Mozilla - CA Program

Case Information

Case Number	00000018	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Government of Japan, Ministry of Internal Affairs and Communications	**Request Status**	Ready for Public Discussion

Additional Case Information

Subject	Add Renewed Japanese Government Application CA Root certificate	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=870185

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	http://www.gpki.go.jp/	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)	National Government	**Verified?**	Verified
Geographic Focus	Japan	**Verified?**	Verified
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.	**Verified?**	Verified
Impact to Mozilla Users	The Japanese government decided to centralize to GPKI from each of the ministry's certification system and it has finished migration on Oct, 2008. 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 is currently included.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those

			practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	Comment #12 in bug: * It does not allow the use of IDN. * We revoke certificates with private keys that are known to be compromised, or for which verification of subscriber information is known to be invalid. * We set Server FQDN to Subject Alternative Names. CP/CPS section "7. Certificate and CRL profiles". * We don't issue certificates to "natural person".	**Verified?**	Verified

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* 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. * No, wildcard SSL certs cannot be issued. * SSL certs are IV/OV, not DV. * subCAs are internally operated. * There is no IPaddress in the Certificate which was issued by APCA2. * We don't issue Certificates containing a new gTLD under consideration. * We issue "full" CRL, and don't put any CRL Issuing Distribution Point (CIDP) extension in the CRL. * We are indicating the contact information in our WebSite. Contact ; http://www.gpki.go.jp/sendto.html	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	ApplicationCA2 Root	**Root Case No**	R00000029
Request Status	Ready for Public Discussion	**Case Number**	00000018

Additional Root Case Information

Subject	Include ApplicationCA2 Root

Technical Information about Root Certificate

O From Issuer Field	Japanese Government	**Verified?**	Verified
OU From Issuer Field	GPKI	**Verified?**	Verified
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	**Verified?**	Verified

	#474706.		
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8673392 https://www.gpki.go.jp/apca2/APCA2Root.der	**Verified?**	Verified
Valid From	2013 Mar 12	**Verified?**	Verified
Valid To	2033 Mar 12	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://www2.gpki.go.jp/apca2/apca2_eng.html	**Verified?**	Verified
CRL URL(s)	http://dir.gpki.go.jp/ApplicationCA.crl http://dir2.gpki.go.jp/ApplicationCA2Root.crl http://dir2.gpki.go.jp/ApplicationCA2Sub.crl SubCA CPS section 4.9.7: The CRL of 48-hour validity period is issued at intervals of 24 hours.	**Verified?**	Verified
OCSP URL(s)	http://ocsp-sub.gpki.go.jp http://ocsp-root.gpki.go.jp	**Verified?**	Verified
Revocation Tested	https://certificate.revocationcheck.com/www2.gpki.go.jp	**Verified?**	Verified
Trust Bits	Code; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested	Not requesting EV treatment	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	Constrain CA hierarchy to *.go.jp domain.	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	F0:0F:C3:7D:6A:1C:92:61:FB:6B:C1:C2:18:49:8C:5A:A4:DC:51:FB	**Verified?**	Verified
SHA-256 Fingerprint	12:6B:F0:1C:10:94:D2:F0:CA:2E:35:23:80:B3:C7:24:29:45:46:CC:C6:55:97:BE:F7:F1:2D:8A:17:1F:19:84	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	This root certificate has one internally-operated subordinate CA that issues end-entity certificates for SSL and code signing.	**Verified?**	Verified
Externally Operated SubCAs	None.	**Verified?**	Verified
Cross Signing	None.	**Verified?**	Verified

Technical Constraint on 3rd party Issuer	LRAs can't issue SSL certificates. LRAs accept and review applications for issuance only. IA issues SSL certificates. In the LRA system, only principle, go.jp domain come by publication application. CPS section 1.6: -IA (Issuing Authority) - An agency that carries out those aspects of CA operations that relate to certificate issuance. A “general IA operators” are persons whose main task is the issuance of certificates. Within the Application CA2(Sub),these peoples are classified into “senior IA operators” and “general IA operators” according to the basis of the authority. The LRAs confirm that the domain holder of the common name (CN) described in the Server certificate application is the organizations of offices or ministries to which the LRA belongs by using the database provided by the third-party body and so on. Also, the LRAs confirm that the organization name of the common name (CN) described in the code-signing application exists and is the organizatio	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Japanese and English. CPS (Japanese): http://www.gpki.go.jp/apca/cpcps/index.html CPS (English): https://www2.gpki.go.jp/apca2/apca2_eng.html Root CA CPS (English): https://www2.gpki.go.jp/apca2/cpcps/cpcps_root_eng.pdf SubCA CPS (English): https://www2.gpki.go.jp/apca2/cpcps/cpcps_sub_eng.pdf	**Verified?**	Verified
CA Document Repository	https://www2.gpki.go.jp/apca2/apca2_eng.html	**Verified?**	Verified
CP Doc Language	English		
CP	https://www2.gpki.go.jp/apca2/cpcps/cpcps_root_eng.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www2.gpki.go.jp/apca2/cpcps/cpcps_sub_eng.pdf	**Verified?**	Verified
Other Relevant Documents	Updated CP/CPS also attached to bug: https://bugzilla.mozilla.org/show_bug.cgi?id=870185	**Verified?**	Verified
Auditor Name	KPMG AZSA LLC	**Verified?**	Verified
Auditor Website	http://www.kpmg.com/global/en/pages/default.aspx	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1793&file=pdf	**Verified?**	Verified

Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	12/25/2014	**Verified?**	Verified
BR Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8667814 Response to Audit Findings: https://bugzilla.mozilla.org/attachment.cgi?id=8667815	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	9/30/2015	**Verified?**	Verified
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	Root and SubCA CP/CPS section 1	**Verified?**	Verified
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). Comment #12: In the internal regulation of LRA, verification processes of the reality of descriptions in certificates are stipulated clearly. As for the server certificates, following verification processes are stipulated. Verifications are processed according to this process. Also the internal audit are scheduled once a year Verification Processes - Verify FQDN of the server which described in the common name (CN) described in the server certificate application is "go.jp" domain and is registration in the name server. - Verify the domain owner name of the domain part of FQDN by using "Whois".	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
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	**Verified?**	Verified

	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". Also see Bug Comment #12: Organization Verification Procedures		
Email Address Verification Procedures	Not requesting Email trust bit	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	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).	**Verified?**	Verified
Multi-Factor Authentication	After the verification of certificate issuance, the LRA Operator(Government officer) login to the LRA system by using smart card and password. Then operates the LRA system. A server certificate and a code-signing certificate are issued from the LRA system. Electronic certificate is stored in the smart card and only LRA Operators have the smart card. So, LRA Operators can communicate with the LRA system on SSL client certification by smart card.	**Verified?**	Verified
Network Security	Network of GPKI is utilizing the closed network which interconnects each LAN of ministries and agencies. Strictly limited personnel are permitted to utilize it. Strict registration and permission processes are implemented and followed. Also transmission data are encrypted.	**Verified?**	Verified

	Therefore we believe minimum security requirements are satisfied.

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www2.gpki.go.jp/apca2/apca2_eng.html	**Verified?**	Verified