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
Certificate Name	KISA RootCA 1
Issuer Field	CN = KISA RootCA 1 OU = Korea Certification Authority Central O = KISA C = KR
Cert summary / comments	This root is for the wired PKI domain in Korea. This root signs subCAs for KISA's Licensed CAs (LCAs).
Root Cert URL	Certificate Downloads: http://rootca.kisa.or.kr/kcac/jsp/kcac_1010_list.jsp http://rootca.kisa.or.kr/kcac/jsp/kcac_1010_view.jsp http://www.rootca.or.kr/certs/root-rsa-3280.der
SHA-1 fingerprint	02:72:68:29:3E:5F:5D:17:AA:A4:B3:C3:E6:36:1E:1F:92:57:5E:AA
Valid from	2005-08-24
Valid to	2025-08-24
Cert Version	3
Modulus length	2048
Test website	https://www.kisa.or.kr/main.jsp
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

	LDAP See the CA/Browser Forum's Baseline Requirements (https://www.cabforum.org/documents.html). Appendix B Subordinate CA Certificate, cRLDistributionPoints: This extension MUST be present and MUST NOT be marked critical. It MUST contain the **HTTP URL** of the CA's CRL service. Subscriber Certficiate, cRLDistributionPoints: This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the **HTTP URL** of the CA's CRL service. See Section 13.2.1 for details. Comment #145: As I've mentioned above, I will be offering with the new test URL as soon as the test is done.(about CRL distribution issue). Since all the LCA's are supportive, it won't take long.
CRL Frequency	Each LCAs CPS states that LCAs should update CRL every 24 hours.
OCSP Responder	None Baseline Requirement #13.2.2: Effective 1 January 2013, the CA SHALL support an OCSP capability using the GET method for Certificates issued in accordance with these Requirements.
CA Hierarchy	These roots only sign intermediate CAs for KISA's Licensed CAs (LCAs).
Externally Operated SubCAs	For details see 335197-subCA-review.pdf The Licensed CAs (LCAs) are listed in Korean at http://www.rootca.or.kr/kor/accredited/accredited02.jsp and http://rootca.kisa.or.kr/kcac/jsp/kcac_2010.jsp Korea Information Certificate Authority Inc (KICA), http://www.signgate.com KICA CPS (Korean): http://www.signgate.com/customer/cus_cps.sg 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 Comment #143: Subordinate CAs chaining to KISA(5 at the moment) are audited every year, there is no possibility that the certificates issued are being used as MITM or "traffic management" of domain names or IPs that the certificate holder does not legitimately own or control. The subordinate CAs are accredited by the government, any action of illegal(dangerous) use of certificate would be accreditation will be cancelled.

	KISA issues the certificate only to the accredited subCAs and not to the third parties. And the accredited subCAs restricted to only issue certificates to domains that they legitimately own or control, and they are specifically not allowed to use their subordinate certificates for the purpose of MITM.
Cross-Signing	None
Requested Trust Bits	Websites Email Code
SSL Validation	OV
EV policy OID(s)	Not requesting EV treatment
CP/CPS	Document Repository: http://www.rootca.or.kr/kor/accredited/accredited02.jsp CPS (Korean): http://www.rootca.or.kr/kor/down/cps15.pdf CPS (English): http://www.rootca.or.kr/kor/down/cps15(en).pdf Electronic Signature Act (English): https://bugzilla.mozilla.org/attachment.cgi?id=594638 Electronic Signature Act (Korean): http://www.law.go.kr/lsSc.do?menuId=0&p1=&subMenu=1&nwYn=1&query=%EC%A0%84%EC%9E%90%EC%84%9C%EB%AA%85%EB%B2%95&x=0&y=0#liBgcolor0 Electronic Signature Act Enforcement Decree (English): https://bugzilla.mozilla.org/attachment.cgi?id=594639 Electronic Signature Act Enforcement Decree (Korean): http://www.law.go.kr/ Electronic Signature Act Enforcement Regulations (English): https://bugzilla.mozilla.org/attachment.cgi?id=594640 Electronic Signature Act Enforcement Regulations (Korean): http://www.law.go.kr/ 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
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 (2009) Need current audit statement. Please explain: Comment #142: KISA claims that "MOPAS audits whether KISA follows its CPS". (See comment No. 108). But I am afraid MOPAS (Ministry of Public Administration and Security) has no expertise to conduct security audit. The

	public servants working in MOPAS have very little or virtually no knowledge of certificate technology. They rely entirely on KISA in matters relating to certification service. In short, KISA's claim is more or less that it audits itself. I do hope that KISA accepts to subject itself to a proper, independent security audit. At a minimum, I wish to see professional credentials of the person from MOPAS who produced an undated statement that MOPAS conducts audits of the CAs under KISA. Does the audit meet Baseline Requirement #17.1? 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 Need current audit statements: 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 LCA audits meet Baseline Requirement #17.5?
Baseline Requirements (SSL)	Comment #147: Our CA operations conform to the CA/Browser Forum's Baseline Requirements for issuance of SSL certificates, and our next audit will include verification of this conformance.
Organization Identity Verification	KISA CPS section 3.2.1 states that verifying the identity of the applicant is performed as prescribed in Provision 3 of Article 13 of the Electronic Signature Law, checking his/her name and resident registration number in accordance with Provision 2:Identity Check Method of Article 13 of the Electronic Signature Law. Electronic Signature Act Enforcement Regulations (English): https://bugzilla.mozilla.org/attachment.cgi?id=594640

	Article 13-3 (Proof of Identity) The proof of identity shall be used in verifying the identity of the name-holder under Article 13-2(1) hereof as follows: <Amended on June 30, 2006 and March 4, 2008> 1. If the name-holder is an individual, a. Where the individual is subject to the issuance of resident registration card, the individual's resident registration card; Provided that if the verification through a resident registration card is not possible, any proof or certificate issued by a central government agency or a local government agency or by a school principal under the Elementary and Secondary Education Act or the Higher Education Act, by which the name can be verified in accordance with Article 13-2(1)-1 hereof; b. Where the individual is not subject to the issuance of resident registration card, any proof issued by a central government agency or a local government agency or by a school principal under the Elementary and Secondary Education Act or the Higher Education Act, by which the name can be verified in accordance with Article 13-2(1)-1 hereof or a certified copy of the record of resident registration of the individual and a proof within the meaning of Item a of this Subparagraph of the individual's legal representative; c. Where the individual resides overseas, the individual's passport or overseas resident card; or d. Where the individual is a foreigner, the individual's alien registration card under the Immigration Control Act; Provided that if no alien registration card is issued, the individual's passport or other proof of identity; 2. A certificated copy of company or commercial registry of the corporation under the Non-Contentious Case Litigation Procedure Act, a certificate of business registration under the Corporate Tax Act, any document in which a tax payment number is assigned under the Income Tax Act or a copy thereof, a certificate of business registration under the Value-Added Tax Act and any document in which an ID number is assigned or a copy thereof; 3. If the name-holder is an organization that is not a corporation, Any proof or documents listed in Subparagraph 1 of this Paragraph by which the identity of the representative of the organization can be verified; Provided that if the organization falls under the proviso to Article 13-2(1)-3 hereof, any document in which the tax payment number or an ID number is assigned or a copy thereof; or 4. If the identity cannot be verified in accordance with Subparagraphs 1 to 3 of this Paragraph, such other confirmation or certificate issued by the relevant authorities or such other proof of identity as determined by the Minister of Public Administration and Safety.
Domain Name Ownership / Control	Digital Signature Certificate Issuing Procedure Guideline for SSL, CodeSigning, and Secure e-Mail (English): https://bugzilla.mozilla.org/attachment.cgi?id=594641 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. Comment #143: in order to issue certificate one has to visit the subordinate CA and must present one's identification card also the application form requiring the data that website or IP is under control. In case of any dangers or the black lists sites requring the certificate will be automatically denied. Do KISA and the LCAs meet Baseline Requirement #11.1.1, regarding authorization by Domain Name Registrant? Do KISA and the LCAs meet Baseline Requirement #11.1.2, regarding authorization for an IP Address?
Email Address Ownership / Control	Digital Signature Certificate Issuing Procedure Guideline for SSL, CodeSigning, and Secure e-Mail (English): https://bugzilla.mozilla.org/attachment.cgi?id=594641 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.
Identity of Code Signing Subscriber	Digital Signature Certificate Issuing Procedure Guideline for SSL, CodeSigning, and Secure e-Mail (English): https://bugzilla.mozilla.org/attachment.cgi?id=594641 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.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL Certs are OV
	• Wildcard DV SSL certificates
	  ○ SSL Certs are OV
	• Email Address Prefixes for DV SSL Certs
	  ○ SSL Certs are OV
	• Delegation of Domain / Email validation to third parties
	  ○ **The LCAs issue end-entity certs, see above.**
	• Issuing end entity certificates directly from roots
	  ○ No

	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ **See 335197-subCA-review.pdf**
	• Distributing generated private keys in PKCS#12 files
	  ○ Not found
	• Certificates referencing hostnames or private IP addresses
	  ○ Not found.
	• Issuing SSL Certificates for Internal Domains
	  ○ **Yes. Comment 124: we not only issue for the internal domains but for the international domains also. – Is this still the case? What types of internal domains do you issue SSL certificates for?**
	• OCSP Responses signed by a certificate under a different root
	  ○ Not applicable.
	• CRL with critical CIDP Extension
	  ○ Fixed, as per Comment 121 and 143.
	• Generic names for CAs
	  ○ CA names include KISA