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 (PKI) Management Authority operates the Federal Common Policy Framework Certification Authority (FCPCA) on behalf of the Federal PKI Policy Authority. The FCPF CA 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: cheryl.jenkins@gsa.gov, wendy.brown@pgs.protiviti.com Phone Number: 202-577-1441, 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
Certificate Signature Algorithm	SHA-256
Signing key parameters	RSA 2048
Test Website URL (SSL)	https://http.icam.pgs-lab.com/ I imported the new root certificate into my Firefox browser, and then tried to browse to the test website. I got following error: An error occurred during a connection to http.icam.pgs-lab.com. SSL peer cannot verify your certificate. (Error code: ssl_error_bad_cert_alert)
CRL URL	URL

	CP section 4.9.7: CAs operating as part of the Shared Service Providers program that only issue certificates to CAs and that operate off-line must issue CRLs at least once every 24 hours, and the nextUpdate time in the CRL may be no later than 48 hours after issuance time (i.e., the thisUpdate time). … 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).
OCSP URL	OCSP URI 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	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, Cybertrust, Operational Research Consultants, Department of the Treasury, Entrust, and the U.S. Government Printing Office.
Externally Operated SubCAs	List of Certified PKI Shared Service Providers: http://www.idmanagement.gov/fpkipa/cpl.cfm Includes SSP organization names and the Security Accreditation 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.

	Auditor Letter of Compliance, Compliance Audit Requirements: http://www.idmanagement.gov/fpkipa/documents/audit_guidance.pdf These requirements apply to all cross-certified entities under the FBCA CP or through the Common Policy (other than the C4CA). Compliance Audit Requirements: http://www.idmanagement.gov/fpkipa/documents/TriennialAnnualAuditGuidance.pdf This document represents the Audit Working Group (AWG) recommendations for annual compliance audit requirements. CP section 4.9.7: CAs operating as part of the Shared Service Providers program that only issue certificates to CAs… What restrictions are placed on sub-CAs? E.g. Are sub-CAs constrained to issue certificates only within certain domains? What sort of sub-CAs can they sign?
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. CP: http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf CPS: http://www.idmanagement.gov/fpkipa/documents/FPKIA_CPS.pdf
Audits	Audit Type: eValidated Methodology (Equivalent to WebTrust CA?) We require that the audit criteria be one or more of the following three, or equivalent. Please indicate which of these audit criteria are encompassed in the eValidated Methodology. ETSI TS 101 456 ETSI TS 102 042 WebTrust Principles and Criteria for Certification Authorities Auditor: Brian Dilley of eValid8, and GSA Office of General Counsel Auditor Website: http://www.evalid8.com/ Evaluation of FPKIMA CA Day Zero Audit: http://www.idmanagement.gov/fpkima/documents/FPKIMA_day_zero_audit.pdf (2010.11.05)
SSL Verification Procedures	Certificates issued under this 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. See section 1.2 of the CP for the list of Policy OIDs defined.

	All device certs must have a human sponsor and both the identity of the human sponsor and the authority of the sponsor to act in the name of the organization is verified. See section 3.2 for details. CP section 3.2.3.2: 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: 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. 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. I see how the identity and authority are verified, but I don't see how the RA confirms that the certificate subscriber owns or controls the domain name to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership
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. 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. 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: … 4) Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution. CP section 3.2.4: Information that is not verified shall not be included in certificates. 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. Practice Note: Examples of signature certificates that assert organizational authority are code signing certificates and FIPS 201 id-PIV-content-signing certificates.
Email Address Verification Procedures	Are you also requesting to enable the Email trust bit? If yes, how does the RA confirm that the certificate subscriber owns/controls the email address to be included in the certificate? Where is this documented? According to the information that you provided below, I see that the identity of the certificate subscriber is verified. But I don't see how the ownership/control of the email address is verified.
Code Signing Subscriber Verification Procedures	See CP section 3.2, and snippets copied above for Organization Verification Procedures. Some subordinate or cross-certified CAs may issue code signing certificates. The Common Policy CP treats these as device certificates and requires verification of the identity of the human sponsor and their authority to act in the name of the organization. The CPS of the issuing CA will have additional requirements.

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

Publicly Available CP and CPS	http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf
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, and includes VeriSign, Cybertrust, Operational Research Consultants, Department of the Treasury, Entrust, and the U.S. Government Printing Office.
Audit Criteria	In addition to the audit requirements stated in the CP, the following documents provide additional guidance. http://www.idmanagement.gov/fpkipa/documents/audit_guidance.pdf http://www.idmanagement.gov/fpkipa/documents/TriennialAnnualAuditGuidance.pdf
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	All device certificates 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) • 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.

	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.
Verifying Email Address Control	All information in certificates is verified. Human subscribers are authenticated no more than 30 days before initial certificate issuance. 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. 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).
Verifying Identity of Code Signing Certificate	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.
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	See information about sub-CAs above, and CP section 9.6.1 (CA Representations and Warranties). RA's are used. See CP sections 1.3.2, 1.5.4 (The CA and RA must meet all requirements of an approved CPS before commencing operations.), 3.2, 5.1.2.2, 5.3.3 (training), 5.8 (termination), and 9.6.2 (RA Representations and Warranties).
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	If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply. 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.