management Framework (RMF) as documented in NIST SP 800-39[9] and NIST SP 800-53[10] in managing National Security Information Systems. NIST SP 800-53 includes security controls (e.g., SC-12) that relate to cryptography. NSS requires the “NSA Approved” selection. Unless NSA states otherwise, the “NSA Approved” cryptography selection includes CNSA 2.0 algorithm requirements as well as all other relevant NSA guidance on product validation and operation.

[8] Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems.

[9] NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.

[10] NIST Special Publication 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations.

Q: How should the broader government community understand CNSSP 15 requirements?

A: NSA establishes NSS requirements. Often these systems require protection for long periods against sophisticated targeted efforts and well-resourced adversaries in potential wartime settings. NIST establishes cryptographic standards for other government systems.

NSA selected the algorithms in CNSSP 15 from those chosen by NIST in order to satisfy both NSA requirements for NSS and to simplify implementation and interoperability by aligning with NIST standards for general government use. If you are uncertain whether NSS requirements apply to a specific system, contact NSA for assistance. Also see NIST SP 800-59[11].

Quantum alternatives

Q: Can I mitigate the quantum threat to NSS by using a pre-shared key?

A: Many commercial protocols allow a pre-shared key option that may mitigate the quantum threat, and some allow the combination of pre-shared and asymmetric keys in the same negotiation. However, this issue can be complex. Customers who wish to explore this option should contact NSA or follow guidance the CSfC program provides.

Q: Will quantum computers affect non-public-key (i.e., symmetric) algorithms?

A: Quantum computing techniques are generally considered much less effective against symmetric algorithms than against current widely used public-key algorithms. While public-key cryptography requires fundamental design changes, symmetric algorithms are considered secure, provided the key size is sufficiently large. CNSA 2.0 symmetric algorithms, which essentially are the same as their CNSA 1.0 counterparts, are quantum-resistant.

Q: Why does NSA care about quantum computing today? Isn't quantum computing a long way off?

A: NSA has specific requirements documented in NSM 10 to provide quantum resistance for NSS by 2035, which requires concrete steps to be taken over the next

[11] NIST Special Publication 800-59, Guideline for Identifying an Information System as a National Security System.

decade to achieve. NSA does not know when there will be a CRQC. Expert assessments disagree significantly about timing. Because NSS often have very long lifecycles, NSA must produce requirements today for systems that will be used many decades in the future. Consequently, the data these systems protect will still require cryptographic protection for decades after these systems are at end of life. There is growing research in the area of quantum computing, and enough progress that NSA must act now to protect NSS by providing the requirements for the transition to CNSA 2.0.

Q: What is quantum key distribution (QKD)?

A: The field of quantum cryptography involves specialized hardware using the physics of quantum mechanics to protect the confidentiality of sensitive information. The most common example today uses quantum physics to distribute keys for use in a traditional symmetric algorithm, known as “quantum key distribution” or QKD. This technology exists today and is distinct from the quantum computing technology that might one day attack cryptographic algorithms. The sole function of QKD is to distribute keys between users. Hence, it is only one part of a cryptographic system.

Q: Can I use a QKD system to protect my national security system from a quantum computer?

A: No. The technology involved is of significant scientific interest, but it only addresses some security threats and requires significant engineering modifications to NSS communications systems. NSA does not generally consider QKD a practical security solution for protecting NSS. NSS owners should not use or research QKD at this time without consulting NSA directly. For specific questions, NSS owners can contact NSA.

Q: What is a quantum random number generator (quantum RNG)?

A: Quantum random number generators are hardware random number generators that use specific quantum effects to generate nondeterministic randomness. The decision on which RNG is appropriate in a specific scenario depends on many factors. In addition, any properly certified/approved RNG should be acceptable if you implement it within the constraints of that approval.

Commercial Solutions for Classified (CSfC) and National Information Assurance Partnership (NIAP)

Q: Can I use any CNSA-capable product(s) in my NSS without going through NIAP/CSfC?

A: No, CNSSP 11 states that all commercial-off-the-shelf information assurance (IA) and IA-enabled information technology products acquired to protect information on NSS shall comply with NIAP program requirements according to NSA-approved processes and, where applicable, the requirements of FIPS cryptographic validation programs. Furthermore, CNSSP 7 states that a CSfC solution may protect NSS, provided the appropriate Authorizing Official approved it and registration with NSA's CSfC Program Management Office showed it is compliant with an NSA-provided Capability Package.

Q: I have long data life concerns and want to adopt CSfC solutions. How can I ensure my communications and data remain secure against an adversary with a quantum computer?

A: Some CSfC solutions may be implemented today using symmetric, pre-shared keys that protect against the long-term quantum computing threat. NSA considers using pre-shared symmetric keys in a standards-compliant fashion a better near-term post-quantum solution than implementing unvalidated post-quantum asymmetric algorithms. Eventually, NSA will provide Capability Packages—to coincide with commercial technological development—to support CNSA 2.0 algorithms.

For details, contact the CSfC program office.

Future cryptographic algorithms

Q: What algorithms should I use for other areas of cryptography (e.g., Blockchain, Private Information Retrieval, Identity Based Encryption)?

A: NSA wants to know about potential use cases for any of the innovative cryptography listed below (or other similar cryptographic innovation). CNSSP 15 mandates using public standards, while allowing exceptions for additional NSA-approved options when needed. Neither NSA nor NIST has produced standards for these areas, and NSA has not issued any general approval for using these technologies on NSS.

Many of these topics involve novel security properties requiring further scrutiny. NSS owners should consult NSA before using any cryptography that CNSA 1.0 or CNSA 2.0 and other published guidance do not specify. In particular, the following have no generally approved solutions:

- Distributed ledgers or blockchains
- Private information retrieval (PIR)
- Private set intersection (PSI)
- Identity-based encryption (IBE)
- Attribute-based encryption (ABE)
- Homomorphic encryption (HE)
- Group signatures
- Ring signatures
- Searchable encryption
- Threshold signatures

Q: I have a novel cryptographic solution. How do I get my solution "NSA Approved?"

A: NSA has programs for certifying solutions built to protect classified information. This certification process applies to developments intended specifically for government use or control. NSA also manages efforts, such as NIAP and the CSfC program, that require strict compliance with traditional cryptographic standards and designs.

NSA does not accept direct requests from commercial vendors to validate their products or offer a general use vendor certification for novel cryptographic solutions. If an NSS customer believes they have a mission need to use cryptography beyond what is currently available, they should engage with NSA directly to discuss their unique situation.

Q: Will NSA be adopting the standards from NIST's Lightweight Cryptography effort?

A: NSA does not intend to add the ciphers resulting from NIST's Lightweight Cryptography effort to CNSA. The Lightweight Cryptography effort resulted in the selection of symmetric primitives based on the Ascon family. Their targeted security is substantially less than AES-256, rendering them generally unsuitable for NSS use cases. If CNSA 2.0 algorithms do not meet mission system performance requirements, early consultation with NSA is required.

Hybrids

Q: What is a hybrid cryptographic solution?

A: A hybrid solution for a protocol is one using multiple algorithms to perform the same function, such as key agreement or authentication. The solution uses algorithms in a way that requires an attacker to break each one to compromise system security. Hybrid solutions can consist of many traditional or QR algorithms. “Component algorithms” are individual algorithms used in a hybrid solution.

Q: What is NSA’s position on the use of hybrid solutions?

A: NSA has confidence in CNSA 2.0 algorithms and will not require NSS developers to use hybrid certified products for security purposes. However, product availability and interoperability requirements may lead to adopting hybrid solutions.

NSA recognizes that some protocols may require using hybrid-like constructions to accommodate the larger sizes of ML-KEM-1024 or ML-DSA-87 and will work with industry and SDOs to identify the best options for implementation.

Q: What complications can using a hybrid solution introduce?

A: Hybrid solutions add complexity to protocols and crypt libraries, as designers need to incorporate additional negotiation and error handling and implementers need to modify APIs and testing.

Rather than ease the transition to quantum resistance, hybrid deployments introduce additional interoperability concerns because all the algorithms and the method of hybridization must be features common to all parties to a communication. Similarly, hybrid deployments add a second transition later as users eventually move away from classical algorithms in the future entirely and use only quantum-resistant algorithms. At the same time, hybrid solutions make the implementations more complex, so one must balance the risk of flaws in an increasingly complex implementation with the risk of a cryptanalytic breakthrough. Because more security products fail due to implementation or configuration errors than failures in their underlying cryptographic algorithms, spending limited resources to add cryptographic complexity can at times weaken security rather than improve it.

In many scenarios, adding a hybrid option will require the standards community to determine non-obvious choices, such as how to negotiate hybrid algorithms or how to combine keys securely, which may slow down the process of standardization past NSA's deployment goals.

Where NSA recognizes a need to support a hybrid solution, extensive work will be performed to ensure that it can be safely implemented, including engineering to a high degree of robustness, and facilitation of a straightforward transition to QR-only solutions.

Q: Is there an example where NSA will recommend hybrid solutions?

A: Due to difficulties introduced when unencrypted IKEv2 messages exceed a certain byte size, it is not possible to directly replace the CNSA 1.0 public key algorithms with ML-KEM-1024 and its larger public key. Because there is no straightforward way to construct a solution that uses a standalone ML-KEM-1024 key establishment without dramatic changes to this part of IKEv2, NSA anticipates using the solution standardized within IETF, which effectively manages this problem by performing a smaller key establishment, followed by a larger but encrypted key establishment. As a result, for the foreseeable future, NSA's profile of this solution will continue the use of CNSA 1.0 key establishment algorithms, but fortified by key establishment using ML-KEM-1024.

Q: Should one use a hybrid or other non-standardized QR solution while waiting for a final NIST post-quantum standard?

A: Do not use a hybrid or other non-standardized QR solution on NSS mission systems except for those exceptions NSA specifically recommends to meet standardization or interoperability requirements. NSA encourages limited purchase and use for research and planning, but only to prepare for transitioning to a CNSA 2.0 Suite. Because NSA is confident that CNSA 2.0 algorithms will sufficiently protect NSS, it does not require a hybrid solution for security purposes. Except as noted above, hybrid solutions will not be integrated into eventual deployable solutions.

Using non-standard solutions entails a significant risk of establishing incompatible solutions. Using a hybrid solution that involves a symmetric key in accordance with established standards (e.g., RFC 8773, RFC 8784) may be appropriate, but key management complexity generally restricts this to specialized applications.

Further information

Q: Where can I get more information?

A: For CSfC-specific questions, customers should contact the Commercial Solutions for Classified Program Management Office at CSfC@nsa.gov.

Other specific questions from NSS users may be addressed via e-mail to NSACryptoToday@nsa.gov or through normal business channels.

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 in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats 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