National Security Agency / Central Security Service

CYBERSECURITY SOLUTIONS

# KEY MANAGEMENT REQUIREMENTS ANNEX V1.0

Version 1.0
26 June 2018

Registration ID:

Solution Name:

Date Submitted:

# 1 KEY MANAGEMENT GENERAL REQUIREMENTS

The following requirements apply to all CSfC Capability Packages unless the requirement number identifies a specific CP that the requirement applies to (i.e., 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 | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-7 | All certificates issued by the Outer and Inner CAs for the solution must be X.509 v3 certificates as defined in ITU-T Recommendation X.509. | T=O | | |
| KM-8 | All certificate profiles for the Outer and Inner CAs for the solution must comply with IETF RFC 5280. | 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 | | |
| KM-11 | Outer and Inner CAs must not have access to private keys used in the Solution Components. | T=O | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-12 | Private keys associated with on-line (i.e., CA is network-accessible), locally run 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. | 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 | None | |
| 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 | CAK management services (enterprise or locally-owned) must be provided through the local Red network. | T=O | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-20 | If the Certificate Management Services operate at the same security level as a Red network, a non-CDS Controlled Interface must be used to control information flow between the Certificate Management Services and the Red network. | T=O | | |
| KM-21 | If the Certificate Management Services operate at a different security level than a Red network or Grey network, a CDS Controlled Interface must be used to control information flow between the Certificate Management Services and the Red network or Grey 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 (e.g., 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 | Outer Components, Inner Components, and Gray and Red Management services Components must be initially keyed and loaded with certificates 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 issue authentication certificates to Outer Components, Inner Components, and Gray and Red Management Services Components. | T=O | | |
| KM-26 | If EUDs require their key pair to be generated on a dedicated management workstation, Red and Gray Management Services must use PKCS#12 for installing certificates and their corresponding private keys to EUDs. | T=O | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-27 | PKCS#12 files must be securely distributed using, at a minimum, a single layer of Data-At-Rest (DAR) protection. | T=O | | |
| KM-28 | Red and Gray Management Services must use PKCS#7 for installing certificates to EUDs. | T=O | | |
| KM-29 | Outer and Inner CAs must use IETF RFC 7030 EST to issue authentication certificates to Outer Components, Inner Components, and Gray and Red Management services Components. | O | KM-42 | |
| 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:<br>• Unique Distinguished Names (DNs)<br>• Appropriate key usages<br>• A registered certificate policy OID<br>• A registered certificate policy OID is not required if all of the following are true:<br>  • The certificates are limited to the specific customer's solution. That is, they are not part of an enterprise solution with multiple customers.<br>  • The certificates only apply to a single security domain (e.g., Secret).<br>  • There is only one certificate type (e.g.,device, not user).<br>  • There is only one issuance process described in the CP/CPS.<br>  • There in only one assurance level. | T=O | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-33 | If not using whitelists, Inner and Outer CAs must assert at least one CRL CDP Uniform Resource Locater (URL) in certificates issued to Solution Infrastructure Outer components, Inner Components, and Gray and Red Management Services Components. The CDP URL specifies the location of the CAs' CRLs. | T=O | | |
| KM-34 | The key validity period for certificates issued by non-Enterprise, locally run CAs to End User Devices must not exceed 14 months. | T=O | | |
| KM-35 | The key validity period for certificates issued by non-Enterprise, locally run CAs to Solution Infrastructure Components must not exceed 36 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 | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-38 | The Outer CA must issue certificates to EUD Clients that contain the Client Authentication OID (1.3.6.1.5.5.7.3.2) in the ExtendedKeyUsage certificate extension. | T=O | | |
| 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 | If over-the-network renewal or rekey of certificates to EUDs occurs over an untrusted network, it must be done using two valid encryption layers to the EUD in cases where EST is not supported. | T | KM-29 | |
| KM-43 | The CSfC solution owner must identify authorized RAs to approve certificate requests. | T | KM-44 | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| 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, 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 Red CA for authentication. | T | KM-46 | |
| KM-46 | For CSfC solutions that deploy central management in accordance with the CSfC Enterprise Gray Implementation Requirements, the Gray Firewall (used as the Inner VPN Gateway for the management plane) and the Outer Encryption Component must both use certificates issued by the same Outer CA for authentication. | O | KM-45 | |

## 1.3 CERTIFICATE RENEWAL AND REKEY REQUIREMENTS

**Table 3. Certificate Renewal and Rekey Requirements**

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-47 | Certificate renewal or rekey should occur prior to a certificate expiring. If renewal/rekey occurs after a certificate expires, then the initial certificate issuance process must be used to renew/rekey the certificate. | T=O | | |
| KM-48 | Certificate renewal or rekey must be performed in accordance with the CA's Certificate Policy and CPS. | T=O | | |
| KM-49 | Inner and Outer CAs must issue renewed/ rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7. | T | KM-50 | |
| KM-50 | Inner and Outer CAs must support over-the-network renewal and rekey of authentication certificates to Solution Components using EST (IETF RFC 7030). | 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 | If not using whitelists, 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. | T=O | | |
| KM-55 | Procedures for requesting certificate revocation must comply with the CA's Certificate Policy and Certification Practices Statement. | T=O | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-56 | Certificate Policies and CPSs for non-Enterprise, locally run CAs must ensure revocation procedures address the following:<br>• Response for a lost, stolen or compromised EUD<br>• Removal of a revoked infrastructure device (i.e., VPN Gateway) from the network<br>• Re-establishment of a Solution Component whose certificate was revoked<br>• Revocation of certificates due to compromise of a EUD<br>• Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP Addresses | T=O | | |
| KM-57 | If not using whitelists for authentication, 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 | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| 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 28 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 newly published CRLs are published at least 7 days prior to the expiration 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 Network 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 | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-65 | CRLs must expire no later than 35 days after their issue date. | T=O | | |
| 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 | | |
| 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. | T=O | | |
| KM-69 | CRLs hosted on Inner CDPs must be signed by the associated Inner CA. | T=O | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| 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 one-way transfer mechanism from Inner CAs to associated Inner CDP servers and Inner OCSP Responders. | T=O | | |
| KM-73 | CRLs must be transferred via an AO-approved one-way transfer mechanism from Outer CAs to associated Outer CDP servers and OCSP Responders. | T=O | | |
| KM-74 | Newly issued CRLs must be transferred to CDP servers and OCSP Responders at least 4 days prior to the expiration of the current CRLs. | T=O | | |
| KM-75 | If not using whitelists for authentication, VPN Gateways must attempt to download the latest CRL from a CDP at least once every 24 hours. | T=O | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| KM-76 | If whitelists are used for authentication, the whitelist must be validated against the latest CRL at least once every 24 hours. | T=O | | |
| KM-77 | CDPs and OCSP Responders must only accept management traffic over TLS 1.2 or Secure Shell (SSH)v2. | T=O | | |
| KM-78 | CDPs and OCSP Responders must only accept connections from authorized VPN Gateway 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 VPN Gateways 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 VPN Gateway 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 AND PRE-SHARED KEY (PSK) REQUIREMENTS

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

**Table 5. Wireless and Pre-Shared Key (PSK) Requirements**

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| MA-KM-1 | PSKs used must be 256 bits. | T=O | | |
| MA-KM-2 | PSKs must be generated by NSA-approved solutions. | T=O | | |
| MA-KM-3 | PSKs must be distributed to, and installed on CSfC devices in a manner that minimizes the exposure of the red PSK to the greatest extent possible. | T=O | | |
| MA-KM-4 | PSKs 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, PSKs must be updated once per year. | T=O | | |
| MA-KM-5 | A PSK must be updated on all CSfC devices that use the PSK as soon as practically possible if the PSK is considered or suspected to be compromised. | T=O | | |

| Req # | Requirement Description | Threshold / Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| MA-KM-6 | If a PSK is considered or suspected to be compromised, the solution components must not accept traffic from devices using that PSK until a new PSK is provisioned. | T=O | | |

## 1.6 CAMPUS WLAN CP KEY MANAGEMENT REQUIREMENTS

**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 | | |

## 1.7 MULTI-SITE CONNECTIVITY CP KEY MANAGEMENT REQUIREMENTS

The following requirements apply to the MSC CP when the MACsec protocol is used.

**Table 7. Multi-Site Connectivity CP Key Management Requirements**

| Req # | Requirement Description | Threshold/ Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| MSC-KM-1 | Enterprise or local CAK management, including key generation and distribution, must follow an NSA-approved symmetric key management procedure. | T=O | | |
| MSC-KM-2 | CAKs issued to Outer Encryption Components are CUI, but they are physically protected as if they were classified to the level of the Red network. | T=O | | |
| MSC-KM-3 | CAKs issued to Inner Encryption Components are classified to the level of the Red network. | T=O | | |
| MSC-KM-4 | All CAKs generated by, or issued to, an Encryption Component are to be used in strict accordance with approved protocols identified in the MSC CP. | T=O | | |
| MSC-KM-5 | Generation of CAKs and their associated CKNs must be performed by an NSA-approved KGS. NSA-approved means: a) a component from the CSfC Approved Products List; or b) a component approved for the CSfC solution by the Deputy National Manager for National Security Systems; or c) an already approved enterprise service. | T=O | | |

| Req # | Requirement Description | Threshold/ Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| MSC-KM-6 | Centralized generation, distribution and management of CAKs and their associated CKNs for Outer and Inner MACsec Devices must be performed by a dedicated KGS located in, or accessed through, the Red network. | T=O | | |
| MSC-KM-7 | CAKs issued to Outer MACsec Devices must be transferred from the Red network to the Gray network using an AO-approved transfer method. | T=O | | |
| MSC-KM-8 | CAKs must be 256 bits. | T=O | | |
| MSC-KM-9 | CAKs must not be exposed in plaintext form until they are ready to be installed on MACsec Devices. Installation of CAKs and their associated CKNs may be performed via file transfer or text input. | T=O | | |
| MSC-KM-10 | CAKs are to only be used with the MACsec protocol. | T=O | | |
| MSC-KM-11 | CAKs and CAK Encryption Key (CEKs) are to be stored within an approved cryptographic boundary within a Solution Component. | T=O | | |
| MSC-KM-12 | A compromised CAK/CEK is to never be used in the MSC Solution. | T=O | | |

| Req # | Requirement Description | Threshold/ Objective | Alternative | Compliance (Explain how your solution meets the requirement) |
|---|---|---|---|---|
| MSC-KM-13 | The same CAK must be used in only one pair of MACsec Devices that are establishing an encryption tunnel. | T=O | | |
| MSC-KM-14 | CAKs and their associated CKNs must be updated periodically as defined by an NSA-approved symmetric key management procedure. | T=O | | |
| MSC-KM-15 | There must be a documented CAK/CEK compromise recovery process, to include:<br>• Removal of a compromised infrastructure device (e.g., MACsec Devices) from the network, and<br>• Re-establishing a MACsec Device after its CAK is compromised. | T=O | | |
| MSC-KM-16 | Accounting procedures need to support CAK and CEK compromise recovery to ensure all copies of compromised CAKs and CEKs are identified and updated (rekeyed). | T=O | | |
| MSC-KM-17 | CAKs/CEKs are to be updated (rekeyed) immediately if they are considered compromised. | T=O | | |
| MSC-KM-18 | If a compromised device is to be reused, that device must go through the initial CAK issuance process. | T=O | | |

# APPENDIX A. ACRONYMS

| Acronym | Definition |
|---|---|
| AO | Authorizing Official |
| CA | Certification Authority |
| CAK | Connectivity Association Key |
| CDP | CRL Distribution Point |
| CDS | Cross Domain Solution |
| CEK | CAK Encryption Key |
| CNSA | Commercial National Security Algorithm |
| CNSS | Committee on National Security Systems |
| CNSSI | Committee on National Security Systems Instruction |
| CNSSP | Committee on National Security Systems Policy |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSfC | Commercial Solutions for Classified |
| CUI | Controlled Unclassified Information |
| DAR | Data-At-Rest |
| DM | Device Management |
| DN | Domain Name |
| ECDH | Elliptic Curve Diffie-Hellman |
| EAP | Extensible Authentication Protocol |
| EST | Enrollment Over Secure Transport |
| EUD | End User Device |
| FIPS | Federal Information Processing Standards |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| IETF | Internet Engineering Task Force |
| IPsec | Internet Protocol Security |
| KM | Key Management |
| KMI | Key Management Infrastructure |
| MA | Mobile Access |
| NPE | Non Person Entity |
| NSA | National Security Agency |
| NSS | National Security Systems |

| Acronym | Definition |
|---|---|
| O | Objective |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OS | Operating System |
| PKCS | Public Key Cryptographic Standard |
| PKI | Public Key Infrastructure |
| PSK | Pre-shared Key |
| RFC | Request for Comment |
| SSH | Secure Shell |
| SSHv2 | Secure Shell Version 2 |
| T | Threshold |
| TLS | Transport Layer Security |
| URL | Uniform Resource Locator |
| VPN | Virtual Private Network |
| WLAN | Wireless Local Area Network |
| WPA2 | Wi-Fi Protected Access II |