Bugzilla ID: 478418
Bugzilla Summary: Please add US FPKI Common Policy CA certificate
CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	U.S. Federal PKI Management Authority (US FPKI)
Website URL	http://www.idmanagement.gov/fpkima
Organizational type	National Government CA
Primark Market / Customer Base	The U.S. Federal Public Key Infrastructure (US FPKI) Management Authority is a National Government CA that operates the Federal Common Policy Framework Certification Authority (FCPCA) on behalf of the Federal PKI Policy Authority. The FCPCA is the Trust Anchor for the Federal Government. CAs under the FCPCA issue PKI credentials to Federal employees and contractors. The FCPCA is also cross certified with the Federal Bridge Certification Authority which provides a trusted path to cross certified Federal Agencies, commercial venders, states governments and other bridges.
Impact to Mozilla Users	Having the Federal Common Policy CA as a trust anchor in Mozilla browsers would enable relying parties to trust U.S. Federal Government websites and other credentials.
CA Contact Information	Email Contact: darlene.gore@gsa.gov, wendy.brown@pgs.protiviti.com Phone Number: 703-306-6109, 703-299-4705 Title: Federal PKI Management Authority Program Manager, FPKI MA Technical Liaison

Technical information about each root certificate

Certificate Name	Federal Common Policy CA
Certificate Issuer Field	CN = Federal Common Policy CA, OU = FPKI, O = U.S. Government, C = US
Certificate Summary	This is the root certificate for the U.S. Federal Common Policy Framework Certificate Authority.
Root Cert URL	http://http.fpki.gov/fcpca/fcpca.crt
SHA1 Fingerprint	90:5F:94:2F:D9:F2:8F:67:9B:37:81:80:FD:4F:84:63:47:F6:45:C1
Valid From	2010-12-01
Valid To	2030-12-01
Certificate Version	V3
Cert Signature Algorithm	SHA-256
Signing key parameters	RSA 2048
Test Website URL (SSL)	https://http.icam.pgs-lab.com
CRL URL	http://http.fpki.gov/fcpca/fcpca.crl LDAP In end-entity cert for the test website. CP section 4.9.7: CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every 18 hours, and the nextUpdate time in the CRL may be no later than 48 hours after issuance time (i.e., the thisUpdate time). For legacy Federal PKIs only, the nextUpdate time in the CRL may be no later than 180 hours after issuance time (i.e., the thisUpdate time).

OCSP URL	The FPKIMA does not run an OCSP responder for the Common Policy CA itself. AIA Extension in end-entity cert for the test website has OCSP: URI: http://ocsp.managed.entrust.com/OCSP/EMSSSPCAResponder CP section 4.9.9: CAs shall support on-line status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth. Where on-line status checking is supported, status information must be updated and available to relying parties within 18 hours of certificate revocation. Where on-line status checking is supported and a certificate issued under id-fpki-common-High is revoked for key compromise, the status information must be updated and available to relying parties within 6 hours. Since some relying parties cannot accommodate on-line communications, all CAs will be required to support CRLs.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV
EV Policy OID(s)	Not requesting EV enablement at this time.

CA Hierarchy information for each root certificate

CA Hierarchy	This is the root certificate for the U.S. Federal Common Policy Framework Certificate Authority (FCPCA). The FCPCA only issues certificates to subordinate CAs. The sub-CAs are operated by the Shared Service Providers (SSPs). End-entity certificates may be issued to Federal employees, contractors, affiliated personnel, and devices operated by or on behalf of Federal agencies. The list of certified SSPs is provided on the FPKIPA website, and includes VeriSign/Symantec, Cybertrust/Verizon, Operational Research Consultants, Department of the Treasury, Entrust, and the U.S. Government Printing Office.
Externally Operated SubCAs	All subCAs are publicly disclosed and separately audited, with the audit letters reviewed by the FPKIPA. http://www.idmanagement.gov/pages.cfm/page/Federal-PKI All CAs issuing certificates subordinate to the Federal Common Policy CA must adhere to the X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, which can be found here: http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf Certified PKI Shared Service Providers (SSP): http://www.idmanagement.gov/pages.cfm/page/Federal-PKI-Policy-Authority-Shared-Service-Provider-Working-Group-Certified-PKI-Shared-Service-Prov Entities cross-certified with FBCA: http://www.idmanagement.gov/pages.cfm/page/Federal-PKI-Management-Authority-entities-crosscertified-with-the-FBCA

	http://fpkiapps.icam.pgs-lab.com/fbcaApps shows the output of a tool that crawls the public repositories starting from the Federal Common Policy CA root certificate and finds all CA certificates with a valid path back through the AIAs. All PKIs participating in the Federal PKI must provide a copy of their annual audit letter to the Federal PKI Policy Authority. Regarding the CA:Subordinate Checklist: 1) The Federal Common Policy CA is the trust anchor for the Common Policy CP – its only "subordinate" CAs are the Shared Service Provider (SSP) CAs which are under contract to GSA to provide PKI services which follow the Common Policy CP. These subordinate CAs could be considered Third-Party as they are independently run by other organizations, but they do not issue certificates to the general public. They are restricted to issuing certificates to Federal employees, federal devices and contractors approved by the Federal agency the contractor supports. 2) Although in a sense these might be considered Private or Enterprise CAs as they are restricted in who they can issue subscriber certificates to, the reason we want the Federal Common Policy CA in the Mozilla trust store is because these subscriber certificates may be encountered by a typical Mozilla user doing business with the US Federal government. 3) The SSP CAs are all required to undergo independent third party audits on an annual basis. And we disclose the CAs – they are all listed on the idmanagement.gov site, as well as in our publicly available repositories available via both LDAP and HTTP. 4) The cross-certified CAs are not sub-CAs of Common Policy. However, they also are required to undergo independent third party audits on an annual basis and are also disclosed both on idmanagement.gov and in our same publicly accessible repositories. Publication of CA information in the Entity repositories is a local decision. Shared Service Provider Roadmap: http://www.idmanagement.gov/fpkipa/documents/SSProadmap.pdf This Shared Service Provider Roadmap is intended to identify the background information, phases, and activities related to the selection process for prospective PKI shared service providers. This document identifies the process by which a vendor qualifies for inclusion on the Certified PKI SSP List. It also describes requirements that must be met to maintain certification, as well as contracting considerations. CP section 1.1.2: This CP states what assurance can be placed in a certificate issued by the CA. The certification practice statement (CPS) states how the CA establishes that assurance. Each CA that issues certificates under this CP shall have a corresponding CPS. CP section 1.1.3: This CP applies to certificates issued to CAs, devices, and Federal employees, contractors and other affiliated personnel.
Cross-Signing	Federal Legacy CAs are cross-certified with the FCPCA or the FBCA. CP Section 1.1.4: Except for legacy Federal PKIs, interoperation with CAs that issue under different policies will be achieved through policy mapping and cross-certification through the Federal Bridge Certification Authority. Legacy Federal PKIs may perform policy mapping and cross- certification with either the Common Policy Root CA or Federal Bridge Certification Authority at their discretion.

Verification Policies and Practices

Policy Documentation	All documents are in English. Repository: http://www.idmanagement.gov/pages.cfm/page/Federal-PKI-Policy-Authority-documentation CP: http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf CPS: http://www.idmanagement.gov/fpkipa/documents/FPKI_CPS_v4_1_Redacted_final_20120515.pdf
Audits	Audit Requirements: http://www.idmanagement.gov/fpkipa/documents/FPKI_Compliance_Audit_Requirements.doc This document provides detailed guidance regarding requirements for performing and reporting annual compliance audits. It incorporates guidance developed by the Audit Working Group (AWG) for performing audits based on a three year cycle, with an initial compliance audit that includes a full audit of all mandatory criteria and subsequent compliance audits that require a review of the previous year's discrepancies, evaluation of modifications and changes made over the last year, core criteria and triennial criteria. Audit Type: ISO 21188:2006 Auditor: Slandala, and U. S. General Services Administration Office of General Counsel Auditor Website: http://slandala.com Audit of audit: http://www.idmanagement.gov/fpkima/documents/FPKI-audit-rev2-2012-jec-signed.pdf (2012.02.28) The ISO document says: Control objectives in the areas of CA environmental controls, CA key life cycle management controls, and certificate life cycle management controls are presented in 7.2 to 7.6, representing baseline control criteria with which a CA shall comply and against which a CA may be evaluated or audited. Such an evaluation may take the form of an internal audit or external audit using any appropriate audit methodology as may be defined by the rules of the contractual environment. The FPKI Compliance Audit Requirements also do not specify a particular audit methodology that must be used but requires that an annual audit takes place, that it is done by a qualified independent auditor, who ensured the CPS conforms to the CP and that operational practices conform to the CPS. See Appendices C & D of http://www.idmanagement.gov/fpkipa/documents/FPKI_Compliance_Audit_Requirements.doc for what the CPWG reviews for all audit letters we receive from the FPKI SSP and Affiliates. The CP that is used for the annual audit of the Federal Common Policy and all subordinate CAs is the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. All the cross-certified affiliates of the FBCA are audited against their own CP which has been mapped to the FBCA CP. Both of these are fully conformant CPs in RFC 3647 format so adhere to the controls specified in section 7 and the tables in section 8 of the ISO standard. in section 8 of the CommonPolicy.pdf (CP) it says: "This specification does not impose a requirement for any particular assessment methodology."

	Comment: This is just meant to say that we will accept any method of doing the audit as long as the audit meets the requirements in our audit guidance – ie the Audit Letter submitted clearly states the qualifications of the auditor, what was covered in the audit, that they checked the CPS against the CP and operations against the CPS – all the things specified in the "cookbook" of appendix c & d. So we will accept a WebTrust audit if they do the extra steps that we require, or as Jimmy did for us a "requirements decompositon", or an eValid8, etc. Comment: "It actually means the auditor can choose to use webtrust or the ETSI audit or any other audit style as long as it meets the FPKI requirements which are detailed here: http://www.idmanagement.gov/fpkipa/documents/FPKI_Compliance_Audit_Requirements.doc In the past John Cornell, the GSA attorney who reviews audit letters on behalf of the FPKI, has stated that a vanilla webtrust audit was not sufficient for us because it didn't clearly require that the CPS had been audited for conformance with the CP and the operations were audited against the CPS. I'm not sure if that is still the case with Webtrust 2.0. Mr. Jung states the methodology he used was: - performing a direct CP-to-CPS traceability analysis - The operations of the Federal PKI systems were evaluated for conformance to the FPKI responsibilities identified in the MOA established between the Federal PKI Policy Authority and other Entities for Cross-Certifying. - The Federal PKI audit was performed using a requirements decomposition methodology Comment: The Triennial allows for a rolling annual audit – that after the first complete audit they start rolling thru so the core requirements are audited every year, as well as any changes made during the year, and a third of the other controls so all controls are audited in a 3-year cycle. This becomes more of a continuous monitoring type of audit – but the details are spelled out in the document I sent. If someone chooses to do the full audit every year that is acceptable as well.
SSL Verification Procedures	All certificates are manually processed. CP section 1.3.4 Subscribers … For this policy, subscribers are limited to Federal employees, contractors, affiliated personnel, and devices operated by or on behalf of Federal agencies. CP section 4.1. CERTIFICATE APPLICATION The Certificate application process must provide sufficient information to: Establish the applicant's authorization (by the employing or sponsoring agency) to obtain a certificate. (per section 3.2.3) Establish and record identity of the applicant. (per section 3.2.3) Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per section 3.2.1) Verify any role or authorization information requested for inclusion in the certificate. These steps may be performed in any order that is convenient for the PKI Authorities and applicants that does not defeat security, but all must be completed before certificate issuance.

	CP section 3.2.4: "Information that is not verified shall not be included in certificates." Comment: This would apply both to domain names in SSL certs (which we call device certs and they require human sponsors who are responsible for providing registration information which includes the DNS name (from 3.2.3.2 Authentication of Devices), and email addresses in certificates issued to individual users. Comment #12: Every device issued a certificate under the Common Policy CP must have a sponsor. The sponsor is authenticated including their authorization for the device. And again all information included in certificates must be verified. The CPS for the issuing CA will specify how that verification takes place. CP section 1.2 lists the defined Policy OIDs. Certificates issued under the Common Policy CP contain a registered certificate policy object identifier (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose. This CP applies only to CAs owned by or operated on behalf of the Federal government that issue certificates according to this policy. CP section 3.2.3.2: Some computing and communications devices (routers, firewalls, servers, etc.) and software applications 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: - Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name - Equipment or software application public keys - Equipment or software application 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. The identity of the sponsor shall be authenticated by: - 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 3.2.3.1.
Organization Verification Procedures	In-person identification of human subscribers is required. CP section 3.2.2: Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, an authority for 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. See CP section 3.2.3 for details about authentication of individual identity. CP section 3.2.5: Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the individual's authority to act in the name of the organization. For pseudonymous certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

Email Address Verification Procedures	CP section 3.2.3.1: The RA shall ensure that the applicant's identity information is verified. Identity shall be verified no more than 30 days before initial certificate issuance. At id-fpki-common-High, the applicant shall appear at the RA in person. For all other policies, RAs may accept authentication of an applicant's identity attested to and documented by a trusted agent to support identity proofing of remote applicants, assuming agency identity badging requirements are otherwise satisfied. 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), below. 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. 2) Verify Applicant's employment through use of official agency records. 3) Establish applicant's identity by in-person proofing before the registration authority, based on either of the following processes: a) Process #1: 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. b) Process #2: 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 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 on-line; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.
Code Signing Subscriber Verification Procedures	See CP section 3.2.
Multi-factor Authentication	Multi-factor authentication is required for all accounts capable of directly causing certificate issuance. CP section 6.4.2 and 6.5.
Network Security	CP section 6.5, 6.6, 6.7.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes, see above urls.
CA Hierarchy	The FCPCA only issues certificates to subordinate CAs. The sub-CAs are operated by the Shared Service Providers (SSPs). End-entity certificates may be issued to Federal employees, contractors, affiliated personnel, and devices operated by or on behalf of Federal agencies. The list of certified SSPs is provided on the FPKIPA website. See above.
Audit Criteria	See above.
Document Handling of IDNs in CP/CPS	The FCPCA is the root for the US Federal Government; therefore, CAs supporting the Common Policy CA will not be issuing any certificates with IDNs.
Revocation of Compromised Certificates	A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are: • 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.
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate	See above.
Subscriber	See information above for authentication of Human subscribers.
DNS names go in SAN	Certificates issued under id-fpki-common-authentication shall include a subject alternative name. At a minimum, the subject alternative name extension shall include the pivFASC-N name type [FIPS 201-1]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth may also include a UUID [RFC 4122] in the subject alternative name extension, if the UUID is included as specified in Section 3.3 of [SP 800-73-3(1)]. Certificates issued under id-fpki-common-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field.
Domain owned by a Natural Person	The FCPCA is the root for the US Federal Government, as such CAs supporting the Common Policy CA will not be issuing any certificates to domains owned by a natural person.
OCSP	CAs shall support on-line status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV.
Wildcard DV SSL certificates	SSL certs are OV.
Email Address Prefixes for DV Certs	SSL certs are OV.
Delegation of Domain / Email validation to third parties	CP section 1.3.2: The registration authorities (RAs) collect and verify each subscriber's identity and information that is to be entered into the subscriber's public key certificate. The RA performs its function in accordance with a CPS approved by the FPKIPA. The RA is responsible for: The identification and authentication process. CP section 1.3.3: The trusted agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., photographs) on presented credentials for applicants who cannot appear in person at an RA. The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness. CP section 1.5.4: CAs issuing under this policy are required to meet all facets of the policy. The FPKIPA will not issue waivers. The FPKIPA shall make the determination that a CPS complies with this policy. The CA and RA must meet all requirements of an approved CPS before commencing operations. In some cases, the FPKIPA may require the additional approval of an authorized agency. The FPKIPA will make this determination based on the nature of the system function, the type of communications, or the operating environment. In each case, the determination of suitability shall be based on an independent compliance auditor's results and recommendations. See section 8 for further details. CP section 8: CAs operating under this policy shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced. For the Common Policy Root CA, the FPKI Management Authority shall have a compliance audit mechanism in place to ensure that the requirements of this CP are being implemented and enforced by its CPS. CP section 8.1: CAs and RAs operating under this policy shall be subject to a periodic compliance audit at least once per year. As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document located at http://www.idmanagement.gov/fpkipa/. Further, the Federal PKI Policy Authority has the right to require aperiodic compliance audits of CAs operating under this policy. The Federal PKI Policy Authority shall state the reason for any aperiodic compliance audit. CP section 9.6.1: CA Representations and Warranties CP section 9.6.2: RA Representations and Warranties CPS section 3.2: Entity registration, identity validation, authentication of organization identity, validation

	of authority, criteria for interoperation. CPS section 5.3.3: All personnel performing duties with respect to the operation of the FPKI Trust Infrastructure receive comprehensive training. Training (including On-The-Job-Training (OJT) and review of procedures) is conducted in the following areas by product engineers: - CA/RA security principles and mechanisms; - All PKI software versions in use for the FPKI Trust Infrastructure CAs; - All PKI duties they are expected to perform; and - Disaster recovery and business continuity procedures. Training in the overall security procedures of the FPKI Trust Infrastructure is conducted for all personnel at the initial full-operation capability of the FPKI Trust Infrastructure. When a person is assigned to a new FPKI Trusted Role, they receive training in all the operational duties for that role; including a period of shadowing another in that role and then a period of reverse shadowing. In addition, training and review of security procedures is conducted at the time a change in procedures occurs and/or annually. Personnel are required to sign acknowledgements that they have received this training. All personnel training records are maintained by the ISSO CPS section 5.8: CA or RA Termination CPS section 8.1: The FPKIMA will arrange, initially and annually, for independent inspections and compliance audits to validate that the FPKI Trust Infrastructure CAs are operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit will be provided to the FPKIPA in the form of an Auditor Letter of Compliance that follows the FPKIPA Audit Letter Guidelines. As an alternative to a full annual compliance audit against the entire CPS, the compliance audit of CAs and RAs may be carried out in accordance with the requirements as specified in the Triennial Audit Guidance document which state after an initial compliance audit, subsequent compliance audits require review of previous year's discrepancies, evaluation of modifications and changes made over the last year, core criteria and triennial criteria.
Issuing end entity certificates directly from roots	The FCPCA is the root CA and it does not issue end-entity certificates. All end entity certificates are issued from subordinate SSP CAs or Federal Legacy CAs cross-certified with the FCPCA or the FBCA.
Allowing external entities to operate subordinate CAs	Only CAs operated by approved SSPs or legacy Federal Agencies are permitted to assert the certificate policies of the FCPCA CP.
Distributing generated private keys in PKCS#12 files	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: • 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(s) 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. o For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it. o 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. The CA must maintain a record of the subscriber acknowledgment of receipt of the token.
Certificates referencing hostnames or private IP addresses	Not applicable.
Issuing SSL Certificates for Internal Domains	Not applicable.
OCSP Responses signed by a certificate under a different root	Only OCSP responders that are an authoritative source for certificates are covered under the Common Policy CP. See section 7.3 for the OCSP profile.
CRL with critical CIDP Extension	At this time, the FCPCA CRLs will not contain an IDP extension.
Generic names for CAs	The Distinguished Name of CAs operating under the FCPCA CP must be meaningful.
Lack of Communication With End Users	A subscriber (or human sponsor for device certificates) shall be required to sign a document containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. Details in 9.6.3 of FCPCA CP.