Mozilla - CA Program

Case Information

Case Number	00000072	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Government of Korea	**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	NEED: - Which types of customers does the CA serve? - Are there particular vertical market segments in which it operates? - Does the CA focus its activities on a particular country or other geographic region?	**Verified?**	Need Response From CA
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: 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:	**Verified?**	Need Response From CA

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		**Verified?**	Not Verified
Root Certificate Download URL	https://bugzilla.mozilla.org /attachment.cgi?id=8719465	**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	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.	**Verified?**	Need Response From CA
CRL URL(s)	NEED CRL URLs and CRL issuing frequency for subscriber certs, with reference to where this is documented in the CP/CPS	**Verified?**	Need Response From CA
OCSP URL(s)	NEED OCSP URL and maximum OCSP expiration time, with reference to where this is documented in the CP/CPS	**Verified?**	Need Response From CA
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	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central /source/security/nss/lib/certdb /genname.c#1551	**Verified?**	Need Response From CA

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

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	Tested with cablint in https://crt.sh/ no errors found	**Verified?**	Verified
Test Website Lint Test	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.	**Verified?**	Need Response From CA
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	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: CP/CPS translated into English CPS (Korean): https://www.gpki.go.kr/upload/download/1.1-GPKI_RootCA%20CPS.pdf	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA

CP Doc Language			
CP		**Verified?**	Need Response From CA
CP Doc Language			
CPS		**Verified?**	Need Response From CA
Other Relevant Documents		**Verified?**	Need Response From CA
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	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	Not requesting EV treatment	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org	**Verified?**	Need Response From CA

	/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org /CA:Recommended_Practices#Verifying_Email_Address_Control		
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org /CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org /CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

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