NSA CYBERSECURITY

CNSA 2.0 and the Future of Security

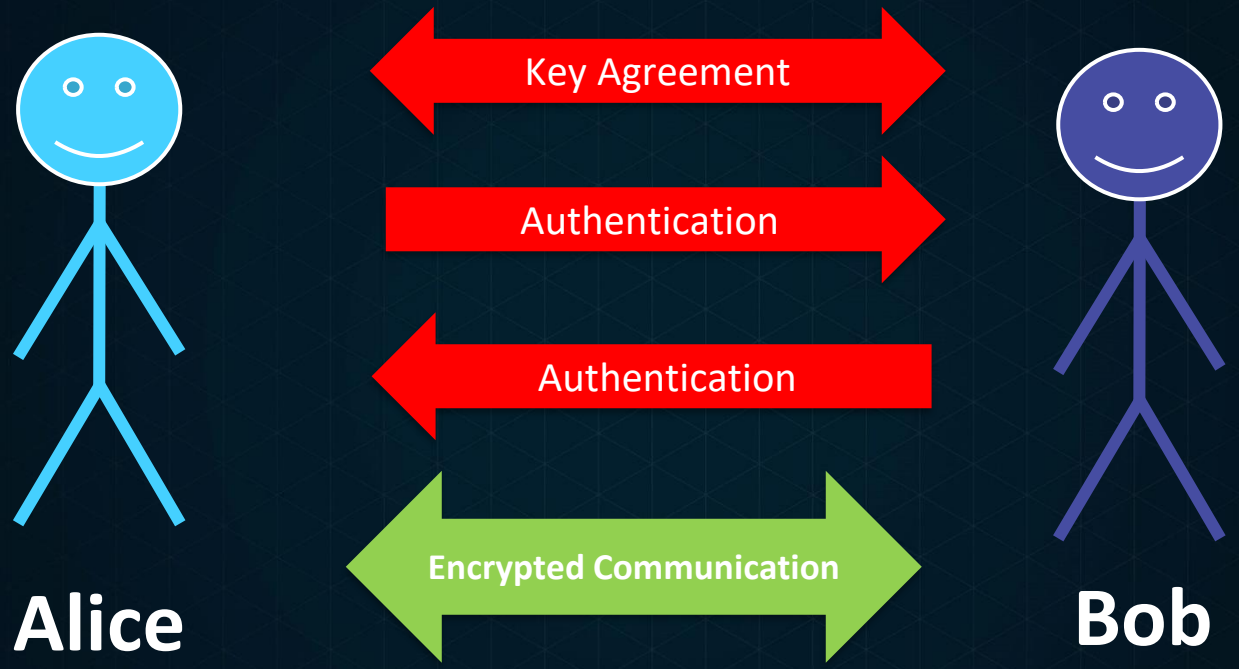
MORGAN STERN, PHD

MARCH 11, 2025

Quantum computing

- A new method of computation based on properties of the some of the smallest systems studied in modern physics, such as single photons or electrons.
- Capable of performing very specific types of calculations exponentially faster than classical computers, including:
  - Physics simulations
  - Chemistry simulations
  - The hard problems underlying the most commonly used key distribution and digital signature algorithms
- While currently there are several quantum computers available for use, and there is great promise in the contributions to science and engineering as the field develops further, they have not yet scaled to be cryptographically relevant.

Cybersecurity ramifications of quantum computing



Red algorithms are currently quantum vulnerable. Any vulnerable algorithm can compromise security.

Our goals with commercially available cryptographic selections

SECURITY

Data must be secured for a long time horizon against a robust set of threats

SIMPLICITY

It must be as easy as possible for our users to comply with our requirements

VALIDATION

It should be simple for our users to validate that their systems comply with NSA guidance

UNIVERSALITY

The requirements should cover the diverse set of use cases that make up the US National Security arena

EASE OF ACQUISITION

It should not be difficult to comply while staying within normal acquisition processes

Commercial National Security Algorithm (CNSA) 2.0 Suite

Quantum Resistant Cryptography approved to protect commercial National Security Systems

Algorithm	Purpose	Relevant NIST standards
General purpose algorithms		
AES-256	Block Cipher	FIPS 197
SHA-384 or SHA-512	Cryptographic Hash	FIPS 180-4
ML-KEM-1024	Public Key Establishment	FIPS 203
ML-DSA-87	Digital Signature	FIPS 204
Specific use case algorithms		
LMS or XMSS (LMS 256-192 recommended)	Software/Firmware Signature	SP 800-208
SHA3-384 or SHA3-512	Hashing in internal hardware (e.g. secure boot)	FIPS 202

Additional guidance available at https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

Committee on National Security Systems Policy 15

USE OF PUBLIC STANDARDS FOR SECURE INFORMATION SHARING

III 4

This Policy… serves as a deprecation of the quantum vulnerable algorithms, defined in the previous version of CNSSP No. 15 (i.e. CNSA 1.0), as well as approval of their quantum resistant (QR) replacements (CNSA 2.0).

IV 10

D/As should consider using this Policy for applications where… protection… may be critical to homeland security and critical infrastructure protection activities as addressed in Executive Order 13228… and Executive Order 13231…

VII 16-17

All previously accepted approvals validated against… (NIAP) protection profiles or Commercial Solutions for Classified Capabilities Packages… are expected to follow the relevant guidance as it updates…

Until fully compliant with CNSA 2.0… requirement for D/As to report annually on their quantum vulnerable systems continues—including any new acquisitions.

CNSA 2.0 Quantum Resistance Timeline*

2022
CNSA 2.0 Released

2024
CNSA 2.0 Finalized

2027
New NSS acquisitions must be QR

2030
All equipment on NSS should be QR capable

2031
All NSS should be QR

2035
NIST proposed date disallowing quantum vulnerable public key

*Specific product lines or technologies and applications will possibly have their own timeline, but barring such separate guidance

Standards and hybrid

- The goal of NSA is to transition quickly and securely to a quantum resistant future
- The fastest standards to use are the ones we have today
- In some cases, such as IPsec, this means having both a quantum-vulnerable and a quantum-resistant key agreement (hybrid)
  - Protocol requires substantial structural changes to use a larger key agreement where presently quantum-vulnerable cryptography is used
- In most cases, adding hybrid agreements requires new standards and more validation
- Importantly, a hybrid agreement offers no quantum-resistant cryptographic security beyond what a pure quantum resistant option offers
- NSA expects CNSA-compliant profiles featuring (for example) TLS, to only use ML-KEM-1024
  - We recognize we may later define more protection profiles for interoperability

CNSA 2.0 in IETF

We have released drafts of CNSA 2.0-compliant configurations of our most used networking standards, and we are actively seeking external input.

- TLS: https://datatracker.ietf.org/doc/draft-becker-cnsa2-tls-profile/01/
- PKIX: https://datatracker.ietf.org/doc/draft-jenkins-cnsa2-pkix-profile/01/
- SSH: https://datatracker.ietf.org/doc/draft-becker-cnsa2-ssh-profile/
- CMC: https://datatracker.ietf.org/doc/draft-jenkins-cnsa2-cmc-profile/
- S/MIME: https://datatracker.ietf.org/doc/draft-becker-cnsa2-smime-profile/
- IPSEC: https://datatracker.ietf.org/doc/draft-guthrie-cnsa2-ipsec-profile/

Coexistence, not Composites

- All PKI transitions take time
- Any CA stood up today will likely still be valid when the first quantum resistant CA's arrive
- Just as today our devices can accept certificates signed with ECDSA and RSA, during the transition we expect certificates signed by ECDSA, RSA, and ML-DSA to exist in the same ecosystem
- In some circumstances, a given device may need both a quantum-vulnerable and a quantum-resistant identity
- Aiming to follow what we historically did as we moved to RSA 2048, and from SHA1 to SHA2
- We do not foresee devices needing a single certificate or identity that incorporates both at once (a "composite")
    - This added complexity increases attack surface and dramatically slows any transition

Takeaways

- The CNSA 2.0 specifications are here
- By the end of 2031 the expectation among commercial NSS will be quantum resistance
- Confidentiality is being quickly added to standards today and we expect fast deployment
- The PKI ecosystem is in a good place to evolve quickly if we work together
    - Stand up a QR root

Questions?