National Security Agency/
Central Security Service

CYBERSECURITY SOLUTIONS

KEY MANAGEMENT REQUIREMENTS ANNEX V2.0

Version 2.0
September 2020

1 KEY MANAGEMENT GENERAL REQUIREMENTS

The following requirements apply to all CSfC CPs unless the requirement number identifies a specific CP that the requirement applies to (e.g., WLAN-KM-1 only applies to the WLAN CP).

1.1 PKI GENERAL REQUIREMENTS

Table 1. PKI General Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-1	All public keys and certificates must be treated as determined by the AO.	T=O		
KM-2	Outer CAs must provide services through either the Gray or Red Network.	T=O		
KM-3	Inner CAs must provide services through the Red Network.	T=O		
KM-4	Locally-run Inner CAs must be physically separate from locally-run Outer CAs.	T=O		
KM-5	All certificates issued by the Outer and Inner CAs for the Solution must be Non-Person Entity (NPE) certificates, except in the case when a MA TLS EUD requires a user certificate for the Inner TLS tunnel.	T=O		
KM-6	All certificates issued by the Outer and Inner CAs for the solution must be used for authentication only.	T=O		
KM-7	Trusted personnel must be used for administrative access to the CAs.	T	KM-15	
KM-8	All certificate profiles for the Outer and Inner CAs for the solution must comply with IETF RFC 5280 and IETF RFC 8603.	T=O		
KM-9	All private keys must be classified as determined by the AO and compliant with CNSSI 4005.	T=O		
KM-10	The key sizes and algorithms for CA certificates and authentication certificates issued to Outer Encryption Components, Inner Encryption Components, and Administrative Device Components must be as specified in CNSSP 15.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-11	Outer and Inner CAs must not have access to private keys used in the Solution Components.	T=O		
KM-12	Private keys associated with on-line (i.e., CA is network-accessible), Outer and Inner CAs must be protected using Hardware Security Modules (HSMs) validated to Federal Information Processing Standards (FIPS) 140-2 Level 2.	T=O		
KM-13	Outer and Inner CAs must operate in compliance with a Certificate Policy and Certification Practice Statement that is formatted in accordance with IETF RFC 3647 and NIST IR 7924.	T=O		
KM-14	CAs must run anti-virus software.	T=O		
KM-15	Trusted personnel under two-person integrity (TPI) procedures must be used for administrative access to the CAs.	O	KM-7	
KM-16	If multiple Red enclaves exist in the Solution and the Outer CA resides in the Red Network, the Outer CA must reside in the Red Network with the highest classification level.	T=O		
KM-17	Certificate Management Services for the inner tunnel must be provided through the Red Network.	T=O		
KM-18	Certificate Management Services for the outer tunnel must be provided through either the Gray Network or Red Network.	T=O		
KM-19	Withdrawn			
KM-20	If the Certificate Management Services operate at the same security level as a Red Network, a Controlled Interface must be used to control information flow between the Certificate Management Services and the Red Network.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-21	If the Certificate Management Services operate at a different security level than a Red Network or Gray Network, a CDS Controlled Interface must be used to control information flow between the Certificate Management Services and the Red Network or Gray Network.	T=O		
KM-22	Copies of CA's own private keys must only be made using AO-approved procedures to support CA continuity of operations and disaster recovery (i.e., backups of private keys or HSMs).	T=O		

1.2 CERTIFICATE ISSUANCE REQUIREMENTS

Table 2. Certificate Issuance Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-23	EUDs, Outer Components, Inner Components, and Gray and Red Management Services Components must be initially keyed and loaded with certificates using an out-of-band process within a physical environment certified to protect the highest classification level of the solution network.	T=O		
KM-24	Private keys for EUDs, Outer Components, Inner Components and Gray and Red Management Services Components must never be escrowed.	T=O		
KM-25	Outer and Inner CAs must use Public Key Cryptographic Standard (PKCS) #10 and PKCS#7 to receive certificate signing requests and issue authentication certificates, respectively, to EUDs, Outer Components, Inner Components, and Gray and Red Management Services Components.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-26	If EUDs cannot generate their own key pairs, a dedicated offline management workstation must be used to generate the key pairs and PKCS#12 must be used for installing certificates and their corresponding private keys to EUDs.	T=O		
KM-27	PKCS#12 files must be securely distributed and use random passwords with a minimum length as defined in the *CSfC Data-At-Rest (DAR) CP* Appendix D.	T=O		
KM-28	If EUDS do not require their key pairs to be generated on a dedicated offline management workstation, Red and Gray Management Services must use PKCS#7 for installing certificates to EUDs.	T=O		
KM-29	Withdrawn			
KM-30	Certificate signing requests must be submitted to the CA by an authorized Registration Authority (RA) and in accordance with the CA's Certificate Policy and CPS. The Solution Owner must identify the authorized Registration Authorities.	T=O		
KM-31	Outer and Inner CAs must issue certificates in accordance with their Certificate Policies and CPSs.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)

KM-32	Certificate Policies and CPSs for non-Enterprise, locally-run CAs must ensure the CAs issue certificates within a defined and limited name space and assert:
	• Unique Distinguished Names (DNs)
	• Appropriate key usages
	• A registered certificate policy OID
	• A registered certificate policy OID is not required if all of the following are true:
	  • The certificates are limited to the specific customer's solution. That is, they are not part of an enterprise solution with multiple customers.
	  • The certificates only apply to a single security domain (e.g., Secret).
	  • There is only one certificate type (e.g., device, not user).
	  • There is only one issuance process described in the CP/CPS.
	  • There in only one assurance level.
		T=O		

KM-33	If using CDPs, Inner and Outer CAs must assert at least one CRL CDP Uniform Resource Locater (URL) in certificates issued to EUDs, Outer components, Inner Components, and Gray and Red Management Services Components. The CDP URL specifies the location of the CAs' CRL Distribution Point.	T=O		
KM-34	The key validity period for certificates issued by non-Enterprise, locally run CAs to End User Devices must not exceed 12 months.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-35	The key validity period for certificates issued by non-Enterprise, locally run CAs to Solution Infrastructure Components must not exceed 24 months.	T=O		
KM-36	Inner CAs must only issue certificates to Inner Components and Red Network Components of the Solution.	T=O		
KM-37	Outer CAs must only issue certificates to Outer Encryption Components and Gray Network Components of Solutions.	T=O		
KM-38	Withdrawn			
KM-39	Certificates issued to Outer VPN Gateways must assert the IP address of the Outer VPN gateway in either the Common Name field of the Distinguished Name, or the Subject Alternative Name certificate extension.	O	None	
KM-40	The Inner Encryption Component must only trust the Inner CA used for its network.	T=O		
KM-41	Outer Encryption Components must only trust the Outer CA used within the solution.	T=O		
KM-42	Withdrawn			
KM-43	The CSfC solution owner must identify authorized RAs to approve certificate requests.	T	KM-44	
KM-44	RAs must use multi-factor authentication to approve certificate requests.	O	KM-43	
KM-45	For CSfC solutions that deploy central management in accordance with the *CSfC Enterprise Gray Implementation Requirements Annex*, the Gray Firewall (used as the Inner VPN Gateway for the management plane) must use a certificate issued by a different CA than the Inner CA for authentication.	Enterprise Gray Annex Implemented: T=O Enterprise Gray Annex Not Implemented: N/A		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-46	When multiple classified enclaves are used, each enclave must have its own separate Inner CA, as Inner CAs cannot be shared between multiple classification levels.	T=O		

1.3 CERTIFICATE REKEY REQUIREMENTS

Table 3. Certificate Rekey Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-47	Certificate rekey should occur prior to a certificate expiring. If rekey occurs after a certificate expires, then the initial certificate issuance process must be used to rekey the certificate.	T=O		
KM-48	Certificate rekey must be performed in accordance with the CA's Certificate Policy and CPS.	T=O		
KM-49	Inner and Outer CAs must receive certificate signing requests and issue rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7, respectively, through an out-of-band process.	T	KM-50	
KM-50	Inner and Outer CAs must support over-the-network rekey of authentication certificates to Solution Components using EST (IETF RFC 7030 using CNSA TLS 1.2 (or a later version) certificate-based authentication).	O	KM-49	

1.4 CERTIFICATE REVOCATION AND CDP REQUIREMENTS

Table 4. Certificate Revocation and CDP Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-51	Inner and Outer CAs must revoke a certificate issued to Solution Components when the binding between the subject information and public key within the certificate issued is no longer considered valid.	T=O		
KM-52	Inner and Outer CAs must make certificate revocation information available in the form of CRLs signed by the CAs.	T=O		
KM-53	CRLs must be X.509 v2 CRLs as defined in ITU-T Recommendation X.509.	T=O		
KM-54	CRL profiles must comply with IETF RFC 5280 and IETF RFC 8603.	T=O		
KM-55	Procedures for requesting certificate revocation must comply with the CA's Certificate Policy and Certification Practices Statement.	T=O		
KM-56	Certificate Policies and CPSs for non-Enterprise, locally run CAs must ensure revocation procedures address the following: • Response for a lost, stolen or compromised EUD • Removal of a revoked infrastructure device (e.g., VPN Gateway) from the network • Re-establishment of a Solution Component whose certificate was revoked • Revocation of certificates due to compromise of a EUD • Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP Addresses	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-57	Inner and Outer CAs must make CRLs available to authorized CRL Distribution Points (CDPs), so that the CRLs can be accessed by Solution Components.	T	KM-63	
KM-58	Enterprise CAs must create and publish CRLs in accordance with the Enterprise CAs' Certificate Policies and CPSs.	T=O		
KM-59	Non-enterprise, locally-run CAs must publish new CRLs at least once every 30 days.	T=O		
KM-60	Non-enterprise, locally-run CAs must publish a new CRL within one hour of a certificate being revoked.	T=O		
KM-61	Solution Infrastructure Components must have access to new certificate revocation information within 24 hours of the CA publishing a new CRL.	T=O		
KM-62	Non-enterprise, locally run CAs must ensure that new CRLs are published at least 7 days prior to the next update date of the current CRLs.	T=O		
KM-63	The Solution must provide certificate revocation status information via an Online Certificate Status Protocol (OCSP) Server on the Red and Gray Networks that is compliant with IETF RFC 6960.	O	KM-57	
KM-64	Certificate revocation status messages delivered by an OCSP server must be digitally signed and compliant with IETF RFC 6960.	T=O		
KM-65	Withdrawn			
KM-66	If OCSP Responders are used, Inner CAs must assert the Authority Information Access certificate extension and include the list of URLs identifying the Inner OCSP Responders from which Inner VPN Gateways can request and receive OCSP revocation status responses.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-67	If OCSP Responders are used, Outer CAs must assert the Authority Information Access certificate extension and include the list of URLs identifying the Outer OCSP Responders from which Outer VPN Gateways can request and receive OCSP revocation status responses.	T=O		
KM-68	CRLs hosted by CDPs must be compliant with IETF RFC 5280 and RFC 8603.	T=O		
KM-69	CRLs hosted on Inner CDPs must be signed by the associated Inner CA.	T=O		
KM-70	CRLs hosted on Outer CDPs must be signed by the associated Outer CA.	T=O		
KM-71	CDPs and OCSP Responders must only issue CRLs and OCSP responses, respectively, to relying parties over port 80 (HTTP).	T=O		
KM-72	CRLs must be transferred via an AO approved method (e.g., CDS) from Inner CAs to associated Inner CDP servers and/or Inner OCSP Responders.	T=O		
KM-73	CRLs must be transferred via an AO approved method (e.g., CDS) from Outer CAs to associated Outer CDP servers and/or Outer OCSP Responders.	T=O		
KM-74	Newly issued CRLs must be transferred to CDP servers and/or OCSP Responders at least 4 days prior to the next update date of the current CRLs.	T=O		
KM-75	Solution Encryption Components must attempt to download the latest CRL from a CDP or an OCSP response from an OCSP Responder at least once every 24 hours.	T=O		
KM-76	Withdrawn			

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
KM-77	CDPs and OCSP Responders must only accept management traffic over TLS 1.2 (or later version) or Secure Shell (SSH)v2.	T=O		
KM-78	CDPs and OCSP Responders must only accept connections from authorized Solution Components or Administration Workstation addresses or address ranges.	T=O		
KM-79	If an integrity check of a CRL or OCSP response received from a CDP or OCSP response fails, then Solution Components must use the current cached CRL or OCSP response.	T=O		
KM-80	If a CDP is offline or contains an invalid CRL, then Inner and Outer Solution Component CRLs must be manually updated prior to the expiration of the current cached CRLs.	T=O		
KM-81	CDPs and OCSP Responders must not provide any other services other than the distribution of CRLs.	T=O		

1.5 Wireless Pre-Shared Key (WPSK) Requirements

The following requirements apply to the MA CP using a Retransmission Device and/or Dedicated Outer VPN with wireless connectivity.

Table 5. Wireless Pre-Shared Key (WPSK) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MA-KM-1	WPSKs used must be 256 bits.	T=O		
MA-KM-2	WPSKs must be generated by NSA-approved solutions.	T=O		
MA-KM-3	WPSKs must be distributed to, and installed on CSfC devices in a manner that minimizes the exposure of the red WPSK to the greatest extent possible.	T=O		

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MA-KM-4	WPSKs must be periodically updated based on the threat environment. The higher the threat environment, the more often the PSKs are to be updated. At a minimum, WPSKs must be updated once per year.	T=O		
MA-KM-5	A WPSK must be updated on all CSfC devices that use the WPSK as soon as practically possible if the WPSK is considered or suspected to be compromised.	T=O		
MA-KM-6	If a WPSK is considered or suspected to be compromised, the solution components must not accept traffic from devices using that WPSK until a new WPSK is provisioned.	T=O		

1.6 CAMPUS WLAN CP KEY MANAGEMENT REQUIREMENTS

The following requirements apply to the WLAN CP.

Table 6. Campus WLAN CP Key Management Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
WLAN-KM-1	The Outer CA must issue certificates to the WLAN Authentication Server that contains the TLS Web Server Authentication OID (1.3.6.1.5.5.7.3.1) in the ExtendedKeyUsage certificate extension.	T=O		
WLAN-KM-2	The Outer CA must issue certificates to the WLAN Client that contains the TLS Web Client Authentication (OID 1.3.6.1.5.5.7.3.2) ExtendedKeyUsage certificate extension.	T=O		

1.7 MACSEC KEY MANAGEMENT REQUIREMENT

The following requirement applies to the MSC CP when the MACsec protocol is used.

Table 7. MACsec Key Management Requirement

Req #	Requirement Description	Threshold / Objective	Alternative	Compliance (Explain how your solution meets the requirement)
MSC-KM-1	Enterprise or local Connectivity Association Key (CAK) management, including key generation and distribution, must follow an NSA-approved symmetric key management procedure. See the *CSfC Symmetric Key Management Requirements Annex* for additional guidance and requirements.	T=O		