Bugzilla ID: 471045
Bugzilla Summary: Add "ACEDICOM Root" 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	ACEDICOM
Website URL (English version)	http://acedicom.edicomgroup.com/en/index.htm
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Public corporation
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?)	Europe The Edicom Certification Authority (ACEDICOM) provides companies, communities and physical persons with secure electronic identification mechanisms that enable them to engage in activities where the digital signature replaces the handwritten with identical legal guarantees. To this end, ACEDICOM issues certificates in accordance with the stipulations of Directive 1999/93/EC of 13th December 1999 and Law 59/2003 of 19th December, on electronic signature, and so has sufficient recognition to operate in all countries of the European Union. The Edicom CA is responsible for obtaining the corresponding official authorisation in those places outside the Union where it operates commercially.

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

Info Needed	Data	Status / Notes
Certificate Name	ACEDICOM Root	COMPLETE
Cert summary / comments		To Do
The root CA certificate URL	http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%20Root.crt	COMPLETE
SHA-1 fingerprint.	e0:b4:32:2e:b2:f6:a5:68:b6:54:53:84:48:18:4a:50:36:87:43:84	COMPLETE

Valid from	4/18/2008	COMPLETE
Valid to	4/13/2028	COMPLETE
Cert Version	3	COMPLETE
Modulus length	4096	COMPLETE
CRL • URL • update frequency for end-entity certificates	The URLs of the CRLs are: • Root CRL: http://acedicom.edicomgroup.com/rootca.crl • CRL acedicom01: http://acedicom.edicomgroup.com/acedicom01.crl • CRL acedicom02: http://acedicom.edicomgroup.com/acedicom02.crl 4.9.9. Frequency of issue of CRLS. ACEDICOM will publish a new CRL in the repository at 24 hour intervals maximum, even though no modifications have taken place in the same (changes in certificate status) during said period. This period is not affected in the event of certificate revocations, which already obtain immediate response in the publication by OCSP.	COMPLETE
OCSP Responder URL	The URLs of the OCSP service are: • OCSP acedicom01: http://ocsp.acedicom.edicomgroup.com/acedicom01 • OCSP acedicom02: http://ocsp.acedicom.edicomgroup.com/acedicom02 The Certificate of the OCSP service are: • http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM01_OCSPSignerCertificate.crt • http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM02_OCSPSignerCertificate.crt CPS section 4.10.1: This is an online validation service (Validation Authority, VA) that implements the Online Certificate Status Protocol according to RFC 2560.	Need to test in Firefox, when test URL(s) provided
List or description of subordinate CAs operated by the CA organization associated with the root CA.	From CPS: The Certification Authorities that make up ACEDICOM are: • "ACEDICOM Root" as first level Certification Authority. Its function is to establish the root of the confidence model of the Public Key Infrastructure or PKI. This CA does not issue certificates for end-user entities. • ACEDICOM Root subordinate CAs. Their function is to issue end-user entity certificates for ACEDICOM subscribers.	Is this correct?

	There are two internally-operated subordinate CAs: ACEDICOM 01 http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2001.crt Issues Qualified certificates for identification and advanced electronic signature, for the use of physical persons or legal organisations (known collectively as subscribers) that need to engage in relations with the Public Administrations and other institutions or companies in the Electronic Data Interchange area and/or to equip themselves with certified storage systems. ACEDICOM 02 http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%2002.crt Issues server certificates and other types of certificates for purposes other than "electronic signature".	
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.		Does this root have any subordinate CAs that are operated by third parties?
List any other root CAs that have issued cross-signing certificates for this root CA		Has this root been involved in cross-signing?
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing	Provide the section numbers where text in the CP/CPS 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)for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; b)for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; c) for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf;
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	IV/OV CPS section 3.2.2, Authentication of identity of an entity • Said verification may also be implemented by means of • consultation in the public register • The documentation that is required to carry out the verifications varies based on the type of body for which the certificate is requested. • In all cases, the applicant must accompany the documentation with the	COMPLETE

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 in addition to verifying the domain name. (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.)	"DIGITAL CERTIFICATION SERVICES SUPPLY CONTRACT" which can be downloaded from the ACEDICOM website: http://acedicom.edicomgroup.com • Methods based on registration documentation that were submitted by mandatory physical means will be admitted as indirect means of authentication (TS 101 456). CPS section 3.2.3, Individual identity authentication.	
EV policy OID(s)	Not EV	COMPLETE
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).		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.

• 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.		
CP/CPS	http://acedicom.edicomgroup.com/doc CPS in English: http://acedicom.edicomgroup.com/en/archivos/politicas/ACEDICOM_CertificationPractice.pdf CPS in Spanish: http://acedicom.edicomgroup.com/es/archivos/politicas/ACEDICOM_PracticasCertificacion.pdf Declaration of Certification Practices and Policies according to Certificate Type http://acedicom.edicomgroup.com/en/contenidos/practicasyPoliticas/punto1.htm	Please review the potentially problematic practices listed at http://wiki.mozilla.org/CA:Problematic_Practices. Provide further information for the items that are applicable.
AUDIT		Please see sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/ We need a publishable statement or letter from an auditor (who meets the policy requirements) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of one of:

		• ETSI TS 101 456 • ETSI TS 102 042 • WebTrust Principles and Criteria for Certification Authorities Note that this can be a letter/statement that is posted into bugzilla, and then I will need to do an independent verification of the authenticity of the document by contacting the auditor directly.

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
- 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.
- Verify identity info in code signing certs is that of subscriber
- Make sure it's clear which checks are done for which context (cert usage)
- All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.

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

- Long-lived DV certificates
    - CPS section 6.3.2: The validity period of certificates of end entities will be stipulated by the Certification Policy applicable in each case, and in no case will it exceed four (4) years of maximum validity.
- Wildcard DV SSL certificates
- Delegation of Domain / Email validation to third parties
- Issuing end entity certificates directly from roots
- Allowing external entities to operate unconstrained subordinate CAs
- Distributing generated private keys in PKCS#12 files

    - CPS section 6.1.1: where the generation of the keys is not done by means under control of the end entity, the corresponding Certification Policy will specify the procedure to be used to deliver the private key to the end entities.
- Certificates referencing hostnames or private IP addresses
- OCSP Responses signed by a certificate under a different root
- CRL with critical CIDP Extension
    - CRLs successfully imported into Firefox without error.

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.
- Review Audit to flag any issues noted in the report