Bugzilla ID: 474706
Bugzilla Summary: Root Inclusion for Japanese Government Application CA

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.

General Information	Data
CA Name	Japanese Government Public Key Infrastructure (GPKI)
Website URL (English version)	http://www.gpki.go.jp http://www.gpki.go.jp/apca/ (Japanese only)
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	National Government
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	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.

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

Info Needed	Data	Status / Notes
Certificate Name	ApplicationCA - Japanese Government Note: No Common Name (CN) in certificate. OU = ApplicationCA O = Japanese Government	COMPLETE
Cert summary / comments	This root is operated by the national government of Japan. It issues server certificates and code signing certificates to national government agencies. This root issues end-entity certificates directly, and does not have any subordinate CAs.	COMPLETE
The root CA certificate URL Download into FireFox and verify	http://www.gpki.go.jp/apcaself/APCAroot.der	COMPLETE

SHA-1 fingerprint.	7F:8A:B0:CF:D0:51:87:6A:66:F3:36:0F:47:C8:8D:8C:D3:35:FC:74	COMPLETE
Valid from	2007-12-12	COMPLETE
Valid to	2017-12-12	COMPLETE
Cert Version	3	COMPLETE
Modulus length / key length	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	http://dir.gpki.go.jp/ApplicationCA.crl CPS Section 4.9.7: The CRL of 48-hour validity period is issued at intervals of 24 hours. However, if an event such as occurrence of a CA private key compromise state, the CRL is issued immediately.	COMPLETE
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation	None	COMPLETE
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	No subordinate CAs	COMPLETE This root CA issues end-entity certs directly.
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and	None	COMPLETE

audited.		
List any other root CAs that have issued cross-signing certificates for this root CA	None	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites From email on 1/22/09 >> Does GPKI also want its certificates to be recognized by Mozilla for >> code signing? Code signing is mentioned in the CPS/CP document. > My understanding is "No, it doesn't ". The team expects just implementation > of the application root into next Firefox version. But I'll ask it to the > counterpart again. OK. Kathleen, for now let's mark this request as for SSL only, until/unless we hear something different.	COMPLETE
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber in addition to verifying the domain name. (This is commonly referred to as an OV certificate.)	OV CPS 3.2.2 Authentication of organization identity As for the application procedure of a Server certificate and code-signing certificate, the LRA shall confirm the authenticity of the organization to which the subscriber belongs according to a prescribed procedure. CPS 3.2.3 Authentication of individual identity As for the application procedure of a Server certificate and code-signing certificate, the LRA shall confirm the authenticity of the subscriber according to a prescribed procedure.	COMPLETE
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV.	https://www.gpki.go.jp/selfcert/finger_print.html	COMPLETE

• Note: mainly interested in SSL, so OK if no email example.		
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	CP/CPS for Japanese Government Public Key Infrastructure (GPKI) In Japanese: http://www.gpki.go.jp/apca/cpcps/index.html In English: https://bugzilla.mozilla.org/attachment.cgi?id=358078	COMPLETE
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org site or elsewhere.)	Audit Type: WebTrust for CA Auditor: Deloitte Touche Tohmatsu Auditor Website URL: http://www.deloitte.com/jp Audit Document URL(s):https://cert.webtrust.org/SealFile?seal=812&file=pdf Japanese only, but the report follows the standard WebTrust format. Reviewed using Google Translate. No issues noted in report. Audit Report Date: 10/22/2008	COMPLETE

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - As per section 7 of http://www.mozilla.org/projects/security/certs/policy/ I need to find text in the CP/CPS that demonstrates that reasonable measures are taken to verify that the domain name is owned/controlled by the subscriber. I was not able to find this.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - Not applicable, not enabling email trust bit.
- Verify identity info in code signing certs is that of subscriber
    - Not applicable, not enabling code signing trust bit.
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices
Please review the potentially problematic practices described at http://wiki.mozilla.org/CA:Problematic_Practices. If any of these are relevant, provide further information.

- 1.1 Long-lived DV certificates
    - The SSL certs are OV.

    - Note: CPS section 1.4.1: “Server certificates shall remain valid for three years from the date on which they take effect.”
- 1.2 Wildcard DV SSL certificates
    - The SSL certs are OV.
- 1.3 Issuing end entity certificates directly from roots
    - Yes. This root issues end entity certificates directly, and not through a subordinate CA.
- 1.4 Allowing external entities to operate unconstrained subordinate CAs
    - No sub-CAs
- 1.5 Distributing generated private keys in PKCS#12 files
    - No, CPS section 6.1.1: “certificate key pairs shall be generated by a subscriber. ”
    - CPS section 6.1.2: “The IA and RA do not deliver a private key to the subscriber.”
- 1.6 Certificates referencing hostnames or private IP addresses
    - Not found.
- 1.7 OCSP Responses signed by a certificate under a different root
    - No OCSP
- 1.8 CRL with critical CIDP Extension
    - CRL downloaded into Firefox successfully.

Verify Audits (COMPLETE)
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
    - Posted on cert.webtrust.org
- For EV CA’s, verify current WebTrust EV Audit done.
    - Not EV
- Review Audit to flag any issues noted in the report
    - No issues noted in report.