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) Ministry of Internal Affairs and Communications
Website URL (English version)	http://www.gpki.go.jp http://www.gpki.go.jp/documents/gpki.html -- about GPKI (Japanese only)
Organizational type.	National Government
Primary 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.

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

Info Needed	Data
Certificate Name	ApplicationCA - Japanese Government Note: No Common Name (CN) in certificate. OU = ApplicationCA O = Japanese Government
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.
The root CA certificate URL	http://www.gpki.go.jp/apcaself/APCAroot.der
SHA-1 fingerprint.	7F:8A:B0:CF:D0:51:87:6A:66:F3:36:0F:47:C8:8D:8C:D3:35:FC:74
Valid from	2007-12-12
Valid to	2017-12-12
Cert Version	3

Modulus length / key length	2048
Test Website	https://www.gpki.go.jp/selfcert/finger_print.html
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.
OCSP Responder URL	None
List or description of subordinate CAs operated by the CA organization associated with the root CA.	No subordinate CAs This root CA issues end-entity certs directly.
For subordinate CAs operated by third parties, if any:	None
List any other root CAs that have issued cross-signing certificates for this root CA	None
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV CP/CPS Section 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 by collating the information (organization and so on) described in the application with the directory of government officials issued by National Printing Bureau and so on. CP/CPS Section 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 by collating the information (name, contact address and so on) described in the application with the directory of government officials issued by National Printing Bureau and so on. And the LRA shall confirm the intention to subscribe by telephone or face to face.
EV Policy OID(s)	Not EV

CP/CPS	CP/CPS for Japanese Government Public Key Infrastructure (GPKI) Japanese: http://www.gpki.go.jp/apca/cpcps/index.html English: https://bugzilla.mozilla.org/attachment.cgi?id=379657
AUDIT	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=886&file=pdf (Japanese) https://bugzilla.mozilla.org/attachment.cgi?id=374841 (English) (2009.01.31)

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

- Verify domain check for SSL
    - CP/CPS Section 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 by collating the information (organization and so on) described in the application with the directory of government officials issued by National Printing Bureau and so on.
    - CP/CPS Section 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 by collating the information (name, contact address and so on) described in the application with the directory of government officials issued by National Printing Bureau and so on. And the LRA shall confirm the intention to subscribe by telephone or face to face.
    - CP/CPS Section 4.1.2, Enrollment process and responsibilities Server certificate: The LRA shall confirm that the domain holder of the common name (CN) described in the Server certificate application is the organizations of offices and ministries to which the LRA belongs by using the database provided by the third-party body and so on, and apply accurate information to the IA and RA.
- 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
    - CP/CPS Section 4.1.2, Enrollment process and responsibilities Code signing certificate: The LRA shall confirm that the organization name of the common name (CN) described in the code-signing application exists and it is the organization name of offices and ministries to which the LRA belongs by using the public documents published by offices and ministries, and apply accurate information to the IA and RA.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- 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.”
- Wildcard DV SSL certificates
  - The SSL certs are OV.
- Delegation of Domain / Email validation to third parties
  - MIC makes use of external registration authorities for specific subscriber registration activities as disclosed in MIC’s business practice disclosures.
  - The “prescribed procedure” is documented in detail in the LRA business management and system operation manual. This document is disclosed for government agencies only because the CA only issues certificates for government agencies, and it contains internal operating details.
- Issuing end entity certificates directly from roots
  - Yes. **This root issues end entity certificates directly, and not through a subordinate CA.**
    - Comment #4: Our CA issues small amount of certificates(for SSL and code signing) and also issues certificates for government agencies only. Our CA are taking security measures in every way (like facilities, operations). And audit has proven that security measures applied to protect our CA are more than sufficient.
- Allowing external entities to operate unconstrained subordinate CAs
  - No sub-CAs
- 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.”
- Certificates referencing hostnames or private IP addresses
  - Not found.
- OCSP Responses signed by a certificate under a different root
  - No OCSP
- CRL with critical CIDP Extension
  - CRL downloaded into Firefox successfully.
- Generic names for CAs
  - No Common Name (CN) in certificate. OU = ApplicationCA, O = Japanese Government

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.