Bugzilla ID: 335197
Bugzilla Summary: Add KISA root CA Certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	Data
CA Name	Korea Information Security Agency (KISA)
Website URL (English version)	http://www.rootca.or.kr/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	National government CA
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	Korea Information Security Agency (KISA) is the Electronic Signature Authorization Management Center for South Korea. The Korean Certification Authority Central (KCAC) of KISA issues certificates to six (6) intermediate CAs ("licensed CAs" or LCAs), which then issue end entity certificates to Korean citizens, businesses, and other organizations. KISA/KCAC appears to provide a service relevant to Mozilla users: it is a government-run CA providing services to Korean citizens, businesses, and other organizations. KISA/KCAC itself is a root CA only; the actual end entity certificates are issued by subordinate CAs ("licensed CAs" or LCAs) under policies set by KISA/KCAC. Its policies (for itself and the LCAs) are documented in the documents published on its website and listed in the entry on the pending applications list.

The first comment period for these roots started on 1/18/2008, as per Comment #61 in Bugzilla.

Mozilla.dev.tech.crypto: **KISA root CA certificate inclusion request**

- March 28, 2008: Just to provide an update on this, since the public comment period ended some time ago. As far as I can determine, the only remaining issue holding up approval of this request is confirming that the MIC audit of KISA was/is acceptable. My basic strategy to do that has been to get confirmation that the audit covered all the points addressed by the WebTrust for CAs criteria. See the bug for more info.

- March 28: I looked into this a while back. Auditing of the subordinate CAs ("licensed CAs" or LCAs) was/is mandated by the relevant Korean law and regulations that set up KSIA in the first place and established MIC authority over it. KISA itself does the auditing of the LCAs, as mandated by the law and regulations.
- March 30: the LCAs subordinate to KISA are subject to regulatory constraints imposed by the government (including regulations mandating verification requirements, etc.) and are subject to oversight by KISA, including audits.
- March 30: KISA itself would most likely meet the policy requirements (once confirmed accordingly, which you are following up), if it weren't for the fact that they are not issuing EE certificates and their sub CAs are all external to their own physical infrastructure. So what about exactly were they audited? Certainly not the issuance of EE certs...And do you remember that the sub CAs don't even have policies nor does the KISA policy clearly define their sub ordinated CAs (if I remember that correctly from the bug report from what I've seen). The various CAs *intend* to publish and implement policies once they are approved (or something along these lines was the response).

Mozilla.dev.tech.crypto: **Dealing with third-party subordinates of T-Systems and others**
http://groups.google.com/group/mozilla.dev.tech.crypto/browse_thread/thread/265f94877056b2bb#
This discussion led to the following:

- “At one end of the spectrum we have situations where we have a small number of subordinate CAs, each of which issues lots and lots of certificates. T-Systems is apparently like this, as are KISA and perhaps others. Here I think it is realistic for us to take a closer look at the subordinates.
- In other cases, like the "enterprise CA" case mentioned above, there are lots of subordinates, and each subordinate issues relatively few certificates. Here I think it is unrealistic to look at each and every CA; it's quite possible we won't even know the actual names of each and every CA. In these case I think we will instead have to look at the overall manner in which the (root) CA oversees and controls the subordinates.

Based on discussions in Mozilla.dev.tech.crypto, a wiki page has been created to provide guidelines for gathering data and evaluating subordinate CAs that are operated by third-parties:
https://wiki.mozilla.org/CA:SubordinateCA_checklist

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**	**Data**	**Data**	**Status / Notes**
Certificate Name	CertRSA01	KISA RootCA 1	KISA RootCA 3	COMPLETE
Cert summary / comments	Certificates are issued from this root only to KISA's 6 LCAs (Licensed CAs), not directly to end entities. Note that this root is apparently being phased out in favor of the KISA RootCA 1.	This root will be replacing CertRSA01. Certificates are issued from this root only to KISA's 6 LCAs (Licensed CAs), not directly to end entities. National PKI in Korea has two kinds of PKI domains, one is	This root is for the wireless PKI domain in Korea. Certificates are issued from this root only to KISA's 6 LCAs (Licensed CAs), not directly to end entities.	COMPLETE

		the wired PKI domain, and the other is the wireless PKI domain. This root is for the wired PKI domain.		
The root CA certificate URL Download into FireFox and verify	http://www.rootca.or.kr/certs/root-rsa.der	http://www.rootca.or.kr/certs/root-rsa-3280.der	http://www.rootca.or.kr/certs/root-wrsa.der	COMPLETE
SHA-1 fingerprint.	F5:C2:7C:F5:FF:F3:02:9A:CF:1A:1A:4B:EC:7E:E1:96:4C:77:D7:84	02:72:68:29:3E:5F:5D:17:AA:A4:B3:C3:E6:36:1E:1F:92:57:5E:AA	5F:4E:1F:CF:31:B7:91:3B:85:0B:54:F6:E5:FF:50:1A:2B:6F:C6:CF	COMPLETE
Valid from	2000-03-03	2005-08-24	2004-11-19	COMPLETE
Valid to	2010-03-03	2025-08-24	2014-11-19	COMPLETE
Cert Version	3	3	3	COMPLETE
Modulus length / key length or type of signing key (if ECC)	2048	2048	2048	COMPLETE
CRL URL update frequency for end-entity certificates	http://www.rootca.or.kr/certs/root-rsa-2459.crl	http://www.rootca.or.kr/certs/root-rsa-3280.crl	http://www.rootca.or.kr/certs/root-wrsa.crl	CRLs successfully downloaded into Firefox. The following info was provided in Bugzilla, but not found in KISA's CPS. Will have to look for in the sub-CA CPS's. > - With what frequency are CRLs issued for end entity certificates issued by > your sub-CAs? CRLs for end entity certificates are issued within 24 hours, there are some difference depending on the sub-CAs.
OCSP (if applicable) OCSP Responder URL Max time until OCSP responders	None	None	None	COMPLETE

updated to reflect end-entity revocation http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Section 26(b): “If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.”				
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	No internally operated subordinate CAs for these roots. Certificates are issued from these roots only to KISA's 6 LCAs (Licensed CAs), not directly to end entities.			COMPLETE
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited. (For example, contractual arrangements	The 6 Licensed CAs (LCAs) are listed at http://www.kisa.or.kr/kisae/kcac/jsp/kcac_80_10.jsp 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")			See https://wiki.mozilla.org/CA:SubordinateCA_checklist For information about the sub-CAs see: 335197-subCA-review

should require third-party subordinates to operate in accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.)	http://www.tradesign.net/ Nonprofit: Korea Financial Telecommunications (KFTC) http://www.yessign.or.kr National Computerization Agency (NCA) http://sign.nca.or.kr	
List any other root CAs that have issued cross-signing certificates for this root CA	None	COMPLETE
Requested Trust Bits One or more of: Websites (SSL/TLS) Email (S/MIME) Code (Code Signing)	Websites Email Code	COMPLETE
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV certificate.) Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)	IV/OV 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	COMPLETE

	to confirm license to use domain in issue.”			
If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	Not EV			N/A
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. For SSL certificates this should also include URLs of one or more web servers using the certificate(s). There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. Note: mainly interested in SSL, so OK if no email example.		https://www.rootca.or.kr/mark/rootca.html		For testing purposes, please provide a URL to a website whose certificate chains up to this root. Note that this can be a test site.
CP/CPS Certificate Policy URL Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	CPS 1.1 (English) Certification Practice Statement of Korea Information Security Agency (thereinafter 'KISA') is established to define the necessities relevant to digital signature certification such as certificate policy, issue & practice of certificate, security control and operational policy & procedure and the matters relevant to obligations and responsibilities of KISA and Licensed Certification Authority (thereinafter 'LCA') according to Digital Signature Act, Digital Signature Ordinance(thereinafter `the Ordinance') and Digital Signature Regulations(thereinafter 'the Regulations'). CPS 1.3 (Korean) Certificate issuing procedure (Korean) Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English) Korea Electronic Signature Act Korea Electronic Signature Act Enforcement Regulations			COMPLETE

	Created an attachment (id=228227) KISA's repositories are as follows: o KISA's Certification Practice Statement : http://www.rootca.or.kr/rca/cps.htm o LCA List : http://www.rootca.or.kr/lca/lca.htm o Certificate List : http://www.rootca.or.kr/cert.htm o Certificate Suspension and Revocation List : http://www.rootca.or.kr/crl.htm	
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the “audit report and management assertions” document available from the webtrust.org site or elsewhere.)	Audit: Government (WebTrust equivalent) Auditor: Ministry of Information and Communication, Republic of Korea Public statement by MIC re KISA/KCAC Audit (comment #48): http://eng.mic.go.kr/eng/user.tdf?a=common.HtmlApp&c=1001&page=resources/resources_f_01.html&mc=E_04_06 This link is broken The “MIC statement about KISA Root CA Audit” attachment in Bugzilla is https://bugzilla.mozilla.org/attachment.cgi?id=274124 updated mapping table, web trust criteria and KISA This version has mapping for all the WebTrust for CAs criteria in section 1 ("business disclosures"), section 2 ("service integrity"), and section 3 ("environmental controls").	Would it be possible to get a statement about an audit performed in 2008, which includes the requirements of a WebTrust CA audit?

Review CPS sections dealing with subscriber verification (COMPLETE)

- Verify domain check for SSL
  - For SSL certificates the LCAs verify the identity of the applicant and his or her authorization to request the certificate.
  - See chapter 2, article 4 in Web Server Security, Code-Signing, Secure E-mail Certificates Issuance Administration Guideline (English)
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber’s legal identity.
  - 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)
- Verify identity info in code signing certs is that of subscriber
  - 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)
- Make sure it’s clear which checks are done for which context (cert usage)

    - It’s clear.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - Certs are IV/OV
- Wildcard DV SSL certificates
    - Certs are IV/OV
- Issuing end entity certificates directly from roots
    - No.
- Allowing external entities to operate unconstrained subordinate CAs
    - Yes. Need to evaluate the subordinate CAs
- Distributing generated private keys in PKCS#12 files
    - Not found
- Certificates referencing hostnames or private IP addresses
    - Not found
- OCSP Responses signed by a certificate under a different root
    - Not applicable
- CRL with critical CIDP Extension
    - CRLs successfully downloaded into Firefox

Verify Audits
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
- For EV CA’s, verify current WebTrust EV Audit done.
    - Not EV
- Review Audit to flag any issues noted in the report