	ACEDICOM root certificate with Mozilla products		Edición	Página 1/6

The following document tries to respond to all the questions on the "Initial Information Gathering Document " from Mozilla and the comments included on the post "Comment #3 From Kathleen Wilson 2009-03-05 17:38:07 PDT"

In blue the reader can view the requests from Mozilla.

In black there are the responses from ACEDICOM.

### OCSP Responder URL

To test the OCSP service please use the test certificated attached The OCSP URL can be found inside.

---

### List or description of subordinate CAs operated by the CA organization associated with the root.

It's correct but in fact there is another subCA called "ACEDICOM Servidores". We haven't still published it on the web because we were waiting for this Mozilla process to do it. We do not plan to create more subCA, just those three, but can this affect this process. I mean, does Mozilla include the subCA on the trusted certificate store or just the root?

This subCA "ACEDICOM Servidores" was created just to sign server/client certificates

<http://acedicom.edicomgroup.com/es/archivos/politicas/ACEDICOM%20-%20Politica%20Certificados%20TLS.pdf>

---

### 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 subordinate are authorized, controlled, and audited.

All ACEDICOM CAs are and will be operated by ACEDICOM technical people. There is no subordinate CA operated by third parties.

---

### List any other root CAs that have issued cross-signing certificates for the root CA

ACEDICOM hasn't been involved in cross-signing processes.

---

### Request Trust Bits. One or more of: - Websites (SSL/TLS), Email (S/MIME), Code Signing


Sections ----- of the document that demonstrates <http://www.mozilla.org/projects/security/certs/policy/section 7>

**\* 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; →**

Section 3.2.2 of the policy "ACEDICOM - Politica Certificados TLS"

<http://acedicom.edicomgroup.com/es/archivos/politicas/ACEDICOM%20-%20Politica%20Certificados>

Written by	Reviewer by	Aprobado
Raúl Santisteban 03/06/2009	Raúl Santisteban 04/02/2009	

	ACEDICOM root certificate with Mozilla products		Edición	Página 2/6

%20TLS.pdf Partial translation at the end of this document.

**\* 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;**

Section 3.2.2 of the policy "ACEDICOM - Política Certificados TLS".  
<http://acedicom.edicomgroup.com/es/archivos/politicas/ACEDICOM%20-%20Politica%20Certificados%20TLS.pdf> . Partial Translation at the end of this document.

**\* 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;**

Section 3.2.2 of the CPS  
[http://acedicom.edicomgroup.com/en/archivos/politicas/ACEDICOM\\_CertificationPractice.pdf](http://acedicom.edicomgroup.com/en/archivos/politicas/ACEDICOM_CertificationPractice.pdf)

• **for certificates to be used for and marked as Extended Validation, the CA complies with Guidelines for the Issuance and Management of Extended Validation Certificates (as modified by the erratum published by the CAB Forum) (or, for CA requests submitted on or before June 30, 2008, draft 11 of these guidelines), and has its compliance attested to in accordance with the requirements of Section J of that document.**

ACEDICOM doesn't issue at the moment EV certificate

**Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable.**

Find the following example certificates attached:

- SSL Websites. <https://cartero.edicom.es/RootCertificatePrograms/test.htm>
- matormo\_tls\_y\_ad.pem
- edicom\_firmacod\_test.pem

## CP/CPS

**Related to the Problematic Practices described at [https://wiki.mozilla.org/CA:Problematic\\_Practices](https://wiki.mozilla.org/CA:Problematic_Practices),**

- Long-lived DV certificates

The expiration period of domain-validated SSL certificates is 2 years in the worst case, as specified on the section "6.3.2 Periodo de uso para las claves públicas y privadas" of the policy for SSL certificates.


- Wildcard DV SSL certificates

Not applicable. ACEDICOM doesn't issues wildcard DV SSL certificates, as described on section 3.1.7 of the policy "ACEDICOM - Política Certificados TLS".  
<http://acedicom.edicomgroup.com/es/archivos/politicas/ACEDICOM%20-%20Politica%20Certificados%20TLS.pdf> . Partial translation at the end of this document

- Delegation of Domain / Email validation to third parties

ACEDICOM does not delegate Domain / Email validation to third parties

Written by	Reviewer by	Aprobado
Raúl Santisteban 03/06/2009	Raúl Santisteban 04/02/2009	

	ACEDICOM root certificate with Mozilla products		Edición	Página 3/6

- Issuing end entity certificates directly from roots  
"ACEDICOM Root" just issue subCA certificates
- Allowing external entities to operate unconstrained subordinate CAs  
ACEDICOM doesn't delegate any subordinate CA
- Distributing generated private keys in PKCS#12 files  
ACEDICOM never generates private keys for the users. User keys are always generated by the user and then the user sends the certificate sign request, as specified on the following sections of the policy: **6.1.1, 6.1.2, 6.1.3**
- Certificates referencing hostnames or private IP addresses  
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 policy.
- OCSP Responses signed by a certificate under a different root  
ACEDICOM OCSP responses are signed wether using the CA certificate or a certificate issued by the same CA. This can be checked with the sample certificate.
- CRL with critical CDP Extension  
ACEDICOM makes full CRLs.

## AUDIT

ACEDICOM passed on 2008 the first audit on ETSI 101 456. It's planned do it annually.

"S21sec" was the third party company which audited ACEDICOM.

The results of the audit can be reviewed at

[http://acedicom.edicomgroup.com/archivos/pdf/ACEDICOM\\_s21sec.pdf](http://acedicom.edicomgroup.com/archivos/pdf/ACEDICOM_s21sec.pdf)

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](http://www.asimelec.es)), as described at [http://ec.europa.eu/information\\_society/eeurope/2005/all\\_about/security/esignatures/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/2005/all_about/security/esignatures/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>

If English translation from this document is needed please ask for them to ACEDICOM.

Attachments.

At [https://bugzilla.mozilla.org/show\\_bug.cgi?id=471045](https://bugzilla.mozilla.org/show_bug.cgi?id=471045) ACEDICOM has attached the following files:


- matormo\_tls\_y\_ad.pem
- edicom\_firmacod\_test.pem

Partial translation from the main parts of the policy "ACEDICOM - Politica Certificados TLS". Here there is a partial translation of the policy "Politica Certificados TLS", including the two most important sections related to validation. It has been used an automatic translation utility, if some isn't clear or seems to be wrong due the the translation please ask for a more specific translation.

### 3.1.7 Using wildcards in the names

The wilcards 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

Written by	Reviewer by	Aprobado
Raúl Santisteban 03/06/2009	Raúl Santisteban 04/02/2009	

 <b>edicom</b>	ACEDICOM root certificate with Mozilla products		Edición	Página 4/6

administering owns.

.....

### 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.

#### 3.2.2.2 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 KYE 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

Written by	Reviewer by	Aprobado
Raúl Santisteban 03/06/2009	Raúl Santisteban 04/02/2009	

 <b>edicom</b>	ACEDICOM root certificate with Mozilla products		Edición	Página 5/6

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.

Written by	Reviewer by	Aprobado
Raúl Santisteban 03/06/2009	Raúl Santisteban 04/02/2009	

 <b>edicom</b>	<b>ACEDICOM root certificate with Mozilla products</b>		Edición	Página 6/6

#### 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.

Written by	Reviewer by	Aprobado
Raúl Santisteban 03/06/2009	Raúl Santisteban 04/02/2009	