National Security Agency/
Central Security Service

CYBERSECURITY SOLUTIONS

KEY MANAGEMENT REQUIREMENTS ANNEX V1.0

Version 1.0
26 June 2018

Key Management Requirements Annex

CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Key Management Requirements Annex	1.0	June 26, 2018	• Initial release of the CSfC Key Management Requirements Annex.

Key Management Requirements Annex

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

1 KEY MANAGEMENT REQUIREMENTS

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 PMO (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 Certificate Authority (CA). In addition, a trusted CA certificate is installed, as well as any other CA signing certificates that connect to the trusted CA, so that a trusted certificate chain is established between the component certificate and the trusted CA certificate. Each CSfC solution infrastructure component must have access to revocation status of certificates (e.g., Certificate Revocation List (CRL) or Online Certificate Status Protocol (OSCP). If CRLs or OCSP are not used, other mechanisms can be implemented (e.g., whitelists) in CSfC Solution Infrastructure Components.

It is preferable for the authentication keys (public/private key pair) to be generated on the security component, where the private keys are never exported out of the component. If the component cannot generate its own key pair, a dedicated management workstation is required to generate the key pair for the component. The public keys are sent in certificate requests to the Outer and Inner CAs that create and sign authentication certificates containing the public keys. If a Mobile Access Transport Layer Security (TLS) EUD requires a user certificate for the Inner TLS tunnel, the request is delivered to the CA in the customer's organization that has the authority to issue user certificates. This CA may not be the same as the Inner CA. The authentication certificates are delivered to, and installed on, the security components during provisioning, along with the private keys if they were not generated on the component. The CAs also issue signed CRLs to provide revocation status information for the certificates issued by the CAs. CRLs are transferred to CRL Distribution Points (CDPs) or OCSP Responders (see Section 1.1), where the certificate revocation status information is made available to CSfC Solution Infrastructure Components.

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 appendix, as CAs are not required in issuing and managing these keys.

The CAs that issue authentication certificates to CSfC solution components operate either as Enterprise CAs (e.g., NSS Public Key Infrastructure (PKI), Key Management Infrastructure (KMI), and Agency PKI) 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 CAs. However, Enterprise CAs that operate on or are accessible via the Black Network are not permitted to be used in CSfC solutions.

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), and offer wide-scale interoperability across CSfC solutions (i.e., the certificate policies and their registered policy Object Identifiers (OIDs) are widely accepted across the Federal Department or Agency). For CSfC solutions

requiring interoperability across a Federal Department or Agency, Department/Agency-level Enterprise CAs should be leveraged. Examples of Department/Agency-level Enterprise CAs include the National Security Agency (NSA) Key Management Infrastructure (KMI); the National Security Systems (NSS) PKI; and the Intelligence Community (IC) PKI. These types of Enterprise solutions, leverage Department/Agency-level Trusted CAs which reside under the same Root CA. Trusted CAs can be used as trust anchors in multiple CSfC solutions throughout a Federal Department or Agency, thereby providing certificate trust interoperability across those CSfC solutions. A user with a CSfC EUD provisioned with certificates from a Department/Agency-level Enterprise CA could use their EUD in many different CSfC solutions deployed throughout a Federal Department or Agency.

When a Root CA is used for both the Inner and Outer tunnels, the CSfC CPs require that at least two Subordinate CAs are used to issue certificates and must be deployed on separate machines. One Subordinate CA issues certificates to Outer Encryption Components (known as the Outer CA) and the other CA is used to issue certificates to Inner Encryption Components (known as the Inner CA). 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 as trust anchors 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.

CSfC solutions can deploy and operate their own locally run CAs that are independent of any Enterprise CAs. In this configuration, certificate policy and interoperability is 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.

Table 1. Certificate Authority Deployment Options

CA Type	Certificate Policy	Interoperability	Operations
Department/ Agency-level Enterprise	Owned and managed at the Department or Agency level (e.g., NSA KMI, NSS PKI, IC PKI)	Department-wide or Agency-wide	Performed by the Enterprise
Subordinate CA (Enterprise)	Owned and managed at the Department or Agency level	Department-wide or Agency-wide	Performed by the Enterprise and the CSfC solution owner
Locally run (Non-Enterprise)	Owned and managed at the CSfC solution level	Constrained to the CSfC solution	Performed by the CSfC solution owner

In all CA configurations identified above, Outer CAs issue and manage authentication certificates for Outer Virtual Private Network (VPN) Components and Gray Management Service Components; Inner CAs, and optionally existing CAs that support enterprise services, issue and manage authentication

[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).*

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 must either be 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, 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. The Gray Firewall and the Outer Encryption Component can both use certificates issued by the same Outer CA for authentication. Using separate CAs for the Inner and Outer tunnels of the Enterprise Gray Management plane provides no additional security benefits, as both the Outer data plane and the Enterprise Gray Management plane are considered part of the Outer layer of the CSfC solution.

The CAs may communicate with management services (e.g., 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 Red Management Services, an Authorizing Official (AO)-approved Cross Domain Solution (CDS) may 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.

CSfC solutions use device authentication certificates, and in some instances, user authentication certificates. Public keys and certificates used in CSfC solutions are treated as determined by the AO. All private keys must be classified as determined by the AO and compliant with CNSSI 4005. The allowable options for use and handling of EUDs is dependent on that classification level of the User and Device private keys.

An out-of-band method must be used to issue the initial certificates to the solution components. Subsequent rekeying, however, should take place over the network through this solution prior to the current key's expiration (see Section 2.0 for additional details regarding over-the-network remote certificate rekey). The key validity period for certificates issued by locally run CAs cannot exceed 14 months, 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.

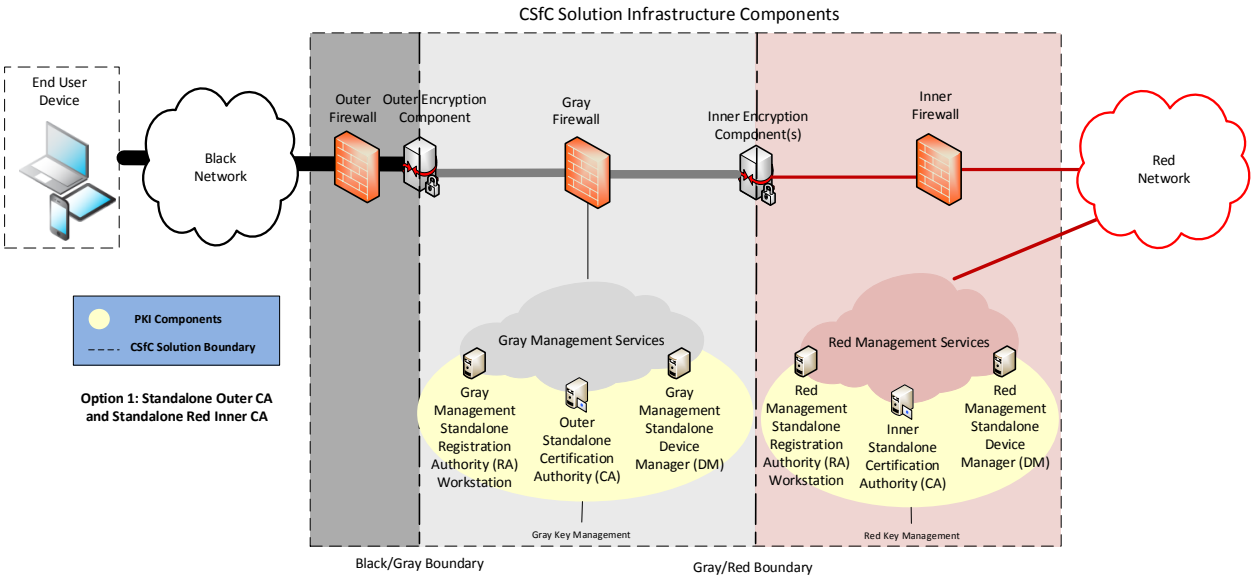

Figure 1. Standalone Outer CA and Standalone Red Inner CA

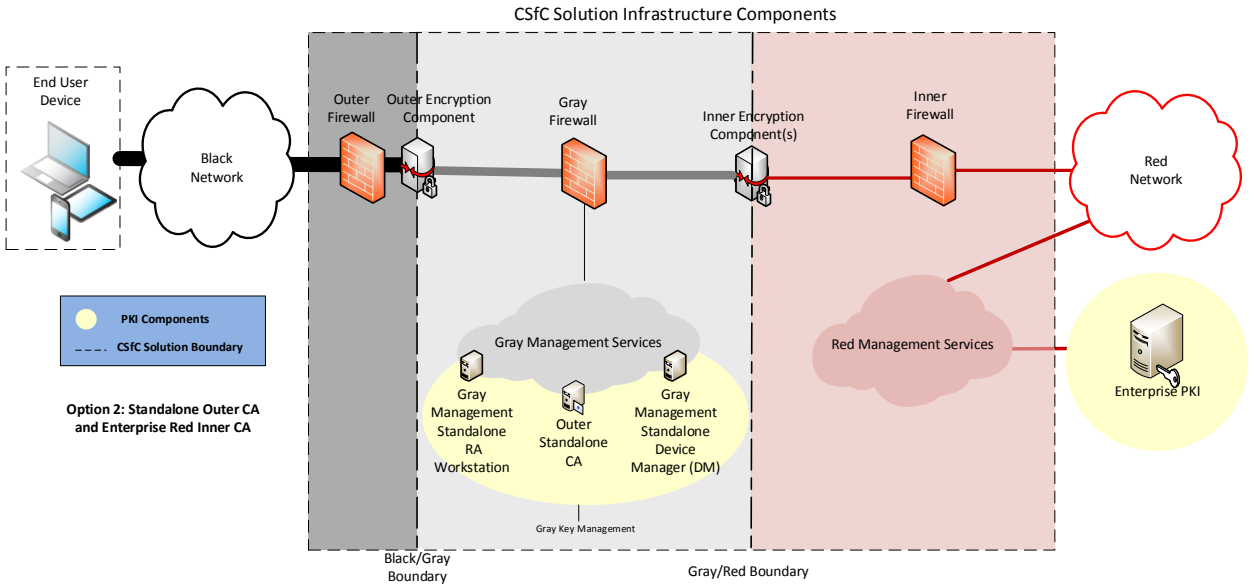

Figure 2. Standalone Outer CA and Enterprise Red Inner CA

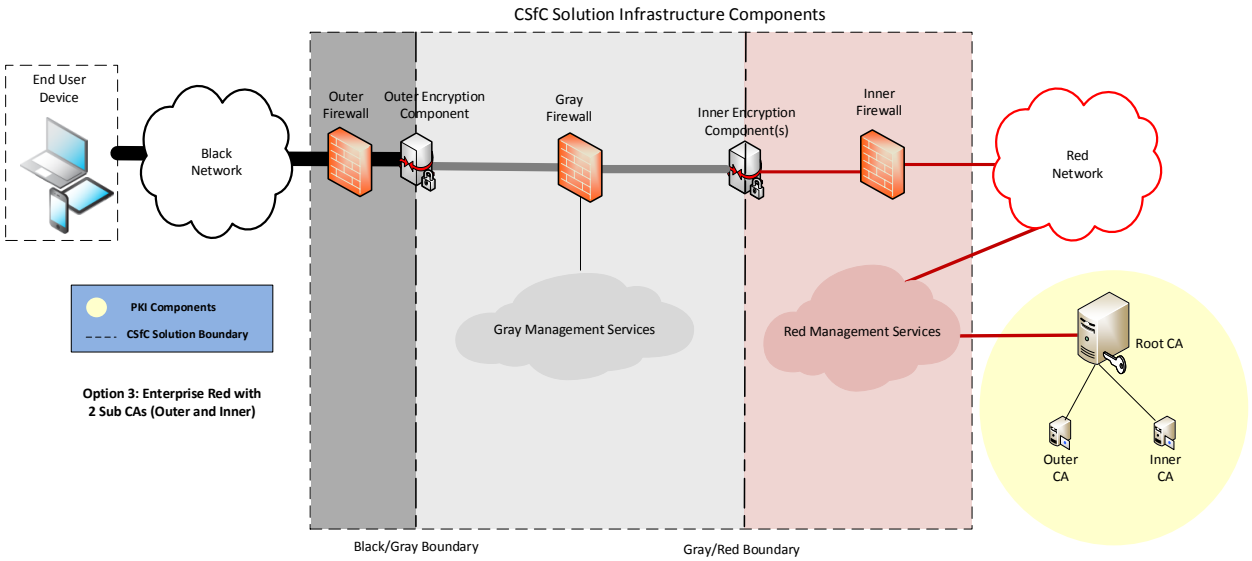

Figure 3. Single Root CA with 2 Sub CAs (Outer and Inner)

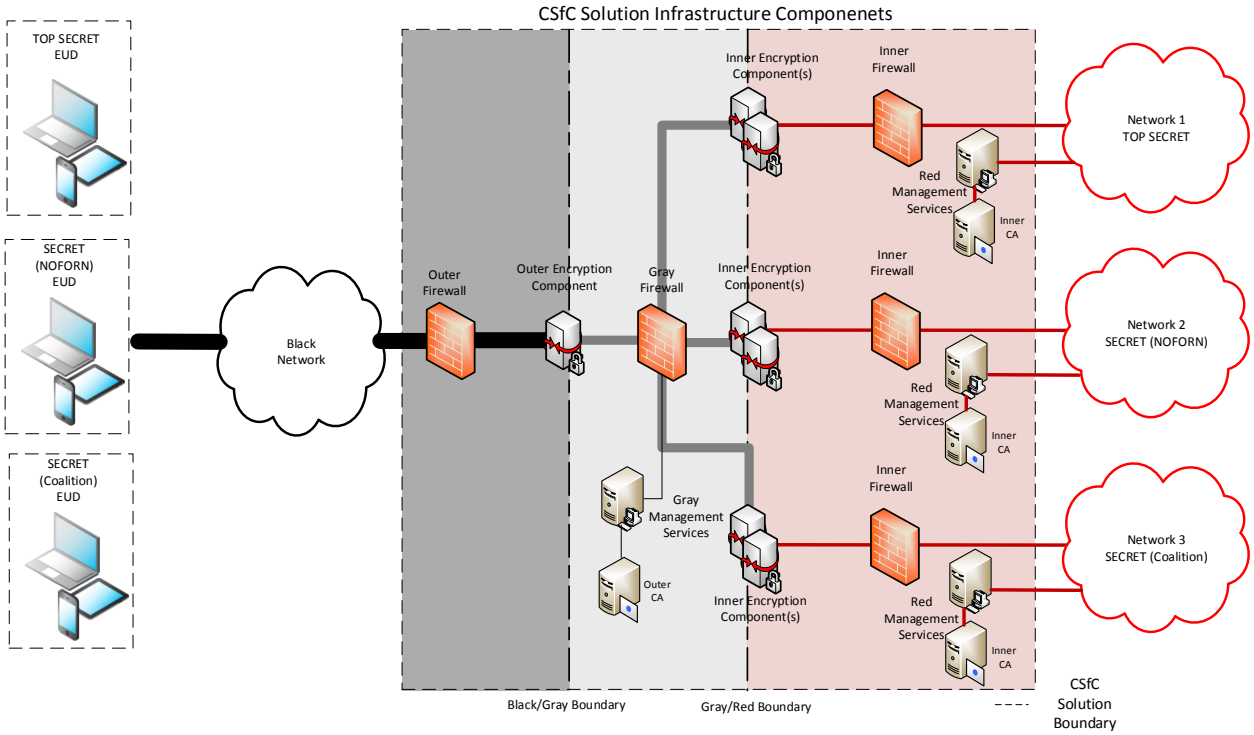

Figure 4. Single Standalone Outer CA with Multiple Standalone Inner CAs for Solution with Networks Operating at Different Classification Levels

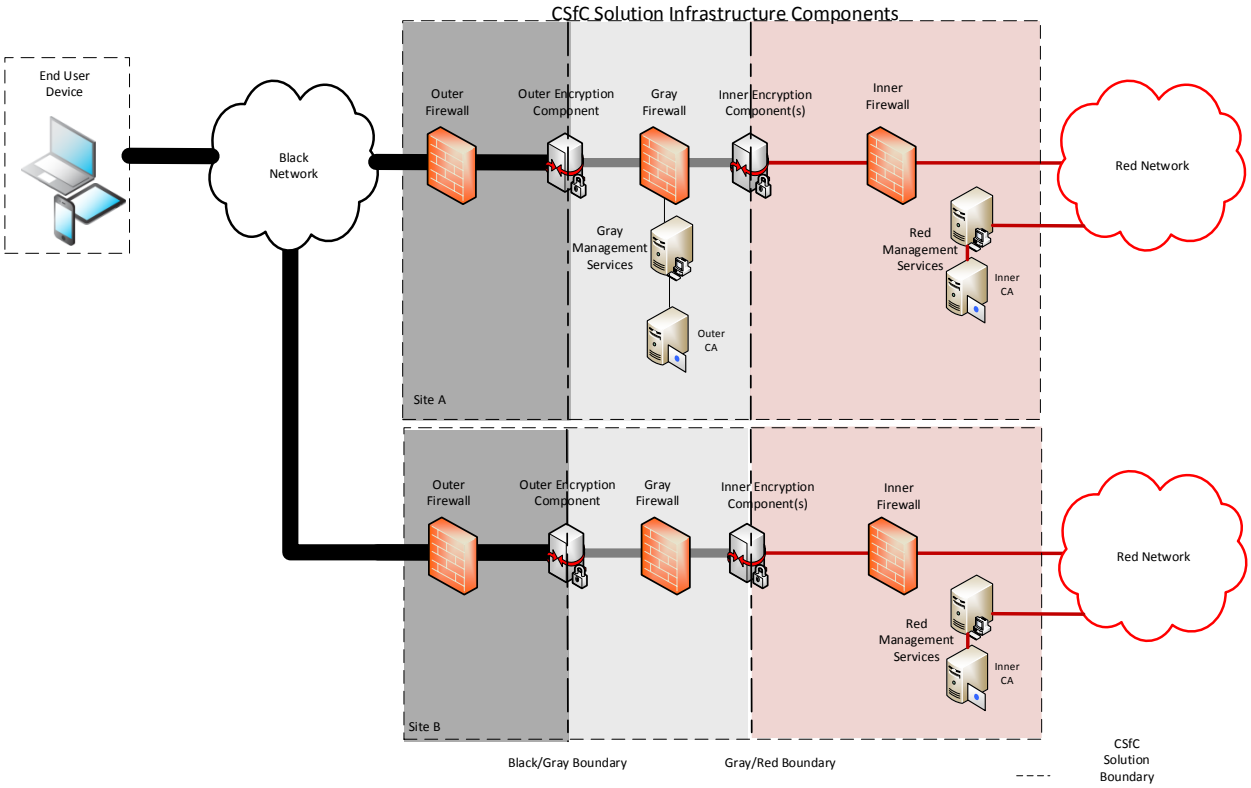

Figure 5. Single Standalone Outer Enterprise Gray CA with Multiple Standalone Inner CAs for Multiple Sites

1.1 Distribution of Certificate Revocation Lists

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.

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 service 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.

Additionally, the CSfC CPs allow for an Inner CDP to be created within the Gray Management Services. Placing an Inner CDP in the Gray Management Services 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 Services, an AO must determine that CRLs generated by the Inner CA are unclassified. These CRLs must also be moved from the Red Network to the Gray Management Services 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 service 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 may reside on the same or different networks. For example, the Outer CA may operate in the Red Network, while the Outer CDP operates in the Gray Network. If they reside on different networks, a one-way transfer mechanism is required to periodically distribute the current CRL from the CA to the CDP. The details and procedures of the one-way transfer mechanism are left to a solution's AO.

CRLs must be downloaded by CSfC solution components over unencrypted Hypertext Transfer Protocol (HTTP). A CRL's integrity is protected by the digital signature of the CA that issued it, 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 may be deployed. The use of multiple CDPs is left to the discretion of the CSfC solution owner. Furthermore, CDPs may 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 whitelists can be used in lieu of CDP Servers. OCSP Responders located in the Gray Network can provide certificate revocation status information to the Outer VPN Gateway or to the Wi-Fi Protected Access II (WPA2) Enterprise authentication server. Additionally, OCSP Responders in the Red Network can provide certificate revocation status information to Inner Encryption Components.

1.2 Wireless Key and Certificate Management

1.2.1 MA CP

As discussed in the Black Network section of the MA CP, EUDs can use a Dedicated Outer VPN device to establish the Outer IPsec tunnel where the Computing Device connects to the external Dedicated Outer VPN device using a WPA2 connection. WPA2 security is achieved using either PSKs or Extensible Authentication Protocol (EAP)-TLS certificates.

For PSKs, a common PSK with at least 256 bits of security needs to be securely generated, distributed, and installed onto both the Computing Device and the external Dedicated Outer VPN device. 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 Computing Device and external Dedicated Outer VPN. 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 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 must be 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).

1.3 MACSEC CONNECTIVITY ASSOCIATION KEYS

This section provides details for securely managing pre-shared symmetric Connectivity Association Keys (CAKs), which is a sensitive and critical function within MSC Solution's utilizing MACsec. CAK management includes secure generation, distribution, installation, update (rekey), accounting, compromise reporting, and destruction of CAKs. In addition to generating CAKs of appropriate strength to protect classified information, CAKs need to be securely distributed and further managed to mitigate the risk of unauthorized disclosure of the CAKs (e.g., insider threat). If a CAK is compromised, all MACsec Devices using that CAK need to be updated with a new CAK. This is different from a certificate-based solution in that revocation of any given certificate only impacts the device associated with that certificate.

Each MACsec Device has at least one CAK, which is used by the MACsec Device to authenticate with another MACsec Device. A different and unique CAK is required for every pair of MACsec Devices establishing an encryption tunnel. Also, if both layers of the solution use MACsec, different and unique CAKs are required for the inner and outer encryption tunnels. Every CAK has a unique Connectivity Association Key Name (CKN) to distinguish it from other CAKs that may be loaded in the MACsec Device.

Enterprise or local CAK management, including key generation and distribution, must follow an NSA-approved symmetric key management procedure.

2 REMOTE REKEY OF END USER DEVICE (EUD) CERTIFICATES

If the EUD is capable of generating its own public/private key pairs and can communicate with the Outer and Inner CAs using Enrollment over Secure Transport (EST) as defined in Internet Engineering Task Force (IETF) RFC 7030, the EUD can have its device certificates remotely rekeyed, as opposed to

physically returning the EUD to the provisioning environment as described in the EUD Provisioning section of the CPs. An EST requires a TLS connection to a trusted server, so that the CA can authenticate a EUD prior to issuing new certificates. A EUD would need to establish a separate TLS tunnel to the Outer and Inner CAs after establishing the Outer and Inner IPsec tunnels.

Once authenticated to the Outer and Inner CAs, the EUD generates two new public/private key pairs. The newly generated public keys are placed into two new certificate requests in accordance with RFC 7030 – one for the Outer Tunnel and one for the Inner Tunnel. The certificate requests are then submitted to the Outer and Inner Tunnel CAs for processing using EST. The Outer and Inner CAs validate that the certificate requests came from a valid and authenticated EUD, process the certificate requests, and return newly signed certificates containing the new public keys to the EUD. The EUD receives and installs the newly rekeyed certificates.

It should be noted that the exact sequence for certificate rekey will vary based on the EUD'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 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).

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	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	

Key Management Requirements Annex

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	
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	

Req #	Requirement Description	Threshold / Objective	Alternative
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	

3.2 CERTIFICATE ISSUANCE REQUIREMENTS

Table 3. Certificate Issuance Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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: o The certificates are limited to the specific customer's solution. That is, they are not part of an enterprise solution with multiple customers. o The certificates only apply to a single security domain (e.g., Secret). o There is only one certificate type (e.g., device, not user). o There is only one issuance process described in the CP/CPS. o There in only one assurance level.	T=O	
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	

Key Management Requirements Annex

Req #	Requirement Description	Threshold / Objective	Alternative
KM-37	Outer CAs must only issue certificates to Outer Encryption Components and Gray Network Components of Solutions.	T=O	
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
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

3.3 CERTIFICATE RENEWAL AND REKEY REQUIREMENTS

Table 4. Certificate Renewal and Rekey Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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

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	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
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 (i.e., 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	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
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	
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	

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	
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	

Req #	Requirement Description	Threshold / Objective	Alternative
KM-81	CDPs and OCSP Responders must not provide any other services other than the distribution of CRLs.	T=O	

3.5 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 6. Wireless and Pre-Shared Key (PSK) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	

3.6 Campus WLAN CP Key Management Requirements

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	

3.7 Multi-Site Connectivity CP Key Management Requirements

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

Table 8. Multi-Site Connectivity CP Key Management Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
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	
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	
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	

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-15	There must be a documented CAK/CEK compromise recovery process, to include: • Removal of a compromised infrastructure device (e.g., MACsec Devices) from the network, and • 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
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

Acronym	Definition
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

APPENDIX B. REFERENCES

Document	Title	Date
CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2014
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2015
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	October 2016
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	March 2006
IPsec VPN Client PP	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*. http://www.niap-ccevs.org/pp	January 2012
NSA Suite B	*NSA Guidance on Suite B Cryptography (including the Secure Sharing Suite (S3))*. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml	November 2010
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE)*. D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* Internet Engineering Task Force	November 2003
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006

Document	Title	Date
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header*. S. Kent	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload*. S. Kent	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*. J. Schiller	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec*. P. Hoffman	December 2005
RFC 4492	*IETF RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk Corriente, B. Moeller, and Ruhr-Uni Bochum.	May 2006
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5759	*IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile*. J. Solinas and L. Zieglar.	January 2010
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
RFC 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6460	*IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS)*. M. Salter and R. Housley.	January 2012
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013

Document	Title	Date
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
SP 800-53	*NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	April 2013
SP 800-56A	*NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	May 2013
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion*. L. Chen.	November 2011
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	January 2011
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et al.	April 2011