| No. | Category | Item | Description | Response | CA Response |
|---|---|---|---|---|---|
| 1 | General | 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?<br>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 | Need Response From CA | Ministry of the Interior of the government of Korea has its Root certificate. Its sub-CAs provide digital certficates and SSL certificates to goverment officials, relevant ministries and government institutes. Thus, as the representative of e-Government of Korea, we officially and directly apply to NSS products for its Root certificate inclusion. |
| 2 | | CA's Response to Recommended Practices | 1) Publicly Available CP and CPS: | Need Response From CA | Root CA CPS:<br>https://www.gpki.go.kr/upload/download/1.1-GPKI_RootCA CPS.pdf<br><br>(1) Ministry of the Interior CA CPS:<br>https://www.gpki.go.kr/upload/download/1.2-GPKI_CA CPS.pdf<br>(2) Ministry of Education CA CPS:https://www.epki.go.kr/resource/data/down/document_no1.pdf<br>(3) Supreme Court of Korea,<br>Confidential document.<br>(4) Supreme Prosecutors' Office<br>Confidential document.<br>(5) Military Manpower Administration<br>Confidential document. |
| 3 | | | 2) CA Hierarchy: | Need Response From CA | We have already submitted a English-translated document of the Root CA CPS. |
| 4 | | | 3) Audit Criteria: | Need Response From CA | WebTrust (for Root CA, Ministry of the Interior, and Ministry of Education) |
| 5 | | | 4) Document Handling of IDNs in CP/CPS: | Need Response From CA | All Sub CAs allow only government official letters to apply certificate issuance. |
| 6 | | | 5) Revocation of Compromised Certificates | Need Response From CA | Acoording to 5.7 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 suspicous certificates and keys. |
| 7 | | | 6) Verifying Domain Name Ownership: | Need Response From CA | WHOIS search |
| 8 | | | 7) Verifying Email Address Control: | Need Response From CA | CA should confirm that the domain's owner is certificate applicant based on the information queried from qualified registrant or the government-run database. |

| | | | | | |
|---|---|---|---|---|---|
| 9 | | | 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is | Need Response From CA | Not Available |
| 10 | | | 9) DNS names go in SAN: | Need Response From CA | There is a DNS name in SAN of SSL certiifcates issued from Sub-Cas |
| 11 | | | 10) Domain owned by a Natural Person: | Need Response From CA | Not available |
| 12 | | | 11) OCSP | Need Response From CA | We operate OCSP according to CA/Browser Forum's baseline requirements. We plans on developing OCSP responder of Root CA. |
| 13 | | | 12) Network Security Controls | Need Response From CA | We comply with Network Security Controls |
| 14 | | CA's Response to Problematic Practices | 1) Long-lived DV certificates: | Need Response From CA | No. We don't issue long-validity certificates. |
| 15 | | | 2) Wildcard DV SSL certificates: | Need Response From CA | No. We don't issue Wildcard DV SSL certificates. |
| 16 | | | 3) Email Address Prefixes for DV Certs: | Need Response From CA | Not Available |
| 17 | | | 4) Delegation of Domain / Email validation to third parties: | Need Response From CA | CA should confirm that the domain's owner is certificate applicant based on the information queried from qualified registrant or the government-run database. |
| 18 | | | 5) Issuing end entity certificates directly from roots: | Need Response From CA | No. Our Root CA doesn't issue any certificate to end-users. |
| 19 | | | 6) Allowing external entities to operate subordinate CAs: | Need Response From CA | No. We don't have any external operating company for Root CA and CA opeartions. |
| 20 | | | 7) Distributing generated private keys in PKCS#12 files: | Need Response From CA | No. Sub-CAs don't generate subscriber key pairs. |
| 21 | | | 8) Certificates referencing hostnames or private IP addresses: | Need Response From CA | No. We don't issue private IP address certificates. |
| 22 | | | 9) Issuing SSL Certificates for Internal Domains: | Need Response From CA | No. Sub-CAs don't generate subscriber key pairs. |
| 23 | | | 10) OCSP Responses signed by a certificate under a different root: | Need Response From CA | No. |
| 24 | | | 11) SHA-1 Certificates: | Need Response From CA | No. |
| 25 | | | 12) Generic names for CAs: | Need Response From CA | Our CAs have meaningul names according to their certificate policies. |
| 26 | | | 13) Lack of Communication With End Users: | Need Response From CA | All subscribers for SSL certificates should accept the user agreement provided by CAs. |
| 27 | | | 14) Backdating the notBefore date: | Need Response From CA | No. |
| 28 | Root Case Record # 1 | Technical Information about Root Certificate | Root Stores Included In | Not Verified | Microsoft Trusted Root Certificate Program<br>Short URL : http://aka.ms/RootCertDownload |
| 29 | | | Test Website Link | Not Verified | |

| | | | | | |
|---|---|---|---|---|---|
| 30 | | 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. | Need Response From CA | (1) Ministry of the Interior CA :<br>https://cert.webtrust.org/ViewSeal?id=1923<br>https://cert.webtrust.org/ViewSeal?id=1924<br>(2) Ministry of Education CA :<br>https://cert.webtrust.org/ViewSeal?id=2029<br>https://cert.webtrust.org/ViewSeal?id=2030<br>(3) Supreme Court of Korea CA :<br>Confidential.<br>(4) Supreme Prosecutors' Office CA :<br>Confidential.<br>(5) Military Manpower Administration CA :<br>Confidential. |