salesforce.com

- Close Window
- Print This Page
- Expand All | Collapse All

R00000112

Information

Case No	00000072	**Owner**	Kathleen Wilson
Root Case No	R00000112	**Request Status**	Initial Request Received
Root Certificate Name	GPKIRootCA1		
All Fields Verified?	No		

Fill this section when changing a currently included Root Certificate

Included CA Owner Name		**Included Certificate**	

Additional Root Case Information

Subject	Include GPKIRootCA1 root certificate	**Date/Time Opened**	2/25/2016 3:07 PM
		Date/Time Closed	

Technical Information about Root Certificate

O From Issuer Field	Government of Korea	**O From Issuer Field (Verified?)**	Verified
OU From Issuer Field	GPKI	**OU from Issuer Field (Verified?)**	Verified
Certificate Summary	The main purpose of the Government of Korea, Root Certificate Authority is to issue the Subordinate Certification Authorities of the GPKI	**Certificate Summary (Verified?)**	Verified
Root Certificate Download URL	https://www.gpki.go.kr/upload/download/GPKIRootCA1.zip	**Root Certificate Download URL (Verified?**	Verified
SHA-1 Fingerprint	76 12 ed 9e 49 b3 65 b4 da d3 12 0c 01 e6 03 74 8d ae 8c f0	**SHA-1 Fingerprint (Verified?)**	Verified
SHA-256 Fingerprint	40:7C:27:6B:EA:D2:E4:AF:06:61:EF:66:97:34:1D:EC:0A:1F:94:34:E4:EA:FB:2D:3D:32:A9:05:49:D9:DE:4A	**SHA-256 Fingerprint (Verified?)**	Verified
Valid From	8/3/2011	**Valid From (Verified?)**	Verified
Valid To	8/3/2031	**Valid To (Verified?)**	Verified
Certificate Version	3	**Certificate Version (Verified?)**	Verified
Certificate Signature Algorithm	SHA-256	**Cert Signature Algorithm (Verified?)**	Verified
Signing Key Parameters	2048	**Signing Key Parameters (Verified?)**	Verified
Test Website URL (SSL) or Example Cert	https://www.gpki.go.kr	**TestWebsiteURL(SSL)orExCert (Verified?)**	Verified
CRL URL(s)	Root CRL : https://www.gpki.go.kr/upload/crl/ARL/arl.zip Government CA CRL : http://ssl-crl.gpki.go.kr/crl/CA131100001/crl3p1dp1.crl	**CRL URL (Verified?)**	Verified
OCSP URL(s)	Government CA OCSP: http://ssl-ocsp-gov.gpki.go.kr:8100 Public CA OCSP: http://ssl-ocsp-pub.gpki.go.kr:8100	**OCSP URL (Verified?)**	Verified
Trust Bits	Websites	**Trust Bits (Verified?)**	Verified
SSL Validation Type	DV	**SSL Validation Type (Verified?)**	Verified
EV Policy OID(s)	Not EV	**EV Policy OID(s) (Verified?)**	Not Applicable
Root Stores Included In	Microsoft	**Root Stores Included In (Verified?)**	Not Verified
Mozilla Applied Constraints	No	**Mozilla Applied Constraints (Verified?)**	Verified

Test Results (When Requesting the Websites Trust Bit)

Revocation Tested	no errors found	**Revocation Tested (Verified?)**	Verified
CA/Browser Forum Lint Test	Tested with cablint in https://crt.sh/ no errors found	**CA/Browser Forum Lint Test (Verified?)**	Verified
Test Website Lint Test	waiting for test tool fixed	**Test Website Lint Test (Verified?)**	Not Verified
EV Tested	Not requesting EV treatment	**EV Tested (Verified?)**	Not Applicable

CA Hierarchy Information

CA Hierarchy	There is a Root CA which is managed by Ministry of the Interior. The Sub-CAs which are Ministry of the Interior, Ministry of Education, Supreme Court of Korea, Supreme Prosecutors' Office and Military Manpower Administration issue digital certificates to government officials and relevant organizations.	**CA Hierarchy (Verified?)**	Need Clarification From CA
Externally Operated SubCAs	No	**Externally Operated SubCAs (Verified?)**	Verified
Cross Signing	No	**Cross Signing (Verified?)**	Verified
Technical Constraint on 3rd party Issuer	No	**Tech Cons on 3rd party Iss (Verified?)**	Verified

Verification Policies and Practices

Policy Documentation	CPS (Korean): https://www.gpki.go.kr/upload/download/1.1-GPKI_RootCA%20CPS.pdf NEED: CP/CPS translated into English	**Policy Documentation (Verified?)**	Need Response From CA
CA Document Repository		**CA Document Repository (Verified?)**	Need Response From CA
CP Doc Language			
CP	MEED : CA provide CP document	**CP (Verified?)**	Need Response From CA
CPS Doc Language	Korean		
CPS	http://www.gpki.go.kr/upload/download/1.1-GPKI_RootCA%20CPS.pdf	**CPS (Verified?)**	Verified
Other Relevant Documents		**Other Relevant Documents (Verified?)**	Need Clarification From CA
Auditor Name	Deloitte Anjin LLC	**Auditor Name (Verified?)**	Verified
Auditor Website	http://www2.deloitte.com/kr/ko.html	**Auditor Website (Verified?)**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Auditor Qualifications (Verified?)**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1923&file=pdf	**Standard Audit (Verified?)**	Verified
Standard Audit Type	WebTrust	**Standard Audit Type (Verified?)**	Verified
Standard Audit Statement Date	9/23/2015	**Standard Audit Statement Dt (Verified?)**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1924&file=pdf	**BR Audit (Verified?)**	Verified
BR Audit Type	WebTrust	**BR Audit Type (Verified?)**	Verified
BR Audit Statement Date	9/23/2015	**BR Audit Statement Date (Verified?)**	Verified
EV Audit	Not EV	**EV Audit (Verified?)**	Not Applicable
EV Audit Type		**EV Audit Type (Verified?)**	Not Applicable
EV Audit Statement Date		**EV Audit Statement Date (Verified?)**	Not Applicable
BR Commitment to Comply	URL to BR audit statement : https://cert.webtrust.org/SealFile?seal=1924&file=pdf	**BR Commitment to Comply (Verified?)**	Need Clarification From CA
SSL Verification Procedures	The URL address of a SSL applicant are confirmed by WHOIS search	**SSL Verification Procedures (Verified?)**	Need Clarification From CA
EV SSL Verification Procedures	Not requesting EV treatment	**EV SSL Verification Proc (Verified?)**	Not Applicable
Organization Verification Procedures	need CP/CPS English translated to confirm	**Org Verification Procedure (Verified?)**	Need Response From CA
Email Address Verification Procedures	The email is confirmed by checking a randomly generated password at application phase.	**Email Addr Verification Proc (Verified?)**	Need Clarification From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Code Signing Subs Verif Proc (Verified?)**	Not Applicable

Multi-Factor Authentication	CA response YES, need CP/CPS English translated to confirm	**Multi-Factor Authentication (Verified?)**	Need Response From CA
Network Security	CA response YES, need CP/CPS English translated to confirm	**Network Security (Verified?)**	Need Response From CA

Software Release Information

NSS Release When First Included		**Firefox Release When First Included**	

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Publ Discl & Audited subCAs (Verified?)**	Need Response From CA

Internal Comments

Comments by Mozilla on Root Case	

Public Comments

Comments	

System Information

Created By	Kathleen Wilson, 2/25/2016 3:07 PM	**Last Sync Date/Time**	
Last Modified By	Aaron Wu, 9/18/2016 8:11 AM		

Root Case History

9/18/2016 8:10 AM

User	**Aaron Wu**
Action	**Changed SSL Verification Procedures (Verified?) from Need Response From CA to Need Clarification From CA. Changed Email Addr Verification Proc (Verified?) from Need Response From CA to Need Clarification From CA.**

9/9/2016 3:26 AM

User	**Aaron Wu**
Action	**Changed Revocation Tested.**

9/9/2016 3:23 AM

User	**Aaron Wu**
Action	**Changed Test Website Lint Test from NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed. to waiting for test tool fixed. Changed Revocation Tested.**

9/9/2016 3:09 AM

User	**Aaron Wu**
Action	**Changed Test Website URL (SSL) or Example Cert from NEED: - If requesting Websites trust bit: URL to a website whose SSL cert chains up to this root. Note that this can be a test site. - If requesting Email trust bit: attach an example cert to the bug. to https://www.gpki.go.kr. Changed SHA-1 Fingerprint from 76:12:ED:9E:49:B3:65:B4:DA:D3:12:0C:01:E6:03:74:8D:AE:8C:F0 to 76 12 ed 9e 49 b3 65 b4 da d3 12 0c 01 e6 03 74 8d ae 8c f0. Changed Certificate Summary to The main purpose of the Government of Korea, Root Certificate Authority is to issue the Subordinate Certification Authorities of the GPKI.**

2/25/2016 3:07 PM

User	**Kathleen Wilson**
Action	**Created.**

Copyright © 2000-2016 salesforce.com, inc. All rights reserved.