National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

Commercial National Security Algorithm Suite and Quantum Computing FAQ

MFQ U/OO/815099-15
January 2016

Commercial National Security Algorithm Suite and Quantum Computing FAQ

General

Q: To whom is the CNSS Advisory Memorandum 02-15 addressed?

A: NSA's announcement of changes from Suite B cryptography to the Commercial National Security Algorithm Suite are for organizations that run classified or unclassified national security systems (NSS) and vendors that build products used in NSS. NSA is operating under authority it has for setting policy and issuing guidance for NSS—codified in National Security Directive 42 (NSD-42), the Federal Information Security Management Act of 2002 (FISMA) and Department of Defense Instruction 8523.01. To reach the broadest set of NSS operators, customers, and vendors, and to facilitate NSA's Commercial Solutions for Classified (CSfC) effort, this information has been posted on the nsa.gov website.

The NSA announcement is designed to provide sufficient notice to NSS developers and operators to plan and budget for new cryptography as they design their systems. Cryptographic upgrades to NSS often require several years of planning. NSA wants to make sure all NSS owners and developers understand the long term need to transition, and include this in their budget, maintenance, and logistics plans.

Q: What is the Commercial National Security Algorithm Suite?

A: The Commercial National Security Algorithm Suite is the suite of algorithms identified in CNSS Advisory Memorandum 02-15 for protecting NSS up to and including TOP SECRET classification. This suite of algorithms will be incorporated in a new version of the National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems (CNSSP-15 dated October 2012). The Advisory Memorandum and Policy define the set of public cryptographic standards that may be used to protect NSS until acceptable public standards for quantum resistant cryptography exist and are approved for use in NSS by the Committee for National Security Systems (CNSS). The Commercial National Security Algorithm Suite includes:

Algorithm	Usage
RSA 3072-bit or larger	Key Establishment, Digital Signature
Diffie-Hellman (DH) 3072-bit or larger	Key Establishment
ECDH with NIST P-384	Key Establishment
ECDSA with NIST P-384	Digital Signature
SHA-384	Integrity
AES-256	Confidentiality

NSA prefers the use of ECDH with P-384 and 3072-bit DH for key establishment.

CNSS Advisory Memo implementation

Q: Doesn't CNSSP-15 require all commercial NSS acquisitions to incorporate Suite B elliptic curve algorithms by October 2015?

A: Prior to the release of CNSS Advisory Memorandum 02-15 in August 2015 it did. That was an important consideration in the timing of the memorandum. CNSS Advisory Memorandum 02-15 removes that requirement. CNSSP-15 is being updated and will take some time to publish. In the interim, CNSS Advisory Memorandum 02-15 describes the most up-to-date algorithm guidance. See the advisories tab at www.cnss.gov.

Q: I have already complied with the current CNSSP-15 requirements incorporating Suite B into my NSS commercial product/solution. Do I need to update any of the algorithms being used?

A: If you have already implemented Suite B algorithms using the larger (for TOP SECRET) key sizes, you should continue to use those algorithms and key sizes through this upcoming transition period. In many products changing to a larger key size can be done via a configuration change. Implementations using only the algorithms previously approved for SECRET and below in Suite B should **not** be used in NSS.

In more precise terms this means that NSS should no longer use

- ECDH and ECDSA with NIST P-256
- SHA-256
- AES-128
- RSA with 2048-bit keys
- Diffie-Hellman with 2048-bit keys

CNSS Advisory Memorandum 02-15 makes one exception allowing the use of RSA with 2048-bit keys for public key infrastructures

Q: What systems are affected by the new CNSS advisory memorandum?

A: CNSS Advisory Memorandum 02-15 applies to all NSS—classified and unclassified, as defined in NSD-42 and FISMA. Users are expected to migrate to comply with the new requirements; however it is understood that not all applications can change easily or immediately. For specific program questions, engage with NSA for further guidance.

Q: Given the range of algorithm options and sizes to choose from, which is best?

A: CNSS Advisory Memorandum 02-15 alerts NSS developers and operators of the need to transition to quantum resistant algorithms in the future and permits greater flexibility in algorithm choice today than was allowed under the existing CNSSP-15. This flexibility avoids making systems that do not already comply with CNSSP-15 first do an upgrade to comply with

CNSSP-15 and then perform a second upgrade to comply with the quantum resistant CNSSP-15 to be issued in the future. Within this framework, developers, operators and users should choose the most cost effective path to come into compliance with CNSS Advisory Memorandum 02-15. NSS developers, operators or users who need additional guidance should contact NSA.

Q: Which specific algorithm parameters should NSS use?

A: NSS users should select groups based upon well established and validated parameter sets that comply with the minimum required sizes. Some specific examples include:

- Elliptic Curves are currently restricted to the NIST P-384 group only for both ECDH and ECDSA, in accordance with existing NIST and NIAP standards.
- RSA moduli should have a minimum size of 3072 bits (other than the noted PKI exception), and keys should be generated in accordance with all relevant NIST standards.
- For Diffie-Hellman use a Diffie-Hellman prime modulus of at least 3072 bits as specified in IETF RFC 3526 (Groups 15-18). Note: A new set of Diffie-Hellman primes is being considered for use in a new Transport Layer Security specification (TLS 1.3) —these may also be acceptable.

Q: I have already provisioned RSA 4096 certificates on a number of devices used in NSS. Should I move to RSA 3072 certificates?

A: Not necessarily—RSA with 4096 modulus size exceeds the 3072 minimum modulus size and is acceptable for use. Interoperability is a concern that must be considered, though. Because of the nature of RSA, the interoperability questions do not have such a clear answer as with elliptic curve systems. If an NSS customer has a question they should contact NSA via the means indicated at the end of this document.

Q: Can I use the NIST P-521 curve for ECDH or ECDSA on NSS?

A: In order to enhance system interoperability NSA recommends the use of NIST P-384. CNSSP-15 does not permit use of NIST P-521. Use of NIST P-521 needs to be approved by NSA as an exception to policy. This continues under CNSS Advisory Memorandum 02-15.

Q: In CNSS Advisory Memorandum 02-15, NSA notes some exceptions for large scale PKIs to remain at 2048 bits for RSA. Is there a similar exception for use of SHA-256 on NSS?

A: The objective of CNSS Advisory Memorandum 02-15 is the use of SHA-384 in NSS. However, there may exist situations where this is not feasible. The developers or operators of such systems should contact NSA for further discussions. In particular, developers of new NSS equipment should implement SHA-384 instead of SHA-256. Any exception needs to be discussed with NSA.

Commercial Solutions for Classified and NIAP

Q: I have a product/solution built for NSS to go against NIAP Protection Profiles and/or a CSfC Capability Package. How does this affect me?

A: Certified solutions will remain acceptable until they are upgraded/replaced. New draft Protection Profiles that come out will generally be adjusted to support the new algorithm choices as quickly as the market can support them, and Capability Packages that depend on those Protection Profiles will follow in turn. Current plans are to allow up to 2-3 cycles for adherence to the new algorithm requirements in Capability Packages. When products go against the new Protection Profiles for certification, they will need to meet the new algorithm requirements. Note that the Protection Profile process is driven by technology available on the market, so the algorithms specified in individual Protection Profiles or Capability Packages may deviate from those in CNSS Advisory Memorandum 02-15 while NSA work towards a long term algorithm solution. NSA is reviewing the Protection Profiles and Capability Packages scheduled to be published in order to begin rollout of the new requirements within these requirements documents.

Q: I have long data life concerns and want to adopt CSfC solutions. When will I be able to ensure my communications and data are secure against an adversary with a quantum computer?

A: For commercial products used in NSS, there will be a two-step process for achieving security. In the longer term, NSA looks to NIST to identify a broadly accepted, standardized suite of commercial public key algorithms that are not vulnerable to quantum attacks. Meanwhile, NSA has updated its cryptographic strategy to allow for a wider range of public key algorithms to be used in the near term as a cost-saving measure while waiting for quantum resistant algorithms and protocol usage to be standardized. At the moment, one can use symmetric key cryptography in many instances to provide a measure of quantum resistance. For further information see https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm .

Q: My CSfC solution does not support the new algorithms. Can I get an exception, or must I cease use?

A: While NSA advises transitioning to the new algorithms as soon as possible, NSA anticipates situations where the larger key sizes cannot be supported by specific technologies or products. NSA will address these in the Capability Package for general cases while special cases will continue to use the CSfC deviation process. CSfC solutions are required only to comply with the Capability Package with which they were registered. These packages will be updated to conform to the new algorithm guidance, providing a broader selection of acceptable algorithms from which implementers can choose. For greater interoperability, NSA will encourage vendors to support a range of algorithms and sizes, but will not mandate universal support of all acceptable algorithms. Customers will need to ensure that the algorithms they choose are validated in their products.

.

Q: The data I have on my particular NSS has short intelligence life—do I really need to upgrade to new sizes of algorithms as indicated in CNSS Advisory Memorandum 02-15?

A: NSA mandates transitioning algorithms for NSS in order to be part of the common standard and to insure interoperability. In addition, because the Capability Packages will be updated to conform to the new guidance, your solution will eventually become a deviation from the CSfC standard and require special approval. NSA does not intend to grant a large number of deviations. If you believe you are incapable of transitioning, please contact the CSfC office to discuss options.

Quantum Computing Threat

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 will use "qubits" that behave in surprising ways, efficiently performing selected mathematical algorithms exponentially faster than a classical computer.

Q: What is the threat if a quantum computer were developed?

A: A sufficiently large quantum computer, if built, would be capable of undermining all widely-deployed public key algorithms used for key establishment and digital signatures. NSS uses public key cryptography as a critical component to protect the confidentiality, integrity, and authenticity of national security information. Especially in cases where such information needs to be protected for many decades, the potential impact of adversarial use of a quantum computer is known and without effective mitigation is devastating to NSS.

Q: What is "quantum resistant cryptography"?

A: By definition, quantum resistant (or post quantum) cryptography refers to algorithms that are resistant to cryptographic attacks from both classical and quantum computers. Algorithms believed to satisfy this definition are often termed quantum resistant since that is a feature they claim; however, just as algorithms that are claimed to be classically secure are often found to be insecure, the same can happen with "quantum resistant" algorithms

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

A: It is generally accepted that quantum computing techniques are much less effective against symmetric algorithms than against current widely used public key algorithms. While public key cryptography requires changes in the fundamental design to protect against a potential future quantum computer, symmetric key algorithms are believed to be secure provided a sufficiently large key size is used.

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

A: The long lifetime of equipment in the military and many kinds of critical infrastructures—as well as the long intelligence lifetime of much national security information—means that many of

our customers and suppliers are required to plan protections that will be good enough to defeat any technologies that might arise within a few decades. Many experts predict a quantum computer capable of effectively breaking public key cryptography within that timeframe, and therefore NSA believes it is important to address that concern.

Q: How long are the lifetimes in NSS for: deployment of algorithms, use of equipment, national security information intelligence value?

A: Algorithms often require 20 years to be fully deployed on NSS. NSS equipment is often used for 30 years or more. National security information intelligence value is often 30 years (sometimes more), although it may vary depending on classification, sensitivity, and subject.

Q: Why is now the right time to make an announcement?

A: Choosing the right time to champion the development of quantum resistant standards is based on 3 points: forecasts on the future development of a large quantum computer, maturity of quantum resistant algorithms, and an analysis of costs and benefits to NSS owners and stakeholders. NSA believes the time is now right—consistent advances in quantum computing are being made, there are many more proposals for potentially useful quantum resistant algorithms than were available 5 years ago, and the mandatory change to elliptic curves that would have been required in October 2015 presented an opportune time to make an announcement. NSA published the advisory memorandum to move to quantum resistant symmetric key options and to allow additional continued use of older public key options as a way to reduce modernization costs in the near term. In the longer term, NSA is looking to all NSS vendors and operators to implement standards-based, quantum resistant cryptography to protect their data and communications.

Q: Aren't the public key algorithms in the CNSS advisory memorandum all vulnerable to quantum attacks?

A: The public-key algorithms (RSA, Diffie-Hellman, ECDH, and ECDSA) are all vulnerable to attack by a sufficiently large quantum computer. The intent of the interim strategy is not to provide quantum resistance, but to allow more flexibility for customers and vendors in the near term to save on costs while quantum resistant standards are being developed.

Q: Is there a quantum resistant public-key algorithm that commercial vendors should adopt?

A: While a number of interesting quantum resistant public key algorithms have been proposed external to NSA, nothing has been standardized by NIST, and NSA is not specifying any commercial quantum resistant standards at this time. NSA expects that NIST will play a leading role in the effort to develop a widely accepted, standardized set of quantum resistant algorithms. Once these algorithms have been standardized, NSA will require vendors selling to NSS operators to provide FIPS validated implementations in their products. Given the level of interest in the cryptographic community, we hope that there will be quantum resistant algorithms widely available in the next decade. NSA does not recommend implementing or using non-standard algorithms, and the field of quantum resistant cryptography is no exception.

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

A: Some protocols do allow a pre-shared key option that may mitigate the quantum threat. This issue can be complex. Customers who wish to explore this option should contact NSA or follow guidance that will be provided as part of the CSfC program.

Q: What can developers do to prepare for a future quantum resistant algorithm suite?

A: The AES-256 and SHA-384 algorithms are symmetric, and believed to be safe from attack by a large quantum computer. Developers can meet these requirements today. In the area of public key algorithms the future is less clear. One area of general agreement appears to be that the key sizes for these algorithms will be much larger than those used in current algorithms. Developers should plan for storing and transmitting public key values that may be larger than those used today. Work will be required to gauge the effects of these larger key sizes on standard protocols as well. NSA encourages those interested to engage with standards organizations working in this area and to analyze the effects of adopting quantum resistant algorithms in standard protocols.

Q: When will quantum resistant cryptography be available?

A: For systems that will use unclassified cryptographic algorithms it is vital that NSA use cryptography that is widely accepted and widely available as part of standard commercial offerings vetted through NIST's cryptographic standards development process. NSA will continue to support NIST in the standardization process and will also encourage work in the vendor and larger standards communities to help produce standards with broad support for deployment in NSS. NSA believes that NIST can lead a robust and transparent process for the standardization of publicly developed and vetted algorithms, and we encourage this process to begin soon. NSA believes that the external cryptographic community can develop quantum resistant algorithms and reach broad agreement for standardization within a few years.

Q: Does the fact NSA is making this change today mean a quantum computer exists?

A: NSA does not know if or when a quantum computer of sufficient size to exploit public key cryptography will exist. The cryptographic systems that NSA produces, certifies, and supports often have very long life-cycles. NSA has to produce requirements today for systems that will be used for many decades in the future, and data protected by these systems will still require cryptographic protection for decades after these solutions are replaced. There is growing research in the area of quantum computing, and enough progress is being made that NSA must act now to protect NSS by encouraging the development and adoption of quantum resistant algorithms.

Q: What about quantum key distribution (QKD)?

A: It is possible to use quantum mechanics to protect secrets using techniques commonly referred to as QKD (when used to establish a secret key then used in symmetric cryptography). This is entirely distinct from the use of quantum computing to attack cryptographic algorithms. The use of QKD is not presently part of the NSA Commercial Solutions for Classified program.

Q: What about quantum cryptography?

A: Quantum cryptography (as opposed to quantum resistant cryptography) is similar to QKD—it uses the same techniques to protect messages directly as opposed to establishing a key for use in symmetric key cryptography. NSA has no current plans to use quantum cryptography as a commercial solution.

Further questions

Q: The commercial world appears to be moving to elliptic curves. Why is NSA continuing to support older algorithms?

A: NSA supports the use of NIST P-384 in NSS. In the original CNSSP-15 both RSA and Diffie-Hellman were included as legacy algorithms which were only to be used until replacement elliptic curve cryptography (ECC) equipment was available. Since that time NSA has come to appreciate that some of these legacy systems will be around for much longer than we had planned. Because of these legacy systems and because there is an eventual need to move to quantum resistant public key algorithms, NSA has decided that it may be more cost effective for some NSS to continue to use RSA and Diffie-Hellman with larger key sizes until the new quantum resistant public key algorithms are ready. NSA does not want to force NSS operators to pay for two cryptographic upgrades: first from RSA/Diffie-Hellman to ECC and then from ECC to quantum resistant cryptography.

Q: Are you telling vendors to stop transitions to elliptic curve cryptography?

A: No. Rather, NSA wants vendors and NSS developers, operators and customers to comply with CNSS Advisory Memorandum 02-15 as soon as feasible. Many NSS owners would not have the resources to switch first to elliptic curves and then to quantum resistant cryptography within a limited timeframe. The advisory memorandum allows these system owners to avoid the extra cost incurred by first transitioning to ECC and then transitioning to quantum resistant cryptography by skipping that first transition where that makes sense. These system owners can continue to use their existing RSA and Diffie-Hellman cryptography by increasing the key size to that required for the protection of TOP SECRET information.

Q: Why eliminate the lower (up to SECRET) level of Suite B in the Commercial National Security Algorithm Suite?

A: Originally, NSA allowed a lower level for SECRET traffic because, at the time, some devices could not manage the computational load of the larger algorithms. However, technological advances are gradually eliminating that barrier. Considering the endurance of certain NSS legacy systems and the long timeline for systems to transition to new cryptographic algorithms, NSA has determined that equipment for NSS that is being built and deployed now using ECC should be held to a higher standard than is offered by P-256, AES-128, and SHA-256.

Elimination of the lower level of Suite B also resolves an interoperability problem raised by having two levels. Some vendors were implementing only SECRET level algorithm sizes and

their NSS customers wanted to use those for protecting TOP SECRET information which is not allowed under CNSSP-15.

Q: I thought ephemeral key establishment was better because it provides forward secrecy. Won't the guidance in CNSS Advisory Memorandum 02-15 decrease the use of ephemeral key establishment?

A: NSA supports the use of ephemeral key establishment, and believes that quantum resistant standards will include ephemeral key establishment techniques. NSA also recognizes that there is a significant use of other key establishment techniques in NSS, and is allowing the continued use of RSA for the ease of NSS operators. Pre-shared key solutions to be used in the interim for quantum resistance also use ephemeral key establishment as part of the protocols. In the interim, ephemeral key agreements are still supported via finite field Diffie-Hellman (3072-bit or larger) and elliptic curve Diffie-Hellman (using P-384).

Q: Did my company waste time/money implementing Suite B curves?

A: NSA extends its gratitude to those vendors who implemented Suite B algorithms in their products. The support provided by vendors to implement each of the Suite B algorithms is much appreciated and represents a great achievement.

NSA does not believe this effort was wasted. CNSS Advisory Memorandum 02-15 specifies the use of P-384 for both ECDH and ECDSA as approved, so there should be a significant NSS market for P-384 algorithms. While the external community appears to be shifting somewhat toward the use of other elliptic curves, the Suite B curves have been widely implemented and adopted, and NSA expects that there will be continued use of them for the foreseeable future.

Q: How did NSA determine the sizes of RSA and Diffie-Hellman to use?

A: In CNSS Advisory Memorandum 02-15 NSA changed the status of these algorithms from legacy to supported in order to allow their extended use until quantum resistant cryptography is available. The selection of a 3072-bit key size for RSA and Diffie-Hellman was made after considering the expected longevity of the NSS that would need to use these algorithms and the practical technology constraints of some of those systems. Larger sizes for RSA and Diffie-Hellman are acceptable, as specified in the guidance. NSA will provide guidance to vendors and NSS developers, operators and users on the appropriate key sizes for their specific application.

Further Info

Q: Where can I get further info?

A: Customers should contact NSA through normal channels. For CSfC specific questions customers should contact the Commercial Solutions for Classified Office at (410) 854-6906. Other specific questions may be addressed via e-mail to NSACryptoToday@nsa.gov.

Disclaimer of Warranty and 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 products, 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.

CONTACT INFORMATION

Industry Inquiries
410-854-6091
email: bao@nsa.gov

CLIENT REQUIREMENTS AND GENERAL INFORMATION ASSURANCE INQUIRIES

IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov