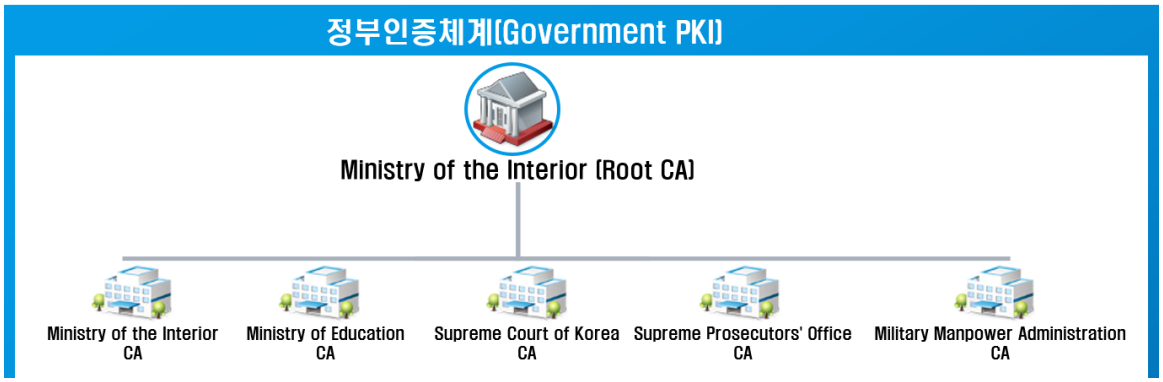
(2) CA Hierarchy

A hierarchical structure of a single root with intermediate certs (subroots) is preferred. The single top-level root's public certificate is supplied for Mozilla's root list; the subroots are not. See CA:Recommendations_for_Roots

CAs that issue certificates under multiple subordinate CAs (i.e., under a root CA whose CA certificate is being requested for inclusion) or under multiple CA hierarchies (i.e., rooted at multiple root CAs, one or more of whose certificates is being requested for inclusion) should provide additional information as noted.

The CA should provide a graphical or textual description of the CA hierarchy or hierarchies, including which subordinates are under which root CAs



The CA should indicate the general types of certificates (i.e., for SSL/TLS servers, email signing/encryption, and code signing) issued by each subordinate CA under each root.

Subordinate CAs issue certificate for the purposes as below.
(1) Ministry of the Interior CA: Individual, organization, special purpose, SSL/TLS server(s), and encryption
(2) Ministry of Education CA: Individual, organization, special purpose, SSL/TLS server(s), and encryption
(3) SUPREME PROSECUTORS' OFFICE CA (only for internal): individual, and organization
(4) Court of Korea CA (only for internal): individual, and organization
(5) Military Manpower Administration CA (only for internal): individual, and organization

Where a CP/CPS applies to multiple subordinate CAs and/or multiple CA hierarchies, the CA should indicate whether particular sections of the CP/CPS apply to different subordinates and/or hierarchies and, if so, what the differences are.

The Root certificate authority and subordinate CAs under the Korea's Government PKI have the basis of establishment and operation by the Korean e-government act. All subordinate CAs including the Root CA comply with the subordinate decrees of e-government act. The Root CA has disclosed CPS at the official website. Among Subordinate CAs, Ministry of the Interior CA and Ministry of Education CA have disclosed their CPSs. The other 3 CAs do not disclose their CPSs to the public area because their certification services are limited and closed.

We also recommend that CAs consider using separate root CA certificates with separate public keys (or separate intermediate CA certificates with separate public keys under a single root) when issuing certificates according to different Certificate Policies, so that we or others may selectively enable or disable acceptance of certificates issued according to a particular policy, or may otherwise treat such certificates differently (e.g., in our products' user interfaces).

Each subordinate CA uses its owned key pairs (public key and private key).

(3) Audit Criteria

CAs should supply evidence of their being evaluated according to one or more of the criteria accepted as suitable per the Mozilla policy.
- The CA should indicate exactly which criteria they are being evaluated against (i.e., which of the criteria listed in the Mozilla policy).
- All documents supplied as evidence should be publicly available.
- Documents purporting to be from the CA's auditor (or other evaluator) should be available directly from the auditor (e.g., as documents downloadable from the auditor's web site).

Root CA WebTrust report: https://cert.webtrust.org/SealFile?seal=1923&file=pdf Root CA WebTrust report (SSL): https://cert.webtrust.org/SealFile?seal=1924&file=pdf Ministry of the Interior CA WebTrust report : https://cert.webtrust.org/SealFile?seal=1923&file=pdf Ministry of the Interior CA WebTrust report (SSL): https://cert.webtrust.org/SealFile?seal=1924&file=pdf Ministry of Education CA WebTrust report: https://cert.webtrust.org/ViewSeal?id=2029 Ministry of Education CA WebTrust report (SSL): https://cert.webtrust.org/ViewSeal?id=2030 *Other subordinate CAs that are used only in a closed network and do not issue SSL, email, codesigning certificates do not perform annual audits.

(4) Document Handling of IDNs in CP/CPS

If a CA allows the use of internationalized domain names (IDNs) in certificates (e.g., as issued for SSL/TLS-enabled servers), the CA should address the issue of homographic spoofing of IDNs in their CP/CPS, even if primary responsibility for dealing with this issue falls on domain registries. (This doesn't mean that the CAs must prevent such spoofing. It merely means that a CA should describe how it handles the issue of spoofing when authenticating the owner of a domain.)

The Ministry of the Interior CA shall conduct WHOIS verification before issuing SSL certificates including IDNs. In addition, the applicant's e-mail address is limited to e-mail accounts used by government agencies of the Republic of Korea.

(6) Verifying Domain Name Ownership

We rely on public documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met.

Section 7 of the Mozilla CA Certificate Inclusion Policy states: “for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate or has been authorized by the domain registrant to act on the registrant's behalf"

The CA's public documentation needs to provide sufficient information describing the steps taken by the CA to confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. For instance, if a challenge-response type of procedure is used, then there needs to be a brief description of the process. If public resources are used, then there should be a description of which public resources are used, what data is retrieved from public resources, and how that data is used to verify that the certificate subscriber owns/controls the domain name.

According to CPS 3.2.2 Authentication of organization identity, the Ministry of the Interior CA uses a requesting organization's Administrative Standard Code (ASC) which is a reliable public resource operated by the government of Korea. Validation specialists of RAs confirm whether a ASC written

in an application form is equal with a search value from the government DB after WHOIS verification.

(12) Network Security Controls

CAs must maintain current best practices for network security, and have qualified network security audits performed on a regular basis. The CA/Browser Forum has published a document called Network and Certificate System Security Requirements which should be used as guidance for protecting network and supporting systems.

It is expected that CAs do the following on a regular basis:

- Maintain network security controls that at minimum meet the Network and Certificate System Security Requirements.

The Ministry of Interior CA meets of Network and Certificate System Security Requirements of CA Browser Forum.

- Check for mis-issuance of certificates, especially for high-profile domains.

According to internal criteria of mis-issuance of certificates, the Ministry of Interior CA is regularly audited by internal auditors. The CA also performs an annual WebTrust audit by an independent third party.

- Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness.

We use an integrated data center operated by the government of Korea. Its network, monitoring, passwords, and outer accesses have been regularly reviewed. The facilities are managed at the highest security level.

- Ensure Intrusion Detection System and other monitoring software is up-to-date.

Intrusion detection and monitoring S/W is regularly monitored and the latest version of S/W is used under the management of the integrated data center.

- Confirm the ability to shut down certificate issuance quickly if alerted of intrusion.

Emergency communication network is established and operated. If there is a problem with intrusion detection monitoring, the certification authorities take immediate action.