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	http://acedicom.edicomgroup.com/en/index.htm
Organizational type	Public corporation
Primary market / customer base	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
Certificate Name	ACEDICOM Root
Cert summary / comments	This root has three internally-operated subordinate CAs. The ACEDICOM 01 subordinate CA issues Qualified certificates for identification and advanced electronic signature, for the use of physical persons or legal organisations. The ACEDICOM 02 subordinate CA issues certificates for purposes other than Qualified electronic signature. The ACEDICOM Servidores subordinate CA issues server/client certificates and code signing certificates.
URL of root cert	http://acedicom.edicomgroup.com/archivos/certificados/ACEDICOM%20Root.crt
SHA-1 fingerprint	e0:b4:32:2e:b2:f6:a5:68:b6:54:53:84:48:18:4a:50:36:87:43:84
Valid from	2008-04-18
Valid to	2028-04-13
Cert Version	3
Modulus length	4096
Test website and certs	https://cartero.edicom.es/RootCertificatePrograms/test.htm
CRL	Root: http://acedicom.edicomgroup.com/rootca.crl acedicom01: http://acedicom.edicomgroup.com/acedicom01.crl (next update 24 hours) acedicom02: http://acedicom.edicomgroup.com/acedicom02.crl (next update 24 hours) ACEDICOM Servidores: http://acedicom.edicomgroup.com/servidoresca.crl (next update 24 hours)

	CPS Section 4.9.9: 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.
OCSP Responder URL	OCSP is available under all the sub-CAs acedicom01: http://ocsp.acedicom.edicomgroup.com/acedicom01 acedicom02: http://ocsp.acedicom.edicomgroup.com/acedicom02 ACEDICOM Servidores: http://ocsp.acedicom.edicomgroup.com/servidores
CA Hierarchy	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. There are three 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 certificates for purposes other than electronic signature. These certificates are not subject to the criteria and procedures required for Qualified certificates, although they do share the whole physical and security infrastructure established for said certificates. ACEDICOM Servidores Issues server/client certificates and code signing certificates as described in the TLS Certificate Policy, http://acedicom.edicomgroup.com/es/archivos/politicas/ACEDICOM%20-%20Politica%20Certificados%20TLS.pdf Specifically, the certificates issued under this policy may contain the following values in the extension extendedKeyUsage: Authentication Server, Client Authentication, Email Protection, MS Smart Card Logon, Internet Key Exchange for IPSEC.
Subordinate CAs operated by third parties…	None. From ACEDICOM: All ACEDICOM CAs are and will be operated by ACEDICOM technical people. There is no subordinate CA operated by third parties.
Cross-signing	None. From ACEDICOM: ACEDICOM hasn't been involved in cross-signing processes.

Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
If SSL: DV, OV, and/or EV	IV/OV CPS section 3.2.2, Authentication of identity of an entity CPS section 3.2.3, Individual identity authentication. Comment #9: For SSL certificates identity/organization is verified also but It's not needed physical validation as on qualified certificates.
EV policy OID(s)	Not EV
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 The following Certification Policies apply to both the ACEDICOM 01 and ACEDICOM 02 sub-CAs: • Certification Policies for Qualified certificates of signature on secure centralised device • Certification Policies for Qualified certificates of signature on secure centralised device for electronic invoicing and certified storage • Identification Policies for Qualified certificates of signature on secure centralised "Smart Card" device • Certification Policies for Qualified certificates of signature on Software Support TLS Certificate Policy (in Spanish): http://acedicom.edicomgroup.com/es/archivos/politicas/ACEDICOM%20-%20Politica%20Certificados%20TLS.pdf Comment #9 in regards to the TLS Certificate Policy: Policy was defined and approved at June 2008. But It was "released" 2009-03-26. I mean, until now no certificate was issued with this policy. ACEDICOM was waiting passing this process to make this policy public, but as It was necessary to issue test certificates we "released" the policy and made it public. The policy was included on the audit process and also the subCA "ACEDICOM Servidores". "ACEDICOM Servidores" was signed by "ACEDICOM Root" at 04/28/08 09:53:40 GMT. You can check this on its certificate. Links to Standards: http://acedicom.edicomgroup.com/en/contenidos/documentacion/enlaces.htm
AUDIT	Audit Type: ETSI 101 456 Auditor: S21sec Auditor Website: http://www.s21sec.com/ Audit Statement: http://acedicom.edicomgroup.com/archivos/pdf/ACEDICOM_s21sec.pdf (2008-09-15) 2009 Audit is in progress, expected to complete in December: https://bugzilla.mozilla.org/attachment.cgi?id=412828

	Comment #9: Audit process by s21 included the root CA and all the level 2 CAs, as described on section "3 ALCANCE DE TRABAJO" ("SCOPE OF THE PROCESS"). Original Text: La propia AC raíz creada por EDICOM, Las Entidades de Certificación de nivel 2. English translation: The root CA created by EDICOM, Level 2 certification authorities. That is: ACEDICOM Root, ACEDICOM 01, ACEDICOM 02, ACEDICOM Servidores were the level 2 CAs at that moment. > From: Antonio Ramos <aramos@s21sec.com> > Subject: RE: Confirming Authenticity of Audit Report for Edicom > To: "'Kathleen Wilson'" <kathleen95014@yahoo.com> > Date: Monday, April 6, 2009, 1:28 AM > Dear Kathleen, > I can confirm you that S21sec has issued the report published in the link you have provided me. Please do not > hesitate to contact me if you need further assistance. > Kind regards, > Antonio Ramos, CISA, CISM, ITIL Found., QSA, Jonah > Director de Unified Management Security Services Additional Audit: There is a private initiative of a voluntary accreditation scheme managed by the "Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones" (ASIMELEC www.asimelec.es), as described at http://ec.europa.eu/information_society/policy/esignature/index_en.htm (Spain section) "s21sec" proposed ACEDICOM to be certified by ASIMELEC. The result can be checked on ACEDICOM web site: http://acedicom.edicomgroup.com/archivos/pdf/081016%20CERTIFICADO%20ASIMELEC%20PSC.pdf
Partial Translation of the TLS Certificate Policy provided by ACEDICOM	Translations provided by ACEDICOM, verified via Google Translate. http://acedicom.edicomgroup.com/es/archivos/politicas/ACEDICOM%20-%20Politica%20Certificados%20TLS.pdf 3.2 INITIAL VERIFICATION OF IDENTITY 3.2.1. Test Methods for possession of the private key. The keys pair associated with certificates through this policy are generated at all times by the applicant using a software or hardware.It is the user who must at all times ensure that private keys are under its control by not using shared computers and using protection mechanisms based on username and password. This policy contains no guidance on the type of device on which they generate and store keys as it is the responsibility of the applicant.

	3.2.2. Proof of identity Is required for the registration of the certificate prove the identity of the certificate to be registered. Specifically, the data in the extensions that identify the subject, referred to in paragraph 3.1.1, must be verified or will not included. The initial verification of the identity of the data required for inclusion in the certificate depends on the subject and the same is as follows: TLS client certificate / email: it will be verified the email address of the applicant, so that once the certificate application process starts, the applicant will get the necessary instructions to continue the same through e-mail address specified in the application and intended to be included in the certificate. TLS server certificates: It is verified that the person or entity controls the Internet domain specified in the CN. Once the certificate application process starts, it will be provided the necessary instructions to continue the same path through the contact (email, phone or physical address) specified in the request and must match the administrative contact list whois the domain. Any other additional information to include in the certificate must be appropriately verified. In any case ACEDICOM reserves the right to require the physical presence of the applicant or person authorized by it in points allowed for registration in order to provide documentation and perform the appropriate checks on identity, as detailed in the Statement of Practice Certification in points 3.2.2 and 3.2.3. 3.2.2.1 Certificates for internal use by ACEDICOM Certificates issued to ACEDICOM personnel and administrative organization, as well as those issued for the infrastructure (servers, email, etc) will no need to save the documentation associated with the validation of identity. 3.3. IDENTIFICATION AND AUTHENTICATION OF APPLICATIONS FOR RENEWAL OF THE KEY. 3.3.1. Identification and authentication of applications for renewal routine. As specified in the certification practice statement (CPS) of the ACEDICOM. 3.3.2. Identification and authentication of applications for renewal of a key after revocation - Key not compromised. The identification and authentication policy for the renewal of a license after a revocation without compromise of the key is the same as for initial registration as described in this document in 3.2.2. so as to ensure reliable and unambiguous manner the identity of the applicant and the authenticity of the request. 3.4. IDENTIFICATION AND AUTHENTICATION OF APPLICATIONS FOR THE KEY REVOCATION The subscriber's certificate may request the revocation proving his identity by: - Sending a document or e-mail signed with the certificate he/she wants to revoke - Using the mechanisms described in section 3.2.2. However, ACEDICOM or any of the entities that comprise the motion may request revocation of a certificate if they had knowledge or suspicion of compromise of the Subscriber's private key, or anything else that would recommend take such action. Shall be grounds for revocation of the certificate of loss of control by the subscriber: The e-mail address included in the client certificate TLS / Email The CN domain associated with the certificate in the case of TLS server certificates.

	6. TECHNICAL SECURITY CONTROLS 6.1. GENERATION AND INSTALLATION OF keypair There is always a reference to the keys generated for certificates issued under the scope of this Certificate Policy. Information on the keys of the entities that make up the Certification Authority is found in paragraph 6.1 of the Certification Practice Statement (CPS) of the ACEDICOM. 6.1.1. Generation of key pair Key pairs for the certificates issued under the scope of this certification policy are generated in the device software that is under the control of the subscriber, usually a browser. The only people who have access to the key signature are owners by possession and protection of the team that made the request. Private keys can be exported and must be protected by the user through mechanisms such as "key word". 6.1.2. Private Key Delivery to Entity The private key is generated by a process initiated by the holder in the device software to it. There isn't any transfer of private key. 6.1.3. Delivery of the public key of the issuer of the certificate The public key to be certified is generated inside the cryptographic software or hardware device by the subscriber and is sent to the PKI ACEDICOM as part of a request in PKCS # 10 format, digitally signed with the private key corresponding to public key certification is sought. 6.1.4. Delivery of the public key of the CA to users As specified in the certification practice statement (CPS) of the ACEDICOM. 6.1.5. Size of the keys The size of the keys to the certificates issued under the scope of this Policy Certification is a minimum of 2048 bits. 6.1.6. Parameters of the public key generation We use the parameters defined in the cryptographic suite 001 specified in the document ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signature ". Signature algorithm Signature algorithm parameters: RSA MinModLen = 2040 Key generation algorithm: rsagen1 Cryptographic method Padding: EMSA-pkcs1-v1_5 Hash function: sha1 6.1.7. Checking the quality of the parameters We use the parameters defined in the cryptographic suite 001 of the document specified in ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signature ". 6.1.8. Hardware / software key generation The key pair is generated in software or hardware device that is in exclusive controlled by the subscriber. The only people who have access to the key signature are owners by possession and protection of the home team. 6.1.9. Purpose of the use of key The keys defined by this policy will be used for purposes described in section 1.3 of this user community and scope.

	The detailed definition of the profile of the certificate and uses the key is in paragraph 7 of this document "Professional license and lists of revoked certificates. It should be noted that the effectiveness of limitations based on extensions of the certificates depends, sometimes the functionality of applications that have not been manufactured or controlled by ACEDICOM.
Domain Name Ownership / Control	TLS Certificate Policy, Section 3.2.2: Proof of identity TLS server certificates: It is verified that the person or entity controls the Internet domain specified in the CN. Once the certificate application process starts, it will be provided the necessary instructions to continue the same path through the contact (email, phone or physical address) specified in the request and must match the administrative contact list whois the domain.
Email Address Ownership / Control	TLS Certificate Policy, Section 3.2.2: Proof of identity TLS client certificate / email: it will be verified the email address of the applicant, so that once the certificate application process starts, the applicant will get the necessary instructions to continue the same through e-mail address specified in the application and intended to be included in the certificate.
Identity of Code Signing Subscriber	TLS Certificate Policy, Section 3.2.2: Proof of identity * Is required for the registration of the certificate prove the identity of the certificate to be registered. Specifically, the data in the extensions that identify the subject, referred to in paragraph 3.1.1, must be verified or will not be included. * Any other additional information to include in the certificate must be appropriately verified. In any case ACEDICOM reserves the right to require the physical presence of the applicant or person authorized by it in points allowed for registration in order to provide documentation and perform the appropriate checks on identity, as detailed in the Statement of Practice Certification in points 3.2.2 and 3.2.3.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are IV/OV. o TLS Certificate Policy, Section 6.3.2: Certificates issued under this policy are valid for 2 years. • Wildcard DV SSL certificates o SSL certs are IV/OV. o TLS Certificate Policy, Section 3.1.7: The wildcards in names are not allowed. Thus, although wildcards, like CN =*.dominio.tld , are common an accepted on the Internet, certificates containing a wildcard will not be issued under this policy. There is one exception: the certificates issued for domains under the control of the organization administering ACEDICOM (see 1.5.1) it may contain wildcards and the ACEDICOM always have control of the domains and subdomains for which the organization administering owns. • Delegation of Domain / Email validation to third parties o ACEDICOM does not delegate Domain / Email validation to third parties

	• Issuing end entity certificates directly from roots
	  o The root only directly issues sub-CAs.
	• Allowing external entities to operate unconstrained subordinate CAs
	  o There are no externally-operated sub-CAs.
	• Distributing generated private keys in PKCS#12 files
	  o TLS Certificate Policy, Section 6.1.1: Key pairs for the certificates issued under the scope of this certification policy are generated in the device software that is under the control of the subscriber, usually a browser. The only people who have access to the key signature are owners by possession and protection of the team that made the request. Private keys can be exported and must be protected by the user through mechanisms such as "key word".
	  o TLS Certificate Policy, Section 6.1.2: The private key is generated by a process initiated by the holder in the device software to it. There isn't any transfer of private key.
	• Certificates referencing hostnames or private IP addresses
	  o Special IP addresses (RFC 3330) are not allowed as a domain name on server certificates, as described on the section 3.1.1 of the TLS Certificate Policy.
	• OCSP Responses signed by a certificate under a different root
	  o ACEDICOM OCSP responses are signed whether using the CA certificate or a certificate issued by the same CA.
	• CRL with critical CIDP Extension
	  o ACEDICOM makes full CRLs.