General information about the CA's associated organization

CA Company	Government of Korea, Ministry of the Interior
Website URL	https://www.gpki.go.kr/
Organizational type	Government Agency
Primark Market / Customer Base	Digital certificates are issued to administration institutions and public offices of the Government of Korea
Inclusion in other major browsers	Microsoft
CA Primary Point of Contact (POC)	POC 1: Name: KIM, IN SOO Direct email :kis@klid.or.kr CA Phone Number : +82-2-2031-9831 POC 2 Name: Cho, So Yeon Direct email : chosoyon@klid.or.kr CA Phone Number : +82-2-2031-9828

Technical information about each root certificate

Certificate Name	GPKIRootCA1
Certificate Issuer Field	cn=GPKIRootCA1, ou=GPKI, o=Government of Korea, c=KR
Certificate Summary	The main purpose of the Government of Korea, Root Certificate Authority is to issue the Subordinate Certification Authorities of the GPKI
Mozilla Applied Constraints	Not applicable
Root Cert URL	https://www.gpki.go.kr/upload/download/GPKIRootCA1.zip
SHA1 Fingerprint	76 12 ed 9e 49 b3 65 b4 da d3 12 0c 01 e6 03 74 8d ae 8c f0
Valid From	2011 Aug 03
Valid To	2031 Aug 03
Certificate Version	V3
Certificate Signature Algorithm	sha256WithRSAEncryption
Signing key parameters	RSA 2048
Test Website URL (SSL) Example Certificate (non-SSL)	https://www.gpki.go.kr
CRL URL	Root ARL : [1] https://www.gpki.go.kr/upload/crl/ARL/arl.zip [2] ldap://cen.dir.go.kr:389/cn=GPKIRootCA1, ou=GPKI, o=Government of Korea, c=KR?authorityRevocationList;binary Government CA CRL : [1]ldap://cen.dir.go.kr:389/cn=crl3p1dp1,cn=CA131100001,ou=GPKI,o=Government of Korea,c=KR?certificateRevocationList;binary [2]http://ssl-crl.gpki.go.kr/crl/CA131100001/crl3p1dp1.crl

	Public CA CRL : [1] ldap://cen.dir.go.kr:389/cn= crl1p1dp100,cn=CA131100002,ou=GPKI,o=Government of Korea,c=KR?certificateRevocationList;binary [2] http://ssl-crl.gpki.go.kr/crl/CA131100002/crl1p1dp100.crl
OCSP URL (Required now for end-entity certs)	Government CA OCSP: http://ssl-ocsp-gov.gpki.go.kr:8100 Public CA OCSP: http://ssl-ocsp-pub.gpki.go.kr:8100
SSL Validation Type	DV(Domain Validation)
EV Policy OID(s)	Not applicable
Non-sequential serial numbers and entropy in cert	The serial number contains 16 random ASCII characters which corresponds to 8*16 =128 bits that are random.
Response to Recent CA Communication(s)	Not applicable

CA Hierarchy information for each root certificate

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.
Externally Operated SubCAs	No
Cross-Signing	No
Technical Constraints on Third-party Issuers	No

Verification Policies and Practices

Policy Documentation	Root CA (Ministry of the Interior) : http://www.gpki.go.kr/upload/download/1.1-GPKI_RootCA%20CPS.pdf Government CA (Ministry of the Interior): http://www.gpki.go.kr/upload/download/1.2-GPKI_CA%20CPS.pdf URL:**https://www.gpki.go.kr/pds/WebTrustAction.action**
Audits	Audit Type: WebTrust Auditor:Deloitte Anjin LLC Auditor Website: http://www2.deloitte.com/kr/ko.html URL to Audit Report and Management's Assertions: https://cert.webtrust.org/SealFile?seal=1923&file=pdf
Baseline Requirements (SSL)	URL to BR audit statement : https://cert.webtrust.org/SealFile?seal=1924&file=pdf
SSL Verification Procedures	The URL address of a SSL applicant are confirmed by WHOIS search.
Organization Verification Procedures	An applicant's organization is confirmed by the government e-approval system using government integrated DB.
Email Address Verification Procedures	The email is confirmed by checking a randomly generated password at application phase.
Code Signing Subscriber Verification Procedures	No

Multi-factor Authentication	Yes
Network Security	Yes