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	http://www.rootca.or.kr/
Organizational type	National government CA
Primary market / customer base	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 intermediate CAs ("licensed CAs" or LCAs), which then issue end entity certificates to Korean citizens, businesses, and other organizations.
CA Contact Information	CA Email Alias: rootca@kisa.or.kr CA Phone Number: 82-2-4055-411 Title / Department: Certification Practices

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

Info Needed	**Data**	**Data**
Certificate Name	KISA RootCA 1	KISA RootCA 3
Cert summary / comments	This root is for the wired PKI domain in Korea. This root signs subCAs for KISA's Licensed CAs (LCAs).	This root is for the wireless PKI domain in Korea. This root signs subCAs for KISA's Licensed CAs (LCAs).
Root Cert URL	http://www.rootca.or.kr/certs/root-rsa-3280.der	http://www.rootca.or.kr/certs/root-wrsa.der
SHA-1 fingerprint	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
Valid from	2005-08-24	2004-11-19
Valid to	2025-08-24	2014-11-19 This root expires relatively soon. Is there a new root that should be included?
Cert Version	3	3
Modulus length	2048	2048
Test website	https://www.rootca.or.kr/mark/rootca.html When I try to browse to this site I get: Error code: sec_error_unknown_critical_extension	For testing purposes, please provide a URL to a website whose SSL cert chains up to this root. Note that this can be a test site.
CRL URL	http://www.rootca.or.kr/certs/root-rsa-3280.crl All CRLs: http://rootca.kisa.or.kr/kcac/jsp/kcac_1020_1.jsp	http://www.rootca.or.kr/certs/root-wrsa.crl
CRL Frequency	Where is it documented that LCAs must provide updated CRLs for end-entity certs every 24 hours?	
OCSP Responder	None	None

CA Hierarchy	These roots only sign intermediate CAs for KISA's Licensed CAs (LCAs).	
Externally Operated SubCAs	335197-subCA-review.pdf – I still need to update this based on the information that was provided in Comment #115. The Licensed CAs (LCAs) are listed at http://rootca.kisa.or.kr/kcac/jsp/kcac_2010.jsp (Korean) Korea Information Certificate Authority Inc (KICA), http://www.signgate.com KICA CPS (English Version): Coming soon Korea Securities Computer Corporation (KOSCOM), http://www.signkorea.com KOSCOM CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=479655 Korea Electronic Certification Authority Inc (CrossCert), http://gca.crosscert.com CrossCert CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=479658 KTNET ("TradeSign" or "KITA"), http://www.tradesign.net/ TradeSign CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=479659 Korea Financial Telecommunications (KFTC), http://www.yessign.or.kr (non-profit) KFTC CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=479657	
Cross-Signing	None	None
Requested Trust Bits	Websites Email Code	Websites Email Code
SSL Validation	OV	OV
EV policy OID(s)	Not EV	Not EV
CP/CPS	CPS v1.5 (English): https://bugzilla.mozilla.org/attachment.cgi?id=483411 Where is this document (or equivalent Korean version) located on the KISA website? None of the links in section 1.1.3.2 of the CPS work. Issuing Procedure Guidelines (English): http://rootca.kisa.or.kr/kcac/down/Guide/8-Digital%20Signature%20Certificate%20Issuing%20Procedure%20Guideline%20for%20SSL,%20CodeSigning,%20and%20Secure%20e-Mail(en).pdf Issuing Procedure Guidelines (Korean): http://rootca.kisa.or.kr/kcac/down/Guide/7-Digital%20Signature%20Certificate%20Issuing%20Procedure%20Guideline%20for%20SSL,%20CodeSigning,%20and%20Secure%20e-Mail.pdf Where is it stated that the LCAs must at a minimum perform the verification procedures described in the Issuing Procedure Guidelines document? If Mozilla accepts and includes a KISA root, then we have to assume that we also accept any of its current and future sub-CAs and their sub-CAs. Therefore, it is important that the root CA (KISA) documents the minimum verification procedures that an LCA must follow and be audited against.	

	Certificate Downloads: http://rootca.kisa.or.kr/kcac/jsp/kcac_1010_list.jsp Korea Electronic Signature Act: https://bugzilla.mozilla.org/attachment.cgi?id=228226 Korea Electronic Signature Act Enforcement Regulations: https://bugzilla.mozilla.org/attachment.cgi?id=228227
Audit	Audit: Government (WebTrust equivalent) Auditor: Ministry of Public Administration and Security (MOPAS) Audit website: http://www.mopas.go.kr Audit Statement: https://bugzilla.mozilla.org/attachment.cgi?id=479645 When audit statements are provided by the company requesting CA inclusion rather than having an audit report posted on the website such as cert.webtrust.org, the Mozilla process requires doing an independent verification of the authenticity of audit statements that have been provided. Therefore, I will need to send email to pjran@mopas.go.kr to confirm the authenticity of the audit statement and ask when the audit was performed and which root certificates were covered in the audit. Comment #108: MOPAS audits whether KISA follows its CPS. … refer to mapping table… Mapping table, web trust criteria and KISA: https://bugzilla.mozilla.org/attachment.cgi?id=313248 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"). KISA audits sub-CAs every year and reports the results to MOPAS. The audit criteria are the same for the LCAs as for KISA, and as per the mapping table the criteria are equivalent to WebTrust CA. For comment #91's b), the criteria of the audit for the LCAs, supported by the Digital Signature Act. article 19.2 whether the LCAs operate the facilities and devices safely, is as follows. - Digital Signature act article 8, whether the CPS is followed - Digital Signature act article 13.4 whether the countermeasures are followed The date the last audit was completed is as follows and the audit for this year (2010) is now in progress. - name of LCA : the date the audit was completed(2009) - KICA : 2009. 7. 6 - KOSCOM : 2009. 12. 3 - KFTC : 2009. 7. 23 - CrossCert : 2009. 9. 11 - TradeSign : 2009. 10. 9 Do the sub-CA audits include verifying that the Issuing Procedure Guidelines are being followed? If yes, where is that stated? Issuing Procedure Guidelines: http://rootca.kisa.or.kr/kcac/down/Guide/7-Digital%20Signature%20Certificate%20Issuing%20Procedure%20Guideline%20for%20SSL,%20CodeSigning,%20and%20Secure%20e-Mail.pdf

Organization Identity Verification	KISA CPS section 3.2.1 states that verifying the identity of the applicant is performed as prescribed in Provisions 2 and 3 of Article 13 of the Electronic Signature Law. I believe this is referring to the “Korea Electronic Signature Act Enforcement Regulations (English)” document: https://bugzilla.mozilla.org/attachment.cgi?id=228227 Correct? Article 13.2 (Standards and Method for Verifying the Identity) and Article 13.3 (Identity Verification Proof).
Domain Name Ownership / Control	KISA Issuing Procedure Guidelines (English): http://rootca.kisa.or.kr/kcac/down/Guide/8-Digital%20Signature%20Certificate%20Issuing%20Procedure%20Guideline%20for%20SSL,%20CodeSigning,%20and%20Secure%20e-Mail(en).pdf 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. It seems like “Enforcement Rule of the Digital Signature Act” refers to: https://bugzilla.mozilla.org/attachment.cgi?id=228227 However, I’m not sure that’s correct. If it is, then I don’t understand why identification is limited to sub-paragraph 1. What text is “Paragraph 1 Sub-Paragraph 1,2” referring to?
Email Address Ownership / Control	Issuing Procedure Guidelines (English): http://rootca.kisa.or.kr/kcac/down/Guide/8-Digital%20Signature%20Certificate%20Issuing%20Procedure%20Guideline%20for%20SSL,%20CodeSigning,%20and%20Secure%20e-Mail(en).pdf 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. What text is “Paragraph 1 Sub-Paragraph 2” referring to?
Identity of Code Signing Subscriber	Issuing Procedure Guidelines (English): http://rootca.kisa.or.kr/kcac/down/Guide/8-Digital%20Signature%20Certificate%20Issuing%20Procedure%20Guideline%20for%20SSL,%20CodeSigning,%20and%20Secure%20e-Mail(en).pdf 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;
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information. • Long-lived DV certificates ○ SSL Certs are OV

	• Wildcard DV SSL certificates o SSL Certs are OV • Email Address Prefixes for DV SSL Certs o SSL Certs are OV • Delegation of Domain / Email validation to third parties o Are the LCAs allowed to have external RAs do the validation for end-entity certs? • Issuing end entity certificates directly from roots o No • Allowing external entities to operate unconstrained subordinate CAs o See 335197-subCA-review.pdf • Distributing generated private keys in PKCS#12 files o Not found • Certificates referencing hostnames or private IP addresses o Not found. • Issuing SSL Certificates for Internal Domains o ? • OCSP Responses signed by a certificate under a different root o Not applicable. • CRL with critical CIDP Extension o See comments #99 and #100 • Generic names for CAs o CA names include KISA