**General information about the CA's associated organization**

| | |
|---|---|
| CA Company | 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 | The Root certificate is included in Microsoft products |
| CA Primary Point of Contact (POC) | POC 1:<br>Name: KIM, Hyun Wook<br>Direct email :hyunwookkim@klid.or.kr<br>CA Phone Number : +82-2-2031-9831<br><br>POC 2<br>Name: Cho, Hyun Woo<br>Direct email : hyunwoo8@klid.or.kr<br>CA Phone Number : +82-2-2031-9828 |

**Technical information about each Sub-CA certificate**

| | | |
|---|---|---|
| Certificate Name | Government CA(cn=CA13110001), | Public CA(cn=CA131100002) |
| Certificate Issuer Field | o=Government of Korea, c=KR | o=Government of Korea, c=KR |
| Certificate Summary | Ministry of the Interior CA issues digital certificates and SSLs to Government institutes, including government officials and organizations, and websites of the government organizations. | Ministry of the Interior CA issues digital certificates to Government institutes, including government officials and organizations, and issues SSLs to websites of public agencies related to the government organizations. |
| Mozilla Applied Constraints | Super-CA | Super-CA |
| CA Cert URL | https://www.gpki.go.kr/upload/download/CA131100001.zip | https://www.gpki.go.kr/upload/download/CA131100002.zip |
| SHA1 Fingerprint | 7b 3e 23 e6 c2 64 9c 13 da 8b 2d 78 7a 33 63 7f e9 7b 8b dd | f9 7b a2 68 b5 4e c0 4d b5 00 42 82 f4 61 04 a0 0f 26 de 7b |
| Valid From | 2011-09-22 | 2011-09-22 |
| Valid To | 2021-09-22 | 2021-09-22 |
| Certificate Version | 3 | 3 |

| | | |
|---|---|---|
| Certificate Signature Algorithm | SHA-256 | SHA-256 |
| Signing key parameters | 2048 | 2048 |
| Test Website URL (SSL) Example Certificate (non-SSL) | https://www.gpki.go.kr | https://www.kosbi.re.kr |
| CRL URL | http://ssl-crl.gpki.go.kr/crl/CA131100001/crl3p1dp2.crl | http://ssl-crl.gpki.go.kr/crl/CA131100002/crl3p1dp1.crl |
| OCSP URL (Required now for end-entity certs) | http://ssl-ocsp-gov.gpki.go.kr:8100 | http://ssl-ocsp-gov.gpki.go.kr:8100 |
| SSL Validation Type | DV | DV |
| EV Policy OID(s) | Not EV | Not EV |

**CA Hierarchy information for each root certificate**

| | |
|---|---|
| CA Hierarchy | Under the Root CA that is managed by Ministry of the Interior, there are Sub-CAs that are Ministry of the Interior, Ministry of Education, Supreme Court of Korea, Supreme Prosecutors' Office and Military Manpower Administration.<br><br>The Ministry of the Interior has 2 CA certificates which are Government CA(CA13110001) and Public CA(CA13110002) as a Sub-CA. |
| Externally Operated SubCAs | No |
| Cross-Signing | No |
| Technical Constraints on Third-party Issuers | No |

**Verification Policies and Practices**

| | |
|---|---|
| Policy Documentation | https://www.gpki.go.kr/upload/download/1.2-GPKI_CA%20CPS.pdf |
| Audits | WebTrust for CA seal on Government CA(CA13110001) and Public CA(CA13110002)<br>https://cert.webtrust.org/SealFile?seal=2183&file=pdf |
| Baseline Requirements (SSL) | WebTrust for CA-SSL seal on Government CA(CA13110001) and Public CA(CA13110002)<br>https://cert.webtrust.org/SealFile?seal=2184&file=pdf |
| 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. |
| Email Address Verification Procedures | Refer to CPS 3.2.5 Validation of authority.<br>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. |
| Code Signing Subscriber Verification Procedures | Mozilla is no longer accepting requests to enable the Code Signing trust bit. |
| Multi-factor Authentication | Refer to CPS 6.5.1 Specific computer security technical requirements<br>The certification system (CA) has the access control function, operator identification and check function, audit log collection function and CRLs. |
| Network Security | Refer to CPS 6.7 Network security controls<br>The network is protected by intrusion detection system and intrusion prevention system. |

**Response to Mozilla's CA Recommended Practices**(https://wiki.mozilla.org/CA:Recommended_Practices)

| | |
|---|---|
| Publicly Available CA and CPS | https://www.gpki.go.kr/upload/download/1.2-GPKI_CA%20CPS.pdf |
| CA Hierarchy | Under the Root CA that is managed by Ministry of the Interior, there are Sub-CAs that are Ministry of the Interior, Ministry of Education, Supreme Court of Korea, Supreme Prosecutors' Office and Military Manpower Administration. |
| Audit Criteria | WebTrust |
| Document Handing of IDNs in CP/CPS | All Sub CAs allow only government official letters to apply certificate issuance. |
| Revocation of Compromised Certificates | According to 5.7 of CPS, Compromise and disaster recovery of CA's CPS, Sub-CAs have policies and procedures for management of all keys and certificates related to compromised and/or suspicious certificates and keys. |
| Verifying Domain Name Ownership | WHOIS search |
| Verifying Email Address Control | CA should confirm that the domain's owner is certificate applicant based on the information queried from qualified registrant or the government-run database. |
| Verifying Identity of Code Signing Certificate Subscriber | Not Available |
| DNS names go in SAN | There is a DNS name in SAN of SSL certificates issued from the Sub-CA. |
| Domain owned by Natural Person | Not Available |
| OCSP | http://ssl-ocsp-gov.gpki.go.kr:8100 |

**Response to Mozilla's list of Potentially Problematic Practices**(https://wiki.mozilla.org/CA:Problematic_Pratices)

| | |
|---|---|
| Long-lived DV certificates | No |
| Wildcard DV SSL certificates | Wildcard DV SSL certificates are issued and used. |
| Email Address Prefixes for DV Certs | No |
| Delegation of Domain / Email validation to third parties | No |
| Issuing end entity certificates directly from roots | No |
| Allowing external entities to operate subordinate CAs | No |
| Distributing generated private keys in PKCS#12 files | No |
| Certificates referencing hostnames or private IP addresses | No |
| Issuing SSL Certificates for internal Domains | No |
| OCSP Responses signed by a certificate under a different root | No |
| SHA-1 Certificats | No |
| Generic names for CAs | No |
| Lack of Communications With End Users | No |
| Backdating the notBefore date | No |