Print this page

Mozilla - CA Program

Case Information

Case Number	00000072	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Government of Korea, Ministry of the Interior	**Request Status**	Initial Request Received

Additional Case Information

Subject	Include Korea Government Root Cert	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1226100

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	https://www.gpki.go.kr/	**Verified?**	Not verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Korea	**Verified?**	Verified
Primary Market / Customer Base	Digital certificates are issued to administration institutions and public offices of the Government of Korea	**Verified?**	Verified
Impact to Mozilla Users	NEED: Why does the CA need to have their root certificate directly included in Mozilla's products, rather than being signed by another CA's root certificate that is already included in NSS? Mozilla CA certificate policy: We require that all CAs whose certificates are distributed with our software product ... provide some service relevant to typical users of our software products	**Verified?**	Need Response From CA

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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: 2) CA Hierarchy: 3) Audit Criteria: 4) Document Handling of IDNs in CP/CPS: 5) Revocation of Compromised Certificates:	**Verified?**	Need Response From CA

6) Verifying Domain Name Ownership:
7) Verifying Email Address Control:
8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates.
9) DNS names go in SAN:
10) Domain owned by a Natural Person:
11) OCSP:
12) Network Security Controls:

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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: 2) Wildcard DV SSL certificates: 3) Email Address Prefixes for DV Certs: 4) Delegation of Domain / Email validation to third parties: 5) Issuing end entity certificates directly from roots: 6) Allowing external entities to operate subordinate CAs: 7) Distributing generated private keys in PKCS#12 files: 8) Certificates referencing hostnames or private IP addresses: 9) Issuing SSL Certificates for Internal Domains: 10) OCSP Responses signed by a certificate under a different root: 11) SHA-1 Certificates: 12) Generic names for CAs: 13) Lack of Communication With End Users: 14) Backdating the notBefore date:	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	GPKIRootCA1	**Root Case No**	R00000112
Request Status	Initial Request Received	**Case Number**	00000072

Additional Root Case Information

Subject	Include GPKIRootCA1 root certificate

Technical Information about Root Certificate

O From Issuer Field	Government of Korea	**Verified?**	Verified
OU From Issuer Field	GPKI	**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	**Verified?**	Verified
Root Certificate Download URL	https://www.gpki.go.kr/upload/download/GPKIRootCA1.zip	**Verified?**	Verified
Valid From	2011 Aug 03	**Verified?**	Verified
Valid To	2031 Aug 03	**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://www.gpki.go.kr	**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	**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	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Not Verified
Mozilla Applied Constraints	No	**Verified?**	Verified

Test Results (When Requesting the SSL/TLS Trust Bit)

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

Digital Fingerprint Information

SHA-1 Fingerprint	76 12 ed 9e 49 b3 65 b4 da d3 12 0c 01 e6 03 74 8d ae 8c f0	**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	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	Under the Root CA which is managed by Ministry of the Interior, there are Sub-CAs which are Ministry of the Interior, Ministry of Education, Supreme Court of Korea, Supreme Prosecutors' Office and Military Manpower Administration. The CAs issue digital certificates to government officials and relevant organizations. Only 2 CAs of Ministry of the Interior and Ministry of Education issue SSL certificates.	**Verified?**	Verified
Externally Operated SubCAs	No	**Verified?**	Verified
Cross Signing	No	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	No	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	CPS (Korean): https://www.gpki.go.kr/upload/download/1.1-GPKI_RootCA%20CPS.pdf	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Verified
CP Doc Language			
CP	According to e-Government Act of the Government of Korea, Root CA and Sub-CAs shall have CPS only without CP.	**Verified?**	Verified
CP Doc Language			
CPS	https://bugzilla.mozilla.org/attachment.cgi?id=8802101	**Verified?**	Verified
Other Relevant Documents	N/A	**Verified?**	Verified
Auditor Name	Deloitte Anjin LLC	**Verified?**	Verified
Auditor Website	http://www2.deloitte.com/kr/ko.html	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1923&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	9/23/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1924&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	9/23/2015	**Verified?**	Verified
EV Audit	Not EV	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
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 CA acquired a WebTrust seal for CAs-SSL Baseline with Network Security and comp	**Verified?**	Verified
SSL Verification Procedures	Refer to CPS 3.2.5 Validation of authority. The authority of a certificate is in effect as soon as the certificate issued. CA should confirm that the domain's owner is certificate applicant based on the information queried from qualified registrant or the government-run database.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	Refer to CPS 3.2.2 Organization Initial Identify Validation (CA) If the administrative standard code of an authority that created GPKI certification application (for authority) is verified, CA will be recognized as a trusted authority	**Verified?**	Verified
Email Address Verification Procedures	Refer to CPS 3.2.5 Validation of authority. The authority of a certificate is in effect as soon as the certificate issued. CA should confirm that the domain's owner is certificate applicant based on the	**Verified?**	Verified

	information queried from qualified registrant or the government-run database.		
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	Refer to CPS 6.5.1 Specific computer security technical requirements The Root CA certification system has the access control function, identify and check operator function, audit log collection function and CTL/ARL generating function. The certification system (CA) has the access control function, operator identification and check function, audit log collection function and CRL	**Verified?**	Verified
Network Security	Refer to CPS 6.7 Network security controls The network is protected by intrusion detection system and intrusion prevention system	**Verified?**	Verified

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.	**Verified?**	Need Response From CA