Root CA Bugzilla ID: 335197
Root CA Company/Organization Name: Korea Information Security Agency (KISA)

This document summarizes the information gathered and verified for subordinate CAs for companies who use their sub-CA to sign other sub-CAs or certificates for other companies or individuals not affiliated with their company. For instance, this document is necessary when the root issues sub-CAs that are used by Certificate Service Providers (CSP). For more background information, see

- https://wiki.mozilla.org/CA:How_to_apply
- https://wiki.mozilla.org/CA:SubordinateCA_checklist

A root with externally-operated sub-CAs needs to provide the following information in their CPS or contractually with the company operating the sub-CA.

Info Needed	**Data**
Root Name	KISA RootCA 1
List or Description of all of the Subordinate CA's operated by third parties	The 5 Licensed CAs (LCAs) are listed at http://www.kisa.or.kr/kisae/kcac/jsp/kcac_80_10.jsp (English) Commercial: Korea Information Certificate Authority Inc (KICA) http://www.signgate.com Korea Securities Computer Corporation (KOSCOM) http://www.signkorea.com Korea Electronic Certification Authority Inc ("CrossCert") http://gca.crosscert.com KTNET ("TradeSign" or "KITA") http://www.tradesign.net/ Nonprofit: Korea Financial Telecommunications (KFTC) http://www.yessign.or.kr
Requirements (technical and contractual) for subordinate CAs in regards to whether or not subordinate CAs are constrained to issue certificates only within certain domains, and whether or not subordinate CAs can create their own subordinates.	KISA issues certificates to the LCA, which is nominated under Sec. 4 of the Digital Signature Act, under Sec. 15 and Sub-Sec. 2 of Sec. 25 and suspends or revokes them under Sec. 16, Sec. 18 or Sub-sec. 2 of Sec.25. We do not have any restricts about issuance area for Commercial Sub-CA(LCA), but for non-profit sub-CA(LCA), KTFC, the issuance area is restricted to banking business.
Requirements for sub-CAs to take reasonable	Korea Electronic Signature Act Enforcement Regulations

measures to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/. a) domain ownership/control b)email address ownership/control c) digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate	Article 13.2 (Standards and Method for Verifying the Identity) Article 13.3 (Identity Verification Proof) These two sections describe the process for verifying the identity of individuals and organizations. "An accredited certification authority shall verify the identity of the applicant for issuance of an accredited certificate pursuant to the regulation prescribed at the end of Paragraph of Article 15 of the Act by checking real information of the applicant as follows:" Digital Signature Certificate Issuing Procedure Guideline for SSL, CodeSigning, and Secure e-Mail (English): https://bugzilla.mozilla.org/attachment.cgi?id=594641 Digital Signature Certificate Issuing Procedure Guideline for SSL, CodeSigning, and Secure e-Mail (Korean): http://www.rootca.or.kr/kor/standard/standard02.jsp Chapter 2 Article 4: While identifying applicants for Web server security certificates in person, certification authorities shall verify the following: 1. Identification certificate set forth in Article 13 Paragraph 3 Sub-Paragraph 1 of the Enforcement Rule of the Digital Signature Act; 2. Domain registration certificate; 3. Domain registration application or registration fee payment receipt. Certificate authorities shall verify the validity of domain stated in the domain registration certificate of Paragraph 1 Sub-Paragraph 2 above via domain information search service. If the domain registrant name does not match the real name of certificate issuance applicant, certificate authorities shall verify the agreement document on domain use containing the signature of domain owner and the identification certificate of domain owner as in Paragraph 1 Sub-Paragraph 1 above to confirm license to use domain in issue. Chapter 2, Article 5: While identifying applicants for code-signing certificates in person, certification authorities shall verify the following: 1. Identification certificate set forth in Article 13 Paragraph 3 Sub-Paragraph 1 of the Enforcement Rule of the Digital Signature Act; 2. Domain registration certificate. Certificate authorities shall verify the validity of domain stated in the domain registration certificate of Paragraph 1 Sub-Paragraph 2 above via domain information search service. Chapter 2, Article 6: While identifying applicants for secure e-mail certificates, certification authorities shall verify the following:

	1. Identification certificate set forth in Article 13 Paragraph 3 Sub-Paragraph 1 of the Enforcement Rule of the Digital Signature Act; 2. E-mail address. Certificate authorities shall verify the validity of e-mail address in Paragraph 1 Sub-Paragraph 2 above.
Description of audit requirements for sub-CAs (typically in the CP or CPS) a) Whether or not the root CA audit includes the sub-CAs. b) Who can perform the audits for sub-CAs. c) Frequency of the audits for sub-CAs.	KISA CPS section 1.3.3 Ministry of Public Administration and Security : The Ministry of Public Administration and Security is a policy-making and supervision agency, which carries out the following activities to ensure the secure and reliable operation of the electronic signature certification system: o Establishing policy for building and operating the electronic signature certification system in a secure and reliable manner. o Designating a certification authority, correction order, work suspension, and cancellation of designation and work investigation. o Managing and supervising the Security Agency's and certification authorities' observance of the Electronic Signature Law, and its Enforcement Ordinances and Enforcement Regulations. o Cross-recognition of electronic signatures between foreign governments. -- Comment #10 LCA(Accredited CAs)s in Korea were audited and accredited by Ministry of Public Administration and Security (MOPAS) according to Article 4 of the Electronic Signature Act. Article 13.2 and Article 13.3 of the Electronic Signature Act Enforcement Regulations defines the standard method of verify the identity and the identity verification proof. And the LCAs shall faithfully abide by the articles. You can find the verification process of applicants for certificates in our regulation. The LCAs are audited every year by KISA according to the article 25 of the Electronic Signature Act. And,MOPAS has supervised and audited every year that KISA develop his technical and physical security plans of the critical information infrastructure(CII) according to Article 6 of the Information Infrastructure Protection Act. Also, MIC has supervised that KISA faithfully implement the accredited certification practice statement. But, the security plans of CII and the audit reports about a CII can't be open to the third party, so we'd like to ask for your understanding.

For each CSP or sub-CA operated by 3rd party, review the CPS and audit to find the following information.
It is best if the sub-CA's CP/CPS and audit statements are translated into English.

This table shows the information for the **Commercial** Sub-CAs. There is another table below for the nonprofit sub-CAs.

Info Needed	**Data**	**Data**	**Data**	**Data**

Sub-CA Company Name	Korea Information Certificate Authority Inc (KICA)	Korea Securities Computer Corporation (KOSCOM) SignKorea (operated by KOSCOM).	Korea Electronic Certification Authority Inc ("CrossCert")	KTNET ("TradeSign" or
Sub-CA Corporate URL	http://www.signgate.com/eng/index.htm	http://www.signkorea.com/eng/	http://gca.crosscert.com	http://www.tradesign.net/
Sub-CA cert download URL	http://rootca.kisa.or.kr/kcac/jsp/kcac_1010_list.jsp (korean version) KICA certificate is as follows Number 6 : Certificate to issue End-Entity's certificate for online transaction Number 7 : Certificate for time stamping server Number 8 : Certificate for OCSP server Number 9 : Certificate to issue Web Server Security, Code-Signing, Secure E-mail Certificates	http://rootca.kisa.or.kr/kcac/jsp/kcac_1010_list.jsp (korean version) KOSCOM certificate is as follows Number 10 : Certificate to issue End-Entity's certificate for online transaction Number 11 : Certificate for time stamping server Number 12 : Certificate for OCSP server Number 13 : Certificate to issue Web Server Security, Code-Signing, Secure E-mail Certificates	http://rootca.kisa.or.kr/kcac/jsp/kcac_1010_list.jsp (korean version) CrossCert certificate is as follows Number 20 : Certificate to issue End-Entity's certificate for online transaction Number 21 : Certificate for time stamping server Number 22 : Certificate for OCSP server Number 23 : Certificate to issue Web Server Security, Code-Signing, Secure E-mail Certificates	http://rootca.kisa.or.kr/kc ac_1010_list.jsp (korean version) KTNET certificate is as f Number 24 : Certificate t End-Entity's certificate f transaction Number 25 : Certificate f stamping server Number 26 : Certificate f server
General CA hierarchy under the sub-CA.	KICA do not have any sub-CA. Licensed CA directly issues the certificates to the end-entity.	KOSCOM do not have any sub-CA. Licensed CA directly issues the certificates to the end-entity.	CrossCert do not have any sub-CA. Licensed CA directly issues the certificates to the end-entity.	KTNET do not have any Licensed CA directly issu certificates to the end-ent
Links to Sub-CA CP/CPS	http://www.signgate.com/eng/e_support/e_sup02.htm	http://www.signkorea.com/eng/support/main1.php	http://www.crosscert.com/service_gcca/library/Main.jsp?_action=SHOW&_param=GCCA_LIBRARY_CPS01_PAGE (KOREAN version)	http://www.tradesign.net/ (KOREAN version)
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for endentity certificates chaining up	LCAs issue the certificates for internet banking and electronic settlement under the attached CPS. There is an additional CPS for	LCAs issue the certificates for internet banking and electronic settlement under the attached CPS. There is an additional CPS for	LCAs issue the certificates for internet banking and electronic settlement under the attached CPS. There is an additional CPS for	LCAs issue the certificat internet banking and elec settlement under the attac CPS. KTNET is not issued We

to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/. a) domain ownership/control b)email address ownership/control c) digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate	Web Server Security, Code-Signing, Secure E-mail Certificates, to confirm the domain ownership/control, email address ownership/control , digitally signing code objects, you can refer to "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)". See chapter 2, article 5 in Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)	Web Server Security, Code-Signing, Secure E-mail Certificates, to confirm the domain ownership/control, email address ownership/control , digitally signing code objects, you can refer to "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)". See chapter 2, article 5 in Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)	Web Server Security, Code-Signing, Secure E-mail Certificates, to confirm the domain ownership/control, email address ownership/control , digitally signing code objects, you can refer to "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)". See chapter 2, article 5 in Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)	Security, Code-Signing, S mail Certificates
Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates. DV: Organization attribute is not verified. Only the Domain Name referenced in the certificate is verified to be owned/controlled by the subscriber. OV: Both the Organization and the ownership/control of the Domain Name are verified.	IV/OV When Sub-CAs issue SSL certificates, they follow "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)" See "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)"	IV/OV When Sub-CAs issue SSL certificates, they follow "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)" See "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)"	When Sub-CAs issue SSL certificates, they follow "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)" See "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)"	KTNET does not issue W Server Security, Code-Si Secure E-mail Certificate
Review the sub-CA CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice.	SSL Certs are IV/OV SSL certificates are issued for 1~2 year. Certificate for online transaction is issued for 1 year. Customer creates key as per http://www.signgate.com/eng/e_s	SSL certificates are issued for 1~2 year. Certificate for online transaction is issued for 1 year. Customer creates key; CPS section 2.1.2.2	Long-lived DV certificates SSL certificates are issued for 1~2 year. Certificate for online transaction is issued for 1 year. Customer creates key	KTNET does not issue W Server Security, Code-Si Secure E-mail Certificate

Provide further info when a potentially problematic practice is found.	ervice/e_serv0106.htm OCSP service is only provided for the online transactions not for SSL certificates. **KICA use delta-CRL.** **one of dCRL is as follow.** URL=ldap://ldap.signgate.com:389/cn=s1dp1p1,ou=crldp,ou=AccreditedCA,O=KISA,C=KR?authorityRevocationList	OCSP service is only provided for the online transactions not for SSL certificates. **KOSCOM use delta-CRL.** **one of dCRL is as follow.** URL=ldap://dir.signkorea.com:389/ou=dp1p1,ou=AccreditedMCA,o=SignKorea,c=KR	OCSP service is only provided for the online transactions not for SSL certificates **CrossCert use delta-CRL.** **one of dCRL is as follow.** URL=ldap://ssldir.crosscert.com/cn=s1dp5p10,ou=crldp,ou=AccreditedCA,o=CrossCert,c=KR?certificateRevocationList	
Audit	KISA audits Sub-CAs every year, and report the results to MOPAS.	KISA audits Sub-CAs every year, and report the results to MOPAS.	KISA audits Sub-CAs every year, and report the results to MOPAS.	KISA audits Sub-CAs ev and report the results to M
CRL update frequency for end entity certificates.	CRL is issued within 24 hours.	CRL is issued within 24 hours.	CRL is issued within 24 hours.	CRL is issued within 24 h

This table shows the information for the **nonprofit** sub-CAs.

Info Needed	**Data**
Sub-CA Company Name	Korea Financial Telecommunications (KFTC) Yessign, operated by KFTC
Sub-CA Corporate URL	http://www.yessign.or.kr
Sub-CA cert download URL	http://rootca.kisa.or.kr/kcac/jsp/kcac_1010_list.jsp (korean version) KFTC certificate is as follows Number 14 : Certificate to issue End-Entity's certificate for online transaction Number 15 : Certificate for time stamping server Number 16 : Certificate for OCSP server Number 17 & 18 : Certificate to issue Web Server Security, Code-Signing, Secure E-mail Certificates
General CA hierarchy under the sub-CA.	This LCA appears to offer certificates to both individuals and organizations, with a focus on internet banking and financial transactions. There is no indication that this LCA signs other sub-CAs. "KFTC operates an inter-bank joint network and offers services such as inter-bank clearing, Giro, and payments through the financial joint network."

Links to Sub-CA CP/CPS	On http://www.yessign.or.kr/ there is a CPS link in the Customer Support section. It is in English. KFTC Certification Practice Statement: http://www.yessign.or.kr/cps.html
The section numbers and text (in English) in the CP/CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/. a) domain ownership/control b)email address ownership/control c) digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate	When Sub-CAs issue SSL certificates, they follow "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)" See "Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)"
Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic practices, only apply to DV certificates. DV: Organization attribute is not verified. Only the Domain Name referenced in the certificate is verified to be owned/controlled by the subscriber. OV: Both the Organization and the ownership/control of the Domain Name are verified.	OV CPS Section 3.1.2.2 and 3.1.2.3 Subscribers providing services on the Internet shall visit KFTC in person and bring the following documents required by KFTC for identity verification purposes: Documents verifying the existence of domain (copy of application for the registration of domain name, copy of the receipt for registration fees, and copy of registration certificate) Representative's identification card Related documents in case the name of a registered patent is used
Review the sub-CA CP/CPS for potentially problematic practices, as per http://wiki.mozilla.org/CA:Problematic_Practices. When found, provide the text (in English) from the CP/CPS that confirms or denies the problematic practice. Provide further info when a potentially problematic practice is found.	Certs are valid for one year according to section 3.4 of CPS. SSL certs are OV User generates private key as per CPS section 2.1.3.3 OCSP service is only provided for the online transactions not for SSL certificates Certificate Suspension and Revocation Lists: http://www.yessign.or.kr/cgi-bin/crl.cgi

If the root CA audit does not include this sub-CA, then for this sub-CA provide a publishable statement or letter from an auditor that meets the requirements of sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/	KISA audits Sub-CAs every year, and report the results to MOPAS
Provide information about the CRL update frequency for end-entity certificates. There should be a statement in the CP/CPS to the effect that the CRL for end-entity certs is updated whenever a cert is revoked, and at least every 24 or 36 hours.	CRL is issued within 24 hours.