National Security Agency/
Central Security Service

CYBERSECURITY SOLUTIONS

COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSFC) SYMMETRIC KEY MANAGEMENT REQUIREMENTS ANNEX V2.0

Version 2.0
September 2020

1 SYMMETRIC KEY MANAGEMENT GENERAL REQUIREMENTS

1.1 PSK GENERATION, DISTRIBUTION AND INSTALLATION REQUIREMENTS FOR CSFC SOLUTIONS

Table 1. PSK Generation, Distribution and Installation Requirements for CSfC Solutions

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-1	Generation of PSKs must be performed by an NSA-approved Key Generation Solution (KGS). NSA-approved means: (a) a component from the CSfC Approved Products List, (b) a component approved for the CSfC solution by the Deputy National Manager for National Security Systems, or (c) an already approved enterprise service.	Contact the CSfC PMO to identify an NSA-approved KGS that can be used within a CSfC solution.	T=O	
PSK-2	Centralized generation, distribution, installation and management of PSKs must be performed by a dedicated KGS.	Deploy a single KGS within the Red Network of the CSfC solution and in accordance with operational deployment instructions provided by the CSfC PMO or the enterprise KGS. In addition, a KCMP 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 and Certificate Management Plan (KCMP)* for a sample structure of a KCMP.	T=O	
PSK-3	PSKs must always be 256 bits.	Configure the KGS to generate 256 bit PSKs.	T=O	

PSK-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 is provided to a second cleared and trusted person. The two authorized individuals distribute the PSK	T=O	

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
		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-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)[1] procedures to ensure that no one person has sole access to the plaintext PSK.	T=O	

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

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-6	Encryption of PSKs must be performed using a password-based encryption algorithm; pre-placed symmetric PEKs; or using a quantum resistant key distribution protocol.	NSA-approved cryptographic solutions must be used for password-based encryption algorithms, PEKs and quantum resistant key distribution protocols.	T=O	
PSK-7	PEKs must always be 256 bits.	Configure the KGS to generate 256 bit PEKs.	T=O	
PSK-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-9	The password length guidance provided in the *CSfC Data-At-Rest CP* must be followed to determine the required minimum password length.	Follow the password strength guidance provided in the CSfC Data-At-Rest Capability Package to determine the minimum password length.	T=O	
PSK-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-11	PSKs issued to Outer Encryption Components are classified as determined by the AO and compliant with CNSSI 4005.	*No additional requirements.*	T=O	
PSK-12	PSKs issued to Inner Encryption Components are classified to the level of the Red network.	*No additional requirements.*	T=O	

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-13	The classification of pre-placed PEKs and passwords is the same as the classification of the PSKs that they are protecting.	*No additional requirements.*	T=O	
PSK-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-15	PSKs and PEKs 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/PEK and use the hash value as the key identifier. The PSK/PEK identifiers must be unique within a given CSfC solution.	T=O	

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-16	PSKs and PEKs must be accounted for throughout their life cycles. Specifically, the KGS needs to account for PSKs and PEKs distributed to DMs, and DMs need to account for PSKs and PEKs 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 update by the DM, which includes generation of a new PSK by the KGS, receipt of the new PSK by 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.	T=O	

Req. #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-17	Accounting procedures for classified PSKs and PEKs must comply with CNSSI 4005 controls and requirements.	CNSSI 4005 accounting procedures for classified PSKs and PEKs may be tailored as needed for the CSfC solution, but must be approved by the AO.	T=O	
PSK-18	Accounting procedures for PSKs and PEKs designated as CUI should leverage CNSSI 4005 controls and requirements. At a minimum, accounting procedures will include: (a) mapping of PSK and PEK unique key identifiers to CSfC components; and (b) individual receipt confirmation for PSKs and PEKs during the distribution process.	CNSSI 4005 accounting procedures for CUI PSKs and PEKs may be tailored as needed for the CSfC solution, but must be approved by the AO.	T=O	
PSK-19	All life-cycle management for PSKs, passwords, and PEKs, from generation through destruction, must be performed in accordance with the approved KCMP.	See APPENDIX C. – Sample Structure For A Key and Certificate Management Plan (KCMP) for a sample structure of a KCMP or use the KCMP provided by the enterprise KGS.	T=O	
PSK-20	Any backups of PSKs and PEKs 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 classified PSKs and PEKs may be tailored as needed for the CSfC solution, but must be approved by the AO.	T=O	

1.2 PSK USAGE

Table 2. PSK Usage Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-21	PSKs must only be used with CSfC protocols that are approved for use with PSKs.	See Table 1 in Annex.	T=O	
PSK-22	PSKs must be stored within a CSfC component in encrypted form.	CSfC security devices using PSKs are to be chosen from an approved list of devices defined by the CSfC Program Office. Approved devices incorporate acceptable protection of PSKs within those devices by storing the PSKs in encrypted form.	T=O	
PSK-23	PSKs and PEKs exported from a CSfC component must be protected from unauthorized disclosure. Encryption of exported PSKs and PEKs is recommended; however, manual procedure protection methods may be used when encryption of exported PSKs and PEKs is not technically feasible.	Technical and procedural controls must be used to securely export PSKs and PEKs from a CSfC device. Technical controls use quantum resistant techniques to encrypt the PSKs and PEKs. Manual controls use trusted and cleared personnel operating under TPI procedures, along with AO-approved storage containers to securely store the PSKs and PEKs.	T=O	
PSK-24	A compromised PSK/PEK must never be used in a CSfC solution.	No additional requirements.	T=O	
PSK-25	Each PSK and PEK must be uniquely identified to ensure a compromised PSK/PEK is never used in a CSfC solution.	Unique identification of the PSK/PEK may be performed using technical or procedural methods.	T=O	

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-26	PSKs must not be shared by more than two CSfC security devices.	Group keys must not be used in CSfC solutions.	T=O	

1.3 PSK UPDATE REQUIREMENTS FOR CSFC SOLUTIONS

Table 3. PSK Update Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-27	PSKs must be updated every 30 to 180 days, or as required by the KCMP.	• Updating of PSKs follows the same implementation requirements defined in Section 2.3.1 for PSK generation, distribution and installation. • The KCMP must define the periodicity of PSK updates for the CSfC solution.	T=O	
PSK-28	PEKs must be updated every 90 days, or as required by the KCMP.	Updating of PEKs follows the same implementation requirements defined in Section 2.3.1 for PSK generation, distribution and installation.	T=O	

1.4 PSK Compromise Recovery Requirements for CSfC Solutions

Table 4. PSK Compromise Recovery Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-29	Accounting procedures must support PSK and PEK compromise recovery to ensure all copies of compromised PSKs and PEKs are identified and updated (rekeyed).	Technical or procedural methods are to be used to support PSK/PEK compromise notification and recovery, which includes identifying the PSK/PEK as compromised, removing copies of the compromised PSK/PEK 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-30	The PSK/PEK compromise recovery process must be documented in the KCMP.	CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures. See Appendix C. – Sample Structure for a Key and Certificate Management Plan (KCMP) for a sample structure of a KCMP or the KCMP provided by the enterprise KGS.	T=O	

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-31	PSKs/PEKs must be updated (rekeyed) as soon as practically possible if they are considered compromised.	Updating of PSKs/PEKs follows the same implementation requirements defined in Section 2.3.1 for PSK generation, distribution and installation.	T=O	
PSK-32	The DM must determine if a PSK/PEK is considered compromised, and submit a compromise notification to the KGS along with a request to update the PSK/PEK.	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-33	The DM and KGS must follow procedures for PSK/PEK compromise reporting as defined by the applicable KCMP.	CNSSI 4003 and 4005 are to be used to develop the compromise notification and recovery procedures. See Appendix C. – Sample Structure for a Key and Certificate Management Plan (KCMP) for a sample structure of a KCMP or the KCMP provided by the enterprise KGS.	T=O	

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-34	Compromise recovery procedures must include response to a lost, stolen or compromised End User Device (EUD).	The DM of 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 updated.	T=O	
PSK-35	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 of 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 updated. 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 updated.	T=O	

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-36	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 2.3.1 for PSK generation, distribution and installation.	T=O	
PSK-37	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 2.3.1 for PSK generation, distribution and installation. This requirement is in addition to the Capability Package requirements for reusing a compromised device.	T=O	

1.5 KGS CONNECTIVITY REQUIREMENTS FOR CSFC SOLUTIONS

Table 5. KGS Connectivity Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-38	PSK management services provided by a KGS (enterprise or locally operated) 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 Network and operates in a stand-alone configuration, the KGS is to be deployed in the Red Network enclave.	T=O	

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-39	If the KGS operates at the same classification level as the local red management network, a non-CDS CI must be used to control information flow between the KGS and the local red 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-40	PSKs 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 to the Gray Network CSfC components.	No additional requirements.	T=O	

1.6 KGS AUDIT REQUIREMENTS FOR CSFC SOLUTIONS

Table 6. KGS Audit Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-41	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	
PSK-42	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	

1.7 PSK TESTING REQUIREMENTS FOR CSFC SOLUTIONS

Table 7. PSK Testing Requirements for CSfC Solutions

Req #	General Requirement	Additional Implementation Requirements	Threshold / Objective	Compliance (Explain how your solution meets the requirement)
PSK-43	Life-cycle testing of PSKs must include initial generation and distribution of PSKs, installation and use of PSKs, scheduled updates of PSKs prior to PSK expiration, and PSK updates 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	