Bugzilla ID: 478418
Bugzilla Summary: Please add US FPKI Common Policy CA certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	US FPKI
Website URL	http://www.cio.gov/fpkipa
Organizational type	National Government CA
Primary market / customer base	The United States Federal Public Key Infrastructure (FPKI) Policy Authority is an interagency body set up under the CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.
CA Contact Information	CA Email Alias: judith.spencer@gsa.gov An email alias is requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. CA Phone Number: 202-208-6576 A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. Title / Department: Chair of the Federal PKI Policy Authority If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	Common Policy - U.S. Government
Certificate Subject	CN = Common Policy OU = FBCA O = U.S. Government
Cert summary / comments	This is the root certificate for the U.S. Federal Common Policy Framework Certificate Authority.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=408655 http://fpkia.gsa.gov/CommonPolicy/CommonPolicy.crt
SHA-1 fingerprint.	cb:44:a0:97:85:7c:45:fa:18:7e:d9:52:08:6c:b9:84:1f:2d:51:b5
Valid from	10/15/2007
Valid to	10/15/2027
Cert Version	3
Modulus length / key length	2048

Test Website	For testing purposes, please provide a URL to a website whose SSL cert chains up to this root. Note that this can either be a live site or a test site.
CRL	Certificates issued from the root can be verified at the following URL: ldap://fpkia.gsa.gov/cn=Common%20Policy,ou=FBCA,o=U.S.%20Government,c=US Please provide a url to the non-ldap-based CRL for end-entity certs chaining up to this root. 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 Responder URL	OCSP may be provided by the sub-CAs 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.
CA Hierarchy	Is the following correct? The Common Policy root certificate is offline and does not sign end-entity certificates directly. It signs subordinate CAs for Shared Service Providers (SSP). The sub-CAs are operated by the 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 FPKI website, and includes VeriSign, Cybertrust, Operational Research Consultants, Department of the Treasury, Entrust, and the U.S. Government Printing Office.
Sub-CAs operated by third parties	Please see https://wiki.mozilla.org/CA:SubordinateCA_checklist, and provide the corresponding information. If the SSPs can only issue end-entity certs to Government-related entities that have been pre-qualified in some way, then I think only the top section need apply. However, if the SSPs can issue end-entity certs to non-government-related entities and truly act as a generic Certificate Service Provider, then the information listed in the second section will need to be provided for all of the SSPs. In either case, the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices) will need to be reviewed on behalf of each SSP, especially in regards to • OCSP Responses signed by a certificate under a different root • CRL with critical CIDP Extension

	Certified PKI Shared Service Providers (SSP) List: http://www.idmanagement.gov/fpkipa/cpl.cfm Shared Service Provider Roadmap: Navigating the Process to Acceptance http://www.idmanagement.gov/fpkipa/documents/SSProadmap.pdf SSP Roadmap Section 3.1: Navigating the Process to Acceptance requires Shared Service Providers to generate key pairs in a trustworthy system. The federal government verifies that key pairs are generated in a trustworthy system through certification and accreditation process – See Section 4.4.2. SSP Roadmap Section 3.2: the Shared Service Provider is required to have a third party auditor warrant that their information and representations with the FCPF CA are true. This information is forwarded to the federal government as part of the certification and accreditation package. CPS Evaluation Matrix For Evaluation Against the Requirements for the Common Policy Framework http://www.idmanagement.gov/fpkipa/documents/CPSmatrix.doc Part of the third party compliance audit required by the SSP Roadmap includes the completion of this Evaluation Mapping Matrix by documenting the text in the SSP CPS that addresses each of the mapping tables herein. The SSPWG reviews the completed Mapping Matrix and makes a determination as to whether the SSP's practices meet the requirements of the Federal PKI Common Policy Framework. The purposes of this CPS Evaluation Mapping Matrix are to: 1) Identify at a high-level the areas of inconsistency and/or similarity between the contents of the SSP CPS and the Common Policy [COMMON], 2) Recommend appropriate changes, if required, to the SSP CPS that would make it more consistent with the [COMMON], and 3) Ensure consistent audits by qualified third parties.
Cross-signing	Is this root involved in cross-signing with any other root?
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type DV, OV, and/or EV	OV
EV policy OID(s)	Not Requesting EV

CP/CPS	X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework: http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf 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. Public X.509 U.S. Federal PKI Architecture Certification Practice Statement: http://www.idmanagement.gov/fpkipa/documents/FPKIA_CPS.pdf Scroll down to Part 2: X.509 Certification Practice Statement (CPS) For the Federal Public Key Infrastructure Common Policy Framework (FCPF) Certification Authority CP Section 2.2.2: The CPS for the Common Policy Root CA will not be published; a redacted version of this CPS will be publicly available from the FPKIA website (see http://www.cio.gov/fpkia). Practice Note: There is no requirement for the publication of CPSs of other CAs that issue certificates under this policy.
AUDIT	Please see sections 8, 9, and 10 of the Mozilla CA Policy athttp://www.mozilla.org/projects/security/certs/policy/ in regards to the audit requirements. A security review of the FCPF CA operations was conducted in accordance with Office of Management and Budget (OMB) A-130 Circular, Appendix III; Federal Information Security Act; NIST publications such as FIPS 199, FIPS 200, and Special Publications 800-30, 800-37, 800-39, 800-53, and 800-53A; GSA IT Security Policy Manual P2100.1D. The Letter of Authorization to Operate can be found at: http://www.cio.gov/fpkia/documents/FPKIAato.pdf
Organization Identity Verification	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. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. CP section 4.1: 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 4.3.1: Upon receiving the request, the CAs/RAs will— • Verify the identity of the requester. • Verify the authority of the requester 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 after confirming that the subscriber has formally acknowledged their obligations as described in section 9.6.3. 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. 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.
Domain Name Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Please point me to the section(s) of the CP/CPS that explain how the RA/CA must verify the ownership/control of the domain name.
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; Please point me to the section(s) of the CP/CPS that explain how the RA/CA must verify the ownership/control of the domain name.
Identity of Code Signing Subscriber	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; Please point me to the section(s) of the CP/CPS that explain the verification procedures for Code Signing certificates.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information. • Long-lived DV certificates o • Wildcard DV SSL certificates

	o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs o