Bugzilla ID: 870185
Bugzilla Summary: Add Renewed Japanese Government Application CA Root 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	Japanese Government Public Key Infrastructure (GPKI) Ministry of Internal Affairs and Communications
Website URL	http://www.gpki.go.jp, http://www.gpki.go.jp/documents/gpki.html -- about GPKI (Japanese only)
Organizational type	National Government
Primark Market / Customer Base	In Japan, there are two root CAs, one is GPKI and the other one is LGPKI (Local government public Key Infrastructure). GPKI is controlled by the Ministry of Internal Affairs/Communications and National Information Security Center, and it is separate from Local government sectors. The Japanese government decided to centralize to GPKI from each of the ministry's certification system and it has finished migration on Oct, 2008.
CA Contact Information	CA Email Alias: apca@gpki.go.jp CA Phone Number: Title / Department:

Technical information about each root certificate

Certificate Name	Japanese Government ApplicationCA2 Root
Certificate Issuer Field	CN = ApplicationCA2 Root OU = GPKI O = Japanese Government C = JP
Certificate Summary	This new root certificate has been created in order to comply with the Baseline Requirements, and will eventually replace the "ApplicationCA - Japanese Government" root certificate that was included via Bugzilla Bug #474706. This new root has one internally-operated subordinate CA.
Root Cert URL	https://www.gpki.go.jp/apcaself/APCA2root.der
SHA1 Fingerprint	F0:0F:C3:7D:6A:1C:92:61:FB:6B:C1:C2:18:49:8C:5A:A4:DC:51:FB
Valid From	2013-03-12
Valid To	2033-03-12
Certificate Version	3
Cert Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Signing key parameters	RSA modulus length; e.g. 2048 or 4096 bits. Or ECC named curve, e.g. NIST Curve P-256, P-384, or P-512.
Test Website URL	Please provide the URL to a test website whose webserver certificate chains up to this root cert.
CRL URL	http://dir.gpki.go.jp/ApplicationCA2Root.crl SubCA CPS section 4.9.7: The CRL of 48-hour validity period is issued at intervals of 24 hours.

OCSP URL (Required now)	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses Testing results a) Browsing to test website with OCSP enforced in Firefox browser b) If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version BR #13.2.2: "The CA SHALL update information provided via an Online Certificate Status Protocol..." BR Appendix B regarding authorityInformationAccess in Subordinate CA Certificate and Subscriber Certificate: "With the exception of stapling .... this extension MUST be present ... and it MUST contain the HTTP URL of the Issuing CA's OCSP responder"
Requested Trust Bits	Websites (SSL/TLS) Code Signing
SSL Validation Type	DV and OV
EV Policy OID(s)	Not applicable. Not requesting EV treatment.
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ... - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."

CA Hierarchy information for each root certificate

CA Hierarchy	This root certificate has one internally-operated subordinate CA that issues end-entity certificates for SSL and code signing.
Externally Operated SubCAs	None
Cross-Signing	None
Technical Constraints on Third-party Issuers	Can LRAs issue SSL certificates? What technical constraints are in place to restrict the types of certificates and domains that LRAs can issue certs for? CPS section 1.6: - LRA (Local Registration Authority) A Registration Authority with responsibility for a local community. This organization be established in the unit of office and ministry. This organization accepts and reviews applications for issuance, re-key and revocation of certificates from subscribers. - RA (Registration Authority) An agency that handles CA operations pertaining to registration. The main tasks are identity checking for parties to which certificates are issued, the registration of information required for the issuance of certificates, and CSR to CAs.

Verification Policies and Practices

Policy Documentation	CPS (Japanese): http://www.gpki.go.jp/apca/cpcps/index.html Root CA CPS (English): https://bug870185.bugzilla.mozilla.org/attachment.cgi?id=755785 SubCA CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=784715

Audits	Audit Type: WebTrust for CA, and WebTrust Readiness (for this new root cert) Audit Report (Japanese and English): https://cert.webtrust.org/SealFile?seal=1241&file=pdf
Baseline Requirements (SSL)	The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3. (https://www.cabforum.org/documents.html) Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results.
Organization Verification Procedures	SubCA CPS section 3.2.2, Authentication of organization identity As for the application procedure of a server certificate, a code-signing certificate and a document signing certificate, the LRA shall verify the authenticity of the organization to which the subscriber belongs according to comparing with organizations which were written in the application by directory of government officials that the Independent Administrative Agency National Printing Bureau issued. SubCA CPS section 3.2.3, Authentication of individual identity As for the application procedure of a server certificate, a code-signing certificate and a document signing certificate, the LRA shall verify the authenticity of the subscriber according to comparing with name, contact, etc. which were written in the application by directory of government officials that the Independent Administrative Agency National Printing Bureau issued. The LRA also check the intention of an application by a telephone or meeting. SubCA CPS section 3.2.5, Validation of authority The appropriateness of authority is confirmed according to the procedures defined in "3.2.2 Authentication of organization identity" and "3.2.3 Authentication of individual identity". **It is still not clear to me how the RA verifies that the certificate subscriber has the authority to request the certificate on behalf of the organization.**
SSL Verification Procedures	SubCA CPS section 4.1.2, Enrollment process and responsibilities (1) Server certificate The subscriber shall apply accurate information on their certificate applications to the LRA. The LRA shall confirm that the owner of the domain name written as a name(cn) of a server certificate in the application form belongs to Ministries and Agencies who have jurisdiction over LRA, or its related organization with the thirdparty databases and apply accurate information to the Application CA2(Sub). Please update the CPS to clearly indicate the steps that are taken to verify that the certificate subscriber owns/controls the domain name to be included in the certificate. See Baseline Requirement (BR) #11.1.1.
Email Address Verification Procedures	Not applicable. Not requesting the email trust bit.
Code Signing Subscriber Verification Procedures	SubCA CPS section 4.1.2, Enrollment process and responsibilities (2) Code signing certificate The subscriber shall apply accurate information on their certificate applications to the LRA. The LRA shall confirm that the organization name written as a name (cn) of code signing certificate in application

	exists and be organization name of Ministries and Agencies with jurisdiction over LRA or highest administrative agency belonging to Ministries and Agencies in accordance with the organization name in public document and then apply accurate information to the Application CA2(Sub).
Multi-factor Authentication	See BR #16.5 Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

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

Publicly Available CP and CPS	See above.
CA Hierarchy	See above.
Audit Criteria	See above.
Document Handling of IDNs in CP/CPS	?
Revocation of Compromised Certificates	?
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	Not applicable.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	?
Domain owned by a Natural Person	?
OCSP	?

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

Long-lived DV certificates	SubCA CPS section 6.3.2: The public and private keys of the server certificate shall be valid for three years from the date they were validated.
Wildcard DV SSL certificates	Can wildcard SSL certs be issued? If yes, see BR #11.1.3.
Email Address Prefixes for DV Certs	If SSL cert can be issued without organizational validation, then list the acceptable email addresses that are used for domain-verification.
Delegation of Domain / Email validation to third parties	Not applicable. Not requesting the email trust bit.
Issuing end entity certificates directly from roots	no
Allowing external entities to operate subordinate CAs	No. subCAs are internally operated.
Distributing generated private keys in PKCS#12 files	no
Certificates referencing hostnames or private IP addresses	? If applicable, see BR #11.1.2.

Issuing SSL Certificates for Internal Domains	? If applicable, see BR #11.1.4.
OCSP Responses signed by a certificate under a different root	?
CRL with critical CIDP Extension	?
Generic names for CAs	Issuer O=Japanese Government
Lack of Communication With End Users	?