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	Status/Notes
Root Name	CertRSA01 KISA RootCA 1 KISA RootCA 3	COMPLETE
List or Description of all of the Subordinate CA's operated by third parties	The 6 Licensed CAs (LCAs) are listed at http://www.kisa.or.kr/kisae/kcac/jsp/kcac_80_10.jsp (English) http://www.rootca.or.kr/lca/lca.htm (Korean) 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 National Computerization Agency (NCA) http://sign.nca.or.kr	COMPLETE
Requirements (technical and contractual) for subordinate CAs in regards to whether or not subordinate CAs are constrained to	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.	?

issue certificates only within certain domains, and whether or not subordinate CAs can create their own subordinates.		
Requirements for sub-CAs to take reasonable 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	Korea Electronic Signature Act Enforcement Regulations Created an attachment (id=228227) 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:" Ownership of Domain Name is described in chapter 2, article 4 in Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English) "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." For S/MIME certificates issued by the various LCAs, the LCAs verify identity of the applicant and validity of the associated email address referenced in the certificate. See chapter 2, article 6 in Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English) For code signing certificates the LCAs verify identity of the applicant. See chapter 2, article 5 in Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)	COMPLETE
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.	KISA CPS section 1.5.3 Ministry of Information and Communication: Ministry of Information and Communication works as a policy maker and inspector for a secure operation of digital signature certification practice structure as described below: o Policy making for securely establishing and running the digital signature certification practice structure	COMPLETE

b) Who can perform the audits for sub-CAs. c) Frequency of the audits for sub-CAs.	o Nomination, correcting order, suspension of a practice, cancellation of the nomination and investigation of LCAs o Managing and inspecting the KISA and LCA's compliance with the Digital Signature Act, the Ordinance and the Regulations o Mutual accreditation of digital signature with a foreign government -- Comment #10 LCA(Accredited CAs)s in Korea were audited and accredited by Ministry of Information and Communication(MIC) 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,MIC 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 "KITA")
Sub-CA Corporate URL	http://www.signgate.com/eng/index.htm	http://www.signkorea.com/eng/	http://gca.crosscert.com Can't find any info in English	http://www.tradesign.net/ Can't find any info in English

Sub-CA cert download URL	???	???	???	???
General CA hierarchy under the sub-CA.	CPS section 2.1, Type of Certification Services The KICA sub-CA appears to issue end-entity certificates to both individuals and organizations, including email certificates to individuals and SSL server certificates to organizations or individuals. I found no indication that the KICA sub-CA signs other CAs.	Hierarchy is shown on http://www.signkorea.com/eng/certificate/main.php There is no indication that the KOSCOM sub-CA signs other CAs. This LCA appears to offer certificates to both individuals and organizations, with a focus on supporting exchange of e-commerce documents	???	???
Links to Sub-CA CP/CPS	http://www.signgate.com/eng/e_support/e_sup02.htm	http://www.signkorea.com/eng/support/main1.php	???	???
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	Could not find. Sub-CA's have to follow the rules set forth in the table above, so this may be OK?	Could not find. Sub-CA's have to follow the rules set forth in the table above, so this may be OK	???	???
Identify if the SSL certificates chaining up to this root are DV and/or OV. Some of the potentially problematic	IV/OV CPS section 4.1,Personal Identification for Issuance of	IV/OV CPS section 4, Identification	???	???

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.	Certificates Requires both individuals and organizations to prove their identity using government-issued documents and by other means.	Requires both individuals and organizations to prove their identity using government-issued documents and by other means.		
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.	Long-lived DV certificates SSL Certs are IV/OV Certs are valid for 1 year as per CPS section 3.3, Validity of Certificates Wildcard DV SSL certificates SSL Certs are IV/OV Issuing end entity certificates directly from roots No Allowing external entities to operate unconstrained subordinate CAs No Distributing generated private keys in PKCS#12 files Customer creates key as per http://www.signgate.com/eng/e_service/e_serv0106.htm Certificates referencing hostnames or private IP	Long-lived DV certificates Certs are issued for 1 year. Wildcard DV SSL certificates SSL Certs are IV/OV Issuing end entity certificates directly from roots No Allowing external entities to operate unconstrained subordinate CAs No Distributing generated private keys in PKCS#12 files Customer creates key; CPS section 2.1.2.2 Certificates referencing hostnames or private IP addresses No OCSP Responses signed by a	??? Long-lived DV certificates Wildcard DV SSL certificates Issuing end entity certificates directly from roots Allowing external entities to operate unconstrained subordinate CAs Distributing generated private keys in PKCS#12 files Certificates referencing hostnames or private IP addresses OCSP Responses signed by a certificate under a different root CRL with critical CIDP Extension	??? Long-lived DV certificates Wildcard DV SSL certificates Issuing end entity certificates directly from roots Allowing external entities to operate unconstrained subordinate CAs Distributing generated private keys in PKCS#12 files Certificates referencing hostnames or private IP addresses OCSP Responses signed by a certificate under a different root CRL with critical CIDP Extension

	addresses No OCSP Responses signed by a certificate under a different root No CRL with critical CIDP Extension What is the URL to their CRL?	certificate under a different root OCSP service is offered http://www.signkorea.com/eng/service/main4.php Unknown if signed under different root. CRL with critical CIDP Extension What is the URL to their CRL?		
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/	???	???	???	???
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.	Could not find	Could not find	???	???

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

Info Needed	**Data**	**Data**
Sub-CA Company Name	Korea Financial Telecommunications (KFTC) Yessign, operated by KFTC	National Computerization Agency (NCA)
Sub-CA Corporate URL	http://www.yessign.or.kr	http://sign.nca.or.kr This url doesn't respond.

		What does the following mean? "The accredited certification authority transferred/takenover/merged under the Article 9 of the Electronic Signature Act"
Sub-CA cert download URL	Certificate of the Korea Certification Authority Central: http://www.rootca.or.kr/cert.html	???
General CA hierarchy under the sub-CA.	Could not find diagram, but 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	Could not find. Sub-CA's have to follow the rules set forth in the table above, so this may be OK?	???

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.	Long-lived DV certificates Certs are valid for one year according to section 3.4 of CPS. Wildcard DV SSL certificates SSL certs are OV Issuing end entity certificates directly from roots No Allowing external entities to operate unconstrained subordinate CAs LCA does not appear to issue sub-CAs Distributing generated private keys in PKCS#12 files User generates private key as per CPS section 2.1.3.3 Certificates referencing hostnames or private IP addresses No	??? Long-lived DV certificates Wildcard DV SSL certificates Issuing end entity certificates directly from roots Allowing external entities to operate unconstrained subordinate CAs Distributing generated private keys in PKCS#12 files Certificates referencing hostnames or private IP addresses OCSP Responses signed by a certificate under a different root CRL with critical CIDP Extension

	OCSP Responses signed by a certificate under a different root Did not find OCSP CRL with critical CIDP Extension CRL downloads fine into Firefox 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/	Not sure about audits, but found this: "Since its designation as an accredited certification authority as per Article 4 (Designation of an Accredited Certification Authority) of the Act by the Ministry of Information and Communication on April 12, 2000, KFTC has been providing accredited certification services."	???
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.	Every 24 hours or less according to CPS section 2.5.2.	???