


NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Symmetric Key Management Requirements Annex 3.0.0 DRAFT.1

Version 3.0.0 DRAFT.1
05 March 2025


CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Symmetric Key Management Requirements Annex	3.0.0 DRAFT.1	05 March 2025	• Added verbiage and revised requirements allowing for multiple Key Generations Solutions (KGSs) (e.g. Red KGS and Grey KGS) • Clarified PSK usage with high availability solutions • Revised KGS RNG requirement • Clarified PSK usage in MACP solutions • Added KGS Approval Criteria Appendix • Updated Appendix B: References. • Minor administrative changes were made in formatting.
CSFC Symmetric Key Management Requirements Annex	2.1	19 May 2022	• Updated KGS product selection criteria. • Updated wording in Section 2.1 to improve and clarify PSK usage guidance. • Updated IPSec with RFC 8784-compliant implementations of IKE v2 PSK usage requirements. • Updated outer PSK classification requirement. • Added role-based personnel requirements. • Updated Appendix B: References. • Minor administrative changes were made in formatting.
CSFC Symmetric Key Management Requirements Annex	2.0	29 January 2021	• Changed document name from *CSfC Additional Key and Certificate Management Requirements Annex* to *CSfC Symmetric Key Management Requirements Annex*. • Updated to add IPSec with RFC 8784-compliant implementations of IKE v2 as an approved protocol for use with Pre-shared Keys (PSKs) in CSfC solutions and removed the use of IKEv1. • Incorporated MSC CP MACsec Symmetric Key Management requirements from the *CSfC Key Management Requirements Annex*. • Replaced Capability Package (CP) requirements mapping column with Threshold / Objective column. • Updated Appendix B: References. • Minor administrative changes were made in formatting.

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Additional Key and Certificate Management Requirements Annex	1.0	21 May 2019	• Initial release of the *CSfC Additional Key and Certificate Management Requirements Annex*.

Table of Contents

Table of Figures

List of Tables

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency's (NSA's) Cybersecurity Directorate (CSD) publishes guidance to empower its customers to implement secure communication solutions using independent, layered Commercial-off-the-Shelf (COTS) products. This guidance is product-neutral and describes system-level solution frameworks documenting security and configuration requirements for customers and/or integrators.

CSD delivers guidance to meet the needs of customers implementing Symmetric Key Management in CSfC data in transit solutions using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components.

This document serves as a design addendum for Commercial Solutions for Classified (CSfC) and specifically defines additional requirements for implementing symmetric key management capabilities defined in CSfC Capability Packages (CPs) to ensure symmetric keys are implemented correctly and securely within CSfC solutions.

2 PURPOSE AND USE

The Symmetric Key Management Requirements Annex is implemented as part of a holistic, risk management and defense-in-depth information security strategy integrated into CSfC architectures. Organizations designing CSfC solutions and implementing Symmetric Key Management capabilities should leverage information gathered from Symmetric Key Management capabilities to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of CSfC systems.

Guidance provided in the Symmetric Key Management Requirements Annex references architecture and corresponding high-level configuration information to help customers develop a solution to meet CSfC Symmetric Key Management requirements. To implement a Symmetric Key Management solution based on this guidance, all Threshold requirements, or the corresponding Objective requirements, must be implemented as described in Section 4.

The requirements in this document supersede existing Symmetric Key Management requirements in published CSfC Capability Packages (CP). Future CP revisions will direct customers to this annex for Symmetric Key Management implementation.

Please provide comments on the usability, applicability, and/or shortcoming of this guidance to an NSA Client Advocate and the KM guidance maintenance team at CSfC_Key_Man_Req_Team@nsa.gov. Solutions adhering to this guidance must also comply with Committee on National Security Systems (CNSS) policies and instruction.

For any additional information on Cross Domain Solutions (CDS) contact the National Cross Domain Strategy Management Office (NCDSMO) at ncdsmo@nsa.gov.

3 LEGAL DISCLAIMER

This guidance is provided "as is". Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a purpose are denied. 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 guidance, even if advised of the possibility of such damage.

The user of this guidance 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.

This guidance is not intended to constitute an endorsement, explicitly or implied, by the U.S. Government of any manufacturer's product or service.

4 PRE-SHARED KEYS (PSKS) OVERVIEW AND REQUIREMENTS

This section provides implementation requirements for the use of PSKs within CSfC solutions.

4.1 OVERVIEW OF PRE-SHARED KEYS (PSKS) IN CSFC SOLUTIONS

Symmetric Pre-Shared Keys (PSKs) should be used instead of, or in addition to, asymmetric public/private key pairs to provide quantum resistant cryptographic protection of classified information within CSfC solutions. For CSfC customers who have a requirement to protect long-life[1] classified information, 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]

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

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

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 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 1 summarizes where PSKs are used in the various CSfC solutions. More detailed implementation requirements for PSKs in these CSfC solutions is provided in Sections 4.3.1 through 4.3.7.

Table 1: 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:	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.

Capability Package	PSK Implementation: Inner Tunnel vs. Outer Tunnel
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	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.

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

4.2 Overview of Symmetric Key Generation Solutions

A National Security Agency (NSA)-approved[3] Key Generation Solution (KGS), using a FIPS 140-2/3 validated or NSA approved Random Number Generator (RNG), is used to generate and manage PSKs for a CSfC solution as shown in Figure 1 and Figure 2.

[3] NSA-approved means: (a) a component approved for the CSfC solution by the Deputy National Manager for National Security Systems, or (b) an already approved enterprise service.

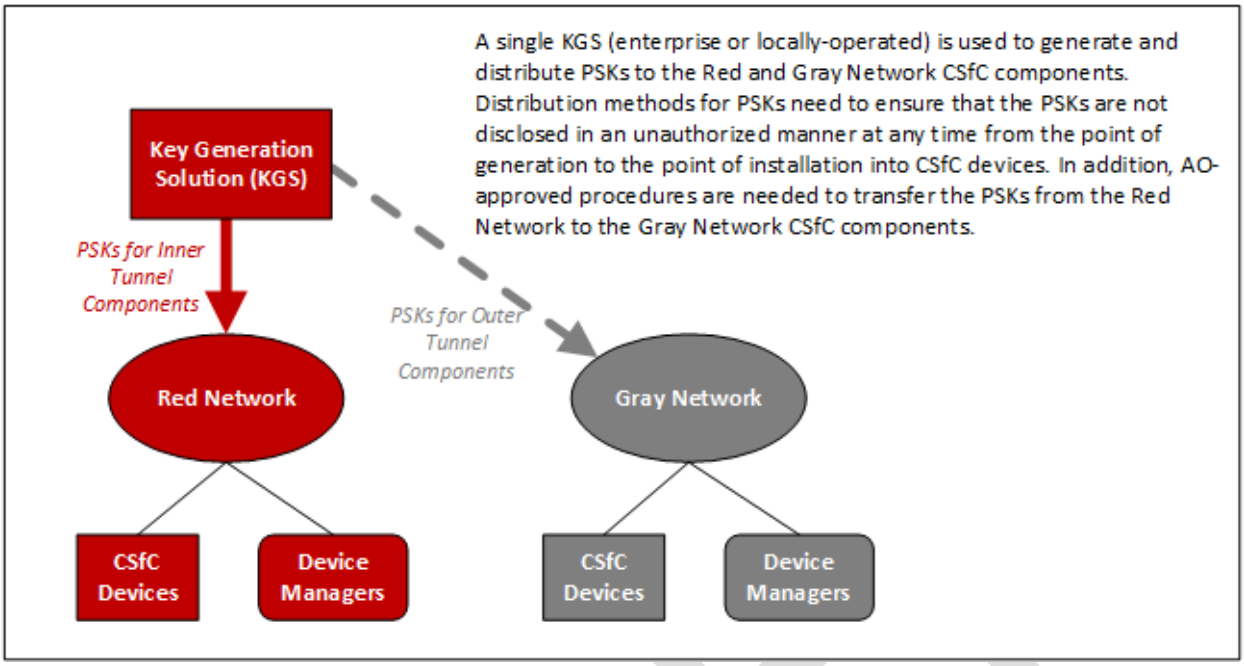

Figure 1: PSK Management Services: Single KGS

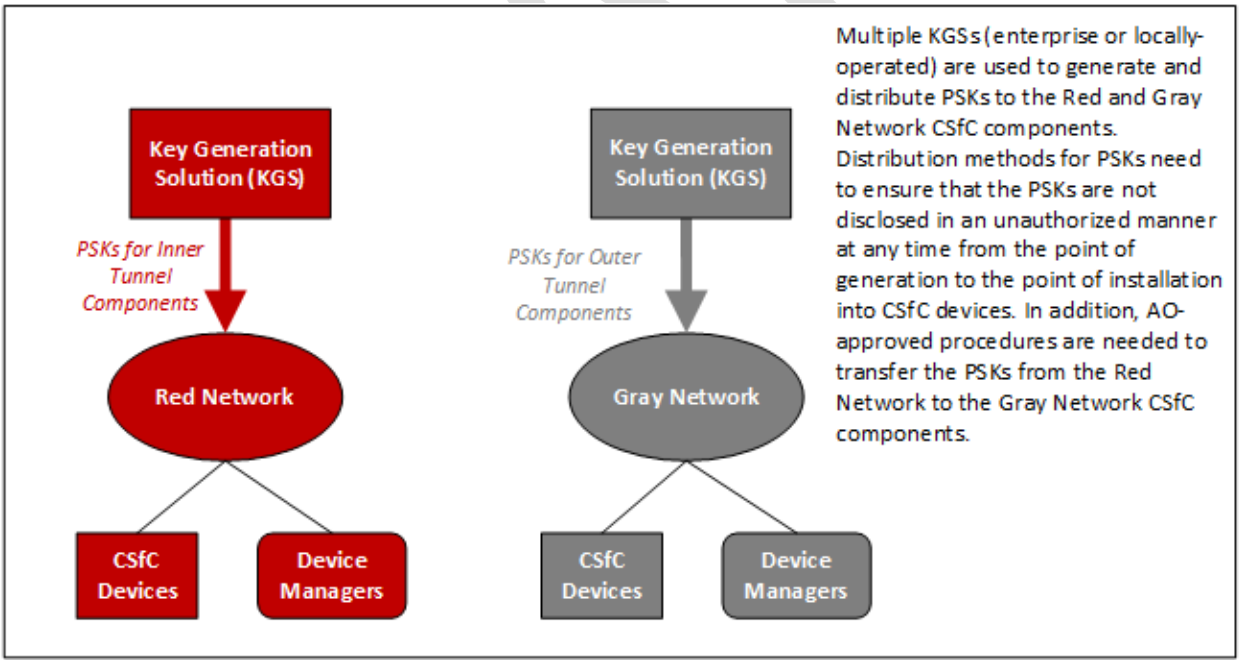

Figure 2: PSK Management Services: Multiple KGSs

The KGS generates and distributes PSKs to CSfC devices operating in the Red and Gray Networks, where the KGS operates in the Red Network enclave and/or Grey Management Network. Device Managers (DMs) are used to ensure that distribution and installation of PSKs onto CSfC devices is performed securely and in a trustworthy manner. PSKs used for inner tunnel components operating on the

Red/Gray Network boundary are classified to the level of the Red Network. PSKs used for outer tunnel components operating on the Gray/Black network boundary are handled as classified at the highest classification level of the solution, and are distributed in accordance with AO approved procedures and methods (e.g., CDS) to move the PSKs from the Red Network enclave to the Gray Network.

The role of the DM in the CSfC solution is further described in Figure 2. The DM requests a PSK from the KGS, and the KGS verifies that the request came from an authorized DM. The KGS generates the PSK and securely distributes the PSK to the DM. Secure distribution can be achieved via technical means (e.g., encryption) or procedural controls. The DM then installs the PSK into the security device, and destroys/deletes any remaining copies of the PSK.[4] Installation is likely performed with the PSK in red form given current capabilities of CSfC solution components.[5] Future capabilities may allow an encrypted form of the PSK to be installed, thereby limiting exposure of the PSK.

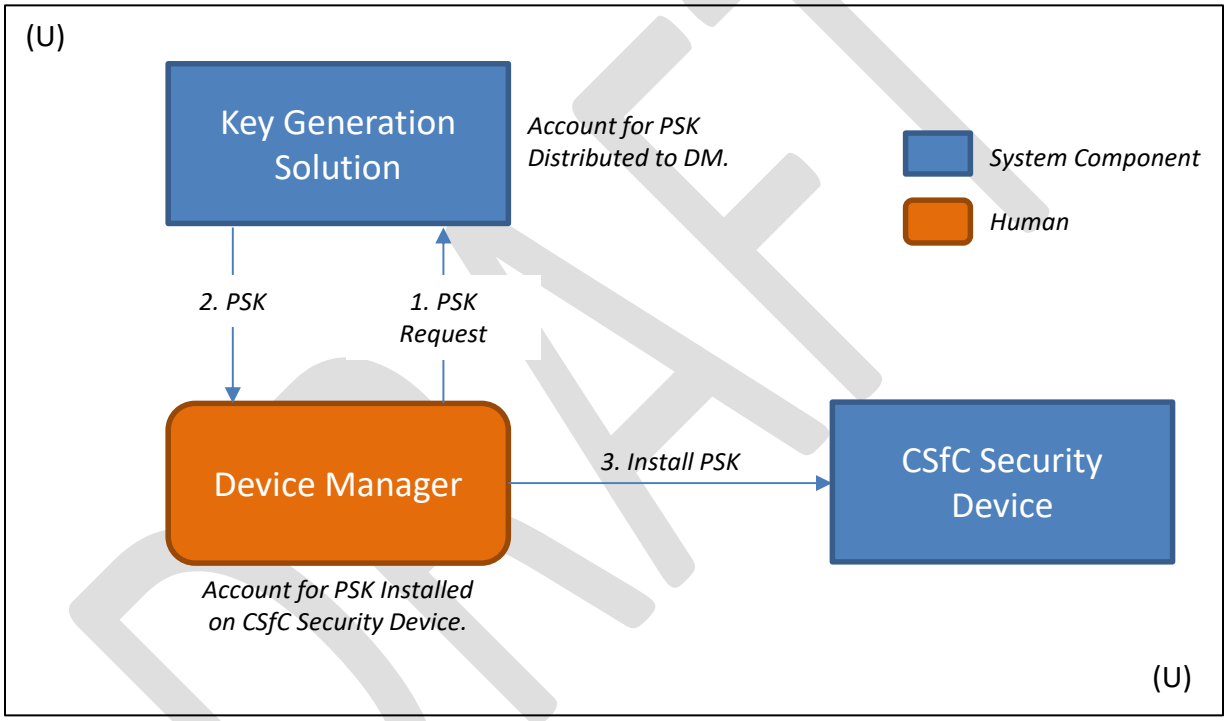

Figure 3: CSfC Security Device Management for PSKs

The KGS and DM also account for the PSK to ensure its location (i.e., the CSfC component containing the PSK) is known at all times. In case of compromise, the KGS and DM need to be able to determine where all instances of a given PSK exist (i.e., all CSfC components containing the compromised PSK) and rekey that PSK in accordance with compromise reporting and recovery procedures.

[4] Removable media, electronic files and memory containing PSKs must be destroyed / deleted using AO-approved procedures and in accordance with CNSSI 4004. This requirement does not apply to storing approved backup copies of the PSK.

[5] The DM may use, if approved by the local AO, a management workstation to establish a secure and authenticated connection (e.g., SSH) to the CSfC Device to install the PSK. However, SSH and other similar protocols are not quantum-resistant key distribution protocols, and the risk for installing the PSK in this manner must be taken into consideration.

In some cases, the DM and KGS operate in different network domains, and potentially at different classification levels. In the latter case, procedures need to be developed and approved by the local Authorizing Official (AO) to ensure the secure and accurate transfer of information between the DM and KGS. (See Section 4.3.5 for connectivity examples.)

Finally, an NSA approved Key Management Plan (KMP) is required that fully describes the life-cycle management of PSKs that are generated by the KGS. The KMP addresses requirements and controls defined in *CNSSI 4005: Safeguarding COMSEC Facilities and Materials*. The requirements and controls defined in CNSSI 4005[6] are to be used as guidance to define solution specific requirements that ensure the secure distribution of PSKs onto CSfC solution components, and the mapping of PSKs to those components for accountability and compromise reporting purposes. Reference *Appendix C. – Sample Structure for a Key Management Plan (KMP)* for additional guidance.

4.3 PSK IMPLEMENTATION REQUIREMENTS

This section defines additional implementation requirements for the use of PSKs in CSfC solutions. Areas addressed include PSK generation, distribution and installation; PSK usage; PSK rekey; PSK compromise recovery; KGS connectivity; KGS audit; and PSK testing.

4.3.1 PSK GENERATION, DISTRIBUTION, AND INSTALLATION

The generation, distribution and installation of PSKs for CSfC solutions is shown in Figure 3. An NSA-approved KGS is used to centrally generate and manage PSKs for CSfC security devices, where two CSfC security devices are required to receive and store the same PSK. The two security devices are used to establish either the outer tunnel or inner tunnel for the CSfC solution. One of the DMs within the CSfC solution initiates a request to the KGS for a PSK. The KGS verifies the request came from an authorized DM and generates a PSK in accordance with the approved KMP. The KGS assigns a unique identifier[7] to the PSK for accounting purposes and distributes the PSK to the DMs that are responsible for installing the PSK onto the CSfC security devices. Preferably, the PSK is encrypted for distribution to each DM either using an approved encryption algorithm that uses an encryption key from a password-based key derivation function (PBKDF) or a pre-placed symmetric Key Encryption Key (KEK) that is shared between the KGS and each DM, or using a quantum-resistant key distribution protocol. The pre-placed PSK Key Encryption Key (KEK) is generated by the KGS and distributed out of band to the DM. A separate KEK should be used for each DM.

Each DM acknowledges receipt of the PSK back to the KGS through a protected channel or method, and the KGS keeps an accounting record of the PSKs delivered to each DM based on the unique identifiers assigned to the PSKs. Each DM is then responsible for installing the PSK on the CSfC security device managed by the DM. PSK installation is typically performed in plaintext form, as that is the common format supported by the CSfC security device. Future capabilities may allow PSK installation to be

[6] Specific attention should be provided to Section VII: Physical Security of COMSEC Material; Section VIII: Electronic Key Management System; Section IX: Key Management Infrastructure; Section X: COMSEC Account / KOA Managers; Section XI: Accounting, Inventory and Audits; Section XII: Issuing and Using COMSEC Material; Section XIII: Encrypted COMSEC Material; and Section XIV: Transportation of COMSEC Material.

[7] The unique identifier may be a technical computation based on the PSK (e.g., hash of the PSK) or it may be a manually generated identifier.

performed using encryption. After PSK installation is complete, the DMs keep an accounting record to know which PSKs are installed on each CSfC security device using the identifier assigned by the KGS.

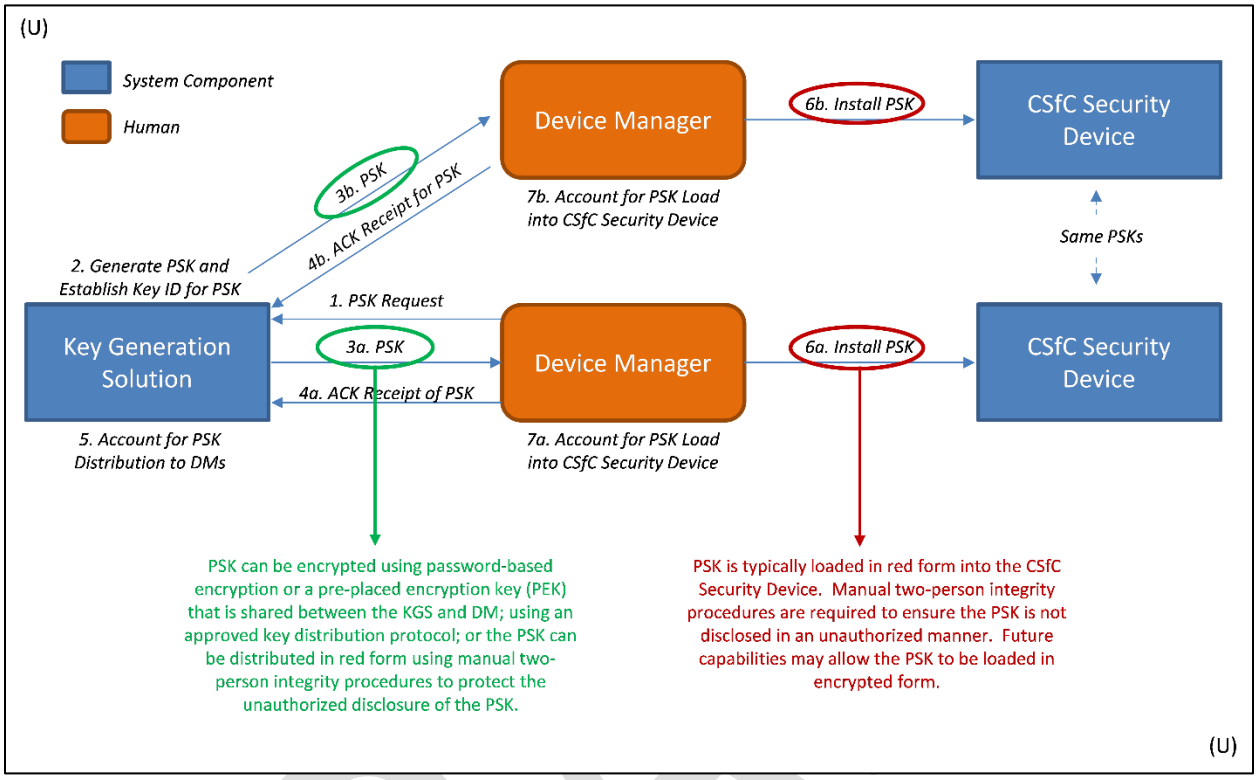

Figure 4. PSK Generation, Distribution and Installation into a CSfC Security Device

Table 2 summarizes general requirement statements for PSK generation, distribution and installation. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully, and securely, implementing the techniques for generation, distribution and installation of PSKs within the CSfC solution.

Table 2: PSK Generation, Distribution and Installation Requirements for CSfC Solutions

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-GD-1	Generation of PSKs must be performed by an NSA-approved[8] Key Generation Solution (KGS) that uses a FIPS 140-2/3 validated[9] or NSA approved[10] Random Number Generator (RNG), as specified in	Contact the CSfC PMO to assist with identifying a KGS that can be used within a CSfC solution. CSfC KGS Approval Criteria Checklist is located in Appendix D.	T=O

[8] NSA-approved means: (a) a component approved for the CSfC solution by the Deputy National Manager for National Security Systems, or (b) an already approved enterprise service.

[9] An active NIST FIPS validation certificate number must be provided.

[10] NSA-approval for non FIPS 140-2/3 validated RNGs must be submitted as request through NSA CSRP, with approval not guaranteed

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
	NIST SP 800-90 using Hash_RBG(SHA-384, SHA-512), HMAC_RBG(SHA-384, SHA-512), or CTR_RBG(AES-256) seeded by a entropy source with a minimum of 256 bits of entropy and in accordance with FIPS 140-2/3.		
PSK-GD-2	Centralized generation, distribution, installation and management of PSKs must be performed by a dedicated KGS.	Deploy a single KGS within the Red Network enclave of the CSfC solution. A second separate KGS can be deployed in the Grey Management Network for generating and managing PSKs for outer encryption components. In addition, a KMP needs to be developed that fully describes the life-cycle management of PSKs that are generated by the KGS. See *Appendix C. – Sample Structure for a Key Management Plan (KMP)* for a sample structure of a KMP.	T=O
PSK-GD-3	PSKs must be no less than 256 bits.	Configure the KGS to generate 256 bit PSKs.	T=O
PSK-GD-4	PSKs must not be exposed in plaintext form once they have been packaged by the KGS for distribution and until they are ready to be installed onto CSfC components. Installation of PSKs is typically performed via file transfer or text input. Note: PSKs may be in plaintext form when generated at the KGS. This guidance applies to the distribution and installation of PSKs.	Technical and procedural controls must be used to ensure PSKs are not exposed in plaintext form during the distribution process and until just prior to installation into a CSfC security device. Technical controls include encryption of the PSKs (e.g., encryption of PSKs on removable media, encryption of PSKs in electronic message exchange). Procedural controls use cleared and trusted personnel and AO-approved procedures. Technical and procedural controls may also be combined. For example, a PSK is encrypted at the KGS and placed on removable media (e.g., CD, USB Drive). The password to decrypt the PSK is provided to one cleared and trusted person, and the removable media containing the encrypted PSK	T=O

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		is provided to a second cleared and trusted person. The two authorized individuals distribute the PSK and password to the CSfC device, where one individual inserts the removable media into the CSfC device and the other individual enters the password to decrypt the PSK.	
PSK-GD-5	PSKs must be protected from unauthorized disclosure when they are distributed outside of a controlled boundary or over unprotected communications channels.	If PSKs are distributed electronically over an unprotected network, they must be encrypted using quantum resistant techniques. If PSKs are distributed manually and outside of a controlled boundary, they must be distributed by cleared and trusted personnel using AO-approved and CNSSI 4005 defined Two-Person Integrity (TPI)[11] procedures to ensure that no one person has sole access to the plaintext PSK.	T=O
PSK-GD-6	When encrypting PSKs, it must be performed with an approved encryption algorithm that uses an encryption key from a PBKDF or pre-placed symmetric KEKs, or using a quantum resistant key distribution protocol.	NSA-approved cryptographic solutions must be used for PBKDFs, KEKs with an approved encryption algorithm, and quantum resistant key distribution protocols.	T=O
PSK-GD-7	KEKs must be no less than 256 bits.	Configure the KGS to generate 256 bit KEKs.	T=O
PSK-GD-8	Passwords used with a password-based encryption algorithm must be randomly generated using an NSA-approved password generation tool.	*No additional requirements.*	T=O
PSK-GD-9	The password length guidance provided in the *CSfC Key Management Requirements Annex* must be followed to determine the required minimum password length.	*No additional requirements.*	T=O

[11] Two-Person Integrity (TPI) procedures as defined in CNSSI 4005 must be applied throughout the entire life-cycle management of PSKs and PSK Key Encryption Keys (KEKs), starting with generation, and through distribution, installation, update and destruction. No one person shall have sole access to the plaintext PSK or KEK at any time during the life-cycle management of PSKs and KEKs.

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-GD-10	Passwords must be different each time a PSK is encrypted using a password-based encryption algorithm.	A new and different password must be used each time a PSK is encrypted using a password-based encryption algorithm. Passwords must not be reused.	T=O
PSK-GD-11	PSKs issued to Outer Encryption Components must be handled as classified at the highest classification level of the solution.	The highest classification level of the solution is equivalent to the classification of the Red Network with the highest classification level.	T=O
PSK-GD-12	PSKs issued to Inner Encryption Components must be classified to the level of the Red Network.	*No additional requirements.*	T=O
PSK-GD-13	The classification of pre-placed KEKs and passwords is the same as the classification of the most sensitive PSKs that they are protecting.	*No additional requirements.*	T=O
PSK-GD-14	Manual distribution procedures and methods may be used for PSKs when encryption of PSKs is not feasible.	If PSKs are distributed manually and outside of a controlled boundary, they must be distributed by cleared and trusted personnel using AO-approved and CNSSI 4005 defined TPI procedures to ensure that no one person has sole access to the plaintext PSK.	T=O
PSK-GD-15	PSKs and KEKs must be identified using unique key identifiers.	Technical or procedural methods are to be used to uniquely identify each PSK generated by the KGS. A technical method is to hash the PSK/KEK and use the hash value as the key identifier. The PSK/KEK identifiers must be unique within a given CSfC solution.	T=O
PSK-GD-16	PSKs and KEKs must be accounted for throughout their life cycles. Specifically, the KGS needs to account for PSKs and KEKs distributed to DMs, and DMs need to account for PSKs and KEKs installed on CSfC security devices.	Technical or procedural methods are to be used to account for each PSK generated by the KGS during the life-cycle of the PSK, where life-cycle includes: 1) PSK generation, 2) PSK receipt by the DM to the KGS, 3) PSK installation into the CSfC device, 4) PSK rekey by the DM, which includes generation of a new PSK by the KGS, receipt of the new PSK by	T=O

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		the DM to the KGS, and installation of the new PSK into the CSfC device, and; 5) PSK compromise notification and recovery, which includes identifying the PSK as compromised, removing copies of the compromised PSK from the CSfC solution, and updating the required CSfC devices with a new PSK.	
PSK-GD-17	Accounting procedures for PSKs and KEKs must leverage CNSSI 4005 defined controls and requirements. At a minimum, accounting procedures will include: (a) mapping of PSK and KEK unique key identifiers to CSfC components; and (b) individual receipt confirmation for PSKs and KEKs during the distribution process.	CNSSI 4005 accounting procedures for PSKs and KEKs may be tailored as needed for the CSfC solution, but must be approved by the AO.	T=O
PSK-GD-18	All life-cycle management for PSKs, passwords, and KEKs, from generation through destruction, must be performed in accordance with an NSA approved KMP.	See *Appendix C. – Sample Structure for a Key Management Plan (KMP)* for a sample structure of a KMP or use the KMP provided by the enterprise KGS.	T=O
PSK-GD-19	Any backups of PSKs and KEKs must be performed in accordance with CNSSI 4005 Section VII.D [Storage of COMSEC Material], Section XI [Accounting, Inventory and Audits], and Section XIII [Encrypted COMSEC Material], or other NSA-approved procedures.	CNSSI 4005 accounting procedures for PSKs and KEKs may be tailored as needed for the CSfC solution, but must be approved by the AO. See *Appendix C. – Sample Structure for a Key Management Plan (KMP)*	T=O

4.3.2 PSK USAGE

PSKs are used by CSfC security devices to provide confidentiality and possibly perform mutual authentication of the devices that establish the CSfC inner or outer security tunnels. Once the PSK is installed into a CSfC security device, the PSK is assumed valid until it requires updating (see Tables 4 and 5).

It is critical that the PSKs (and KEKs, if used), be stored securely within the CSfC security device to prevent unauthorized disclosure of the PSK/KEK. In addition, any export of the PSK/KEK needs to ensure that the plaintext version of the PSK/KEK is not disclosed in an unauthorized manner.

Table 3 summarizes general requirement statements for the usage of PSKs. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully, and securely, implementing the techniques for the usage of PSKs within the CSfC solution.

Table 3: PSK Usage Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-U-1	PSKs must only be used with CSfC protocols that are approved for use with PSKs as stated in Table 1.	See Table 1.	T=O
PSK-U-2	PSKs must be stored within a CSfC component in encrypted form.	CSfC security devices using PSKs are to be chosen from the CSfC Component's List. Approved devices incorporate acceptable protection of PSKs within those devices by storing the PSKs in encrypted form.	T=O
PSK-U-3	PSKs and KEKs exported from a CSfC component must be protected from unauthorized disclosure. Encryption of exported PSKs and KEKs is recommended; however, manual procedure protection methods may be used when encryption of exported PSKs and KEKs is not technically feasible.	Technical and procedural controls must be used to securely export PSKs and KEKs from a CSfC device. Technical controls use quantum resistant techniques to encrypt the PSKs and KEKs. Manual controls use trusted and cleared personnel operating under TPI procedures, along with AO-approved storage containers to securely store the PSKs and KEKs.	T=O
PSK-U-4	A compromised PSK/KEK must never be used in a CSfC solution.	*No additional requirements.*	T=O
PSK-U-5	Each PSK and KEK must be uniquely identified to ensure a compromised PSK/KEK is never used in a CSfC solution.	Unique identification of the PSK/KEK may be performed using technical or procedural methods.	T=O
PSK-U-6	PSKs must not be shared by more than two CSfC security devices.	Group keys must not be used in CSfC solutions. If multiple redundant VPN Gateways are implemented in a solution to provide high availability, per-EUD PSKs are permitted to be installed on each VPN Gateway providing high availability for that encryption layer.	T=O
PSK-U-7	At least one solution layer must use public key certificates for	*No additional requirements.*	T=O

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
	mutual authentication between devices.		
PSK-U-8	For solutions using RFC 8784-compliant IKEv2 to provide quantum resistant IPsec, public key certificates must be used for mutual authentication in addition to PPKs.	*No additional requirements.*	T=O

4.3.3 PSK REKEY

PSKs require periodic updating to limit the amount of operational exposure for the PSKs. If a PSK existed for a long operational time, and an adversary was able to compromise the PSK without detection, the adversary would be able to use the PSK (i.e., execute a man-in-the-middle attack) until the PSK was rekeyed. Frequent rekeying of PSKs minimize the window of opportunity an adversary may have in compromising and using the PSK before being detected. Therefore, considerations for periodicity of PSK rekeying include:

- *The number of CSfC solution components that share the same PSK* – As more components share the same PSK, the more frequent the PSK rekeying should occur.
- *Sensitivity of the information being protected by the CSfC solution that uses PSKs* – As the sensitivity level of the information increases, the more frequent the PSK rekeying should occur.
- *Accessibility or level of difficulty to compromise a CSfC solution component and the PSK* – As the level of accessibility increases (or level of difficulty decreases), the more frequent the PSK rekeying should occur.

The PSK update process is shown in Figure 4, which is the same as the PSK generation, distribution and installation process described in Section 4.3.1.

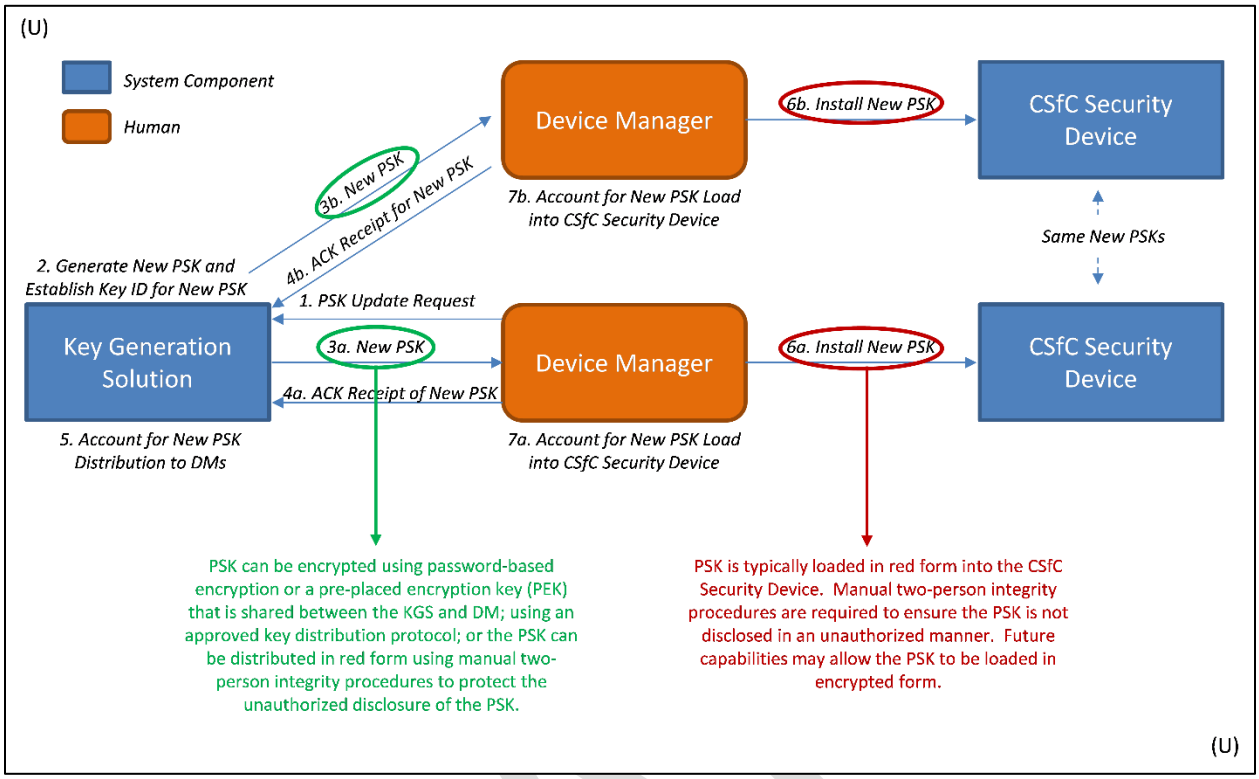

Figure 5: PSK Rekey for a CSfC Security Device

Table 4 summarizes general requirement statements for the rekey of PSKs. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully, and securely, implementing techniques for the updating of PSKs within the CSfC solution.

Table 4: PSK Rekey Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-RK-1	PSKs must be rekeyed every 30 to 180 days, or as required by the NSA-approved KMP.	• Updating of PSKs follows the same implementation requirements defined in Section 4.3.1 for PSK generation, distribution and installation. • The KMP must define the periodicity of PSK rekeying for the CSfC solution.	T=O
PSK-RK-2	KEKs must be rekeyed every 210 days, or as required by the NSA-approved KMP.	Updating of KEKs follows the same implementation requirements defined in Section 4.3.1 for PSK generation, distribution and installation.	T=O

4.3.4 PSK Compromise Recovery

PSK compromise recovery is a critical function within a CSfC solution[12]. Because a PSK is shared between two CSfC security devices, compromise of one device and its PSK ends up compromising the other device that shares the same PSK. Therefore, the CSfC solution must maintain accurate accounting records to know which PSKs are installed on which CSfC security devices. The KGS needs to be able to contact DMs and inform them of a PSK compromise. The DMs then need to determine which CSfC security devices use the compromised PSK, and execute the *PSK rekey* process to replace the compromised PSK.

Figure 5 shows the PSK compromise recovery process. The process begins with one of the DMs detecting a PSK compromise, suspending the use of the PSK, and sending a compromise notification to the KGS that a particular PSK has been compromised, along with a PSK rekey request to obtain a new PSK. Using the unique key identifier assigned to the PSK, the KGS is able to determine the other DM that was provided with the same PSK that was compromised. The KGS generates a new PSK and distributes the new PSK to the DMs that require it. The KGS also informs the remaining DM that the prior PSK was compromised, thereby providing rationale for the distribution of the new PSK. The DMs acknowledge receipt of the new PSK back to the KGS through a protected channel or method, ensure that the compromised PSK is removed and no longer used, and install the new PSK onto the CSfC security devices.

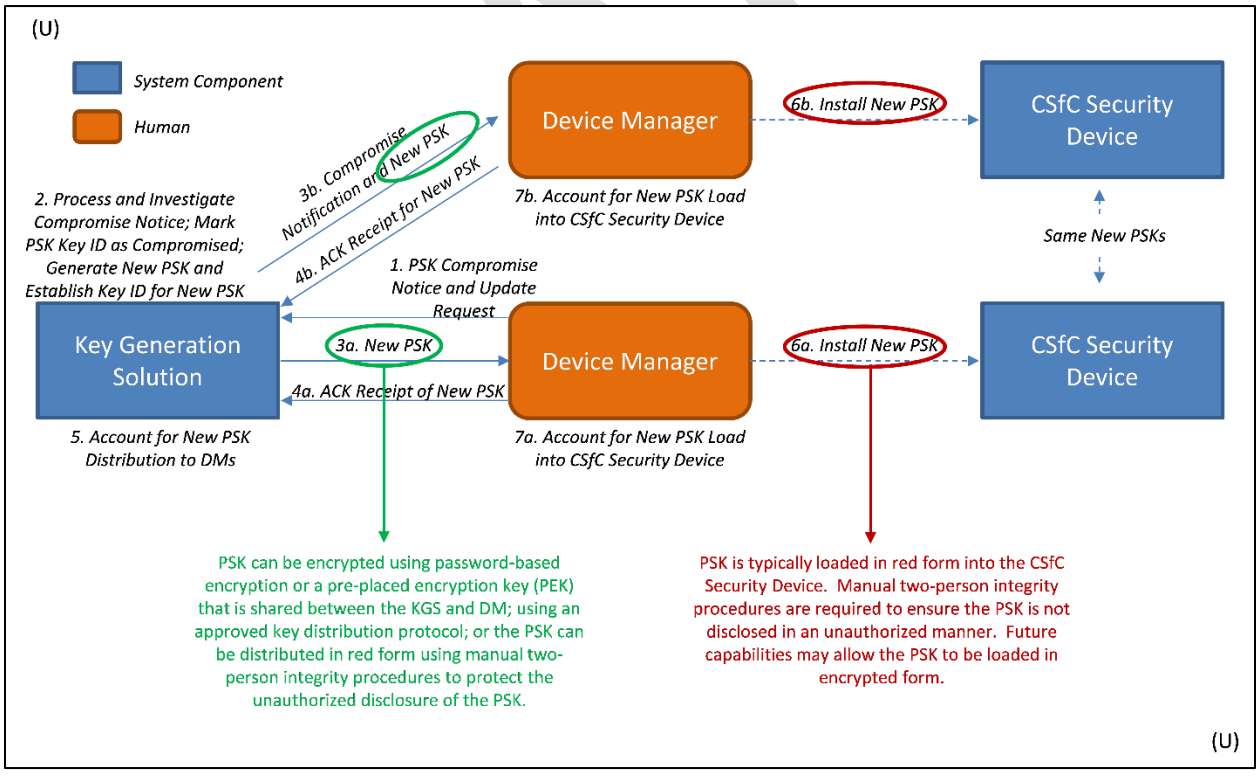

Figure 6: PSK Compromise Recovery for CSfC Security Devices

[12] CNSSI 4003 is the authoritative source for reporting and evaluating COMSEC incidents.

Table 5 summarizes general requirement statements for the compromise recovery of PSKs. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully, and securely, implementing techniques for the compromise recovery of PSKs within the CSfC solution.

Table 5: PSK Compromise Recovery Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-CR-1	Accounting procedures must support PSK and KEK compromise recovery to ensure all copies of compromised PSKs and KEKs are identified and rekeyed.	Technical or procedural methods are to be used to support PSK/KEK compromise notification and recovery, which includes identifying the PSK/KEK as compromised, removing copies of the compromised PSK/KEK from the CSfC solution, and updating the required CSfC devices with a new PSK. CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures.	T=O
PSK-CR-2	The PSK/KEK compromise recovery process must be documented in the KMP.	CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures. See *Appendix C. – Sample Structure for a Key Management Plan (KMP)* for a sample structure of a KMP or the KMP provided by the enterprise KGS.	T=O
PSK-CR-3	If they are considered compromised, PSKs/KEKs must be rekeyed as soon possible.	Updating of PSKs/KEKs follows the same implementation requirements defined in Section 4.3.1 for PSK generation, distribution and installation.	T=O
PSK-CR-4	The DM must determine if a PSK/KEK is considered compromised, and submit a compromise notification to the KGS along with a request to rekey the PSK/KEK.	The DM submits a compromise notification using a procedure that is agreed upon with the KGS, such that the KGS can trust the authenticity of the compromise notification (e.g., signed email, signed form). CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures.	T=O
PSK-CR-5	The DM and KGS must follow procedures for PSK/KEK compromise reporting as defined by the applicable KMP.	CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures. See *Appendix C. – Sample Structure for a Key Management Plan (KMP)*	T=O

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		for a sample structure of a KMP or the KMP provided by the enterprise KGS.	
PSK-CR-6	Compromise recovery procedures must include response to a lost, stolen or compromised End User Device (EUD).	The DM associated with an EUD is to be notified when the device is lost, stolen or compromised so that the DM can report the PSK associated with the device as compromised. All other devices that share the same PSK are to be considered compromised and the PSKs for all devices need to be rekeyed.	T=O
PSK-CR-7	Compromise recovery procedures must include removal of a compromised infrastructure device (e.g., VPN Gateway) from the network.	If an infrastructure device is determined to be compromised, the DM associated with the infrastructure device needs to physically disconnect the device from the network when the device is considered compromised, and only reconnect the device to the network after all of the compromised PSKs associated with that device are successfully rekeyed. The DM also needs to identify all other devices that share the PSKs of the compromised infrastructure device so that those devices can have their PSKs rekeyed. If an EUD is compromised, an assessment needs to be made if the infrastructure device is to be removed from the network prior to updating the PSK in the infrastructure device.	T=O
PSK-CR-8	Compromise recovery procedures must address re-establishing a CSfC security device after its PSK is compromised.	Re-establishment of PSKs follows the same implementation requirements defined in Section 4.3.1 for PSK generation, distribution and installation.	T=O
PSK-CR-9	If a compromised device is to be reused, that device must go through the initial PSK issuance process.	Reuse of a compromised CSfC security device follows the same implementation requirements defined in Section 4.3.1 for PSK generation, distribution and	T=O

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
		installation. This requirement is in addition to the Capability Package requirements for reusing a compromised device.	

4.3.5 KGS CONNECTIVITY GUIDANCE

Figure 6 and Figure 7 address connectivity of KGSs in CSfC solutions. Figure 6 shows a single KGS that connects with the local red management network and provides PSK management services for CSfC components located in the Red and Gray Networks. A Control Interface (CI) that is also a Cross Domain Solution (CDS) may be used to transfer the PSKs generated by the KGS from the Red Network enclave to the Gray Network. Figure 7 shows two KGSs; one KGS connected to the Red Management Network and provides PSK management services for Inner Encryption Components and one KGS connected to the Grey Management Network and provides PSK management services for Outer Encryption Components.

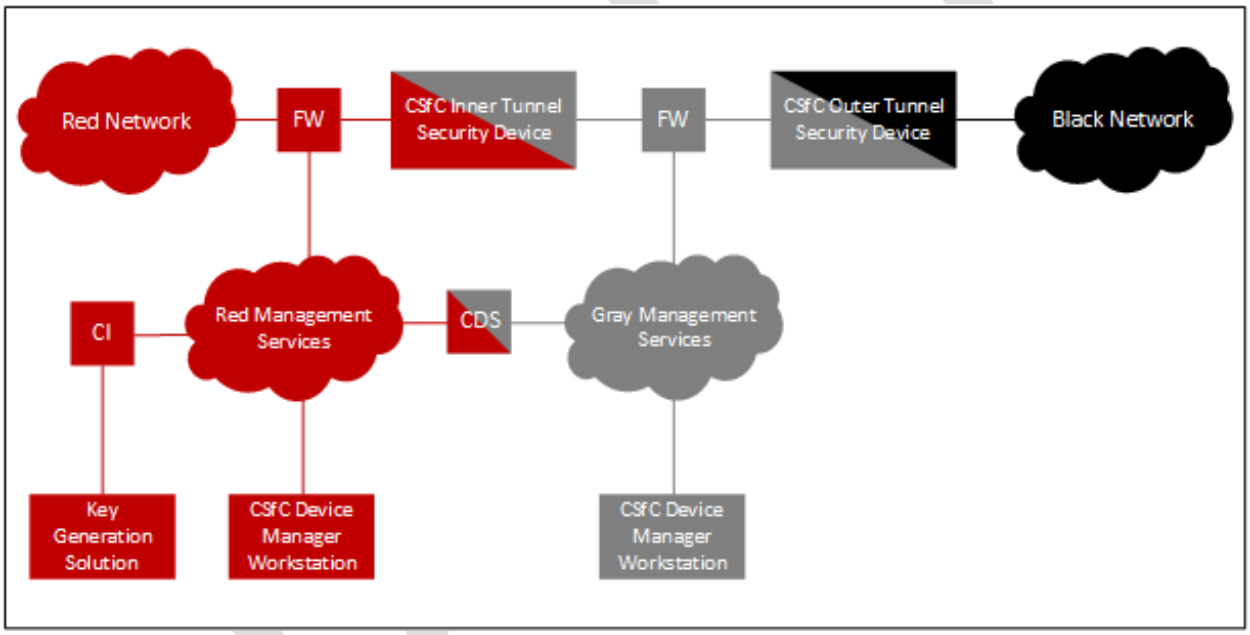

Figure 7: Connectivity Guidance for Locally Operated Single Key Generation Solution

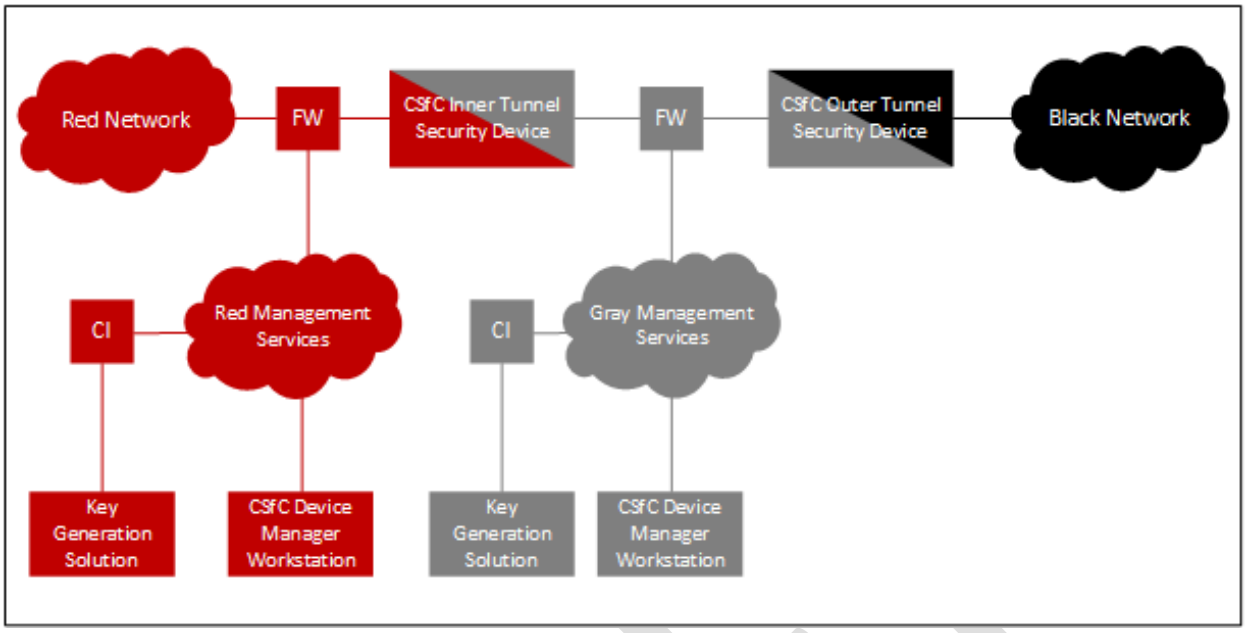

Figure 8: Connectivity Guidance for Multiple Key Generation Solutions (Inner KGS and Outer KGS)

Table 6 summarizes general requirement statements for KGS connectivity in CSfC solutions. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully and securely installing the KGS services into the CSfC solution network.

Table 6: KGS Connectivity Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-KC-1	PSK management services provided by a KGS (enterprise or locally operated) used for generating and managing PSKs for inner tunnel components must be connected to the local red management network.	Installation of KGS services is to be performed in accordance with AO-approved installation instructions. Even if the KGS is not connected to the red management network and operates in a stand-alone configuration, the KGS is to be deployed in the Red Network enclave.	T=O
PSK-KC-2	If the KGS operates at the same classification level as the management network it is connected to, a non-CDS CI must be used to control information flow between the KGS and the management network.	The information flows into and out of the KGS are to be well defined and only support the life-cycle management of PSKs. The CI (e.g., firewall) is to enforce these information flows and ensure no other information flows into and out of the KGS.	T=O
PSK-KC-3	When using a single KGS located in the Red Network enclave, PSKs	No additional requirements.	T=O

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
	used for outer tunnel components operating on the Gray/Black network boundary must be distributed in accordance with an AO-approved method to move the PSKs from the red network enclave to the gray network CSfC components.		
PSK-KC-4	If using separate KGSs for the inner and outer encryption components (i.e. Inner KGS for inner component PSKs and Outer KGS for outer component PSKs), PSK management services provided by a KGS (enterprise or locally operated) used for generating and managing PSKs for outer encryption components must be connected to the gray management network.	No additional requirements.	T=O

4.3.6 KGS AUDIT GUIDANCE

PSK management services are delivered by KGSs that operate in accordance with an approved KMP. The KMP defines the technical and procedural requirements for performing life-cycle management of PSKs. KGSs that deliver PSK management services for CSfC solutions are to comply with any audit and assessment requirements defined by the CSfC customer's operational security doctrine. The audits and assessments are to be performed by personnel who are knowledgeable in the KGSs' operations, as well as the KGSs' KMP requirements and processes, respectively.

Table 7 summarizes general requirement statements for the auditing of a KGS. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in periodically auditing the KGS of the CSfC solution.

Table 7: Additional KGS Audit Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-KA-1	KGSs that deliver PSK management services for CSfC solutions must comply with audit and assessment requirements defined by the CSfC customer's operational security doctrine and enterprise KGS (if applicable).	AO-approved audit procedures are to be used to periodically audit and assess a locally operated KGS.	T=O

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-KA-2	Audits and assessments must be performed by personnel who are knowledgeable in the KGS's operations, as well as the KGS's audit requirements and processes, respectively.	AO-approved audit personnel are to be used to periodically audit and assess a locally operated KGS.	T=O

4.3.7 PSK TESTING GUIDANCE

Life-cycle solution testing of PSKs should be performed prior to the operational deployment of KGS, using test PSKs vs. operational PSKs. The KGS should be capable of generating and distributing test PSKs to the DMs to validate the secure PSK distribution capabilities, as well as the installation of the PSKs onto the CSfC security devices. Use of the PSKs should be tested to ensure they can be used to mutually authenticate CSfC components and established the CSfC tunnels. Finally, the PSK rekey process needs to be tested (both for normal rekey functions and in response to a compromise scenario) to ensure the KGS is able to generate and distribute rekeyed PSKs to DMs for installation onto the CSfC security devices.

Table 8 summarizes general requirement statements for the testing of a KGS. For each general requirement statement, additional implementation requirements are defined to assist the CSfC solution owner in successfully testing the KGS of a CSfC solution. Where applicable, CP requirements are identified to assist the CSfC solution owner in mapping the additional implementation requirements to specific KCM requirements defined in a CSfC CP.

Table 8: PSK Testing Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-TR-1	Life-cycle testing of PSKs must include initial generation and distribution of PSKs, installation and use of PSKs, scheduled rekeying of PSKs prior to PSK expiration, and PSK rekeying in response to PSK compromise.	AO-approved test plans and procedures are to be used to fully test the operations of a locally operated KGS.	T=O

4.3.8 ROLE-BASED PERSONNEL REQUIREMENTS

This section identifies all roles and responsibilities for performing the PSK management functions identified. Roles include the KGS Operator, KGS Administrator, Auditor, CSfC Device Manager, End User, and any other trusted roles to satisfy the PSK management requirements.

KGS Operator – Responsible for the general operations of the KGS to generate, distribute, manage and account for PSKs. The KGS Operator role can be combined with the KGS Administrator role.

KGS Administrator – Responsible for the system administration of the KGS by ensuring its hardware and software baseline is maintained, and that the KGS is correctly configured to support the required operations. The KGS Administrator role can be combined with the KGS Operator role.

Auditor – Responsible for reviewing the events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the KGS and CSfC solution.

CSfC Device Manager – Responsible for managing the CSfC device that will use PSKs, securely installing PSKs into the CSfC device using TPI procedures defined in the KMP, accounting for the PSKs installed on the CSfC device, destroying expired and compromised PSKs, and supporting PSK compromise recovery procedures.

Other Trusted Roles – Responsible for assisting KGS operations personnel and CSfC device managers with the secure life-cycle management of PSKs to ensure that no one person at any given time has sole access to plaintext PSKs used in the CSfC solution.

Table 9: Role-Based Personnel Requirements

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective
PSK-RB-1	All personnel holding trusted roles must be cleared to the highest level of data protected by the CSfC solution.	No additional requirements.	T=O
PSK-RB-2	The Auditor role must not be combined with any other trusted roles.	No additional requirements.	T=O
PSK-RB-3	KGS operations personnel (e.g., KGS Operator, KGS Administrator) must be a different individual(s) from the CSfC Device Manager(s).	No additional requirements.	T=O
PSK-RB-4	All personnel holding trusted roles must meet local Information Assurance (IA) training requirements.	No additional requirements.	T=O
PSK-RB-5	Mandatory Access Control policy must specify roles using role-based access controls.	No additional requirements.	O
PSK-RB-6	Auditing of KGS operations must be performed by individuals who were not involved in the integration of the CSfC solution.	No additional requirements.	T=O

APPENDIX A. ACRONYMS

Acronym	Meaning
AO	Authorizing Official
CAK	Connectivity Association Key
CDS	Cross Domain Solution
CI	Control Interface
CKN	Connectivity Association Key Name
CNSS	Committee on National Security Systems
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CP	Capability Package
CSfC	Commercial Solutions for Classified
DM	Device Manager
EUD	End User Device
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
KM	Key Management
KMP	Key Management Plan
KGS	Key Generation Solution
MACsec	Media Access Control Security
MitM	Man-in-the-Middle
MSC	Multi-site Connectivity
NSA	National Security Agency
NSS	National Security System
NSSI	National Security Systems Instruction
KEK	PSK Key Encryption Key
PBKDF	Password Based Key Derivation Function
PMO	Program Management Office
PPK	Post-quantum PSK
PSK	Pre-Shared Key
SRTP	Secure Real-Time Protocol
SSH	Secure Shell
TLS	Transport Layer Security
TPI	Two-Person Integrity
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

APPENDIX B. REFERENCES

Document	Title	Date
CNSSI 4003	*Committee on National Security Systems (CNSS) Instruction Number 4003, Reporting and Evaluating COMSEC Incidents*	June 2016
CNSSI 4004	*CNSS Instruction (CNSSI) Number 4004, Destruction and Emergency Protection Procedures for COMSEC and Classified Material*	August 2006
CNSSI 4005	*CNSS Instruction (CNSSI) Number 4005, Safeguarding COMSEC Facilities and Materials*	August 2011
CNSSI 4009	*CNSS Instruction (CNSSI) Number 4009, Committee for National Security Systems (CNSS) Glossary.*	April 2015
CNSSP 7	*CNSS Policy (CNSSP) Number 7, National Policy on the Use of Commercial Solutions to Protect National Security Systems*	December 2015
CNSSP 11	*CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*	June 2013
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*	October 2016
CSfC Campus WLAN CP	*Commercial Solutions for Classified (CSfC): Campus Wireless Local Area Network (WLAN) Capability Package (CP), v3.1.0*	January 2025
CSfC MA CP	*Commercial Solutions for Classified (CSfC): Mobile Access Capability Package (CP), v2.7.0*	January 2025
CSfC MSC CP	*Commercial Solutions for Classified (CSfC): Multi-Site Connectivity (MSC) Capability Package (CP), v1.2.0*	March 2023
CSfC KM Annex	*Commercial Solutions for Classified (CSfC): Key Management Requirements Annex, v2.1*	May 2022
IEEE 802.1AE-2018	*IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security*	December 2018
IEEE 802.1X-2020	*IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control*	January 2020
RFC 7296	*IETF RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2). C. Kaufman, et. al.*	October 2014
RFC 8784	*IETF RFC 8784 Mixing Preshared Keys in IKEv2 for Post-Quantum Security. S. Fluhrer, et. al.*	June 2020
RFC 9151	*IETF RFC 9151 Commercial National Security Algorithm (CNSA) Profile for TLS and DTLS 1.2 and 1.3.* D. Cooley.	April 2022

Document	Title	Date
RFC 9152	*IETF RFC 9152 The SODP (Secure Object Delivery Protocol) Server Interfaces: NSA's Profile for Delivery of Certificates, CRLs, and Symmetric Keys to Clients.* S. Turner, M. Jenkins.	April 2022
SP 800-57-1	*NIST Special Publication 800-57 Part 1 Rev. 5, Recommendation for Key Management - General.* E. Barker.	May 2020
SP 800-57-2	*NIST Special Publication 800-57 Part 2 Rev. 1, Recommendation for Key Management – Best Practices for Key Management Organizations.* E. Barker, et. al.	May 2019
SP 800-57-3	*NIST Special Publication 800-57 Part 3 Rev. 1, Recommendation for Key Management – Application-Specific Key Management Guidance.* E. Barker, et. al.	Jan 2015
SP 800-77	*NIST Special Publication 800-77 Rev. 1, Guide to IPsec VPNs.* E. Barker, et. al.	June 2020
	CSfC Key and Certificate Management Guidance: Use Cases Appendix, Version 0.2	June 2015
	CSfC Key and Certificate Management Guidance, Version 0.7	October 2015

314

315

APPENDIX C. SAMPLE STRUCTURE FOR A KEY MANAGEMENT PLAN (KMP)

The following sample structure may be used to develop a KMP for a locally operated KGS. The KMP is required for CSfC solutions that use a symmetric Key Generation Solution (KGS) to generate and manage Pre-shared Keys (PSKs).

TITLE: Key Management Plan for Pre-Shared Keys used in Support of <CSfC Customer Solution>

SECTION 1: Introduction

This section identifies:

- The document as a KMP for managing PSKs for the customer's CSfC solution.
- The type of CSfC solution (e.g., Mobile Access, Campus WLAN, Multi-site Connectivity), and which security tunnel(s) will use PSKs.
- The rationale for using PSKs in the CSfC solution.

SECTION 2: CSfC Solution Overview

This section:

- Provides an overview of the CSfC solution, to include a diagram of the solution architecture that depicts the KGS in relation to the other CSfC components.
- Identifies whether an enterprise or locally operated KGS is used.
- Identifies the types and sizes of PSKs that will be generated by the KGS and used within the CSfC solution (this will typically be 256 bits for use with the AES algorithm).
- Provides a general overview of the key management concept for PSKs and the entities involved (both solution components and humans).

SECTION 3: Key Management Plan

This section addresses the specifics of the key management plan for PSKs[13]. Diagrams showing information flows for PSK management functions are strongly encouraged throughout each section of the KMP.

3.1 Roles and Responsibilities

This section identifies all roles and responsibilities for performing the PSK management functions identified in the ensuing sections. Roles include the KGS Operator; KGS Administrator; KGS Security Officer; CSfC Device Manager; End User; and any other trusted roles to satisfy the PSK management requirements.

[13] If PSK Key Encryption Keys (KEKs) are used to protect PSKs during the life-cycle of the PSKs, KEKs are to be addressed as well in the KMP. The sections in the KMP apply to PSKs and KEKs.

KGS Operator – Responsible for the general operations of the KGS to generate, distribute, manage and account for PSKs.

KGS Administrator – Responsible for the system administration of the KGS by ensuring its hardware and software baseline is maintained, and that the KGS is correctly configured to support the required operations.

Auditor – Responsible for reviewing the events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the KGS and CSfC solution.

CSfC Device Manager – Responsible for managing the CSfC device that will use PSKs; securely installing PSKs into the CSfC device using TPI procedures defined in this KMP; accounting for the PSKs installed on the CSfC device; destroying expired and compromised PSKs; and supporting PSK compromise recovery procedures.

Other Trusted Roles – Responsible for assisting KGS operations personnel and CSfC device managers with the secure life-cycle management of PSKs to ensure that no one person at any given time has sole access to plaintext PSKs used in the CSfC solution.

3.2 Key Request and Generation

This section identifies the procedures that will be used to request and generate PSKs for CSfC solution components. Specifically, this section addresses:

- Who is authorized to initiate a PSK request and for which CSfC solution component? If multiple CSfC solution components require PSKs, are different requesters used?
- What size PSK is requested and for which algorithm? Typically, the PSK will be 256 bits in support of AES.
- How does the PSK request identify multiple authorized recipients for the PSK? A PSK may need to be distributed to two different locations (e.g., VPN sites) that require the same PSK to establish a CSfC security tunnel.
- How is the PSK request sent from the requester to the KGS Operator (e.g., electronically, physically)? What is the format for the PSK request? Is it cryptographically protected (e.g., signed, encrypted)?
- How does the KGS Operator verify that the PSK request is authentic and from an authorized requestor? How does the KGS Operator verify that the recipients identified in the PSK request are authorized to receive the PSK?
- How does the KGS generate the PSK using TPI procedures? What is the media (electronic, physical) and specification format for the output containing the PSK?

3.3 Key Distribution and Installation

This section identifies the procedures that will be used to distribute and install PSKs onto CSfC solution components. Specifically, this section addresses:

- How is the PSK output from the KGS secured for distribution to the authorized recipients (e.g., CSfC Device Managers)?

- If the PSK output is encrypted:
  - How is it encrypted? Using a password-based encryption algorithm? Using a pre-placed PSK Key encryption key (KEK)? Using a quantum-resistant key distribution protocol?
  - How are TPI procedures applied to ensure that no one person can decrypt the PSK and recover it in plaintext form?
- If the PSK output is physical and in plaintext:
  - How is it packaged for secure physical distribution to the authorized recipients?
  - How are TPI procedures applied to ensure that no one person can gain access to the plaintext physical PSK?
- How does the authorized recipient of the PSK verify that the package containing the PSK (electronic or physical) has not been tampered with during distribution from the KGS to the Device Manager?
- How are TPI procedures applied to recover the plaintext PSK (e.g., decrypt, unwrap physical package) for installation into the CSfC solution component?
- How are TPI procedures applied to install the PSK into the CSfC solution component?
- How are TPI procedures applied to destroy all remaining copies of the PSK after it has been installed into the CSfC solution component?
- How are TPI procedures applied to ensure no one person can view or export the PSK in plaintext form after it has been installed on the CSfC solution component?

3.4 Key Rekey

This section identifies the procedures that will be used to rekey PSKs for CSfC solution components. Specifically, this section addresses:

- What are the circumstances that require the PSK to be rekeyed (e.g., PSK expiration and regular rekey, compromise recovery, forced rekey for some other reason)?
- Under normal operations, how often are PSKs and KEKs rekeyed?
- Is the PSK rekey process the same as the PSK request and generation process identified in Section 3.2 and 3.3? If not, explain any differences.

3.5 Key Compromise Reporting and Recovery

This section identifies the procedures that will be used to report the potential compromise of PSKs and to recover from PSKs deemed to be compromised[14]. Specifically, this section addresses:

[14] Information in this section is taken directly from CNSSI 4003. The term "COMSEC material" in CNSSI 4003 has been replaced with "PSK". In some cases, the language from CNSSI 4003 has been modified to be more applicable to PSKs used in CSfC solutions.

- What are the incidents that may result in the compromise of a PSK? CNSSI 4003, Section VIII, identifies reportable COMSEC incidents, some of which are identified below as being mostly applicable to CSfC solutions[15]:
    - Cryptographic incidents – Any product malfunction or human error that adversely affects the security of PSK material. Examples include:
        - Unauthorized exposure of the PSK in plaintext form.
        - Use of expired PSKs.
        - Use of PSKs not generated by an NSA-approved KGS.
        - Use of defective PSKs that result in the transmission of classified information in plaintext form.
    - Personnel incidents – Any capture, attempted recruitment, known or suspected control by a hostile intelligence entity; intentional or unintentional exposure of PSK material to an unauthorized person; or unauthorized absence or defection of an individual having knowledge of or access to PSK material. Examples include:
        - Unauthorized disclosure of PSK material (to include unauthorized disclosure of PINs and passwords that are used to protect PSK material).
        - Attempts by unauthorized persons to affect such disclosure.
        - Deliberate falsification of PSK management records (e.g., accounting records).
    - Physical incidents – Any loss of control, theft, capture, recovery by salvage, tampering, emergency destruction, unauthorized modification, unauthorized viewing or access, or unauthorized photographing that has the potential to jeopardize PSK material. Examples include:
        - Unauthorized access to PSK material, including access by persons who are mistakenly believed to have held appropriate clearances.
        - PSK material discovered outside of required PSK accountability or physical control.
        - Unexplained/undiagnosed zeroization or damage of PSK material.
        - PSK material improperly packaged.
        - PSK material improperly shipped.
        - PSK material received with a damaged inner wrapper.
        - Destruction of PSK material by other than authorized means.
        - Emergency destruction of PSK material.
        - Inadvertent or unintentional destruction or zeroization of PSK material, or destruction without authorization.
        - Evidence that product software configuration has been modified by non-authorized source or any un-authorized modification or update has taken place.
        - PSK material discovered to not have been destroyed within required time limits.
        - PSK material not completely destroyed as directed.

[15] The reportable incidents identified in CNSSI 4003, Section VIII should be reviewed in their entirety to determine those incidents that are applicable to the CSfC solution.

        - Actual or attempted unauthorized maintenance (including maintenance by unqualified personnel) or the use of a maintenance procedure that deviates from established standards. *[Note: This is applicable to the KGS and to the CSfC devices that use the PSKs.]*
        - Tampering with or penetration of PSK material.
        - Unexplained or unauthorized removal of PSK material from its protective technology.
        - Unauthorized copying, reproduction, or photographing of PSK material.
        - Loss of TPI or No-Lone Zone for PSK material.
        - Failure to perform audit trail management which results in subsequent loss of PSK material or data protected by the PSK material.
- What are the procedures for reporting a potential PSK compromise?
    - Who is authorized to report a potential PSK compromise?
    - To whom is the PSK compromise report sent? How is the compromise report sent (electronically or physically)?
    - How does the recipient of the PSK compromise report validate its authenticity and that the sender was authorized to submit the report?
    - Who is authorized to make the decision that a PSK is deemed compromised?
    - How is a compromised PSK reported to the parties that manage the CSfC solution components using the compromised PSK?
- What are the procedures for updating the PSK due to a PSK compromise? Explain any differences from those procedures already identified in sections 3.2 through 3.4.

3.6 Key Backup and Recovery

This section identifies the procedures that will be used to perform backup and recovery of PSKs used in CSfC solutions. Specifically, this section addresses:

- Who is authorized to create backups of PSKs, and for what authorized purposes are the PSK backups required?
- What is the process to request the recovery of a backed up PSK, and how is that request validated to ensure the requester has an authorized need for the backed up PSK?
- Who is authorized to recover a backed up PSK and install it in a CSfC solution component?
- How do the recovery procedures ensure that the integrity of the PSK was maintained since it was originally backed up?
- How are TPI procedures applied to the PSK backup and recovery procedures to ensure no one person has access to the plaintext PSK?

3.7 Key Destruction

This section identifies the procedures that will be used to destroy PSKs (electronically or physically) such that they cannot be used in CSfC solutions. Specifically, this section addresses:

- What are the incidents that result in the destruction of a PSK? Examples include those incidents identified in section 3.5.
- Who is authorized to request the destruction of a PSK, and how is that request validated to ensure the requester is authorized to make such a request?
- Who is authorized to destroy the PSK?
- What means are used to destroy the PSK (electronic and/or physical)?
- What procedures are used to ensure all copies of a PSK are destroyed, especially of those copies exist in different physical locations?

3.8 Key Accounting

This section identifies the procedures that will be used to account for PSKs throughout their entire life-cycle. Specifically, this section addresses:

- How does the KGS Operator account for a PSK generated by the KGS? What identifier is used to uniquely identify the PSK (e.g., hash of PSK, manual recording of identifier)?
- How does the KGS Operator account for distribution of PSKs to CSfC Device Managers and other trusted entities, to include acknowledgment of receipt of the PSKs?
- How does a CSfC Device Manager or other trusted entity account for PSKs that are installed in CSfC solution components to support life-cycle management operations such as PSK rekey and compromise reporting?
- How do the accounting procedures ensure that a compromised or expired PSK is never used?
- How do the accounting procedures ensure that a rogue copy of a destroyed PSK is never used?
- How do the accounting procedures ensure that each PSK within a CSfC solution is identified uniquely?

SECTION 4: References

This section lists any direct references made in the KMP, as well as other informative references that assist in understanding the contents of the KMP.

APPENDIX D. KEY GENERATION SOLUTION (KGS) APPROVAL CRITERIA CHECKLIST

This checklist is only approved for the identified CSfC Registration. Each CSfC Registration must complete and submit this checklist for NSA approval as part of the CSfC Registration process.

Classification when Complete: After completing the checklist, this document must be classified as determined by the appropriate solution classification authority used for other registration artifacts.

#	KGS Approval Criteria	SKM Annex Requirements Mapping	How does the KGS meet the Approval Criteria? (completed by System Owner/ Product Vendor/Trusted Integrator)	Approval Criteria Met (Y/N) / Reviewer Notes (completed by the CSfC PMO Reviewer)
1	The KGS generates PSKs and KEKs using a FIPS 140-3 validated[1] or NSA-approved RNG as specified in NIST SP 800-90 using Hash RBG(SHA-384, SHA-512), HMAC_RBG(SHA-384, SHA-512), or CTR_RBG(AES-256) seeded by a entropy source with a minimum of 256 bits of entropy and in accordance with FIPS 140-3. [1]An active NIST FIPS validation certificate number must be provided. [2]NSA-approval for non FIPS 140-3 validated RNGs must be submitted as request through CSRP, with approval not guaranteed	PSK-GD-1		
2	The KGS is deployable as a dedicated component within the Red Network enclave of the CSfC solution, connected either to the local red management network or in a stand-alone configuration and/or the KGS is deployable as a dedicated component within the Grey Management Network.	PSK-GD-2		
3	The KGS can generate at least 256 bit PSKs and PSK Key Encryption Keys (KEKs).	PSK-GD-3 PSK-GD-7		
4	The KGS can export PSKs in encrypted form, and encryption of PSKs is performed with a CSFC Capability Package/Annex approved	PSK-GD-4 PSK-GD-5 PSK-GD-6		

#	KGS Approval Criteria	SKM Annex Requirements Mapping	How does the KGS meet the Approval Criteria? (completed by System Owner/ Product Vendor/Trusted Integrator)	Approval Criteria Met (Y/N) / Reviewer Notes (completed by the CSfC PMO Reviewer)
	encryption algorithm that uses an encryption key from a PBKDF or pre-placed symmetric KEKs, or using a quantum resistant key distribution protocol. Or The KGS can export PSKs/KEKs unencrypted to secure storage containers without exposing the PSKs in plaintext form for manual distribution using AO-approved and CNSSI 4005 defined Two-Person Integrity (TPI) procedures.	PSK-GD-14		
5	The KGS can, using technical or procedural methods, produce a unique identity for each PSK and KEK generated.	PSK-GD-15 PSK-U-5		
6	The KGS can, using technical or procedural methods, account for each PSK and KEK generated including: - Mapping of PSKs and KEKs unique key identifiers to CSfC components in the solution; - Processing individual receipt confirmations for PSKs and KEKs after distribution to Device Managers.	PSK-GD-16 PSK-GD-17 PSK-CR-1		
7	The KGS can receive and authenticate PSK/KEK compromise notifications using technical or procedural methods.	PSK-CR-4 PSK-CR-5		
8	The KGS can, using technical or procedural methods, identify all PSKs/KEKs generated and distributed to CSfC devices, including compromised PSKs/KEKs.	PSK-GD-16 PSK-GD-17 PSK-CR-1 PSK-CR-4 PSK-CR-5		
9	The KGS can, using technical or procedural methods, categorize PSKs/KEKs as compromised after receiving an authenticated compromise notification.	PSK-CR-1 PSK-CR-4 PSK-CR-5		

#	KGS Approval Criteria	SKM Annex Requirements Mapping	How does the KGS meet the Approval Criteria? (completed by System Owner/ Product Vendor/Trusted Integrator)	Approval Criteria Met (Y/N) / Reviewer Notes (completed by the CSfC PMO Reviewer)
10	The KGS can, using technical or procedural methods, receive and authenticate rekey requests.	PSK-CR-1 PSK-CR-3 PSK-CR-4		
11	The KGS uses a Controlled Interface (e.g., firewall) to control information flows into and out of the KGS. The information flows into and out of the KGS are well defined and only support the life-cycle management of PSKs.	PSK-KC-2		
12	The KGS can produce and store audit logs. At a minimum, log entries record information as stated by the threshold requirements in the *CSfC Continuous Monitoring Annex* Table 14 Logging Requirements.	PSK-KA-1		
13	The KGS implements controls to prevent unauthorized access.	PSK-RB-3 PSK-RB-5		
14	Backups of PSKs and KEKs by the KGS are performed in accordance with CNSSI 4005 Section VII.D [Storage of COMSEC Material], Section XI [Accounting, Inventory and Audits], and Section XIII [Encrypted COMSEC Material], or other NSA-approved procedures.	PSK-GD-19		
15	The KGS is compliant with an associated NSA approved Key Management Plan (KMP).	PSK-GD-18		

530

531

532