Commercial National Security Algorithm (CNSA) Suite 2.0

Commercial National Security Algorithm (CNSA) Suite 2.0

- Released by NSA Sep 2022
- Addresses problem that future deployment of a cryptanalytically relevant quantum computer (CRQC) would break public-key systems still used today
- Need 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
- Is an update to CNSA 1.0 Algorithms
- 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.
- Per CNSSP 11, software and hardware providing cryptographic services require NIAP or NSA validation in addition to meeting the requirements of the appropriate version of CNSA

Commercial National Security Algorithm (CNSA) Suite 1.0 Algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

CNSA Suite 2.0
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, Recommendation for Stateful Hash-Based Signature Schemes

CNSA Suite 2.0
Algorithms for Software and Firmware Signing

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.

- NSA recommends Leighton-Micali with SHA-256/192, but all NIST SP 800-208 algorithms are approved for this use case

CNSA Suite 2.0
Allowable 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.

CNSA Suite 2.0
General-use 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.

- Are neither final standards nor Federal Information Processing Standard (FIPS)-validated implementations available at this time
- 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
- Effectively deprecate the use of RSA, Diffie-Hellman (DH), and elliptic curve cryptography (ECDH and ECDSA) when mandated

Transitioning to CNSA Suite 2.0

- The timing of the transition depends on the proliferation of standards-based implementations
- 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

General NIAP Transition Plan for CNSA Suite 2.0

- Will release protection profiles specifying that products support CNSA 2.0 algorithms in accordance with NIST and other standards
- All new equipment must meet the requirement at its next protection profile requirements update to remain NIAP; older compliant
- Using CNSA 2.0 algorithms as the preferred configuration option will begin as soon as validated and tested solutions are available
- NIAP Protection Profile requirements and NSM-10 technology refresh requirements will determine the removal of legacy algorithm support
- At that point, legacy equipment and software not refreshed regularly will require a waiver and a plan to bring it into compliance

Detailed NIAP Transition Plan for CNSA Suite 2.0

- Currently all NIAP PPs must have CNSA 1.0 algorithms
- Will add SHA-512 to all NIAP PPs
- Will require either CNSA 1.0 or CNSA 2.0 be mandatory on all NIAP PPs
- Will implement CNSA asymmetric algorithms for software/firmware signing per following
  - LMS – 1H 2023
  - XMSS – 2H 2023
- Will implement following Key Establishment CNSA 2.0 algorithms in all NIAP PPs when they are standardized and all relevant Assurance Activities have been defined and agreed upon:
  - CRYSTALS - Kyber
  - CRYSTALS – Dilithium (used for Digital Signatures)
- Will deprecate CNSA 1.0 in 2030 – 2033 timeframe
- No current timeline established to make CNSA 2.0 mandatory
  - Will make use of CNSA 2.0 mandatory to be listed on PCL at some point
- Will work with vendors to help try to meet NSA schedule
- Will discuss with CCRA and engage with iTCs how best to integrate CNSA 2.0 into cPPs

Transitioning to CNSA Suite 2.0
Timing for software signing and firmware signing

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

Transitioning to CNSA Suite 2.0
How to prepare for use of CNSA 2.0

- AES-256, SHA-384, SHA-512, and the NIST hash-based signatures listed in NIST SP 800-208 are considered safe against attack by a large quantum computer
  - Should also begin implementing other quantum-resistant algorithms NIST and NSA chose and provide feedback about any issues they discover
- CNSA 1.0 Suite continues to represent the interim strategy as the commercial space transitions to the algorithms in CNSA 2.0
- NSA encourages vendors to use CNSA 2.0 approved hash-based signatures for software- and firmware-signing
- NSA does not approve using pre-standardized or non FIPS-validated CNSA 2.0 algorithms (even in hybrid modes) for NSS missions
- NSA recommends limited use of pre-standardized or non-FIPS-validated CNSA 2.0 algorithms and modules in research settings to prepare for the transition
- NSA requests vendors begin preparing to implement CNSA 2.0 algorithms so they are primed to provide products soon after NIST completes standardization

Commercial National Security Algorithm (CNSA) Suite 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

Transitioning to CNSA Suite 2.0
Timing for software signing and firmware signing

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