Print this page

Mozilla - CA Program

Case Information

Case Number	00000048	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	U.S. Federal Public Key Infrastructure (US FPKI)	**Request Status**	Need Information from CA

Additional Case Information

Subject	New Owner/Root inclusion requested	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=478418

General information about CA's associated organization

Company Website	http://www.idmanagement.gov/federal-public-key-infrastructure	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	U.S.A.	**Verified?**	Verified
Primary 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.	**Verified?**	Verified
Impact to Mozilla Users	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. Having the FCPCA as a trust anchor in Mozilla browsers would enable relying parties to trust U.S. Federal Government websites and other credentials.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.

CA's Response to Recommended Practices	* 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. * 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. * 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.	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	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 in accordance with the FPKI Compliance Audit Requirements document. 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.	**Verified?**	Verified

CP section 9.6.1: CA Representations and Warranties
CP section 9.6.2: RA Representations and Warranties

Root Case Record # 1

Root Case Information

Root Certificate Name	Federal Common Policy CA	**Root Case No**	R00000065
Request Status	Need Information from CA	**Case Number**	00000048

Additional Root Case Information

Subject	Include Federal Common Policy CA

Technical Information about Root Certificate

O From Issuer Field	U.S. Government	**Verified?**	Verified
OU From Issuer Field	FPKI	**Verified?**	Verified
Certificate Summary	This is the root certificate for the U.S. Federal Common Policy Framework Certificate Authority.	**Verified?**	Verified
Root Certificate Download URL	http://http.fpki.gov/fcpca/fcpca.crt	**Verified?**	Verified
Valid From	2010 Dec 01	**Verified?**	Verified
Valid To	2030 Dec 01	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	NEED: URL to website whose SSL cert chain up to this root.	**Verified?**	Need Response From CA
CRL URL(s)	http://http.fpki.gov/fcpca/fcpca.crl CP section 4.9.7: for subscriber certs nextUpdate may be no later than 48 hours... SSP CRL requirements: http://www.idmanagement.gov/sites/default/files/documents/CertCRLprofileForCP.pdf	**Verified?**	Verified
OCSP URL(s)	The FPKIMA does not run an OCSP responder for the Common Policy CA itself. 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.	**Verified?**	Verified

Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	Mozilla plans to constrain this CA hierarchy, because of the size and complexity of the hierarchy (i.e. FBCA). NEED: Please confirm the list of domains to constrain this hierarchy to. Comment #36 and #46: *gov.us, *.gov, *.mil (CP section 3.1.1)	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	90:5F:94:2F:D9:F2:8F:67:9B:37:81:80:FD:4F:84:63:47:F6:45:C1	**Verified?**	Verified
SHA-256 Fingerprint	89:4E:BC:0B:23:DA:2A:50:C0:18:6B:7F:8F:25:EF:1F:6B:29:35:AF:32:A9:45:84:EF:80:AA:F8:77:A3:A0:6E	**Verified?**	Verified

CA Hierarchy Information

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. NEED: URL to the list of SSPs.	**Verified?**	Need Response From CA
Externally Operated SubCAs	See: https://wiki.mozilla.org/CA:SubordinateCA_checklist#CA_Policies_about_Third-Party_Subordinate_CAs 1. General: http://www.idmanagement.gov/pki-shared-service-provider-working-group 2. Selection criteria: http://www.idmanagement.gov/sites/default/files/documents/SSProadmap.pdf 3. CP/CPS that the SSPs are required to follow: http://www.idmanagement.gov/sites/default/files/documents/FCPCA%20CP%20v1%2023_0.pdf 4. Mozilla plans to constrain full hierarchy (see above) 5. NEED: Requirements (documented in the CP or CPS) for sub-CAs to take reasonable measures to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, NOTE: Since we are constraining the hierarchy, may not require this.	**Verified?**	Need Response From CA

	6. Audit Requirements for SSPs http://www.idmanagement.gov/sites/default/files/documents/AuditStandards.pdf http://www.idmanagement.gov/sites/default/files/documents/audit_guidance.pdf		
Cross Signing	Federal Legacy CAs are cross-certified with the FCPCA or the FBCA. CP section 1.1.4	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Mozilla plans to constrain full hierarchy (see above) RA Requirements: http://www.idmanagement.gov/sites/default/files/documents/RArequirements.pdf	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	All documents are in English. http://www.idmanagement.gov/federal-public-key-infrastructure-policy-authority http://www.idmanagement.gov/pki-shared-service-provider-working-group	**Verified?**	Verified
CA Document Repository	http://www.idmanagement.gov/federal-public-key-infrastructure-policy-authority	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.idmanagement.gov/sites/default/files/documents/FCPCA%20CP%20v1%2023_0.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	Each SSP has their own CPS.	**Verified?**	Not Applicable
Other Relevant Documents	CP section 1.1: 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. NEED: URL to published list of the SSPs and their CPS documents.	**Verified?**	Need Response From CA
Auditor Name		**Verified?**	Need Response From CA
Auditor Website		**Verified?**	Need Response From CA
Auditor Qualifications		**Verified?**	Need Response From CA
Standard Audit	NEED: URL to list of SSPs and their Current audit statement(s) NEED: Audit statement regarding the root.	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: URL to the SSPs that can issue SSL certs, and their BR audit statement(s) Please see https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA

BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED: See Baseline Requirements section 8.3	**Verified?**	Need Response From CA
SSL Verification Procedures	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 request for inclusion in the certificate. CP section 3.2.3.2: Authentication of Devices In such cases, the device must have a human sponsor. The sponsor is responsible for providing the following registration inforamtion: - Equipment identification (e.g. serial number) or service name (.e.g., DNS name) ... These certificates shall be issued only to authorized devices under the subscribing organization's control. The CPS shall describe procedures to ensure that certificate accountability is maintained. CP section 4.3.1: Upon receiving the request, the CAs/RAs will... The responsibility for verifying prospective subscriber data shall be described in the CA's CPS. ** Note: this is another reason Mozilla plans to constrain this CA hierarchy. The CP doesn't meet our usual requirements of the CA stating the steps each subCA must take to confirm that each certificate subscriber owns/controls the domain name to be included in the cert.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	CP section 3.2.3.1: Authentication of Human Subscribers At a minimum, authentication procedures for employees must included 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	**Verified?**	Verified

	in-person proofing before the registration authority, based on either of the following processes: ... For contractors and other affiliated personnel, the authentication procedures must include the following steps: ...		
Email Address Verification Procedures	Note: The CP doesn't meet our usual requirements of the CA stating the steps each subCA must take to confirm that each certificate subscriber owns/controls the email address to be included in the cert. This may be OK due to how Mozilla plans to constrain this CA hierarchy.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	CP section 3.2.5: Validation of Authority 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. CP section 4.1.1.4: An application for a code signing certificate shall be submitted by an authorized representative of the organization.	**Verified?**	Verified
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.	**Verified?**	Verified
Network Security	CP section 6.5, 6.6, 6.7.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED: URL to publicly disclosed subCAs, included their CP/CPS documents and their annual audit statements.	**Verified?**	Need Response From CA