



National Security Agency/
Central Security Service



CYBERSECURITY SOLUTIONS

KEY MANAGEMENT REQUIREMENTS ANNEX V2.0

Version 2.0
January 2021



Key Management Requirements Annex



CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Key Management Requirements Annex	1.0	26 June 2018	<ul style="list-style-type: none">• Initial release of the CSfC Key Management Requirements Annex.
CSfC Key Management Requirements Annex	2.0	31 January 2021	<ul style="list-style-type: none">• Updated based on stakeholder feedback to KM Annex v1.0.• Relocated MACsec pre-shared symmetric Connectivity Association Keys (CAKs) management requirements to CSfC Symmetric Key Management Requirements Annex.• Updated wording in Section 1 to improve clarity.• Removed the use of whitelists as an alternative to Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) Responders for certificate revocation checking.• Updated requirements to align with CNSS Policy (CNSSP) 25 and CNSS Directive (CNSSD) 506.• Updated Appendix B: References• Minor administrative changes were made in formatting and punctuation.



Key Management Requirements Annex



TABLE OF CONTENTS

1	Key Management Requirements	4
1.1	Certificate Revocation Checking	9
1.2	Wireless Key and Certificate Management.....	11
1.2.1	Mobile Access (MA) CP	11
1.2.2	Campus Wireless Local Area Network (WLAN) CP.....	11
2	Remote Rekey of Component Certificates.....	11
3	Key Management General Requirements.....	12
3.1	PKI General Requirements.....	12
3.2	Certificate Issuance Requirements	14
3.3	Certificate Rekey Requirements	16
3.4	Certificate Revocation and CDP Requirements	17
3.5	Wireless Pre-Shared Key (WPSK) Requirements.....	19
3.6	Campus WLAN CP Key Management Requirements	20
3.7	MACsec Key Management Requirement.....	20
	Appendix A. Acronyms.....	21
	Appendix B. References	23

TABLE OF FIGURES

Figure 1.	Standalone Outer CA and Standalone Inner CA.....	7
Figure 2.	Standalone Outer CA and Enterprise PKI Inner CA	7
Figure 3.	Standalone Outer CA and Standalone Inner CA both located in the Red Network.....	8
Figure 4.	Single Standalone Outer CA with Multiple Standalone Inner CAs for Solution with Networks Operating at Different Classification Levels.....	8
Figure 5.	Single Standalone Outer Gray CA with Multiple Standalone Inner CAs for Multiple Sites.....	9

LIST OF TABLES

Table 1.	Certificate Authority Deployment Options	6
Table 2.	PKI General Requirements	12
Table 3.	Certificate Issuance Requirements.....	14
Table 4.	Certificate Rekey Requirements.....	16



Key Management Requirements Annex



Table 5. Certificate Revocation and CDP Requirements.....	17
Table 6. Wireless Pre-Shared Key (WPSK) Requirements.....	19
Table 7. Campus WLAN CP Key Management Requirements.....	20
Table 8. MACsec Key Management Requirement	20



Key Management Requirements Annex



1 KEY MANAGEMENT REQUIREMENTS

Commercial Solutions for Classified (CSfC) solutions use asymmetric algorithms, as defined in the Commercial National Security Algorithm (CNSA) Suite, and X.509 certificates for component authentication to establish the Outer and Inner encryption tunnels. Customers protecting long life intelligence data should contact the CSfC Program Management Office (csfc@nsa.gov) for additional details on how symmetric key cryptography can be leveraged in the Capability Packages (CPs).

Each CSfC solution component contains a private authentication key and a corresponding public certificate issued by a trusted Certification Authority (CA). It is preferable for the authentication keys (public/private key pair) to be generated on the solution component, where the private keys are never exported out of the component. If the component cannot generate its own key pair, a dedicated offline management workstation is required to generate the key pair for the component. The public keys are sent in certificate requests to a trusted CA that creates and signs authentication certificates containing the public keys. The authentication certificates are then delivered to, and installed on the solution components during provisioning, along with the private keys if they were not generated on the component.

To provide confidentiality services within CSfC solutions, the components use key agreement protocols (such as Elliptic Curve Diffie-Hellman (ECDH)) to generate ephemeral encryption keys. The use of ephemeral encryption keys is not part of key management discussed in this annex.

In CSfC solutions, at least two CAs are used to issue certificates and are deployed on separate machines. One CA (known as the Outer CA) issues certificates to Outer Encryption Components and the other CA (known as the Inner CA) is used to issue certificates to Inner Encryption Components. To ensure that the same certificate cannot be used for authenticating both the Outer and Inner tunnels, the Outer CA and Inner CA are used to validate the Outer Tunnel and Inner Tunnel authentication certificates, respectively. When multiple classified enclaves are used, each enclave will have its own Inner CA, as Inner CAs cannot be shared between multiple classification levels. Additionally, each CSfC solution infrastructure component will have access to revocation status of certificates (e.g., Certificate Revocation List (CRL) or Online Certificate Status Protocol (OSCP)). All certificates issued by the Outer and Inner CAs for the Solution are Non-Person Entity (NPE) certificates, except in the case when a Mobile Access (MA) Transport Layer Security (TLS) EUD requires a user certificate for the Inner TLS tunnel.

The CAs that issue authentication certificates to CSfC solution components operate either as Enterprise CAs (i.e., NSS Public Key Infrastructure (PKI), National Security Agency (NSA) Key Management Infrastructure (KMI), Intelligence Community (IC) PKI), Department/Agency-level Non-Person Entity (NPE) Only Locally Trusted (OLT) CAs, or locally-run CAs. Existing Enterprise CAs should be used whenever possible, as the advantages for using these CAs outweigh those associated with locally-run



Key Management Requirements Annex



CAs. However, Enterprise CAs that operate on or are accessible via the Black Network are not permitted to be used in CSfC solutions. CNSSP 25 is the governing policy and CNSSD 506 is the governing directive for PKI solutions in support of CSfC solutions protecting networks operating at the Secret level (typically the red network of the solution).

Enterprise CAs have established operations, as well as Certificate Policies and Certification Practice Statements (CPSs) that customer organizations can leverage for their CSfC solution. These Enterprise CAs operate at Federal Department and Agency levels (e.g., NSS PKI, KMI, IC PKI), and offer wide-scale interoperability across Department and Agency networks and CSfC solutions (i.e., the certificate policies and their registered policy Object Identifiers (OIDs) are widely accepted across Federal Departments or Agencies). These types of Enterprise solutions, leverage Department/Agency-level trusted CAs that reside under the same Root CA. Enterprise CAs can be used in multiple CSfC solutions throughout Federal Departments or Agencies, thereby providing certificate trust interoperability across those CSfC solutions. A user with a CSfC EUD provisioned with certificates from an Enterprise CA could use their EUD in many different CSfC solutions deployed throughout Federal Departments or Agencies. CSfC solutions utilizing Enterprise CAs install the Issuing CA and Root CA certificates into solution components so that a trusted certificate chain is established between the component certificate and the trusted Root CA certificate.

Departments and Agencies can also deploy Non-Person Entity (NPE) Only Locally Trusted (OLT) CAs to support the need to issue certificates to NPEs that will only be trusted within the Department/Agency network. NPE OLT CAs can be operated as standalone systems or can be part of a Department/Agency NPE OLT PKI.

CSfC solutions can also deploy and operate their own locally-run CAs for closed operational networks that are independent of any Enterprise CAs. In this configuration, certificate policy and interoperability are constrained to the specific CSfC solution. Furthermore, the CSfC solution owner is required to develop and maintain CPSs that detail the operational procedures for the locally-run CAs. In addition, the customer may need to develop and maintain a higher-level Certificate Policy if one does not already exist.¹ Table 1 summarizes the differences between Enterprise and locally-run CAs.

¹ CNSSP 25 is the governing policy for PKI solutions in support of Secret CSfC solutions. For CSfC solutions that are higher than Secret, the CSfC solution owner is required to develop a Certificate Policy that is approved by the local Approving Official (AO).



Key Management Requirements Annex



Table 1. Certificate Authority Deployment Options

CA Type	Certificate Policy/ Certification Practice Statement	Interoperability	Operations
Enterprise CAs	Owned and managed by the Enterprise PKI (e.g., NSS PKI, NSA KMI, IC PKI)	Across Department and Agency networks	Performed by the Enterprise PKI and Departments/Agencies
Department/ Agency-level Non-Person Entity (NPE) Only Locally Trusted (OLT) CAs	Owned and managed at the Department or Agency level	Constrained to a Department or Agency network	Performed by the Department or Agency
Locally-run (Non-Enterprise) CAs	Owned and managed at the CSfC solution level	Constrained to a CSfC solution	Performed by the CSfC solution owner

In all CA configurations identified above, Outer CAs issue and manage authentication certificates for Outer Encryption Components and Gray Management Service Components; Inner CAs issue and manage authentication certificates for Inner Encryption Components and Red Management Service Components. Outer CAs can be included as either part of the Gray Network or Red Network. If the solution supports multiple classified enclaves the Outer CA is either located in the Gray Management Network or in the Red Network of the highest classified enclave. Inner CAs can only be located in the Red Network.

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) uses a certificate issued by a different CA than the Inner CA for authentication. The Gray Firewall and the Outer Encryption Component can both use certificates issued by the same Outer CA for authentication.

The CAs communicate with management services (i.e., Device Managers (DMs)) deployed in the corresponding network to support enrollment and life-cycle certificate management for CSfC solution components. Outer and Inner CAs in the Red Network are limited to directly communicating with Red Management Services. Outer CAs in the Gray Network are limited to directly communicating with Gray Management Services. When the CA is not located in the same network as the Management Services, an Authorizing Official (AO)-approved method (e.g., CDS) can be used allowing indirect communication (for example Certificate Enrollment). The Red and Gray Management Services enable the certificate request/response process between a CSfC solution component and a CA.

An out-of-band method is used to issue the initial certificates to the solution components. Subsequent rekeying, however, can take place over the network through the solution prior to the current key's expiration (see Section 2 for additional details regarding over-the-network remote certificate rekey). The



Key Management Requirements Annex



key validity period for certificates issued by locally run CAs does not exceed 12 months for EUDs and 24 months for Solution Infrastructure Components, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA certificate policy. Updates to CRLs are distributed to Outer and Inner Infrastructure Encryption components within 24 hours of CRL issuance.

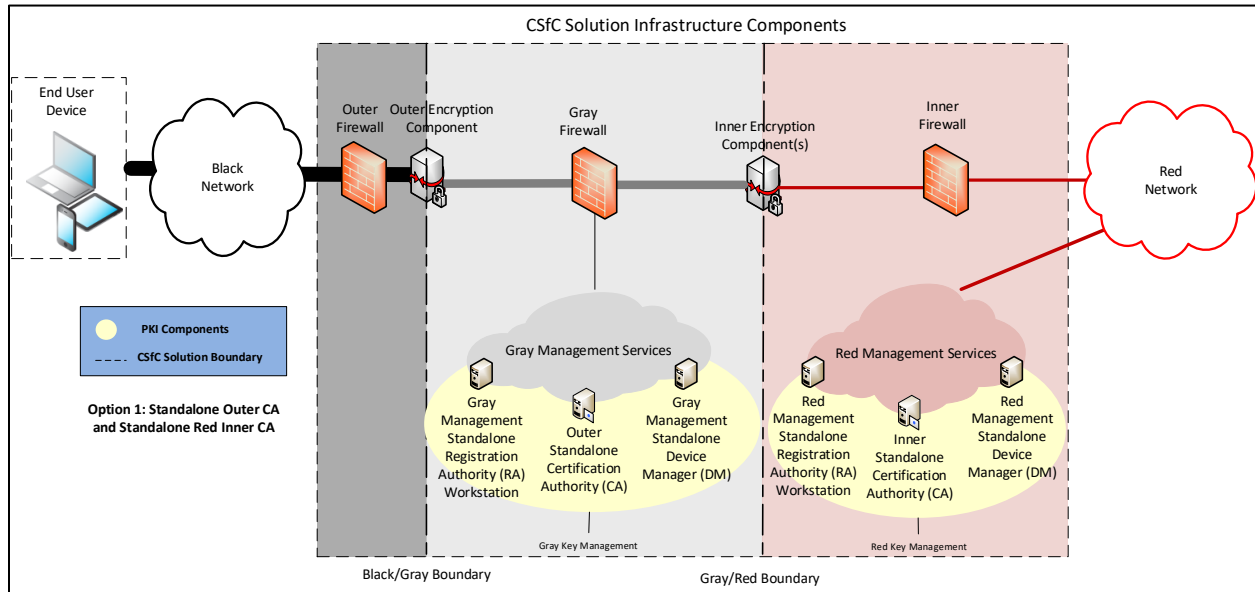


Figure 1. Standalone Outer CA and Standalone Inner CA

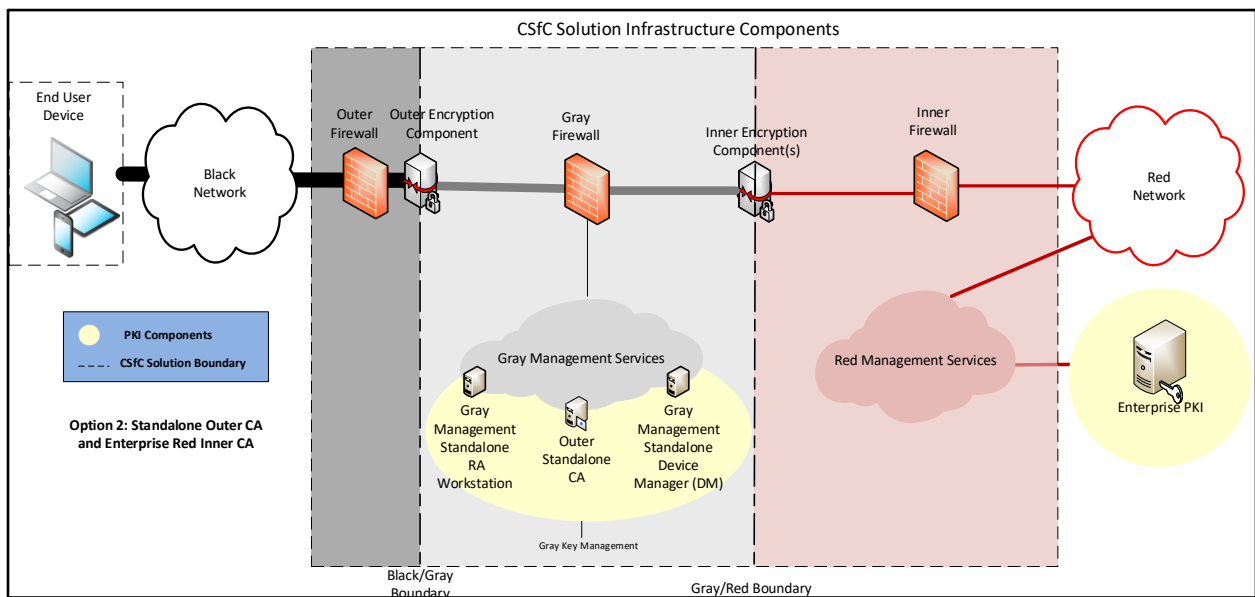


Figure 2. Standalone Outer CA and Enterprise PKI Inner CA



Key Management Requirements Annex

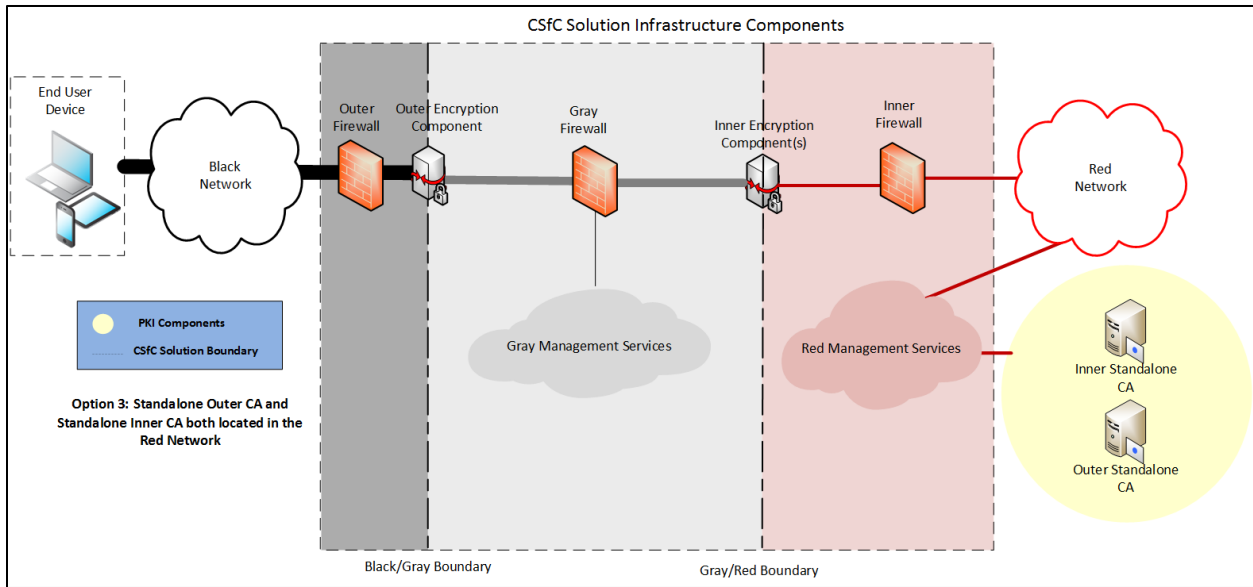


Figure 3. Standalone Outer CA and Standalone Inner CA both located in the Red Network

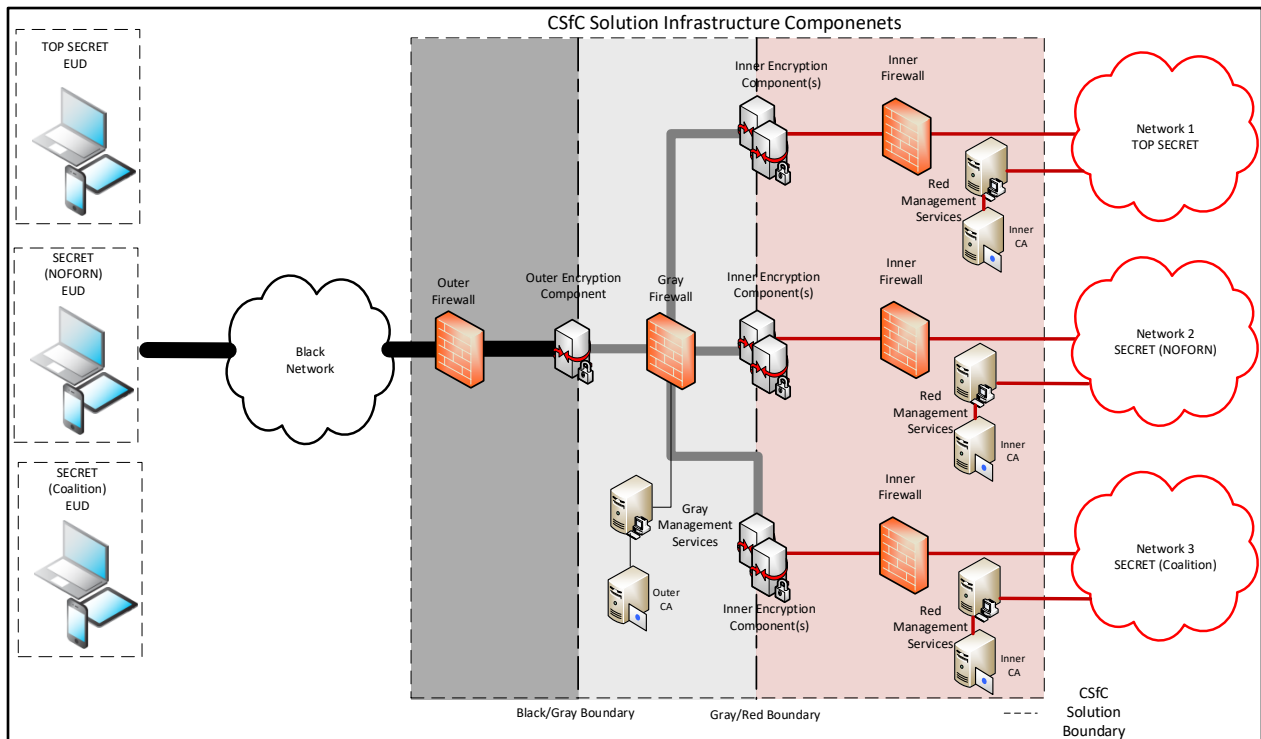


Figure 4. Single Standalone Outer CA with Multiple Standalone Inner CAs for Solution with Networks Operating at Different Classification Levels



Key Management Requirements Annex

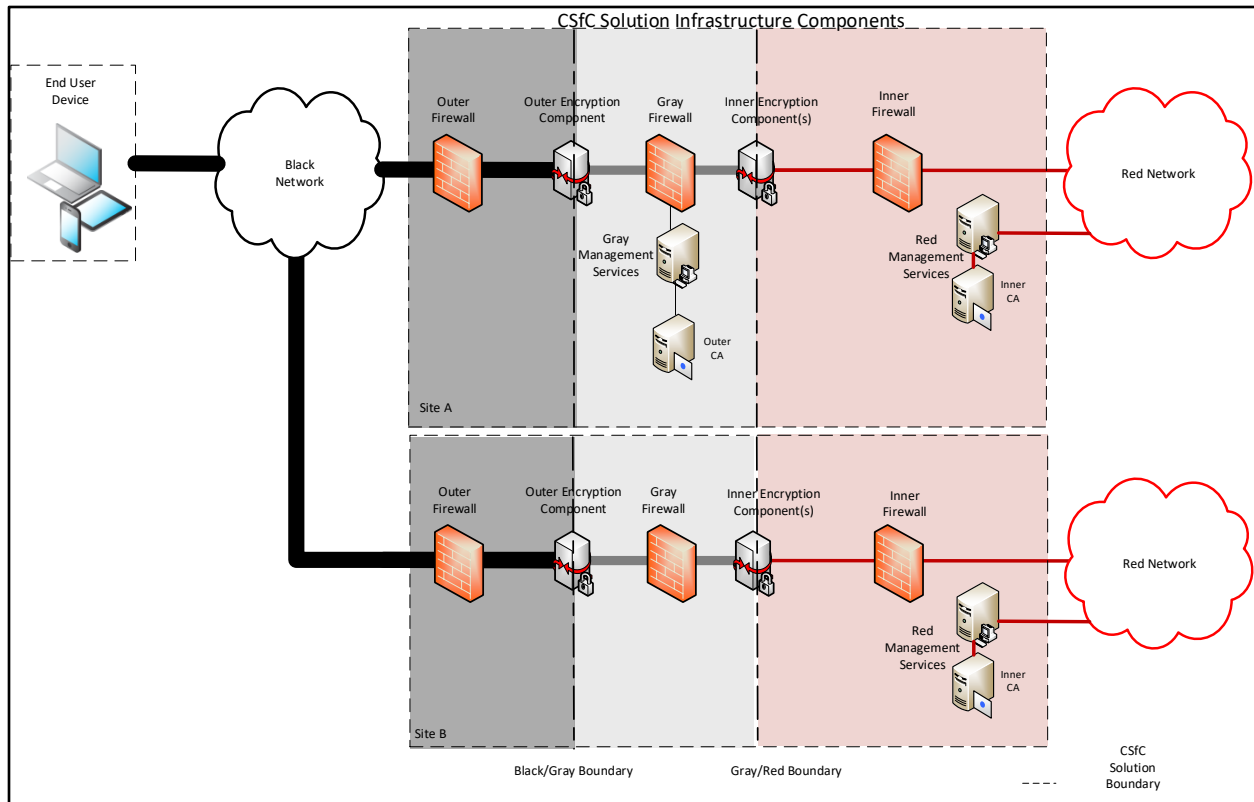


Figure 5. Single Standalone Outer Gray CA with Multiple Standalone Inner CAs for Multiple Sites

1.1 CERTIFICATE REVOCATION CHECKING

CRLs are used by CAs to convey the revocation status of certificates issued by those CAs, and those CRLs need to be made available to the CSfC solution components.

A CRL Distribution Point (CDP) is a web server whose sole function is to provide external distribution of, and access to CRLs issued by CAs. CDPs do not serve any other content, and, in particular, do not host any dynamically generated content. CDPs also do not provide any other services other than the distribution of CRLs. CDPs are optional in a CSfC solution, and they can exist in the Gray and/or Red Networks. Alternatives to CDPs include Online Certificate Status Protocol (OCSP) Responders and locally-stored or cached CRLs.

The Outer Encryption Component in the solution infrastructure accesses an Outer CDP, located in the Gray Network, to obtain CRLs and check revocation status of other Outer Encryption Components, and EUDs when applicable, prior to establishing the Outer encryption tunnel. Furthermore, a CDP operating in the Gray Network can be accessed by Gray Management Services Components to obtain CRLs and check the revocation status of the Outer Encryption Component's certificate prior to establishing a device management tunnel with the Outer Encryption Component.



Key Management Requirements Annex



Additionally, the CSfC CPs allow for an Inner CDP to be located within the Gray Management Services Network. Placing an Inner CDP in the Gray Management Network allows EUDs to check the certificate status of the Inner Encryption Component prior to establishing a tunnel. To use an Inner CDP in the Gray Management Network, an AO determines that CRLs generated by the Inner CA are unclassified. These CRLs are moved from the Red Network to the Gray Management Network using an AO approved method (e.g., CDS).

Inner Encryption Components access an Inner CDP, located in the Red Network, to obtain CRLs and check revocation status of other Inner Encryption Components, and EUDs when applicable, prior to establishing the Inner encryption tunnel. Likewise, a CDP operating in the Red Network can be accessed by Red Management Services Components to obtain CRLs and check the revocation status of the Inner Encryption Component's certificate prior to establishing a device management tunnel with the Inner Encryption Component.

An Outer CDP and an Outer CA can reside on the same or different networks. For example, the Outer CA can operate in the Red Network, while the Outer CDP operates in the Gray Network. If they reside on different networks, an AO approved method (e.g., CDS) is needed to periodically distribute the current CRL from the CA to the CDP.

CRLs are downloaded by CSfC solution components over unencrypted Hypertext Transfer Protocol (HTTP). A CRL's integrity is protected by the digital signature of the issuing CA, and additional integrity protection during CRL download is not required. Placement of CDPs on the Gray Network for the Outer Encryption Component and Red Network for Inner Encryption Components reduces the exposure to external threat actors.

To provide redundancy and ensure that current CRLs are always made available to CSfC solution components, multiple Outer and Inner CDPs can be deployed. The use of multiple CDPs is left to the discretion of the CSfC solution owner. Furthermore, CDPs can host partition or delta CRLs in addition to complete CRLs. In large CSfC solutions, the use of partition or delta CRLs can reduce the amount of network traffic needed to distribute updates to CRLs. A CA's Certificate Policy will define whether the use of partition or delta CRLs is permissible.

OCSP Responders or locally-stored/cached CRLs can be used in lieu of CDP Servers. OCSP Responders located in the Gray Network can provide certificate revocation status information to the Outer Encryption Components or to the Authentication Server. Additionally, OCSP Responders in the Red Network can provide certificate revocation status information to Inner Encryption Components.



Key Management Requirements Annex



1.2 WIRELESS KEY AND CERTIFICATE MANAGEMENT

1.2.1 MOBILE ACCESS (MA) CP

As discussed in the Black Network section of the MA CP, EUDs can operate over any Black Network when used in conjunction with a Government-owned Retransmission Device (RD) or a physically separate Dedicated Outer VPN to establish the Outer IPsec Tunnel. When the RD or Dedicated Outer VPN is wirelessly connected to an EUD using Wi-Fi, the Wi-Fi network must implement Wi-Fi Protected Access II (WPA2) with Pre-Shared Key (PSK).

For WPA2 with PSKs, a common PSK with at least 256 bits of security needs to be securely generated, distributed, and installed onto both the EUD and the external Dedicated Outer VPN device or RD. Exposure of the PSK in red form needs to be minimized to the greatest extent possible and only exposed to authorized and trusted personnel responsible for managing and installing the PSK onto the EUD and external Dedicated Outer VPN or RD. Updates to the PSK are to be performed periodically based upon the threat environment. The higher the threat environment, the more often the PSK should be updated.

1.2.2 CAMPUS WIRELESS LOCAL AREA NETWORK (WLAN) CP

Since the Campus Wireless Local Area Network (WLAN) CP relies on WPA2 Enterprise for the Outer Encryption tunnel, the EUD will require an EAP-TLS certificate. This certificate is issued by the Outer CA. Issuance of the WPA2 Enterprise certificate should be integrated into the overall provisioning process for the EUD described in the EUD Provisioning section of the CPs. For the WLAN CP, revocation status information for EAP-TLS certificates issued to EUDs also needs to be made available in the Gray Network so that the WPA2 Enterprise authentication server can check the revocation status of EUD EAP-TLS certificates (see Section 1.1 for additional details regarding distribution of certificate revocation lists).

2 REMOTE REKEY OF COMPONENT CERTIFICATES

If a solution component is capable of generating its own public/private key pairs and can communicate with the Outer or Inner CAs using Enrollment over Secure Transport (EST), as defined in Internet Engineering Task Force (IETF) RFC 7030, the solution component can have its device certificates remotely rekeyed, as opposed to physically returning the solution component to the provisioning environment as described in the provisioning section of the CPs. EST requires a TLS connection to a trusted server, so that the CA can authenticate a solution component prior to issuing new certificates. A solution component would need to establish a separate TLS tunnel to the Outer CA or Inner CA after establishing the Outer and Inner encryption tunnels.

Once authenticated to the Outer CA or Inner CA, the solution component generates a new public/private key pair. The newly generated public key is placed into a new certificate request in accordance with RFC 7030. The certificate request is then submitted to the Outer CA or Inner CA for processing using EST. The CA validates that the certificate requests came from a valid and authenticated



Key Management Requirements Annex



solution component, processes the certificate request, and returns a newly signed certificate containing the new public key to the solution component. The solution component then receives and installs the newly rekeyed certificate. All CSfC EST implementations use CNSA TLS 1.2 (or a later version) certificate-based authentication.

It should be noted that the exact sequence for certificate rekey will vary based on the solution component's implementation of EST. For example, one certificate rekey with one of the CAs may need to be performed first, followed by the second certificate rekey with the other CA.

3 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).

3.1 PKI GENERAL REQUIREMENTS

Table 2. PKI General Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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	



Key Management Requirements Annex



Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	



Key Management Requirements Annex



3.2 CERTIFICATE ISSUANCE REQUIREMENTS

Table 3. Certificate Issuance Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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 <i>CSfC Data-At-Rest (DAR) CP</i> 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	



Key Management Requirements Annex



Req #	Requirement Description	Threshold / Objective	Alternative
KM-32	<p>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:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 Locator (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	
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



Key Management Requirements Annex



Req #	Requirement Description	Threshold / Objective	Alternative
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 <i>CSfC Enterprise Gray Implementation Requirements Annex</i> , 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	
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	

3.3 CERTIFICATE REKEY REQUIREMENTS

Table 4. Certificate Rekey Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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



Key Management Requirements Annex



3.4 CERTIFICATE REVOCATION AND CDP REQUIREMENTS

Table 5. Certificate Revocation and CDP Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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: <ul style="list-style-type: none"> • 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	
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	



Key Management Requirements Annex



Req #	Requirement Description	Threshold / Objective	Alternative
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	
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		



Key Management Requirements Annex



Req #	Requirement Description	Threshold / Objective	Alternative
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	

3.5 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 6. Wireless Pre-Shared Key (WPSK) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	



Key Management Requirements Annex



3.6 CAMPUS WLAN CP KEY MANAGEMENT REQUIREMENTS

The following requirements apply to the WLAN CP.

Table 7. Campus WLAN CP Key Management Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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	

3.7 MACSEC KEY MANAGEMENT REQUIREMENT

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

Table 8. MACsec Key Management Requirement

Req #	Requirement Description	Threshold / Objective	Alternative
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 <i>CSfC Symmetric Key Management Requirements Annex</i> for additional guidance and requirements.	T=O	



Key Management Requirements Annex



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
CKN	Connectivity Association Key Name
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	Capability Package
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
KGS	Key Generation Solution
KM	Key Management
KMI	Key Management Infrastructure
MA	Mobile Access
MACsec	Media Access Control Security
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security Systems
O	Objective
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
PKCS	Public Key Cryptographic Standard



Key Management Requirements Annex



Acronym	Definition
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



Key Management Requirements Annex



APPENDIX B. REFERENCES

Document	Title	Date
CNSSD 505	<i>CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)</i>	March 2012
CNSSD 506	<i>CNSS Directive (CNSSD) 506, National Directive to Implement Public Key Infrastructure on Secret Networks</i>	January 2019
CNSSI 1300	<i>CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy</i>	December 2014
CNSSI 4009	<i>CNSSI 4009, Committee for National Security Systems (CNSS) Glossary</i>	April 2015
CNSSP 7	<i>CNSS Policy (CNSSP) Number 7, National Policy on the Use of Commercial Solutions to Protect National Security Systems</i>	December 2015
CNSSP 11	<i>CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products</i>	June 2013
CNSSP 15	<i>CNSS Policy (CNSSP) Number 15, National Policy on the Use of Public Standards for Secure Information Sharing</i>	October 2016
CNSSP 25	<i>CNSS Policy (CNSSP) Number 25, National Policy for Public Key Infrastructure in National Security Systems (NSS)</i>	December 2017
CSfC Campus WLAN CP	<i>Commercial Solutions for Classified (CSfC): Campus Wireless Local Area Network (WLAN) Capability Package (CP), v2.2</i>	June 2018
CSfC EG Annex	<i>Commercial Solutions for Classified (CSfC): Enterprise Gray Implementation Requirements Annex, v1.0</i>	April 2019
CSfC MA CP	<i>Commercial Solutions for Classified (CSfC): Mobile Access Capability Package (CP), v2.1</i>	June 2018
CSfC MSC CP	<i>Commercial Solutions for Classified (CSfC): Multi-Site Connectivity (MSC) Capability Package (CP), v1.1</i>	June 2018
CSfC SKM Annex	<i>Commercial Solutions for Classified (CSfC): Symmetric Key Management Requirements Annex, v2.0</i>	September 2020
FIPS 140	<i>Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication</i>	March 2019
FIPS 180	<i>Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)</i>	August 2015
FIPS 186	<i>Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)</i>	July 2013
FIPS 197	<i>Federal Information Processing Standard 197, Advanced Encryption Standard (AES)</i>	November 2001
IR 7924	<i>NIST Interagency Report (IR) 7924, Reference Certificate Policy, Second Draft. H. Booth and A. Regenscheid.</i>	May 2014



Key Management Requirements Annex



Document	Title	Date
PP CA	<i>Protection Profile for Certification Authorities.</i> http://www.niap-ccevs.org/pp	December 2017
RFC 3647	<i>IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</i> Internet Engineering Task Force. S. Chokhani, et. al.	November 2003
RFC 4308	<i>IETF RFC 4308 Cryptographic Suites for IPsec.</i> P. Hoffman.	December 2005
RFC 4754	<i>IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA).</i> D. Fu and J. Solinas.	January 2007
RFC 5216	<i>IETF RFC 5216 The EAP-TLS Authentication Protocol.</i> D. Simon, B. Aboba, and R. Hurst.	March 2008
RFC 5246	<i>IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2.</i> T. Dierks and E. Rescorla.	August 2008
RFC 5280	<i>IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.</i> D. Cooper, et. al.	May 2008
RFC 6818	<i>IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.</i> P. Yee	January 2013
RFC 6960	<i>IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP,</i> S. Santesson, et. al.	June 2013
RFC 7030	<i>IETF RFC 7030 Enrollment over Secure Transport.</i> M. Pritikin, P. Yee, and D. Harkins.	October 2013
RFC 7296	<i>IETF RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2).</i> C. Kaufman, et. al.	October 2014
RFC 8247	<i>IETF RFC 8247 Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2).</i> Y. Nir, et. al.	September 2017
RFC 8295	<i>IETF RFC 8295 EST (Enrollment over Secure Transport) Extensions</i> S. Turner.	January 2018
RFC 8422	<i>IETF RFC 8422 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier.</i> Y. Nir, et. al.	August 2018
RFC 8446	<i>IETF RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3.</i> E. Rescorla.	August 2018
RFC 8603	<i>IETF RFC 8603 Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile.</i> M. Jenkins, and L. Ziegler.	May 2019
SP 800-53	<i>NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations.</i> Joint Task Force Transformation Initiative.	April 2013



Key Management Requirements Annex



Document	Title	Date
SP 800-56A	<i>NIST Special Publication 800-56A Rev. 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.</i> E. Barker, et. al.	April 2018
SP 800-56B	<i>NIST Special Publication 800-56B Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography.</i> E. Barker, et. al.	March 2019
SP 800-56C	<i>NIST Special Publication 800-56C Rev. 2, Recommendation for Key Derivation through Extraction-then-Expansion.</i> E. Barker, et. al.	August 2020
SP 800-57-1	<i>NIST Special Publication 800-57 Part 1 Rev. 5, Recommendation for Key Management - General.</i> E. Barker.	May 2020
SP 800-57-2	<i>NIST Special Publication 800-57 Part 2 Rev. 1, Recommendation for Key Management – Best Practices for Key Management Organizations.</i> E. Barker, et. al.	May 2019
SP 800-57-3	<i>NIST Special Publication 800-57 Part 3 Rev. 1, Recommendation for Key Management – Application-Specific Key Management Guidance.</i> E. Barker, et. al.	Jan 2015
SP 800-77	<i>NIST Special Publication 800-77 Rev. 1, Guide to IPsec VPNs.</i> E. Barker, et. al.	June 2020
SP 800-131A	<i>NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths.</i> E. Barker.	March 2019