

CPS Evaluation Matrix
For Evaluation Against the
Requirements for the
Common Policy Framework

NIST

Booz | Allen | Hamilton
900 Elkridge Landing Road
Linthicum, MD 21090

Version 1.1

21 December 2003

TABLE OF CONTENTS

DETAILED ASSESSMENT MATRIX..... 3

REFERENCES 49

CONTACT DETAILS..... 49

DETAILED ASSESSMENT MATRIX

The document or collection of documents (such as CPS, Registration Practices Statement (RPS), Subscriber Agreement, etc.) that describe the practices followed by subscribers, administrators, etc. of a PKI constitutes a PKI's CPS.

This specification provides a template for determining the compliance of a CPS with the Common Policy Framework. Compliance of a CPS with the CP is one aspect of the compliance audit that each CA must undergo before approval to issue under the common policy. This document was developed to ensure consistent audits by qualified third parties.

This section of the report presents the detailed comparison results for the Common Policy Framework CP and the XXXX CPS.

The following four evaluation terms and their definitions, listed in order of degree of conformity, were used to assess the XXXX CPS alignment to the Common Policy CP elements:

- 1) **Acceptable** - The XXXX CPS implements the functionality specified for this Common Policy CP requirement
- 2) **Not Comparable** - The XXXX CPS contains dissimilar policy contents, which provides a lower level of assurance/security than the Common Policy CP requirement.
- 3) **Missing** - The XXXX CPS does not contain procedures that can be compared to the Common Policy CP requirement in any way.
- 4) **Not Applicable** – The requirement contained within the Common Policy CP is not transferable or applied with the XXXX CPS.

Table No.	CP/CPS Sections	Relevant Excerpt
1	COMMON POLICY: 1.2	<p>Certificates issued in accordance with this CP shall assert at least one of the following OIDs in the certificate policy extension:</p> <p>id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}</p> <p>id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}</p> <p>id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}</p> <p>Certificates issued to CAs may contain any or all of these OIDs. Certificates issued to users may contain either the id-fpki-common-policy or id-fpki-common-hardware. Certificates issued to devices under this policy include the id-fpki-common-devices.</p>
	CPS:	
Overall Match:		Comments:
2	COMMON POLICY: 3.1.1	<p>The CA shall assign X.500 distinguished names to all subscribers. These distinguished names may be in either of two forms: an X.501 distinguished name specifying a geo-political name; and an Internet domain component name.</p>
	CPS:	
Overall Match:		Comments:
3	COMMON POLICY: 3.1.1	<p>All X.501 distinguished names assigned to federal employees shall be in one of the following directory information trees:</p> <p style="padding-left: 40px;">C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>] C=US, [o=<i>department</i>], [ou=<i>agency</i>]</p> <p>New implementations shall assign names in the following directory tree:</p> <p style="padding-left: 40px;">C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>]</p> <p>Legacy implementations which predate this policy may use the directory tree:</p> <p style="padding-left: 40px;">C=US, [o=<i>department</i>], [ou=<i>agency</i>]</p> <p>Common name fields shall be populated as specified above.</p>
	CPS:	
Overall Match:		Comments: Applies to CAs that assign X.501 distinguished names

Table No.	CP/CPS Sections	Relevant Excerpt
4	COMMON POLICY: 3.1.1	<p>The organizational units <i>department</i> and <i>agency</i> appear when applicable and are used to specify the federal entity that employs the subscriber. At least one organizational unit must appear in the DN. The distinguished name of the federal employee subscriber will take one of the four following forms:</p> <ul style="list-style-type: none"> • C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>], cn=<i>nickname lastname</i> • C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>], cn=<i>firstname initial. lastname</i> • C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>], cn=<i>firstname middlename lastname</i> • C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>], cn=<i>firstname middlename lastname</i>, dnQualifier=<i>integer</i> <p>In the first name form, <i>nickname</i> may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. In the last form, dnQualifier is an integer value that makes the name unique. The last form shall be used only if the other three name forms have already been assigned to subscribers.</p>
	CPS:	
Overall Match:	Comments:	Applies to CAs that assign X.501 distinguished names to employees. For legacy implementations (see Table 3), modify the DIT to eliminate o=U.S. Government

Table No.	CP/CPS Sections	Relevant Excerpt
5	COMMON POLICY: 3.1.1	<p>The organizational units <i>department</i> and <i>agency</i> appear when applicable and are used to specify the federal entity that employs the subscriber. At least one organizational unit must appear in the DN.</p> <p>[text regarding employee names deleted.]</p> <p>X.501 distinguished names assigned to federal contractors and other affiliated persons shall be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take one of the four following forms:</p> <ul style="list-style-type: none"> • C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>], cn=<i>nickname lastname</i> (affiliate) • C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>], cn=<i>firstname initial. lastname</i> (affiliate) • C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>], cn=<i>firstname middlename lastname</i> (affiliate) • C=US, o=U.S. Government, [ou=<i>department</i>], [ou=<i>agency</i>], cn=<i>firstname middlename lastname</i> (affiliate), dnQualifier=<i>integer</i>
	CPS:	
Overall Match:	Comments:	Applies to CAs that assign X.501 distinguished names to contractors and affiliates. For legacy implementations (see Table 3), modify the DIT to eliminate o=U.S. Government
6	COMMON POLICY: 3.1.1	<p>Distinguished names based on Internet domain component names shall be in the following directory information trees:</p> <p style="text-align: center;">dc=gov, dc=<i>org0</i>, [dc=<i>org1</i>],... [dc=<i>orgN</i>] dc=mil, dc=<i>org0</i>, [dc=<i>org1</i>],... [dc=<i>orgN</i>]</p>
	CPS:	
Overall Match:	Comments:	Applies to CAs that assign Internet domain component distinguished names to certificate subjects (employees, affiliates, or devices).

Table No.	CP/CPS Sections	Relevant Excerpt
7	COMMON POLICY: 3.1.1	<p>The distinguished name of the federal employee subscriber may take one of the four following forms when their agency's Internet domain name ends in .gov:</p> <ul style="list-style-type: none"> • dc=gov, dc=org0, [dc=org1], ...[dc=orgN], cn=<i>nickname lastname</i> • dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname initial. lastname</i> • dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname middlename lastname</i> • dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname middlename lastname, dnQualifier=integer</i> <p>The distinguished name of the federal contractors and affiliated subscribers may take one of the four following forms when the agency's Internet domain name ends in .gov:</p> <ul style="list-style-type: none"> • dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=<i>nickname lastname (affiliate)</i> • dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname initial. lastname (affiliate)</i> • dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname middlename lastname (affiliate)</i> • dc=gov, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname middlename lastname (affiliate), dnQualifier=integer</i>
	CPS:	
Overall Match:	Comments:	Applies to CAs that assign Internet domain component distinguished names to certificate subjects (employees, affiliates, or devices) in the .gov domain.

Table No.	CP/CPS Sections	Relevant Excerpt
8	COMMON POLICY: 3.1.1	<p>Distinguished names based on Internet domain component names shall be in the following directory information trees:</p> <p style="text-align: center;">dc=gov, dc=org0, [dc=org1],...[dc=orgN] dc=mil, dc=org0, [dc=org1],...[dc=orgN]</p> <p>The distinguished name of the federal employee subscriber may take one of the four following forms when their agency's Internet domain name ends in .mil:</p> <ul style="list-style-type: none"> • dc=mil, dc=org0, [dc=org1], ...[dc=orgN], cn=<i>nickname lastname</i> • dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname initial. lastname</i> • dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname middlename lastname</i> • dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname middlename lastname, dnQualifier=integer</i> <p>The distinguished name of the federal contractors and affiliated subscribers may take one of the four following forms when the agency's Internet domain name ends in .mil:</p> <ul style="list-style-type: none"> • dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=<i>nickname lastname (affiliate)</i> • dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname initial. lastname (affiliate)</i> • dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname middlename lastname (affiliate)</i> • dc=mil, dc=org0, [dc=org1],...[dc=orgN], cn=<i>firstname middlename lastname (affiliate), dnQualifier=integer</i>
	CPS:	
Overall Match:	Comments:	Applies to CAs that assign Internet domain component distinguished names to certificate subjects (employees, affiliates, or devices) in the .mil domain.
9	COMMON POLICY: 3.1.2	The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 3280, even if the subject's name is not meaningful.
	CPS:	
Overall Match:	Comments:	Applies to CAs that issue CA certificates

Table No.	CP/CPS Sections	Relevant Excerpt
10	COMMON POLICY: 3.1.4	Name uniqueness for certificates issued by each CA must be enforced. Each CA and its associated RAs shall enforce name uniqueness within the X.500 name space. When other name forms are used, they too must be allocated such that name uniqueness is ensured for certificates issued by that CA.
	CPS:	
Overall Match:		Comments:
11	COMMON POLICY: 3.1.7	In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value supplied by the CA. The CA shall then validate the signature using the party's public key. The PA may allow other mechanisms that are at least as secure as those cited here.
	CPS:	
Overall Match:		Comments:
12	COMMON POLICY: 3.1.8	Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. The issuing CA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.
	CPS:	
Overall Match:		Comments:
13	COMMON POLICY: 3.1.9	At a minimum, authentication procedures for employees must include the following steps: 1) Verify that a request for certificate issuance to the applicant was submitted by agency management;
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
14	COMMON POLICY: 3.1.9	[At a minimum, authentication procedures for employees must include the following steps:] 2) Applicant's employment shall be verified through use of official agency records;
	CPS:	
Overall Match:	Comments:	

Table No.	CP/CPS Sections	Relevant Excerpt
15	COMMON POLICY: 3.1.9	<p>[At a minimum, authentication procedures for employees must include the following steps:]</p> <p>3) Applicant’s identity shall be established by in-person proofing before the Registration Authority, based on either of the following processes:</p> <p>a) Process #1:</p> <ul style="list-style-type: none"> i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver’s license) as proof of identity, and ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used. <p>b) Process #2:</p> <ul style="list-style-type: none"> i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver’s license) as proof of identity, and ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a photograph of applicant securely stored and linked to the credential), and iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the identifying information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). [Practice Note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.]
	CPS:	
Overall Match:	Comments:	

Table No.	CP/CPS Sections	Relevant Excerpt
16	COMMON POLICY: 3.1.9	[At a minimum, authentication procedures for employees must include the following steps:] 4) A biometric of the applicant (e.g., a photograph or fingerprint) shall be recorded and maintained by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.)
	CPS:	
Overall Match:	Comments:	
17	COMMON POLICY: 3.1.9	For contractors and other affiliated personnel, the authentication procedures must include the following steps: 1) Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer's technical representative);
	CPS:	
Overall Match:	Comments:	
18	COMMON POLICY: 3.1.9	[For contractors and other affiliated personnel, the authentication procedures must include the following steps: ...] 2) Sponsoring Agency employee's identity and employment shall be verified through either of the following methods: a) A digital signature verified by a currently valid employee signature certificate issued by the CA, may be accepted as proof of both employment and identity, or b) Employee's identity shall be established by in-person proofing before the Registration Authority as in employee authentication above and employment validated through use of the official agency records.
	CPS:	
Overall Match:	Comments:	

Table No.	CP/CPS Sections	Relevant Excerpt
19	COMMON POLICY: 3.1.9	<p>[For contractors and other affiliated personnel, the authentication procedures must include the following steps: ...]</p> <p>3) Applicant’s identity shall be established by in-person proofing before the Registration Authority, based on either of the following processes:</p> <p>a) Process #1:</p> <ul style="list-style-type: none"> i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver’s license) as proof of identity, and ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying official records maintained by the organization that issued the credential. <p>b) Process #2:</p> <ul style="list-style-type: none"> i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver’s license) as proof of identity, and ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA.
	CPS:	
Overall Match:	Comments:	

Table No.	CP/CPS Sections	Relevant Excerpt
20	COMMON POLICY: 3.1.9	[For contractors and other affiliated personnel, the authentication procedures must include the following steps: ...] A biometric of the applicant (e.g., a photograph or fingerprint) shall be recorded and maintained by the RA or CA.
	CPS:	
Overall Match:	Comments:	
21	COMMON POLICY: 3.1.9	[...] the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following: <ul style="list-style-type: none"> • The identity of the person performing the identification; • A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury); • Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s); • The biometric of the applicant; • The date and time of the verification; and • A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).
	CPS:	
Overall Match:	Comments:	Applies to any certificates issued to employees, contractors and/or other affiliated personnel

Table No.	CP/CPS Sections	Relevant Excerpt
22	COMMON POLICY: 3.1.9	<p>Where it is not possible for applicants to appear in person before the RA, a trusted agent may serve as proxy for the RA. The trusted agent forwards the information collected from the applicant directly to the RA in a secure manner. The requirement for recording a biometric of the applicant may be satisfied by providing passport-style photographs to the notary. The trusted agent shall verify the photographs against the appearance of the applicant and the biometrics on the presented credentials and securely incorporate the biometric as a component in the notarized package. Packages secured in a tamper-evident manner by the trusted agent satisfy this requirement; other secure methods are also acceptable.</p> <p>Authentication by a trusted agent does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), above.</p>
	CPS:	
Overall Match:		Comments: Applies to CAs that rely on trusted agents when issuing certificates to employees, contractors and/or other affiliated personnel
23	COMMON POLICY: 3.1.10	<p>Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is responsible for providing the following registration information:</p> <ul style="list-style-type: none"> • Equipment identification (e.g., serial number) or service name (e.g., DNS name) • Equipment public keys • Equipment authorizations and attributes (if any are to be included in the certificate) • Contact information to enable the CA or RA to communicate with the sponsor when required
	CPS:	
Overall Match:		Comments: Applies to CAs that issue device certificates
24	COMMON POLICY: 3.1.10	<p>The identity of the sponsor shall be authenticated by:</p> <ul style="list-style-type: none"> • Verification of digitally signed messages sent from the sponsor using a certificate issued under this policy; or • In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.1.9.
	CPS:	
Overall Match:		Comments: Applies to CAs that issue device certificates

Table No.	CP/CPS Sections	Relevant Excerpt
25	COMMON POLICY: 3.2.1	Subscriber certificates issued under this policy shall not be renewed, except during recovery from CA key compromise (see 4.8.3).
	CPS:	
Overall Match:	Comments:	

Table No.	CP Section	Relevant Excerpt
26	COMMON POLICY: 3.2.2	If it has been less than 6 years since a subscriber was identified as required in Section 3.1, a CA may authenticate an electronic request for a new certificate using the currently valid certificate issued to the subscriber by the CA. Subscribers shall identify themselves for the purpose of re-keying through use of current signature key.
	CPS:	
Overall Match:		Comments:
27	COMMON POLICY: 3.2.2	CA certificate Re-Key shall follow the same procedures as initial certificate issuance. If more than 6 years have passed since a subscriber's identity was authenticated as specified in Section 3.1, a subscriber certificate re-key shall follow the same procedures as initial certificate issuance.
	CPS:	
Overall Match:		Comments:
28	COMMON POLICY: 3.2.3	<i>[When updating a certificate,]</i> the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.
	CPS:	
Overall Match:		Comments:
29	COMMON POLICY: 3.2.3	<i>[When updating a certificate,]</i> If an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent in order for a certificate with the new name to be issued.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
30	COMMON POLICY: 3.2.3	<i>[When updating a certificate,]</i> If an individual's authorizations or privileges change, the RA will verify those authorizations. If authorizations have reduced, the old certificate must be revoked.
	CPS:	
Overall Match:		Comments:
31	COMMON POLICY: 3.2.3	<i>[When updating a certificate,]</i> when a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. CAs that distribute self-signed certificates shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa.
	CPS:	
Overall Match:		Comments: Key rollover certificates are optional for CAs that do not distribute self-signed certificates.
32	COMMON POLICY: 3.2.3	Where distribution of the new self-signed certificate to current users is required, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.
	CPS:	
Overall Match:		Comments: This applies only to CAs that distribute self-signed certificates.
33	COMMON POLICY: 3.3	In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process.
	CPS:	
Overall Match:		Comments:
34	COMMON POLICY: 3.4	Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised..
	CPS:	
Overall Match:		Comments:
35	COMMON POLICY: 4.1	The PKI Authorities must perform the following steps when an applicant (prospective subscriber) applies for a certificate: <ul style="list-style-type: none"> • Verify any role or authorization information requested for inclusion in the certificate.
	CPS:	
Overall Match:		Comments: Policy specifies additional items in this list. Remaining items in the list were covered in previous tables.

Table No.	CP/CPS Sections	Relevant Excerpt
36	COMMON POLICY: 4.1	All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.
	CPS:	
Overall Match:		Comments:
37	COMMON POLICY: 4.1.1	Public keys must be delivered for certificate issuance in a way that binds the applicant principal's verified identification to the public key. This binding may be accomplished using cryptography. If cryptography is used it must be at least as strong as that employed at certificate issuance. This binding may be accomplished using non-cryptographic physical and procedural mechanisms. Regardless of the method selected, the mechanism used for public key delivery shall be set forth in the CA's CPS.
	CPS:	
Overall Match:		Comments:
38	COMMON POLICY: 4.1.1	In those cases where public/private key pairs are generated by the CA on behalf of the subscriber, the CA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper subscriber. The CA shall also implement procedures to ensure that the token is not activated by an unauthorized entity.
	CPS:	
Overall Match:		Comments: Note to CP author – check later tables for redundancy. If redundant, eliminate this table from matrix and the paragraph from the CP.

Table No.	CP/CPS Sections	Relevant Excerpt
39	COMMON POLICY: 4.2	<p><i>[When processing certificate requests...]</i> Upon receiving the request, the CAs/RAs will—</p> <ul style="list-style-type: none"> • Verify the identity of the requestor • Verify the authority of the requestor and the integrity of the information in the certificate request • Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate) • Make the certificate available to the subscriber. <p>The certificate request may already contain a certificate built by either the RA or the subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.</p>
	CPS:	
Overall Match:		Comments:
40	COMMON POLICY: 4.2	<p><i>[When processing certificate requests...]</i> All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in a CA's CPS.</p>
	CPS:	
Overall Match:		Comments:
41	COMMON POLICY: 4.2.1	<p><i>[Delivering Private keys to the Subscriber...]</i> If the key is generated elsewhere, the cryptographic token must be delivered to the subscriber. Accountability for the location and state of the cryptographic token must be maintained until the subscriber accepts possession of it. The subscriber shall acknowledge receipt of the cryptographic token. Anyone who generates a private signing key for a subscriber shall not retain any copy of the key.</p>
	CPS:	
Overall Match:		Comments:
42	COMMON POLICY: 4.2.1	<p><i>[Delivering Private keys to the Subscriber...]</i> This policy allows a certificate to be issued only to a single subscriber. Certificates shall not be issued that contain a public key whose associated private key is shared.</p>
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
43	COMMON POLICY: 4.2.2	<p>Acceptable methods for Trusted Certificate delivery include but are not limited to—</p> <ul style="list-style-type: none"> • The RA loading a Trusted Certificate onto tokens delivered to relying parties via secure mechanisms, such as: <ul style="list-style-type: none"> • The Trusted Certificate is loaded onto the token during the subscriber’s appearance at the RA. • The Trusted Certificate is loaded onto the token when the RA generates the subscriber’s key pair and loads the private key onto the token. • Distribution of Trusted Certificates through secure out-of-band mechanisms; • Comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); or • Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.
	CPS:	
Overall Match:		Comments:
44	COMMON POLICY: 4.3	<p>[Certificate Acceptance] Before a subscriber can make effective use of its private key, a PKI Authority shall—</p> <ul style="list-style-type: none"> • Explain to the subscriber its responsibilities as defined in Section 2.1.5 • Inform the subscriber of the creation of a certificate and the contents of the certificate. <p>The ordering of this process, and the mechanisms used, will depend on factors such as where the key is generated and how certificates are posted.</p>
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
45	COMMON POLICY: 4.4.1.1	<p>A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are—</p> <ul style="list-style-type: none"> • Identifying information or affiliation components of any names in the certificate becomes invalid. • Privilege attributes asserted in the subscriber's certificate are reduced. • The subscriber can be shown to have violated the stipulations of its subscriber agreement. • There is reason to believe the private key has been compromised. • The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked. <p>Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.</p>
	CPS:	
Overall Match:		Comments:
46	COMMON POLICY: 4.4.1.2	<p><i>[Who Can Request a Revocation..]</i> Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that its own certificate be revoked. Other authorized agency officials may request revocation as described in the CPS.</p>
	CPS:	
Overall Match:		Comments:
47	COMMON POLICY: 4.4.1.3	<p>A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The steps involved in the process of requesting a certification revocation are detailed in the CPS.</p>
	CPS:	
Overall Match:		Comments:
48	COMMON POLICY: 4.4.1.4	<p>Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.</p>

Table No.	CP/CPS Sections	Relevant Excerpt
	CPS:	
Overall Match:		Comments:
49	COMMON POLICY: 4.4.2	Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.
	CPS:	
Overall Match:		Comments:
50	COMMON POLICY: 4.4.3	CAs shall issue CRLs covering all unexpired certificates issued under this policy.
	CPS:	
Overall Match:		Comments:
51	COMMON POLICY: 4.4.3.1	CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. CAs that only issue certificates to CAs and that operate offline must issue CRLs at least once every 24 hours. When a CA certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued within 6 hours of notification.
	CPS:	
Overall Match:		Comments: This applies to CAs that only issue certificates to CAs and that operate offline.
52	COMMON POLICY: 4.4.3.1	CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 18 hours. When a CA certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued within 6 hours of notification.
	CPS:	
Overall Match:		Comments: This applies to CAs that only issue certificates to subscribers or operate online
53	COMMON POLICY: 4.4.5	A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements: <ul style="list-style-type: none"> The alternative method must be described in the CA's approved CPS; The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified..
	CPS:	
Overall Match:		Comments: Applies only to CAs that use additional methods to distribute certificate status.

Table No.	CP/CPS Sections	Relevant Excerpt
54	COMMON POLICY: 4.4.7	<p>In the event of a CA private key compromise, the following operations must be performed.</p> <p>If the CA distributed the private key in a Trusted Certificate, the CA shall perform the following operations:</p> <ul style="list-style-type: none"> • Generate a new signing key pair and corresponding Trusted Certificate; • Initiate procedures to notify subscribers of the compromise; and • Securely distribute the Trusted Certificate. • Optionally, the CA may renew current certificates under the new signing key. (see 3.2.1) <p>If the CA's private key appears as the subject public key in certificates issued by other CAs, the CA will notify the issuer(s) of these certificates within 24 hours.</p>
	CPS:	
Overall Match:		Comments:
55	COMMON POLICY: 4.5.1	All security auditing capabilities of CA operating system and PKI CA applications shall be enabled during installation
	CPS:	
Overall Match:		Comments:
56	COMMON POLICY: 4.5.1	<p>At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):</p> <ul style="list-style-type: none"> • The type of event • The date and time the event occurred • A success or failure indicator when executing the CA's signing process • A success or failure indicator when performing certificate revocation • The identity of the entity and/or operator that caused the event.
	CPS:	
Overall Match:		Comments:
57	COMMON POLICY: 4.5.2	Review of the audit log shall be required at least once every two months. Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA since the last review shall be examined. This amount will be described in the CPS.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
58	COMMON POLICY: 4.5.2	All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.
	CPS:	
Overall Match:		Comments:
59	COMMON POLICY: 4.5.3	Audit logs shall be retained onsite for at least 2 months in addition to being retained in the manner described below. The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.
	CPS:	
Overall Match:		Comments:
60	COMMON POLICY: 4.5.4	The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the CA equipment.
	CPS:	
Overall Match:		Comments:
61	COMMON POLICY: 4.5.5	Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent offsite in accordance with the CPS, on a monthly basis.
	CPS:	
Overall Match:		Comments:
62	COMMON POLICY: 4.5.6	Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown.
	CPS:	
Overall Match:		Comments:
63	COMMON POLICY: 4.5.6	Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem has been remedied. The PA shall determine whether to resume operations.
	CPS:	
Overall Match:		Comments:
64	COMMON POLICY: 4.5.8	The CA will perform routine self-assessments of security controls.

Table No.	CP/CPS Sections	Relevant Excerpt
	CPS:	
Overall Match:		Comments:
65	COMMON POLICY: 4.6.1	<p>CA archive records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:</p> <ul style="list-style-type: none"> • CA accreditation (if applicable) • Certificate Policy • Certification Practice Statement • Contractual obligations • Other agreements concerning operations of the CA • System and equipment configuration • Modifications and updates to system or configuration • Certificate requests • All certificates issued and/or published • Record of Re-key • Security audit data (in accordance with Section 4.5) • Revocation requests • Subscriber identity Authentication data as per Section 3.1.9 • Subscriber agreements • Documentation of receipt of tokens • All CARLs and CRLs issued and/or published • Other data or applications to verify archive contents • Documentation required by compliance auditors.
	CPS:	
Overall Match:		Comments:
66	COMMON POLICY: 4.6.1	CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys.
	CPS:	
Overall Match:		Comments:
67	COMMON POLICY: 4.6.2	The archive records must be kept for a minimum of 10 years and 6 months without any loss of data.
	CPS:	
Overall Match:		Comments:
68	COMMON POLICY: 4.6.3	No unauthorized user shall be permitted to write to, modify, or delete the archive.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
69	COMMON POLICY: 4.6.3	The contents of the archive shall not be released except (1) in accordance with agency policy, or (2) as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.
	CPS:	
Overall Match:		Comments:
70	COMMON POLICY: 4.6.3	Archive media shall be stored in a safe, secure storage facility separate from the CA.
	CPS:	
Overall Match:		Comments:
71	COMMON POLICY: 4.6.5	CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.
	CPS:	
Overall Match:		Comments:
72	COMMON POLICY: 4.6.7	Procedures detailing how to create, verify, package, transmit, and store the CA archive information shall be published in the CPS.
	CPS:	
Overall Match:		Comments:
73	COMMON POLICY: 4.7	<i>[CA Key Rollover]</i> To minimize risk from compromise of a CA's private signing key, that key may be changed often. From that time on, only the new key will be used for certificate signing purposes. If the old private key is used to sign CRLs that contain certificates signed with that key, the old key must be retained and protected.
	CPS:	
Overall Match:		Comments:
74	COMMON POLICY: 4.8	Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used.
	CPS:	
Overall Match:		Comments:
75	COMMON POLICY: 4.8	The CA shall have recovery procedures in place to reconstitute the CA within 72 hours in the event of a catastrophic failure, as described in the following subsections.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
76	COMMON POLICY: 4.8.1	<i>[Computing Resources, Software, and/or Data are Corrupted]</i> If the CA equipment is damaged or rendered inoperative, but the CA signature keys are not destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information. The PA shall be notified as soon as possible.
	CPS:	
Overall Match:		Comments:
77	COMMON POLICY: 4.8.2	<i>[CA Cannot Generate CRLs]</i> If the CA cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL, the PA shall be informed, as well as the Agency PMA(s) where appropriate.
	CPS:	
Overall Match:		Comments:
78	COMMON POLICY: 4.8.3	<i>[CA Signature Keys are Compromised]</i> In case of a CA key compromise, the PA shall be immediately informed, as well as any superior or cross-certified CAs. Subsequently, the CA installation shall be reestablished. If the CA distributes a trusted certificate for use as a trust anchor, the new self-signed certificate must be distributed via secure out-of-band mechanisms. The CPS shall detail the secure out-of-band mechanisms.
	CPS:	
Overall Match:		Comments:
79	COMMON POLICY: 4.8.3	<i>[CA Signature Keys are Compromised]</i> Subscriber certificates may be renewed automatically by the CA under the new key pair, or the CA may require subscribers to repeat the initial certificate application process.
	CPS:	
Overall Match:		Comments:
80	COMMON POLICY: 4.8.4	In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the PA shall be notified at the earliest feasible time, and the PA shall take whatever action it deems appropriate.
	CPS:	
Overall Match:		Comments:
81	COMMON POLICY: 4.9	In the event of termination of the CA operation, certificates signed by the CA shall be revoked. Prior to CA termination, the CA shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.
	CPS:	

Table No.	CP/CPS Sections	Relevant Excerpt
Overall Match:		Comments:
82	COMMON POLICY: 5.1	CA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The CA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens shall be protected against theft, loss, and unauthorized use.
	CPS:	
Overall Match:		Comments:
83	COMMON POLICY: 5.1.1	The location and construction of the facility housing the CA equipment shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.
	CPS:	
Overall Match:		Comments:
84	COMMON POLICY: 5.1.2	<p>At a minimum, the physical access controls shall—</p> <ul style="list-style-type: none"> • Ensure that no unauthorized access to the hardware is permitted • Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers. • Be manually or electronically monitored for unauthorized intrusion at all times • Ensure an access log is maintained and inspected periodically • Require two-person physical access control to both the cryptographic module and computer system
	CPS:	
Overall Match:		Comments:
85	COMMON POLICY: 5.1.2	Removable cryptographic modules shall be inactivated before storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
86	COMMON POLICY: 5.1.2	<p>A security check of the facility housing the CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:</p> <ul style="list-style-type: none"> • The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open,” and secured when “closed,” and for the CA, that all equipment other than the repository is shut down) • Any security containers are properly secured • Physical security systems (e.g., door locks, vent covers) are functioning properly • The area is secured against unauthorized access. <p>A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.</p>
	CPS:	
Overall Match:		Comments:
87	COMMON POLICY: 5.1.3	The CA shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.
	CPS:	
Overall Match:		Comments:
88	COMMON POLICY: 5.1.3	The directories (containing CA-issued certificates and CARLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.
	CPS:	
Overall Match:		Comments:
89	COMMON POLICY: 5.1.4	<i>[Physical Controls]</i> CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).
	CPS:	
Overall Match:		Comments:
90	COMMON POLICY: 5.1.6	<i>[Physical Controls]</i> Media shall be stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic). Media that contain audit, archive, or backup information shall be duplicated and stored in locations separate from the CAs.
	CPS:	

Table No.	CP/CPS Sections	Relevant Excerpt
Overall Match:		Comments:
91	COMMON POLICY: 5.1.7	Sensitive media and documentation that are no longer needed for operations shall be destroyed in the disposal process. For example, sensitive paper documentation shall be shredded, burned, or other wise rendered unrecoverable.
	CPS:	
Overall Match:		Comments:
92	COMMON POLICY: 5.1.8	Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in a CA's CPS. Backups are to be performed and stored offsite not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.
	CPS:	
Overall Match:		Comments:
93	COMMON POLICY: 5.2.1	The primary trusted roles defined this policy are Administrator, Officer, Auditor, and Operator.
	CPS:	
Overall Match:		Comments:
94	COMMON POLICY: 5.2.1.1	<p>The administrator role is responsible for—</p> <ul style="list-style-type: none"> • Installation, configuration, and maintenance of the CA hardware and software • Establishing and maintaining CA system accounts • Configuring certificate profiles or templates and audit parameters • Generating and backing up CA keys. <p>Administrators do not issue certificates to subscribers.</p>
	CPS:	
Overall Match:		Comments:
95	COMMON POLICY: 5.2.1.2	<p>The officer's responsibility is to ensure the following functions occur according to the stipulations of this policy, that is—</p> <ul style="list-style-type: none"> • Registering new subscribers and requesting the issuance of certificates • Verifying the identity of subscribers and the accuracy of information included in certificates • Approving and executing the issuance of certificates • Requesting, approving, and executing the revocation of certificates.

Table No.	CP/CPS Sections	Relevant Excerpt
	CPS:	
Overall Match:		Comments:
96	COMMON POLICY: 5.2.1.3	The auditor role is responsible for— <ul style="list-style-type: none"> • Reviewing, maintaining, and archiving audit logs • Performing or overseeing internal compliance audits to ensure that the CA and associated RAs are operating in accordance with its CPS.
	CPS:	
Overall Match:		Comments:
97	COMMON POLICY: 5.2.1.4	The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery, or changing recording media.
	CPS:	
Overall Match:		Comments:
98	COMMON POLICY: 5.2.2	Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.
	CPS:	
Overall Match:		Comments:
99	COMMON POLICY: 5.2.3	An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.
	CPS:	
Overall Match:		Comments:
100	COMMON POLICY: 5.3.1, 5.3.2	[5.3.1] All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the CPS. [5.3.2] Background check procedures shall be described in the CPS and shall demonstrate that requirements set forth in Section 5.3.1 are met.
	CPS:	

Table No.	CP/CPS Sections	Relevant Excerpt
Overall Match:		Comments:
101	COMMON POLICY: 5.3.3	<p>All personnel performing duties with respect to the operation of the CA shall receive comprehensive training. Training shall be conducted in the following areas:</p> <ul style="list-style-type: none"> • CA (or RA) security principles and mechanisms • All PKI software versions in use on the CA (or RA) system • All PKI duties they are expected to perform • Disaster recovery and business continuity procedures • Stipulations of this policy.
	CPS:	
Overall Match:		Comments:
102	COMMON POLICY: 5.3.4	<p>All individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.</p>
	CPS:	
Overall Match:		Comments:
103	COMMON POLICY: 5.3.6	<p>The CA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its RAs that are not authorized in this CP, CPSes, or other published procedures.</p>
	CPS:	
Overall Match:		Comments:
104	COMMON POLICY: 5.3.7	<p>Contracting personnel requirements are the same as specified in Section 5.3.1</p>
	CPS:	
Overall Match:		Comments:
105	COMMON POLICY: 5.3.7	<p>PKI vendors who provide any services shall establish procedures to ensure that any subcontractors perform in accordance with this policy and the CPS.</p>
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
106	COMMON POLICY: 5.3.8	Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.
	CPS:	
Overall Match:		Comments:
107	COMMON POLICY: 6.1.1.1	[CA Key Pair Generation] Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140 validated cryptographic modules. The module(s) shall meet or exceed Security Level 2. Multiparty control is required for CA key pair generation, as specified in Section 5.2.2.
	CPS:	
Overall Match:		
108	COMMON POLICY: 6.1.1.1	[CA Key Pair Generation] CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The audit trail must identify and document any failures or anomalies in the key generation process, and any corrective actions taken. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.
	CPS:	
Overall Match:		Comments:
109	COMMON POLICY: 6.1.1.2	[Subscriber Key Pair Generation] Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met. Key generation shall be performed using a FIPS approved method.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
110	COMMON POLICY: 6.1.2	<p>[Private Key Delivery to Subscribers] When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:</p> <ul style="list-style-type: none"> • Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber. • The private key must be protected from activation, compromise, or modification during the delivery process. • The Subscriber shall acknowledge receipt of the private key(s). • Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. <ul style="list-style-type: none"> ○ For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. ○ For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel. <p>The CA must maintain a record of the subscriber acknowledgement of receipt of the token.</p>
	CPS:	
Overall Match:		Comments:
111	COMMON POLICY: 6.1.3	<p>[Public Key Delivery to Certificate Issuer] Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.</p>
	CPS:	
Overall Match:		Comments:
112	COMMON POLICY: 6.1.4	<p>When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate or in a key rollover certificate.</p>
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
113	COMMON POLICY: 6.1.4	Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks.
	CPS:	
Overall Match:		Comments: Pre-approved methods for distribution of self-signed certificates are defined in the CP; others may be acceptable.
114	COMMON POLICY: 6.1.5	This CP requires use of RSA PKCS#1 signatures . Certificates issued under this policy shall contain RSA public keys.
	CPS:	
Overall Match:		Comments:
115	COMMON POLICY: 6.1.5	Trusted Certificates shall contain subject public keys of at least 2048 bits, and be signed with the corresponding private key.
	CPS:	
Overall Match:		Comments:
116	COMMON POLICY: 6.1.5	CAs that generate certificates and CRLs under this policy shall use SHA-1 or SHA-256 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued before January 1, 2007 shall be generated using SHA-1. Signatures on certificates and CRLs that are issued on or after January 1, 2009 shall be generated using SHA-256.
	CPS:	
Overall Match:		Comments:
117	COMMON POLICY: 6.1.5	End entity certificates that expire before January 1, 2009 shall contain RSA public keys that are at least 1024 bits in length. End entity certificates that expire on or after January 1, 2009 shall contain RSA public keys that are at least 2048 bits.
	CPS:	
Overall Match:		Comments:
118	COMMON POLICY: 6.1.5	Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/08. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/08.
	CPS:	

Table No.	CP/CPS Sections	Relevant Excerpt
Overall Match:		Comments:
119	COMMON POLICY: 6.1.6	Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used.
	CPS:	
Overall Match:		Comments:
120	COMMON POLICY: 6.1.7	Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-2.
	CPS:	
Overall Match:		Comments:
121	COMMON POLICY: 6.1.8	<i>[Hardware/Software Subscriber key generation]</i> Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.
	CPS:	
Overall Match:		Comments:
122	COMMON POLICY: 6.1.9	Public keys that are bound into subscriber certificates shall be used only for signing or encrypting, but not both. Certificates to be used for digital signatures (including authentication) shall assert the <i>digitalSignature</i> and/or <i>nonRepudiation</i> bits. Certificates to be used for key transport shall assert the <i>keyEncipherment</i> bit.
	CPS:	
Overall Match:		Comments:
123	COMMON POLICY: 6.1.9	Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the <i>keyCertSign</i> bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the <i>cRLSign</i> bit. If the CA certificate is to be used to verify both certificate and CRLs, both the <i>keyCertSign</i> and <i>cRLSign</i> bits shall be asserted.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
124	COMMON POLICY: 6.1.9	The <i>dataEncipherment</i> , <i>encipherOnly</i> , and <i>decipherOnly</i> bits shall not be asserted in certificates issued under this policy.
	CPS:	
Overall Match:		Comments:
125	COMMON POLICY: 6.2.1	The CA and RA shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module.
	CPS:	
Overall Match:		Comments:
126	COMMON POLICY: 6.2.1	Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations.
	CPS:	
Overall Match:		Comments:
127	COMMON POLICY: 6.2.1	Subscribers issued certificates under the hardware users policy (<i>id-fpki-common-hardware</i>) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.
	CPS:	
Overall Match:		Comments:
128	COMMON POLICY: 6.2.2	A single person shall not be permitted to invoke the complete CA signature process or access any cryptomodule containing the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.
	CPS:	
Overall Match:		Comments:
129	COMMON POLICY: 6.23	CA private keys are never escrowed.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
130	COMMON POLICY: 6.2.3	Subscriber key management keys may be escrowed to provide key recovery. The method for this shall be described in the CA's CPS.
	CPS:	
Overall Match:		Comments:
131	COMMON POLICY: 6.2.3	Under no circumstances shall a subscriber signature key be held in trust by a third party.
	CPS:	
Overall Match:		Comments: Where the signature is encrypted under an algorithm and key size of commensurate strength, under a key known solely to the subscriber, the signature key is deemed to be in the subscriber's control even if stored on a remote server.
132	COMMON POLICY: 6.2.4.1	The CA private signature keys shall be backed up under the same multiperson control as the original signature key. Such backup shall create only a single copy of the signature key at the CA location; a second copy may be kept at the CA backup location. Backup procedures shall be included in the CA's CPS.
	CPS:	
Overall Match:		Comments:
133	COMMON POLICY: 6.2.4.2	Subscriber private signature keys whose corresponding public key is contained in a certificate may be backed up or copied, but must be held in the subscriber's control. Backed up subscriber private keys must be encrypted using a symmetric algorithm of consistent strength or stored in a cryptographic module validated at FIPS 140 Level 2..
	CPS:	
Overall Match:		Comments:
134	COMMON POLICY: 6.2.5	CA private signature keys and subscriber private signatures keys shall not be archived.
	CPS:	
Overall Match:		Comments:
135	COMMON POLICY: 6.2.5	Subscriber key management keys may be escrowed to provide key recovery. The method for this shall be described in the CA's CPS.
	CPS:	

Table No.	CP/CPS Sections	Relevant Excerpt
Overall Match:		Comments:
136	COMMON POLICY: 6.2.6	Subscriber keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary. Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.
	CPS:	
Overall Match:		Comments:
137	COMMON POLICY: 6.2.7	The subscriber must be authenticated to the cryptographic token before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).
	CPS:	
Overall Match:		Comments:
138	COMMON POLICY: 6.2.8	Cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS. CA cryptographic modules shall be removed and stored in a secure container when not in use.
	CPS:	
Overall Match:		Comments:
139	COMMON POLICY: 6.2.9	Private signature keys shall be destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked.
	CPS:	
Overall Match:		Comments: This will likely be performed by executing a “zeroize” command. Physical destruction of hardware is not required.
140	COMMON POLICY: 6.3.2	The usage period for a CA key pair is a maximum of six years. The CA private key may be used to generate certificates for the first half of the usage period (3 years), and the public key may be used to validate certificates for the entire usage period. If the CA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period.
	CPS:	

Table No.	CP/CPS Sections	Relevant Excerpt
Overall Match:		Comments:
141	COMMON POLICY: 6.3.2	Subscriber public keys have a maximum usage period of one half the CA key pair usage period. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.
	CPS:	
Overall Match:		Comments:
142	COMMON POLICY: 6.4.1	CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.
	CPS:	
Overall Match:		Comments:
143	COMMON POLICY: 6.4.1	RA and Subscriber activation data may be user-selected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.
	CPS:	
Overall Match:		Comments:
144	COMMON POLICY: 6.4.2	Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be either biometric in nature or memorized (not written down). If written down, activation data shall be physically secured or encrypted under a FIPS approved cryptographic algorithm, and shall not be stored with the cryptographic module.
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
145	COMMON POLICY: 6.5	<p>Computer security controls are required to ensure CA/RA operations are performed as specified in this policy. The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards:</p> <ul style="list-style-type: none"> • Require authenticated logins • Provide Discretionary Access Control • Provide a security audit capability • Restrict access control to CA services and PKI roles • Enforce separation of duties for PKI roles • Require identification and authentication of PKI roles and associated identities • Prohibit object reuse or require separation for CA random access memory • Require use of cryptography for session communication and database security • Archive CA history and audit data • Require self-test security-related CA services • Require a trusted path for identification of PKI roles and associated identities • Require a recovery mechanism for keys and the CA system • Enforce domain integrity boundaries for security-critical processes. <p>When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements, the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.</p>
	CPS:	
Overall Match:		Comments:
146	COMMON POLICY: 6.6.1	<p><i>[System Development Controls for the CA and RA]</i></p> <p>The CA shall use software that has been designed and developed under a formal, documented development methodology.</p>
	CPS:	
Overall Match:		Comments:
147	COMMON POLICY: 6.6.1	<p><i>[System Development Controls for the CA and RA]</i></p> <p>Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).</p>
	CPS:	
Overall Match:		Comments:

Table No.	CP/CPS Sections	Relevant Excerpt
148	COMMON POLICY: 6.6.1	<i>[System Development Controls for the CA and RA]</i> Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
	CPS:	
Overall Match:		Comments:
149	COMMON POLICY: 6.6.1	<i>[System Development Controls for the CA and RA]</i> The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform can support multiple CAs.
	CPS:	
Overall Match:		Comments:
150	COMMON POLICY: 6.6.1	<i>[System Development Controls for the CA and RA]</i> Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.
	CPS:	
Overall Match:		Comments:
151	COMMON POLICY: 6.6.1	<i>[System Development Controls for the CA and RA]</i> Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.
	CPS:	
Overall Match:		Comments:
152	COMMON POLICY: 6.6.2	The configuration of the CA system, in addition to any modifications and upgrades, shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA shall periodically verify the integrity of the software as specified in the CPS.

Table No.	CP/CPS Sections	Relevant Excerpt
	CPS:	
Overall Match:		Comments:
153	COMMON POLICY: 6.7	A network guard, firewall, or filtering router must protect network access to CA equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the CA equipment to those required to perform CA functions.
	CPS:	
Overall Match:		Comments:
154	COMMON POLICY: 6.7	Protection of CA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CA equipment shall be necessary to the functioning of the CA application.
	CPS:	
Overall Match:		Comments:
155	COMMON POLICY: 6.7	Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.
	CPS:	
Overall Match:		Comments:
156	COMMON POLICY: 7.1	Certificates issued by a CA under this policy shall conform to the Common CP Certificate Profile [CCP-PROF].
	CPS:	
Overall Match:		
157	COMMON POLICY: 7.1.1	The CA shall issue X.509 v3 certificates (populate version field with integer "2").
	CPS:	
Overall Match:		
158	COMMON POLICY: 7.1.3	Certificates issued under this CP shall use the following OIDs for signatures: sha1WithRSAEncryption ::= {1 2 840 113549 1 1 5} sha256WithRSAEncryption ::= {1 2 840 113549 1 1 11}
	CPS:	

Table No.	CP/CPS Sections	Relevant Excerpt
Overall Match:		
159	COMMON POLICY: 7.1.3	Certificates issued under this CP shall use the following OID to identify the algorithm associated with the subject key: RsaEncryption ::= {1 2 840 113549 1 1 1}
	CPS:	
Overall Match:		
160	COMMON POLICY: 7.1.6	Certificates issued under this CP shall assert one of the following OID in the certificate policies extension, as appropriate: id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6} id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7} id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}
	CPS:	
Overall Match:		
161	COMMON POLICY: 7.1.8	Certificates issued under this CP shall not contain policy qualifiers.
	CPS:	
Overall Match:		
162	COMMON POLICY: 7.1.9	Certificates issued under this policy shall not contain a critical certificate policy extension .
	CPS:	
Overall Match:		
163	COMMON POLICY: 7.2	CRLs issued by a CA under this policy shall conform to the CRL Profile specified in [CCP-PROF].
	CPS:	
Overall Match:		
164	COMMON POLICY: 7.2.1	The CAs shall issue X.509 Version two (2) CRLs.
	CPS:	

Table No.	CP/CPS Sections	Relevant Excerpt
Overall Match:		
165	COMMON POLICY: 4.5	The CA shall record the events identified in the list below. Where these events cannot be electronically logged, the CA shall supplement electronic audit logs with physical logs as necessary.
	CPS:	
Overall Match:		Comments: The auditor shall identify the section of the CPS that indicates each event is logged.

#	Basic Auditable Events	CPS
	SECURITY AUDIT	
1	Any changes to the Audit parameters, e.g., audit frequency, type of event audited	
2	Any attempt to delete or modify the Audit logs	
	IDENTIFICATION AND AUTHENTICATION	
3	Successful and unsuccessful attempts to assume a role	
4	Change in the value of maximum authentication attempts	
5	Maximum number of unsuccessful authentication attempts during user login	
6	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	
7	An Administrator changes the type of authenticator, e.g., from password to biometrics	
	KEY GENERATION	
8	Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	
	PRIVATE KEY LOAD AND STORAGE	
9	The loading of Component private keys	
10	All access to certificate subject private keys retained within the CA for key recovery purposes	
	PUBLIC KEY ENTRY, DELETION AND STORAGE	
11	All changes to the XXXX public keys, including additions and deletions	
	PRIVATE KEY EXPORT	
12	The export of private keys (keys used for a single session or message are excluded)	
	CERTIFICATE REGISTRATION	
13	All certificate requests	
	CERTIFICATE REVOCATION	
14	All certificate revocation requests	
	CERTIFICATE STATUS CHANGE APPROVAL	
15	The approval or rejection of a certificate status change request	
	CA CONFIGURATION	
16	Any security-relevant changes to the configuration of the CA	
	ACCOUNT ADMINISTRATION	
17	Roles and users are added or deleted	
18	The access control privileges of a user account or a role are modified	
	CERTIFICATE PROFILE MANAGEMENT	
19	All changes to the certificate profile	
	REVOCATION PROFILE MANAGEMENT	
20	All changes to the revocation profile	
	CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	
21	All changes to the certificate revocation list profile	
	MISCELLANEOUS	
22	<i>Installation of the Operating System</i>	
23	<i>Installation of the CA</i>	
24	<i>Installing hardware cryptographic modules</i>	
25	<i>Removing hardware cryptographic modules</i>	
26	<i>Destruction of cryptographic modules</i>	
27	<i>System Startup</i>	

#	Basic Auditable Events	CPS
28	<i>Logon Attempts to CA Apps</i>	
29	<i>Receipt of Hardware / Software</i>	
30	<i>Attempts to set passwords</i>	
31	<i>Attempts to modify passwords</i>	
32	<i>Backing up CA internal database</i>	
33	<i>Restoring CA internal database</i>	
34	<i>File manipulation (e.g., creation, renaming, moving)</i>	
35	<i>Posting of any material to a repository</i>	
36	<i>Access to CA internal database</i>	
37	<i>All certificate compromise notification requests</i>	
38	<i>Loading tokens with certificates</i>	
39	<i>Shipment of Tokens</i>	
40	<i>Zeroizing tokens</i>	
41	<i>Rekey of the CA</i>	
	<i>Configuration changes to the CA server involving:</i>	
42	<i>Hardware</i>	
43	<i>Software</i>	
44	<i>Operating System</i>	
45	<i>Patches</i>	
46	<i>Security Profiles</i>	
	PHYSICAL ACCESS / SITE SECURITY	
47	<i>Personnel Access to room housing CA</i>	
48	<i>Access to the CA server</i>	
49	<i>Known or suspected violations of physical security</i>	
	ANOMALIES	
50	<i>Software Error conditions</i>	
51	<i>Software check integrity failures</i>	
52	<i>Receipt of improper messages</i>	
53	<i>Misrouted messages</i>	
54	<i>Network attacks (suspected or confirmed)</i>	
55	<i>Equipment failure</i>	
56	<i>Electrical power outages</i>	
57	<i>Uninterruptible Power Supply (UPS) failure</i>	
58	<i>Obvious and significant network service or access failures</i>	
59	<i>Violations of Certificate Policy</i>	
60	<i>Violations of Certification Practice Statement</i>	
61	<i>Resetting Operating System clock</i>	

REFERENCES

[1] Request for Comments (RFC): 2527; Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999, <http://www.ietf.org/rfc/rfc2527.txt>

[2] X.509 Certificate Policy For Common Policy Framework, 21 December 2003.

CONTACT DETAILS

Comments about this document may be sent to the following people:

Tim Polk, NIST	301-975-3348	tim.polk@nist.gov
John Cornell, GSA	202-501-1598	john.cornell@gsa.gov
Mark Lentz, Booz Allen Hamilton	410-684-6520	lentz_mark@bah.com