NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

CSfC Post Quantum Cryptography Guidance Addendum 1.0

Draft .5

Version 1.0 Draft .5
4 April 2025

CHANGE HISTORY

Title	Version	Date	Change Summary
CSfC Post Quantum Cryptography Guidance Addendum	1.0 Draft .5	4 April 2025	Initial Release

Table of Contents

1 Introduction 1

2 Purpose and Use 1

3 Legal Disclaimer 2

4 Overview 2

4.1 CNSA 2.0 Timeline 3

4.1.1 CNSSP 15 Considerations 3

4.2 Post Quantum Cryptography using Certificates 4

4.3 Post Quantum using Pre-Shared Keys 5

4.4 Software and Firmware Signing 8

4.5 Certificate and Certificate Revocation List 8

5 CNSA 2.0 Protocols Considerations 9

5.1 IPsec 9

5.1.1 CNSA Suite 2.0 Profile for IPsec 9

5.1.2 Other Relevant Standards for CNSA 2.0 and Post Quantum for IPsec 10

5.2 TLS 11

5.2.1 CNSA Suite 2.0 Profile for TLS 1.3 11

5.2.2 Other Relevant Standards for CNSA 2.0 and Post Quantum for TLS 11

5.3 EAP TLS 11

5.4 Certificate and Certificate Revocation List 12

5.4.1 CNSA Suite 2.0 Profile for Certificate and Certificate Revocation List 12

5.5 Wi-Fi 12

5.5.1 WPA3 SAE 12

5.6 SSH 13

5.6.1 CNSA Suite 2.0 Profile for SSH 13

6 Mobile Access CP 13

6.1 MA CP IPsec Changes 13

6.2 MA CP TLS Changes 14

7 Campus WLAN CP 14

7.1 CWLAN IPsec Changes 14

7.2 CWLAN WPA3 Enterprise Changes 15

8 Multi-Site Connectivity CP 15
8.1 MSC IPsec Changes 16
8.2 MSC MACsec Changes 16
9 Data-at-Rest CP 17
Appendix A. Glossary of Terms 18
Appendix B. Acronyms 20
Appendix C. References 22

Table of Figures

Figure 1. CNSA 2.0 IKE Exchange 10

List of Tables

Table 1. CNSA 2.0 Post Quantum public-key algorithms 4
Table 2. Applicability of PQC to CSfC Capability Packages 5
Table 4. CNSA 2.0 Symmetric-Key and Hashing Algorithms 8
Table 5. CNSA 2.0 Algorithms for Software and Firmware Signing 8
Table 6. Approved CNSA 2.0 Suite for MA IPsec 13
Table 7. Approved CNSA 2.0 Suite for MA TLS 14
Table 8. Approved CNSA 2.0 Suite for CWLAN IPsec 14
Table 9. Approved CNSA 2.0 Suite for CWLAN EAP-TLS 15
Table 10. Approved CNSA 2.0 Suite for MSC IPsec 16
Table 11. Approved CNSA Suite for MSC MACsec 16
Table 12. Approved CNSA 2.0 Suite for MSC MACsec EAP-TLS 16
Table 13. Approved Commercial National Security Algorithm (CNSA) Suite for DAR 17

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency's (NSA) Cybersecurity Directorate (CSD), publishes Capability Packages (CPs) to provide configurations that empower NSA customers to implement secure solutions using independent, layered Commercial Off-the-Shelf (COTS) products. The CPs are product-neutral and describe system-level solution frameworks documenting security and configuration requirements for customers and/or Integrators.

This document is an Addendum to the *CSfC Mobile Access (MA), Campus WLAN (CWLAN), Multi-Site Connectivity (MSC) and Data at Rest (DAR) CPs* that conveys a structural change to encryption standard to clarify the usage of post quantum cryptography (PQC) technologies, product selections, and other changes. This addendum is provided to allow for the customer base and interested parties to comment on these changes before they are made within the above-mentioned CPs and released as minor increments to these CPs. This addendum will have two separate releases first being the release of the objective requirements and the second release making the requirements in this document the requirements for all CSfC Solutions.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a National Information Assurance Partnership (NIAP)-validated component in a CSfC solution may invalidate its certification and require a revalidation process. To avoid delays, customers and integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/scheme-pub-6.pdf) to determine whether such a modification will affect the component's certification.

If a component is modified, NSA's CSfC Program Management Office (PMO) requires a statement from NIAP that states the modification does not alter the certification, or the security of the component. Modifications that trigger the revalidation process include, but not limited to configuring the component in a manner different from its NIAP-validated configuration and modifying the Original Equipment Manufacturer's code (to include digitally signing the code).

2 PURPOSE AND USE

This Addendum provides high-level reference designs, corresponding configuration requirements, and timelines implementing Post-Quantum cryptography that allow customers to select COTS products from the CSfC Components List, available on the CSfC web page (https://www.nsa.gov/resources/commercial-solutions-for-classified-program), to use Post Quantum Cryptography to meet the requirements needs of the MA, CWLAN, MSC and DAR CPs. As described throughout this Addendum, customers must ensure that the components selected from the CSfC Components List provide the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold (T) Requirements, or the corresponding Objective (O) Requirements applicable to the selected capabilities, must be implemented.

Please provide comments on usability, applicability, and/or shortcomings to your NSA Client Advocate and the Key Management Maintenance Team at CSfC_Key_Man_Req_Team@nsa.gov. CSfC solutions

must also comply with the Committee on National Security Systems (CNSS) Policies and Instructions. Any conflicts identified between this Addendum and CNSS or local policy should be provided to the Addendum Maintenance Team. . CSfC solutions must also comply with the Committee on National Security Systems (CNSS) Policies and Instructions. Any conflicts identified between this Addendum and CNSS or local policy should be provided to the Key Management Maintenance Team at CSfC_Key_Man_Req_Team@nsa.gov.

Customers and integrators must adhere to all applicable data transfer policies for their organization when designing and implementing these capabilities within their CSfC solution architecture. For example, DoD customers must follow DoDI 8540.01 when deploying a CDS within a CSfC solution and if any discrepancies are found between the guidance in this document and DoDI 8540.01 report according to the instruction found in this section.

3 LEGAL DISCLAIMER

This Addendum is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed.

In no event must the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Addendum, even if advised of the possibility of such damage.

The user of this Addendum agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this Addendum is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 OVERVIEW

This Addendum describes a structural change to the encryption used within CSfC Data in Transit and Data at Rest solution that clarifies the usage of technologies, product selections, and other changes within the MA, CWLAN, and DAR CPs to mitigate the threat of a cryptographically relevant quantum computer. The following changes will be made to the overall CSfC program: The addition of Commercial National Security Algorithm (CNSA) 2.0 encryption schemes to the CSfC Encryption Components (WLAN Access System, VPN Gateways, MACsec devices, TLS Protected Servers, File Encryptor and Full Disk Encryption) as an objective encryption algorithm. The use of Pre-Shared Key material within CSfC Solutions as a near-term Post-Quantum solution. A timeline for implementation of CNSA 2.0 algorithms and other mitigations for protections against cryptographically relevant quantum computer.

4.1 CNSA 2.0 TIMELINE

NSM-10 mandates all NSS must implement Post-Quantum cryptography by 2035 to mitigate the threats of a cryptographically relevant quantum computer. For the CSfC Program, there are four important components for CSfC: Software/Firmware Signing, Web Browsers, Network Equipment, and operating systems. These four technology types cover nearly all cryptographically relevant components within the CSfC Program. The following is the mapping of the technology type to specific CSfC Components:

- Software/Firmware Signing – All components
- Web Browsers – TLS Protected Clients, TLS Protected Server, SRTP Clients and SRTP Server
- Network Equipment – IPsec Gateway, MACsec Gateway, WLAN Access System
- Operating Systems – IPsec Client, WLAN Client, File Encryption, Software Full Disk Encryption and Hardware Full Disk Encryption

The timelines for the four components will be simplified into a single timeline for the CSfC Program with the goal of all CSfC solutions deployed to implement Post Quantum Cryptography by 2030. Currently, within the CSfC Program all customers who process long life data are required to implement Pre-Shared Keys within one but preferably two layers of the CSfC Cryptographic boundary to ensure that data will remain protected for the entire lifetime of the data. The following is the currently planned timeline for CNSA 2.0 in the CSfC Program:

- 2026 - NIAP updates the relevant Protection Profiles to Include CNSA 2.0 algorithms and software/firmware signing.
- 2026 - The CSfC Program will update MA, CWLAN, MSC, DAR CPs, and KM Annex to include CNSA 2.0 algorithms and software/firmware signing as objective requirements.
- 2027 - CSfC Components begin to appear on the list with CNSA 2.0 algorithms supported.
- 2028 - CSfC MA, CWLAN, MSC, DAR CPs, and KM Annex updated to require CNSA 2.0 for all encryption and software/firmware signing for all components listed on the CSfC Components list.
- 2030 - All registered solutions have CNSA 2.0 algorithms or other Post-Quantum mitigations in place for all CSfC cryptographic layers.

This timeline is subject to change and may be adjusted depending on both vendor and customer feedback and feasibility of the implementation of such technologies.

4.1.1 CNSSP 15 CONSIDERATIONS

The update of *CNSSP 15 Use of Public Standards for Secure Information Sharing* includes adoption of the new CNSA 2.0 standards into all Cyber Security elements of the National Security Systems. CNSSP 15 offers a timeline to ensure the adoption of CNSA 2.0 within NSS systems and the timeline is the following:

- December 31 2025 - CNSA 1.0 algorithms accepted without waiver.
- January 1 2027 - CNSA 2.0 required in all new products and services unless stipulated by CSfC CP, NIAP PP or a Waiver is in place.
- December 31 2030 - Equipment not supporting CNSA 2.0 should be replaced; CNSA 2.0 is the preferred protocol.
- December 31 2031 - CNSA 2.0 mandated for all systems unless stipulated by CSfC CP, NIAP PP or a Waiver is in place.
- This timeline matches up with the CSfC Programs timeline for CNSA 2.0 implementation with the program planning on beginning transition over to CNSA 2.0 in 2028 and finishing the transition by 2030 with all registered solutions.

4.2 Post Quantum Cryptography using Certificates

Certificate-based cryptography is the preferred method for Data-in-Transit solutions for CSfC solutions, as it provides scalable authentication with easily revocability allowing devices to be easily denied network access in case of lose or compromise of the device. The use of certificate-based cryptography is required for all communication for EUDs within CSfC solutions because of the nature of the EUDs being mobile devices with access to protected information. Currently, CNSA 1.0 algorithms are required to secure these communications, but CNSA 1.0 key establishment and digital signature algorithms are vulnerable to a cryptographically relevant quantum computer. As a near-term mitigation, Pre-Shared Keys can be used in conjunction with certificate-based authentication to mitigate the vulnerability that is detailed in section 4.3.

Table 1. CNSA 2.0 Post Quantum public-key algorithms

Algorithm	Function	Specification	Parameters
Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM)	Asymmetric algorithm for key establishment	FIPS 203	ML-KEM-1024 approved for all classification levels
Module-Lattice-Based Digital Signature Algorithm (ML-DSA)	Asymmetric algorithm for digital signatures	FIPS 204	ML-DSA-87 approved for all classification levels

As part of the Post-Quantum strategy, the CNSA 1.0 key exchange algorithms Elliptic-curve Diffie–Hellman (ECDH) and Rivest–Shamir–Adleman (RSA) will be replaced by the CNSA 2.0 ML-KEM. For digital signatures, Elliptical Curve Digital Signature Algorithm (ECDSA) and RSA will be replaced by ML-DSA. ML-

KEM and ML-DSA deployments in CSfC will be required to adhere to the specification and parameters as shown in Table 1.

Table 2. Applicability of PQC to CSfC Capability Packages

Capability Package	PQC Implementation: Inner Tunnel vs. Outer Tunnel
MA CP	The outer tunnel uses IPsec and inner using IPsec or TLS thus the Key Exchange algorithms will be changed out for ML-KEM and the Digital Signatures will be replaced with ML-DSA; Hashing will include options for usage of SHA-384 or SHA-512.
CWLAN CP	The outer encryption uses WPA3 Enterprise and inner using IPsec thus the Key Exchange algorithms will be changed out for ML-KEM and the Digital Signatures will be replaced with ML-DSA; Hashing will include options for usage of SHA-384 or SHA-512.
MSC CP	The outer encryption uses IPSec or MACsec with EAP-TLS and inner using IPSec or MACsec with EAP-TLS thus the Key Exchange algorithms will be changed out for ML-KEM and the Digital Signatures will be replaced with ML-DSA; Hashing will include options for usage of SHA-384 or SHA-512.
DAR CP	Digital Signatures will be replaced to use ML-DSA; Hashing will include options for usage of SHA-384 or SHA-512.

For more information on the particular changes to the CP see sections 6 through 9 and for information on the particular considerations of any of the CSfC Encryption Layer protocols see section 5.

4.3 Post Quantum using Pre-Shared Keys

For CSfC customers who have a current requirement to protect long-life classified information[1], Symmetric Pre-Shared Keys (PSKs) / Post-Quantum PSKs (PPKs) should be used at this time instead of, or in addition to, certificate-based cryptography (depending on the cryptographic protocol) to provide quantum resistant cryptographic protection of classified information within CSfC solutions, and mitigate the threat of capture data now and decrypt later. As specified in the CSfC Symmetric Key Management

[1] Long-life is defined as needing protection for 15 years or longer.

Requirements Annex, at least one of the two CSfC solution tunnels must use PSKs to provide the required quantum resistant cryptographic protection for that information. Both tunnels should use PSKs when possible to provide quantum resistant protection to the entire CSfC solution, however at least one tunnel must use asymmetric public/private key pairs for mutual authentication per the requirements of the applicable CP and the *CSfC Key Management Requirements Annex*.

There are two protocols which are currently approved to use PSKs in CSfC solutions to enable quantum resistant confidentiality protection of data:

- Internet Protocol Security (IPsec) with Internet Engineering Task Force (IETF) Request for Comments (RFC) 8784-compliant implementations of Internet Key Exchange (IKE) v2
- Media Access Control Security (MACsec)
- Other protocols may be approved in the future by the CSfC program office[2]

PSKs used for MACsec devices are referred to as pre-shared Connectivity Association Keys (CAKs) in the MSC CP. Every CAK has a unique Connectivity Association Key Name (CKN) to distinguish it from other CAKs that may be loaded in the MACsec Device. CAKs are used in MACsec by the MACsec Key Agreement (MKA) protocol which is based on a hierarchical key derivation structure, with the CAK being the root of the key hierarchy. In a CSfC solution that implements MACsec on both layers and complies with the Multi-Site Connectivity (MSC) CP, MACsec devices should use PSKs for one layer while the other layer of the solution uses certificate-based MACsec.

In order for CSfC solutions using IPsec on one or both layers to incorporate quantum resistant protection, RFC 8784-compliant implementations of IKEv2 must be used. RFC 8784 adds an extension to IKEv2 to enable it to be quantum resistant by using symmetric keys shared between peers, known in the RFC as a Post-quantum PSKs (PPKs), which are used as one of the inputs to the key derivation function used for establishing security associations in IKEv2 and IPsec.

The PPKs described in RFC 8784 are independent of and used in addition to authentication methods supported by IKEv2. RFC 8784 supports the possibility to use either public key certificates or authentication PSKs for IKEv2 authentication in addition to the RFC 8784 defined PPKs to enable quantum resistant confidentiality protection. In CSfC solutions using RFC 8784-compliant IKEv2 to provide quantum resistant IPsec, public key certificates must be used for mutual authentication in addition to PPKs. PPKs and PSKs are synonymous in regards to the requirements and guidance described in this document and the CSfC Symmetric Key Management Requirements Annex for managing PSKs.

When PSKs are used in a CSfC solution, they should be used for at least the inner tunnel when possible. In some cases, PSKs cannot be used for the inner tunnel if the inner tunnel protocol is not approved for use with PSKs (e.g., Mobile Access CP where the inner tunnel uses Transport Layer Security [TLS] version 1.2). Table 3 summarizes where PSKs are used in the various CSfC solutions. More detailed implementation requirements for PSKs in these CSfC solutions is provided in the CSfC Symmetric Key Management Requirements Annex.

[2] The CSfC program office plans to approve TLS 1.3 for use with PSKs in the future.

183 **Table 3: Applicability of PSKs to CSfC Capability Packages**

Capability Package	PSK Implementation: Inner Tunnel vs. Outer Tunnel
Mobile Access (MA)	If the Inner and outer tunnels use IPsec, then PSKs must be implemented on at least one of the tunnels with IPsec RFC 8784-compliant IKEv2. PSKs should be implemented on the outer tunnel with IPsec RFC 8784-compliant IKEv2 when the inner tunnel is TLS/SRTP, or when there are multiple Red Network enclaves of different security levels in the solution. PSKs should be implemented on both the inner AND the outer tunnel with IPsec RFC 8784-compliant IKEv2 if technically feasible.
Campus Wireless Local Area Network (WLAN)	The inner tunnel always uses IPsec. Therefore, PSKs must be implemented on the inner tunnel with IPsec RFC 8784-compliant IKEv2.
Multi-Site Connectivity (MSC) There are four configurations supported by the MSC CP: 1. Outer VPN Device and Inner VPN Device 2. Outer VPN Device and Inner MACsec Device 3. Outer MACsec Device and Inner VPN Device 4. Outer MACsec Device and Inner MACsec Device	For each configuration, PSKs must be implemented as follows: 1. PSKs must be implemented on both the inner and outer tunnel VPN Devices with IPsec RFC 8784-compliant IKEv2. 2. PSKs must be used for the inner tunnel MACsec Devices AND PSKs must be used for the outer tunnel VPN Devices with IPsec RFC 8784-compliant IKEv2. 3. PSKs must be used for the outer tunnel MACsec Devices AND PSKs must be used for the inner tunnel VPN Devices with IPsec RFC 8784-compliant IKEv2. 4. PSKs must be used for either the Inner tunnel MACsec Devices OR the Outer tunnel MACsec Devices.

184

185 CSfC customers need to be aware of the risks involved in using PSKs. First, PSKs need to be of adequate
186 strength for them to be used to access and protect classified information. Second, PSKs need to be
187 securely generated, distributed, installed, and managed to mitigate the risk of unauthorized disclosure
188 of the PSKs (e.g., insider threat). A compromised PSK permits an adversary attack, and affects at least
189 two CSfC solution components. Upon detection of a compromised PSK, CSfC solution components that
190 use that PSK need to be rekeyed with a new PSK. In cases where compromised CSfC solution
191 components are suspected as the source of a PSK compromise, the solution components must follow
192 analysis and destruction requirements as stated in the CPs (e.g., MA-EU-10 and MA-EU-11). Therefore,
193 PSK management, which includes the generation, distribution, installation, rekey, destruction, and
194 accounting of symmetric PSKs, is a critical function for CSfC solutions that use PSKs. PSK management
195 can be provided by enterprise services or via locally operated solutions. The PSK implementation

requirements defined in this document applies to both enterprise and locally operated symmetric key generation and management solutions used to support PSK management within CSfC solutions.

Table 3. CNSA 2.0 Symmetric-Key and Hashing 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

4.4 Software and Firmware Signing

As part of the requirement laid out in NSM-10, the CSfC Program will be adding Software and Firmware Signing requirements for all components listed on the CSfC Components list. The implementation timeline of this will be the same as the CNSA 2.0 timeline in CSfC and subject to change depending on market acceptance, vendor and customer feedback into this new requirement.

There are three acceptable algorithms for software and firmware digital signatures, which are all included as part of the CNSA 2.0 cipher suites. These algorithms are enumerated within Table 5 and only one of the algorithms will be required to meet this requirement.

Table 4. CNSA 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 800-2	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
Module-Lattice-Based Digital Signature Algorithm (ML-DSA)	Asymmetric algorithm for digital signatures	FIPS 204	ML-DSA-87 approved for all classification levels

4.5 Certificate and Certificate Revocation List

The change in asymmetric cryptography to support the new larger key exchanges and signing algorithms requires changes to the Certificate Authorities (CA) and Certificate Revocation Lists (CRL) supporting all

CSfC Solutions. All CSfC certificates supporting the Inner and Outer Encryption Tunnels must use X.509 v3 Certificates and the CRLs must use X.509 v2 CRLs. For more details see Section 5.4.

Since this is a major change to all solutions it is recommended that the customer base work as early as possible ensure that the CA's support the new standards to allow for a more seamless transition to the new algorithms. In addition, customers should consider limiting the validity timeline of all CA certificates using CNSA 1.0 to the timeline for CNSA 2.0 being mandated as detailed in Section 4.1.

5 CNSA 2.0 PROTOCOLS CONSIDERATIONS

This section covers relevant IETF Profiles, RFCs, and other security considerations that are relevant for the implementation of the CNSA 2.0 algorithms into CSfC. This includes the four major encryption mechanisms within CSfC DIT CPs:

- IPsec
- TLS
- MACsec using EAP-TLS
- Wi-Fi WPA3 Enterprise

There are additional security relevant functions such as SSH that are used in a majority of products for administration and Wi-Fi WPA3 SAE which is used for wireless communication in edge cases of the CSfC Program such as the Dedicated Outers, Retransmission Devices and within the Tactical CP.

5.1 IPSEC

The CNSA 2.0 is relevant for IPsec for the IKE portion of the specification thus NSA has worked with industry to update the Profile for implementation, *CNSA Suite 2.0 Profile for IPsec (draft-guthrie-cnsa2-ipsec-profile).*

5.1.1 CNSA SUITE 2.0 PROFILE FOR IPSEC

The draft profile *(draft-guthrie-cnsa2-ipsec-profile)* covers the implementation of CNSA 2.0 compliant algorithms ML-KEM-1024 [FIPS203] for key establishment and ML-DSA-87 [FIPS204] for digital signatures within IPSec. It also covers the RFCs that are required to address the new larger key sizes such as:

- RFC 9370 Multiple Key Exchanges in Internet Key Exchange Protocol version 2 (IKEv2)
- RFC 9242 Intermediate Key Exchanges in IKEv2
- RFC7383 IKEv2 Message Fragmentation

These additional RFCs are required because if ML-KEM-1024 were used in the initial IKEv2 Security Association (SA) key exchange, the sizes of its public key and ciphertext would cause the initiator and responder messages to exceed the typical path MTU and necessitate IP-level fragmentation, which can cause operational challenges and prevent the establishment of a connection.

RFC 9370 Multiple Key Exchanges: Allows multiple key exchanges to take place while computing a shared secret during an IKEv2 SA setup that is resistant to quantum-computer attacks. The initial IKEv2

key exchange (IKE_SA_INIT) messages do not have any inherent fragmentation support within IKE. Additional key exchanges are performed using IKEv2 intermediate key exchange (IKE_INTERMEDIATE) messages that follow the initial key exchange (IKE_SA_INIT). This allows the standard IKE fragmentation mechanisms (which cannot be used in IKE_SA_INIT) to be available for the potentially large key exchange messages with post-quantum algorithm data.

RFC 9242 Intermediate Key Exchanges: This exchange can be used for transferring large amounts of data in the process of IKEv2 SA establishment. The Intermediate Exchange makes it possible to use the existing IKE fragmentation mechanism (that cannot be used in the initial IKEv2 exchange), helping to avoid IP fragmentation of large IKE messages if they need to be sent before IKEv2 SA is established.

RFC7383 IKEv2 Fragmentation: Describes a way to avoid IP fragmentation of large IKEv2 messages. This allows IKEv2 messages to traverse network devices that do not allow IP fragments to pass through.

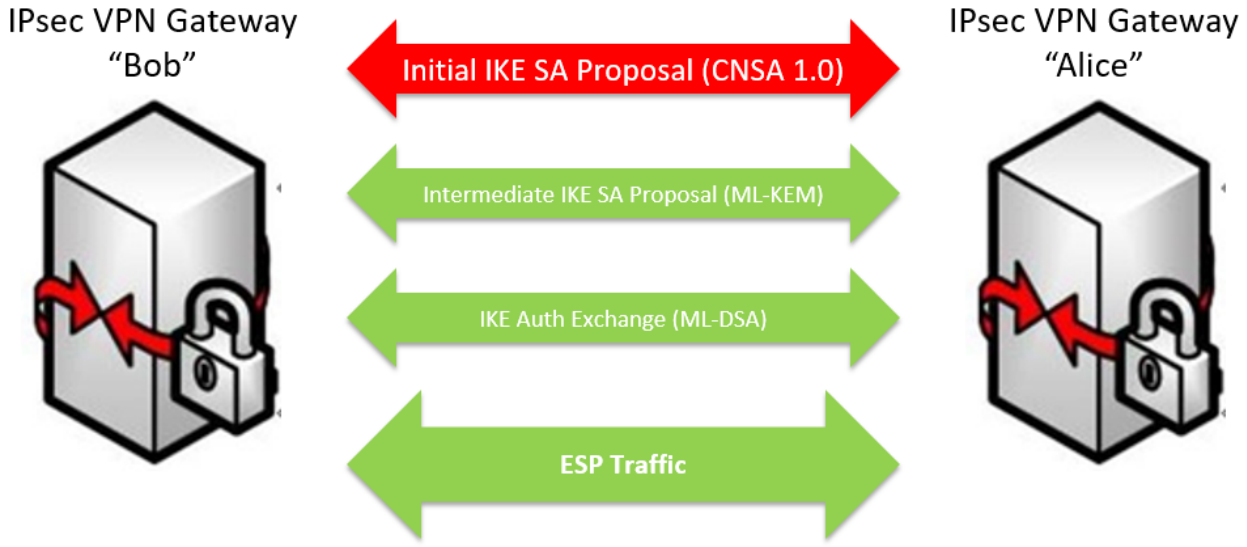

Figure 1. CNSA 2.0 IKE Exchange

As detailed in Figure 1, RFC 9370 enables peers to perform multiple key exchanges. The Initial IKE SA key establishment algorithm must be constrained enough in size as to not induce IP fragmentation. The ML-KEM-1024 key sizes are too large for this initial exchange and thus an initial establishment key exchange using a CNSA 1.0 algorithm must be used. A subsequent key establishment algorithm then must be performed in the Intermediate IKE exchange as specified in RFC9242 that will use the ML-KEM key exchange, which precedes IKE Authentication. This exchange, because it is encrypted by the initial key establishment algorithm, can now leverage the IKEv2-level fragmentation mechanism specified in RFC7383, which allows public keys and ciphertexts to be exchanged in messages that exceed path MTU and avoids IP fragmentation.

5.1.2 Other Relevant Standards for CNSA 2.0 and Post Quantum for IPsec

Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2) (draft-kampanakis-ml-kem-ikev2) describes how ML-KEM can be used as a quantum-resistant KEM in

IKEv2 in an IKE_SA_INIT key exchange, or in one additional IKE_INTERMEDIATE or IKE_FOLLOWUP_KE key exchange after an initial IKE_SA_INIT or CREATE_CHILD_SA respectively.

Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC (draft-reddy-ipsecme-ikev2-pqc-auth) specifies the use of the ML-DSA and SLH-DSA algorithms in IKEv2.

Mixing Preshared Keys in the IKE_INTERMEDIATE and in the CREATE_CHILD_SA Exchanges of IKEv2 for Post-quantum Security (draft-ietf-ipsecme-ikev2-qr-alt). This specification defines an alternative way to use PPKs to get protection against quantum computers, which is similar to the solution defined in RFC8784, but protects the initial IKEv2 SA too. A disadvantage of RFC8784 is that it assumes that PPKs are static and thus they are only used when an initial IKEv2 Security Association (SA) is created. If a fresh PPK is available before the IKE SA expired, then the only way to use it is to delete the current IKE SA and create a new one from scratch, which is inefficient. This new specification also defines a way to use PPKs in active IKEv2 SA for creating additional IPsec SAs and for rekey operations. The draft profile *[draft-guthrie-cnsa2-ipsec-profile]* supports the use of PSKs as specified in *[draft-ietf-ipsecme-ikev2-qr-alt]* and acknowledges that there may be a period of transition in which implementations support the use of a PSK via [RFC8784], but have not yet added support for *draft-ietf-ipsecme-ikev2-qr-alt.*

5.2 TLS

For the TLS components within CSfC such as TLS Protected Server and Client, SRTP server and Client and additionally any components that rely on EAP-TLS, TLS 1.3 will be mandated for the implementation of CNSA 2.0 within with CSfC. For more information on EAP-TLS, see Section 5.3.

5.2.1 CNSA Suite 2.0 Profile for TLS 1.3

The draft profile*, CNSA 2.0 Suite Profile for TLS 1.3 (draft-becker-cnsa2-tls-profile)***,** covers the implementation of CNSA 2.0 compliant algorithms ML-KEM-1024 [FIPS203] for key establishment and ML-DSA-87 [FIPS204] as a digital signature within TLS 1.3.

For implementations of CNSA 2.0 TLS, all TLS negotiations for the encryption layers must use TLS 1.3 to be compliant with CNSA 2.0. TLS 1.3. CNSA 2.0 also allows SHA-512 to be used in HKDFs, but at the time of writing, only SHA-384 is supported by TLS. AES must use AES-256 GCM Mode.

5.2.2 Other Relevant Standards for CNSA 2.0 and Post Quantum for TLS

RFC 8773 specifies an extension that allows an external PSK to be used in addition to (and not in lieu of) certificate-based authentication during the initial handshake. The PSK also contributes to the TLS 1.3 key schedule.

5.3 EAP TLS

For the implementations of EAP-TLS to use CNSA 2.0 compliant algorithms, TLS 1.3 will be mandated per RFC 9190 *EAP-TLS 1.3 Using the Extensible Authentication Protocol with TLS 1.3*. Combine the usage of TLS 1.3 with the CNSA Suite 2.0 Profile for TLS 1.3 detailed in section 5.2.1 will allow for EAP-TLS to use the new CNSA 2.0 algorithms. This will cover both the use of EAP-TLS within MACsec and WPA3-Enterprise configurations for CSfC.

5.4 Certificate and Certificate Revocation List

5.4.1 CNSA Suite 2.0 Profile for Certificate and Certificate Revocation List

The draft document, *CNSA 2.0 Suite Certificate and Certificate Revocation List Profile (draft-jenkins-cnsa2-pkix-profile)*, covers the use of CNSA 2.0 within both the Certificates and the Certificate Revocation Lists and defines a CNSA-compliant profile of "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC5280].

All CSfC certificates supporting the Inner and Outer Encryption Tunnels must use X.509 v3 Certificates. Also the CRLs must use X.509 v2 CRLs. Every X.509 v3 certificate relying on CNSA 2.0 contain one of the following:

- A ML-DSA-87 signature verification key
- A ML-KEM-1024 public encapsulation key

The signature applied to all CNSA Suite certificates and CRLs MUST be made with a ML-DSA-87 signing key. The CNSA Suite Base Certificate Required Values:

- signature and signatureAlgorithm
  - ML-DSA-87 is indicated by the id-ML-DSA-87 OID in the AlgorithmIdentifier
- signatureValue
  - ML-DSA digital signature generation is described in [FIPS204]
- Version
  - For this profile, version MUST be 'v3', with INTEGER value 2

5.5 Wi-Fi

For Wi-Fi there are two encryption modes used within the CSfC Program. The main one is the WPA3-Enterprise 192 bit mode that currently relies on CNSA 1.0 Algorithms. For that mode, EAP-TLS is used to negotiate the authentication and thus it will follow the same path as detailed in section 5.3. The other use of Wi-Fi is using the WPA3 SAE mode and currently it is not considered Post-Quantum secure, but there is a bit more nuisance to that.

5.5.1 WPA3 SAE

The Dragonfly Key Exchange (IETF RFC 7664: Dragonfly Key Exchange) has been adopted by Wi-Fi Alliance as part of WPA3 to replace the 4 way handshake in WPA2 to take a password-based key exchange and protect against offline password-guessing attacks. Passive offline attacks against a sufficiently securely implemented WPA3 Dragonfly protocol should not be able to recover the password or read any traffic without breaking the elliptic curve exchange, even if a low-entropy password is used. With the possibility of a cryptographically relevant quantum computer that is effective against the elliptic curve exchange used in the Dragonfly Key Exchange.

- Dragonfly Key Exchange
  - WPA3 SAE relies on known secret key and a number of other primitives to derive the session key for a Wi-Fi connection

- Currently WPA3 SAE uses AES-128 but Wi-Fi 7 will mandate AES-256
- The discrete log and offline protections are rendered useless by a cryptographically relevant post quantum computer because of the reliance of ECDSA algorithms
- Leaving the complexity of the key being secret the only protection mechanism to protect the data from being decrypted

5.6 SSH

SSH is currently not considered a layer for CSfC but it is a core component in the secure management of the CSfC Components. Thus, it encourages vendors of all network devices and operating systems to implement SSH with CNSA 2.0 support.

5.6.1 CNSA Suite 2.0 Profile for SSH

Implementing CNSA 2.0 within SSH is similar to the implementation of TLS 1.3 in terms of algorithms and keys exchanges used. This profile, *CNSA 2.0 Suite Profile for SSH (draft-becker-cnsa2-ssh-profile)*, specifies the use of SHA-384 but SHA-512 is also accepted in general within CNSA 2.0. AES must use AES-256 GCM Mode. Also, the MAC Algorithms being used must be AEAD_AES_256_GCM [RFC5647].

6 MOBILE ACCESS CP

For Mobile Access there will be the addition of three tables as objective cryptographic algorithm tables and associated text and requirements for implementation of these tables. There will be two additional tables for objective CNSA 2.0 cipher suites covering both IPsec and TLS use within MA CP. Additionally, there will be a section and table added for objective firmware and software-signing requirements, where all installed and updated firmware and software packages must be signed using the one of the given algorithms.

6.1 MA CP IPsec Changes

Table 5. Approved CNSA 2.0 Suite for MA IPsec

Function	CNSA Suite Algorithms	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	RSA 3072 (Threshold), or ECDSA over the curve P-384 (Threshold) ML-DSA-87 (Objective)	FIPS PUB 186-4 FIPS PUB 186-4 FIPS 204
Key Exchange/ Establishment	RSA 3072 (Threshold), or ECDH over the curve P-384 using DH Group 20 (Threshold)	NIST SP 800-56A, IETF RFC 7296, NIST SP 800-56A

Function	CNSA Suite Algorithms	Specifications
	ML-KEM-1024 (Objective)	FIPS 203
Integrity (Hashing)	SHA-384 Or SHA-512 (Threshold)	FIPS PUB 180-4

373

374 6.2 MA CP TLS CHANGES

375 **Table 6. Approved CNSA 2.0 Suite for MA TLS**

Function	CNSA Suite Algorithms	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	RSA 3072 (Threshold), or ECDSA over the curve P-384 (Threshold) ML-DSA-87 (Objective)	FIPS PUB 186-4 FIPS PUB 186-4 FIPS 204
Key Exchange/ Establishment	RSA 3072 (Threshold), or ECDH over the curve P-384 using DH Group 20 (Threshold) ML-KEM-1024 (Objective)	NIST SP 800-56A, IETF RFC 7296, NIST SP 800-56A FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512 (Threshold)	FIPS PUB 180-4

376 7 CAMPUS WLAN CP

377 For CWLAN there will be the addition of three tables as objective cryptographic algorithm tables and
378 associated text and requirements for implementation of these tables. There will be two additional tables
379 for objective CNSA 2.0 cipher suites covering both IPsec and EAP TLS use within CWLAN CP.
380 Additionally, there will be a section and table added for objective firmware and software signing
381 requirements where all installed and updated firmware and software packages must be signed using the
382 one of the given algorithms.

383 7.1 CWLAN IPSEC CHANGES

384 **Table 7. Approved CNSA 2.0 Suite for CWLAN IPsec**

Function	CNSA Suite Algorithms	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197

Authentication (Digital Signature)	RSA 3072 (Threshold), or ECDSA over the curve P-384 (Threshold) ML-DSA-87 (Objective)	FIPS PUB 186-4 FIPS PUB 186-4 FIPS 204
Key Exchange/ Establishment	RSA 3072 (Threshold), or ECDH over the curve P-384 using DH Group 20 (Threshold) ML-KEM-1024 (Objective)	NIST SP 800-56A, IETF RFC 7296, FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512 (Threshold)	FIPS PUB 180-4

7.2 CWLAN WPA3 ENTERPRISE CHANGES

Table 8. Approved CNSA 2.0 Suite for CWLAN EAP-TLS

Function	CNSA Suite Algorithms	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197
Authentication (Digital Signature)	RSA 3072 (Threshold), or ECDSA over the curve P-384 (Threshold) ML-DSA-87 (Objective)	FIPS PUB 186-4 FIPS PUB 186-4 FIPS 204
Key Exchange/ Establishment	RSA 3072 (Threshold), or ECDH over the curve P-384 using DH Group 20 (Threshold) ML-KEM-1024 (Objective)	NIST SP 800-56A, IETF RFC 7296, FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512 (Threshold)	FIPS PUB 180-4

8 MULTI-SITE CONNECTIVITY CP

For MSC there will be the addition of three tables as objective cryptographic algorithm tables and associated text and requirements for implementation of these tables. There will be two additional tables for objective CNSA 2.0 cipher suites covering both IPsec and MACsec EAP TLS usage within MSC CP. Additionally, there will be a section and table added for objective firmware and software signing

requirements where all installed and updated firmware and software packages must be signed using the one of the given algorithms.

8.1 MSC IPSEC CHANGES

Table 9. Approved CNSA 2.0 Suite for MSC IPsec

Function	CNSA Suite Algorithms	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	RSA 3072 (Threshold), or ECDSA over the curve P-384 (Threshold) ML-DSA-87 (Objective)	FIPS PUB 186-4 FIPS PUB 186-4 FIPS 204
Key Exchange/ Establishment	RSA 3072 (Threshold), or ECDH over the curve P-384 using DH Group 20 (Threshold) ML-KEM-1024 (Objective)	NIST SP 800-56A, IETF RFC 7296, FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512 (Threshold)	FIPS PUB 180-4

8.2 MSC MACSEC CHANGES

Table 10. Approved CNSA Suite for MSC MACsec

Function	CNSA Suite Algorithms	Specifications
Confidentiality (Encryption)	Galois Counter Mode (GCM)- AES-256 GCM-AES-XPN-256	FIPS PUB 197 IEEE 802.1AE-2018
Key Wrap	AES Key Wrap	IETF RFC 3394

Table 11. Approved CNSA 2.0 Suite for MSC MACsec EAP-TLS

Function	CNSA Suite Algorithms	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197

Function	CNSA Suite Algorithms	Specifications
Authentication (Digital Signature)	RSA 3072 (Threshold), or ECDSA over the curve P-384 (Threshold) ML-DSA-87 (Objective)	FIPS PUB 186-4 FIPS PUB 186-4 FIPS 204
Key Exchange/ Establishment	RSA 3072 (Threshold), or ECDH over the curve P-384 using DH Group 20 (Threshold) ML-KEM-1024 (Objective)	NIST SP 800-56A, IETF RFC 7296, FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512 (Threshold)	FIPS PUB 180-4

9 DATA-AT-REST CP

For DAR CP there will be the addition of two tables as an objective cryptographic algorithm table and associated text and requirements for implementation of these tables. There will be an additional table for objective CNSA 2.0 cipher suites covering DAR Encryption. Additionally, there will be a section and table added for objective firmware and software-signing requirements where all installed and updated firmware and software packages must be signed using the one of the given algorithms.

Table 12. Approved Commercial National Security Algorithm (CNSA) Suite for DAR

Function	CNSA Suite Algorithms	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197
Authentication (Digital Signature)	RSA 3072 (Threshold), or ECDSA over the curve P-384 (Threshold) ML-DSA-87 (Objective)	FIPS PUB 186-4 FIPS PUB 186-4 FIPS 204
Integrity (Hashing)	SHA-384 or SHA-512 (Threshold)	FIPS PUB 180-4

APPENDIX A. GLOSSARY OF TERMS

Assurance – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (CNSSI 4009)

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Audit Log – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective actions are required.

Availability – Ensuring timely and reliable access to and use of information. (NIST SP 800-37).

CP – Guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. CP instantiations are built using products selected from the CSfC Components List.

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Computing Device – An EUD such as a phone, laptop, or tablet.

Control Plane Protocol – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

Cross Domain Solution (CDS) – A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)

Dedicated Outer VPN - A dedicated piece of hardware that can be part of an EUD and terminates the Outer layer of IPsec encryption.

End User Device (EUD) – A form-factor agnostic component of the MA solution that can include a mobile phone, tablet, or laptop computer. EUDs can be composed of multiple components to provide physical separation between layers of encryption.

External Interface – The interface of the Outer VPN Gateway that connects to the internal interface of the Outer Firewall.

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

Gray Network – A network that contains classified data that has been encrypted once.

Internal Interface – The interface on a VPN Gateway or Inner Encryption Component that connects to the Inner network (i.e., the Gray Network on the Outer VPN Gateway or the Red Network on the Inner Encryption Component).

Locally Managed Device – A device that is being managed by the direct connection of the Administration Workstation to the device in a hardwired fashion (such as a console cable).

Platform Certificate - A Trusted Computing Group (TCG) defined X.509 Attribute Certificate that asserts the platform's security properties and configuration as shipped.

Protection Profile – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates.

Red Network - Contains only Red data and is under the control of the solution owner or a trusted third party. The Red Network begins at the internal interface(s) of Inner Encryption Components located between the Gray Firewall and Inner Firewall.

Retransmission Device (RD) – A standalone piece of hardware used to provide Black Network connectivity to EUDs.

SRTP Client – A component on the EUD that facilitates encryption for voice communications.

TLS Client – A component on a TLS EUD that can provide the Inner layer of data in transit encryption.

TLS Component – Refers to both TLS Clients and TLS-Protected Servers.

Virtual EUD – An EUD that contains at least four virtual machines (End User Domain, Inner Encryption domain, Outer Encryption Domain and a Black Transport Domain).

VPN Client – A VPN application installed on an EUD.

VPN Component – The term used to refer to VPN Gateways and VPN Clients.

VPN Gateway – A VPN device physically located within the VPN infrastructure.

VPN Infrastructure – Physically protected in a secure facility and includes Inner and Outer VPN Gateways, Certificate Authorities, and Administration Workstations, but does not include EUDs.

APPENDIX B. ACRONYMS

Acronym	Meaning
BIOS	Basic Input/Output System
CDS	Cross Domain Solution
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CP	Capability Package
cPP	Collaborative Protection Profile
CSD	Cybersecurity Directorate
CSfC	Commercial Solutions for Classified
CWLAN	Campus Wireless Local Area Network
DAR	Data-At-Rest
DiT	Data-in-Transit
DoD	Department of Defense
DSC	Dedicated Security Component
EUD	End User Device
FIPS	Federal Information Processing Standards
FDE	Full Disk Encryption
GPCP	General Purpose Compute Platform
GPOS	General Purpose Operating System
GSM	Hardware Security Modules
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HWFDE	Hardware Full Disk Encryption
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
MA	Mobile Access
MDF	Mobile Device Fundamentals
NCDSMO	National Cross Domain Strategy Management Office
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
O	Objective
OS	Operating System
PE	Platform Encryption
PMO	Program Management Office
PP	Protection Profile
RD	Retransmission Device
RFC	Request for Comment
RSA	Rivest Shamir Adelman algorithm
SAs	Security Administrators

Acronym	Meaning
SDE	Secure Data Element
SDO	Security Data Objects
SE	Secure Elements
SEP	Secure Enclave Processor
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Manager
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
SWFDE	Software Full Disk Encryption
T	Threshold
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
UEFI	Universal Extensible Firmware Interface
VoIP	Voice over Internet Protocol
VVoIP	Voice and Video over IP
VM	Virtual Machine
VPN	Virtual Private Network
vTPM	Virtual Trusted Platform Module
WLAN	Wireless Local Area Network
WPA3	Wi-Fi Protected Access 3

475

APPENDIX C. REFERENCES

Document	Title	Date
CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2014
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2015
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	December 2024
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	November 2021
DoDI 8420.01	*Commercial Wireless Local-Area Network Devices, Systems, and Technologies.* Office of the CIO of the DOD	November 2017
DoDI 8540.01	Department of Defense Instruction 8540.01: *Cross Domain Policy*	August 2017
FIPS 140-3	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf	March 2019
FIPS 180-4	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	August 2015
FIPS 186	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 201-2	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	August 2013
IPsec VPN Client PP 2.1	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*. https://niap-ccevs.org/MMO/PP/mod_vpn_cli_v2.1.pdf	October 2017
ISO 9594-8	*Public-Key and Attribute Certificate Frameworks*	May 2017
NSA Suite B	*NSA Guidance on Suite B Cryptography (including the Secure Sharing Suite (S3))*. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml	November 2010
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force	November 2003
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004

Document	Title	Date
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman	December 2005
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5288	*IETF RFC 5288 AES Galois Counter Mode (GCM) Cipher Suite2 for TLS*. J. Salowey, A. Choudhury, D. McGrew	August 2008
RFC 5289	*IETF RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*. E. Rescorla	August 2008
RFC 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 2010
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
RFC 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
RFC 7296	*Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen	October 2014

Document	Title	Date
RFC 8422	*Elliptic Curve Cryptography (ECC) Cypher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*. Y. Nir, S. Josefsson, M. Pegourie-Gonnard	August 2018
RFC 8446	*The Transport Layer Security (TLS) Protocol Version 1.3*. E. Rescorla	August 2018
RFC 8603	*Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile*. M. Jenkins, L. Zieglar	May 2019
SP 800-37	*Risk Management Framework for Information Systems and Organizations.* Joint Task Force	April 2021
SP 800-53	*NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	September 2020
SP 800-56A	*NIST Special Publication 800-56A Rev. 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	April 2018
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	March 2019
SP 800-56C	*NIST Special Publication 800-56C Rev 2, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	August 2020
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	March 2019
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et al.	April 2011
RFC 7714	*AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP). D. McGrew*	December 2015
	TCG Platform Certificate Profile, Version 1.1 Revision 15	February 2019
	Trusted Computing Group, TCG PC Client Reference Integrity Manifest Specification, version 0.15.	March 2020
	TCG Reference Integrity Manifest (RIM) Information Model, Version 1.00, Revision 0.13, 2019 TCG Reference Integrity Manifest (RIM) Information Model, Version 1.0, Revision 0.13.	December 2019
	Unified Extensible Firmware Interface Specification (UEFI), Version 2.4 (Errata B) or later.	June 2013
	TCG PC Client Platform Firmware Integrity Measurement, Version 1.0 Revision 24.	December 2019
	CSfC Mobile Access Capability Package 2.7.0	January 2025
	CSfC Campus WLAN Capability Package 3.1.0	January 2025

Document	Title	Date
	CSfC Multi-Site Connectivity Capability Package 1.2.0	March 2023
	CSfC Data At Rest Capability Package 5.0	November 2020
	CSfC Key Management Requirements Annex 2.1	May 2022

477

478

479

480