Bugzilla ID: 477314
Bugzilla Summary: Add Japanese Local Government Application CA G2 Root

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 Local Public Key Infrastructure (LGPKI)
Website URL (English version)	http://www.lgpki.jp/ (Japanese only)
Organizational type.	National Government
Primary market / customer base.	In Japan there are two root CAs, one is GPKI which acts as a root for national government agencies, and the other one is LGPKI which serves the same function for regional and local governments. LGPKI is controlled by the Local Government Wide Area Network (LGWAN) Operation Committee.

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

Info Needed	Data
Certificate Name	Japan Local Government PKI Application CA Note: No Common Name (CN) in certificate. OU = Application CA G2 O = LGPKI C = JP
Cert summary / comments	Certificates issued by the Application CA G2 are mainly issued for use in services provided by local governments to residents and companies etc., and also by ASP service providers and public institutions to local governments. The LGPKI issues the following certificates: (1) Manager certificates and user certificates as certificates issued from an Organization CA, (2) Email certificates, web certificates, and code signing certificates as certificates issued from an Application CA.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=371920 and https://www.lgpki.jp/CAInfo/AppCAG2.cer
SHA-1 fingerprint.	96:83:38:F1:13:E3:6A:7B:AB:DD:08:F7:77:63:91:A6:87:36:58:2E
Valid from	2006-03-31
Valid to	2016-03-31

Cert Version	3
Modulus length / key length	2048
CRL • URL • update frequency for end-entity certificates	http://www.lgpki.jp/Information/CRL/AppCACrl.crl Section 2.3: "the revocation list is made available in the public repository in 24 hour intervals after revocations are completed. But when an emergency revocation request was made, the revocation list is made available in the public repository urgently after the revocation was completed."
OCSP Responder URL	None

List or description of subordinate CAs operated by the CA organization associated with the root CA	The Application CA G2 issues two types of subordinate CAs:
	• Organization CA issues
	  ○ Manager Certificates
	  ▪ Used by a manager of a local government in electronic signatures on public documents, either between local governments or to residents / companies / etc.
	  ○ User Certificates
	  ▪ Used to authenticate the user when each system is used. Also used in encryption and electronic by the person in charge of handling documents in the LGWAN electronic document exchange system.
	• Application CA issues
	  ○ Email Certificates
	  ▪ Used in email electronic signatures for sending email newsletters to residents and companies.
	  ○ Web Server Certificates
	  ▪ These apply to web servers which handle public notices and request work etc. for residents and companies, used in encryption of SSL communications, etc.
	  ○ Code Signing Certificates
	  ▪ Used in electronic signatures for programs etc. distributed to residents and companies.
	
	Please provide a diagram and/or specific description of the intermediate CAs and end-entity certificates that the LGPKI Application CA G2 root issues.
	Are there multiple Organization and Application sub-CAs?
	Are the sub-CAs able to sign their own sub-CAs?
	Who operates the sub-CAs?

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	Does this root have any subordinate CAs that are operated by external third parties? For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. Also, see https://wiki.mozilla.org/CA:SubordinateCA_checklist

arrangements are by which those subordinates are authorized, controlled, and audited.	
List any other root CAs that have issued cross-signing certificates for this root CA	Has this root been involved in cross-signing with any other root?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV LGPKI Registration Authority Branch Operation Handbook , section 4.3.2, Examiner Work: For an applicant which submitted Request Documents, do a face-to-face confirmation (if the applicant is not known personally, compare the applicant's identity and job position document, etc.), or phone to check based on the organization's predetermined telephone number list etc., and thereby confirm the applicant's identity, authenticate the organization to which the applicant belongs, and confirm the intention to own the certificate.
EV policy OID(s)	Not EV
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	CP/CPS in Japanese: http://www.lgpki.jp/unei/C-6-3-5_CPCPS_ApCA_20070320.pdf I received the following two documents via email. May I attach them to this bug? Are the corresponding documents available in Japanese from your website? If yes, please provide the URLs. 20090205_JapanLGPKI_RegistrationAuthorityBranche_excerpt.doc Is this translation of part of the LGPKI Registration Authority Branch Operation Handbook? 20090205_JapanLGPKIAPCA_excerpt.doc Is this translation of part of the LGPKI Application Certification Authority CP/CPS?
Translations into English of sections of CP/CPS documents pertaining to verification and potentially problematic practices.	Please provide translations into English of the sections of the CP/CPS documents pertaining to: • Verification of Identity and Organization • Verification of ownership/control of domain name • Verification of ownership/control of email address • Section 7 of http://www.mozilla.org/projects/security/certs/policy/ • Potentially Problematic Practices, http://wiki.mozilla.org/CA:Problematic_Practices
URL of one or more web servers using the certificate(s).	https://www.lgpki.jp/CAInfo/fingerprint.htm

AUDIT	Audit Type (WebTrust, ETSI etc.): 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=840&file=pdf Content copying not allowed in permissions on the report, so I cannot review it using Google Translate. Please provide translation into English.

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

- Verify domain check for SSL
- 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.
- Verify identity info in code signing certs is that of subscriber
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)
Need further information if any are relevant.

- 1.1 Long-lived DV certificates
  - The SSL certs are OV.
- 1.2 Wildcard DV SSL certificates
  - The SSL certs are OV.
- 1.3 Issuing end entity certificates directly from roots
  - Looks like end entity certs are issued via subordinate CAs. Need to confirm.
- 1.4 Allowing external entities to operate unconstrained subordinate CAs
  - Not sure.
- 1.5 Distributing generated private keys in PKCS#12 files
  - ?
- 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.