Commercial National Security Algorithm (CNSA) Suite 2.0. FAQ

On Thursday April 18th 2024, the NSA released an updated "Frequently Asked Question - FAQ" regarding its Commercial National Security Algorithm (CNSA) Suite 2.0. FAQ: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF).

Crypto4A completed a side-by-side comparison of this new revision and the previous version and found the following additions/changes:

Question: Can I continue to use larger sizes of RSA or ECC to address the threat?
Answer: No. RSA and Elliptic Curve Cryptography are the main algorithms that need to be replaced to achieve quantum resistance.
Crypto4A: This is a new topic that was not included in the prior version of the FAQ.

Question: Can I use HSS or XMSSMT from NIST SP 800-208?
Answer: From NIST SP 800-208, NSA has only approved LMS and XMSS for use in NSS. The multitree algorithms HSS and XMSSMT are not allowed.
Crypto4A: This is a new topic that was not included in the prior version of the FAQ.

Question: Can I use SLH-DSA (aka SPHINCS+) to sign software?
Answer: While SLH-DSA is hash-based, it is not part of CNSA and is not approved for any use in NSS.
Crypto4A: This is a new topic that was not included in the prior version of the FAQ.

Question: I'm going to adopt LMS or XMSS for software/firmware validation. Which components need to be validated, and how? If my hardware security module (HSM) is not FIPS-validated, can I get a waiver?
Answer: 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 validating 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 code sources (signers) that are not NSS are not subject to CNSA requirements, they are expected to use code that meets the same development and operational quality as the validated code, that is, code that can pass CAVP testing.
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."

Crypto4A: This is a new topic that was not included in the prior version of the FAQ. Unless you're an HSM vendor, your product only needs to pass the CAVP testing.

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

Answer: NIAP validates products against its published Protection Profiles, which will start including quantum-resistant signatures in line with our published transition timelines. For commercial vendors, we do not anticipate NIAP Protection Profiles will perform 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 for such products.

Crypto4A: This is a new topic that was not included in the prior version of the FAQ.

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

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

- NIST has standardized the algorithms in NIST SP 800-208 already and has CAVP validation available, while other post-quantum signatures are not yet standardized,
- 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, how many times a given public key was used in signing software or firmware when deploying these signatures.

Crypto4A: This is an updated topic with additional clarifications and highlighted points from the previous version of the FAQ.

Question: Why are firmware signatures more urgent?

Answer: 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 our timelines to avoid unexpected costs and security issues later in our transition.

Crypto4A: This is an updated topic with additional clarifications from the previous version of the FAQ.

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

Answer: No, neither SHA-3 nor SHAKE are approved for use in CNSA as a 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 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.

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 called as a function significantly increases the interoperability testing burden and breaks many use cases for CNSA 2.0.

Crypto4A: This is a new topic that was not included in the prior version of the FAQ with a very non-ambiguous answer.

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

Answer: At this time LMS and XMSS are the only approved digital signing algorithms which have finished standards and validation paths. 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. NSA prefers to see this transition begin now rather than wait for ML-DSA due to the long timeframes involved in moving from small components and/or early designs to completed products.

ML-DSA is approved for all signing use cases and when it is available (i.e., standardized and validated) it may be reasonable 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."

Crypto4A: This is a new topic that was not included in the prior version of the FAQ. Crypto4A's QxHSM already provides LMS algorithm support. Crypto4A's implementation was the first to pass CAVP testing and is available today.

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

Answer: NSA does not currently plan to add future NIST post-quantum standards to CNSA.

Crypto4A: This is a new topic that was not included in the prior version of the FAQ.

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

Answer: If a commercial product does not use CNSA 2.0 algorithms, it is not allowed to be used to protect NSS unless it is approved through the waiver process. 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.

Crypto4A: This is a new topic that was not included in the prior version of the FAQ.

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

Answer: When validated products become available, they should be deployed in mission systems. Meanwhile, NSA encourages responsible testing in vendor and government.

Crypto4A: This is a new topic that was not included in the prior version of the FAQ.

For more details contact:

Robert Grapes
Crypto4A Technologies, Inc.
www.crypto4a.com
https://www.linkedin.com/company/crypto4a
T: +1 613.454.2222 | C: +1 613.266.2323