Print this page

# Mozilla - CA Program

## Case Information

| | | | |
|---|---|---|---|
| **Case Number** | 00000077 | **Case Record Type** | CA Owner/Root Inclusion Request |
| **CA Owner/Certificate Name** | EDICOM | **Request Status** | Ready for Public Discussion |

## Additional Case Information

| | | | |
|---|---|---|---|
| **Subject** | Include Renewed EDICOM root | **Case Reason** | |

## Bugzilla Information

| | |
|---|---|
| **Link to Bugzilla Bug** | https://bugzilla.mozilla.org /show_bug.cgi?id=1239329 |

## General information about CA's associated organization

| | | | |
|---|---|---|---|
| **CA Email Alias 1** | acedicom@edicomgroup.com | | |
| **CA Email Alias 2** | | | |
| **Company Website** | http://acedicom.edicomgroup.com /en/index.htm | **Verified?** | Verified |
| **Organizational Type** | Commercial Organization | **Verified?** | Verified |
| **Organizational Type (Others)** | | **Verified?** | Not Applicable |
| **Geographic Focus** | European Union, Global | **Verified?** | Verified |
| **Primary Market / Customer Base** | CAs of Edicom are targeted to private customers, legal or natural person. EDICOM works with companies worldwide and is now the technology provider for B2B communications project development and data integration. | **Verified?** | Verified |
| **Impact to Mozilla Users** | This root will eventually replace the currently included ACEDICOM Root. | **Verified?** | Verified |

## Response to Mozilla's list of Recommended Practices

| | | | |
|---|---|---|---|
| **Recommended Practices** | https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices | **Recommended Practices Statement** | I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below. |
| **CA's Response to Recommended Practices** | 1) Publicly Available CP and CPS: Yes<br>2) CA Hierarchy: Yes<br>3) Audit Criteria: Yes<br>4) Document Handling of IDNs in CP/CPS: No internationalized domain names are allowed at certificates issued by CAEDICOM.<br>5) Revocation of Compromised Certificates: CPS section 4.8<br>6) Verifying Domain Name Ownership: CP section 3.1, 3.2, | **Verified?** | Verified |

3.3
7) Verifying Email Address Control: Challenge-response mechanism
8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable.
9) DNS names go in SAN: Sample certificates have been validated by auditors to check that this requirements are satisfied
10) Domain owned by a Natural Person: Proposal is compatible with actual certificate profile.
11) OCSP: OCSP Server has been checked at the audit process.
12) Network Security Controls: Network Security Controls have been audited against "WebTrust Principles and Criteria SSL Baseline with Network Security – Version 2."

### Response to Mozilla's list of Potentially Problematic Practices

| | | | |
|---|---|---|---|
| **Potentially Problematic Practices** | https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices | **Problematic Practices Statement** | I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below. |
| **CA's Response to Problematic Practices** | 1) Long-lived DV certificates: 2 years, according to CP section 7.1.2.5.<br>2) Wildcard DV SSL certificates: CP section 3.1.7 - Not allowed, with one exception: the certificates issued for domains under the control of the organization administering Edicom it may contain wildcards and Edicom always have control of the domains and subdomains for which the organization<br>3) Email Address Prefixes for DV Certs: Edicom own operators are in charge of domain/e-mail validation requirements described in sections 3.1 , 3.2 and 3.3 of the Policy<br>4) Delegation of Domain / Email validation to third parties:<br>5) Issuing end entity certificates directly from roots: This is not allowed. "CAEDICOM Root" just issue subCA certificates.<br>6) Allowing external entities to operate subordinate CAs: No third party management is considered<br>7) Distributing generated private keys in PKCS#12 files User keys are generated by the user and then the user sends the certificate sign request, as specified on the following sections of the policy 6.1<br>8) 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.<br>9) Issuing SSL Certificates for Internal Domains: Internal Domains are not valid for CAEDICOM certificates, as described on the section 3.1.1 of the policy.<br>10) OCSP Responses signed by a certificate under a different root: OCSP responses are signed by Root certificate<br>11) SHA-1 Certificates: All certificates under this CA tree "CAEDICOM ROOT" -> "CAEDICOM01 " -> "End entity Certificate" use SHA256<br>12) Generic names for CAs: Subject of "CAEDICOM Root" describes perfectly the company<br>13) Lack of Communication With End Users: Different communication channels (website, e-mail, phone) are open for end-users or third party.<br>14) Backdating the notBefore date: No | **Verified?** | Verified |

# Root Case Record # 1

### Root Case Information

| | | | |
|---|---|---|---|
| **Root Certificate Name** | CAEDICOM Root | **Root Case No** | R00000107 |
| **Request Status** | Ready for Public Discussion | **Case Number** | 00000077 |

## Additional Root Case Information

| | |
|---|---|
| **Subject** | Include SHA256 CAEDICOM Root |

## Technical Information about Root Certificate

| | | | |
|---|---|---|---|
| **O From Issuer Field** | EDICOM | **Verified?** | Verified |
| **OU From Issuer Field** | | **Verified?** | Verified |
| **Certificate Summary** | This SHA256 CAEDICOM Root cert will eventually replace the ACEDICOM Root cert that was included via Bugzilla Bug #471045. It will have internally-operated subordinate CAs. | **Verified?** | Verified |
| **Root Certificate Download URL** | https://acedicom.edicomgroup.com/archivos/certificados/CAEDICOMRoot.cer | **Verified?** | Verified |
| **Valid From** | 2014 May 21 | **Verified?** | Verified |
| **Valid To** | 2034 May 21 | **Verified?** | Verified |
| **Certificate Version** | 3 | **Verified?** | Verified |
| **Certificate Signature Algorithm** | SHA-256 | **Verified?** | Verified |
| **Signing Key Parameters** | 4096 | **Verified?** | Verified |
| **Test Website URL (SSL) or Example Cert** | https://rootcertificateprograms.edicom.es/ | **Verified?** | Verified |
| **CRL URL(s)** | http://acedicom.edicomgroup.com/caedicomroot.crl<br>http://acedicom.edicomgroup.com/caedicom01.crl<br>CPS section 4.9.9: CAEDICOM shall publish a new CRL in its repository at maximum intervals of 24<br>hours for subordinate CAs | **Verified?** | Verified |
| **OCSP URL(s)** | http://ocsp.acedicom.edicomgroup.com/caedicomroot<br>http://ocsp.acedicom.edicomgroup.com/caedicom01 | **Verified?** | Verified |
| **Revocation Tested** | https://certificate.revocationcheck.com/rootcertificateprograms.edicom.es<br>no errors | **Verified?** | Verified |
| **Trust Bits** | Email; Websites | **Verified?** | Verified |
| **SSL Validation Type** | OV | **Verified?** | Verified |
| **EV Policy OID(s)** | Not EV | **Verified?** | Not Applicable |
| **EV Tested** | Not requesting EV treatment | **Verified?** | Verified |
| **Root Stores Included In** | Microsoft | **Verified?** | Verified |
| **Mozilla Applied Constraints** | None | **Verified?** | Verified |

## Digital Fingerprint Information

| | | | |
|---|---|---|---|
| **SHA-1 Fingerprint** | 55:9B:BA:7B:0F:FE:80:D6:D3:82:9B:1F:D0:7A:A4:D3:22:19:47:90 | **Verified?** | Verified |
| **SHA-256 Fingerprint** | 15:01:F8:9C:5C:4D:CF:36:CF:58:8A:17:C9:FD:7C:FC:EB:9E:E0:1E:87:29:BE:35:5E:25:DE:80:EB:62:84:B4 | **Verified?** | Verified |

## CA Hierarchy Information

| | | | |
|---|---|---|---|
| **CA Hierarchy** | This root will only issue internally-operated subordinate CAs. Currently one subCA exists, CAEDICOM01. | **Verified?** | Verified |
| **Externally Operated SubCAs** | None, and none allowed according to CPS. | **Verified?** | Verified |
| **Cross Signing** | None. | **Verified?** | Verified |
| **Technical Constraint on 3rd party Issuer** | Edicom own operators are in charge of domain/e-mail validation requirements described in sections 3.1 , 3.2 and 3.3 of the Policy. | **Verified?** | Verified |

## Verification Policies and Practices

| | | | |
|---|---|---|---|
| **Policy Documentation** | Documents are in Spanish and translated into English.<br>CAEDICOM Certification Practices Statement: https://acedicom.edicomgroup.com/en/archivos/politicas_caedicom/1_0/CAEDICOM01%20-%20CertificationPractices.pdf<br>Certification Policies for TLS Server and Client certificate: https://acedicom.edicomgroup.com/en/archivos/politicas_caedicom/1_0/CAEDICOM%20-%20TLS%20Certificates%20Policy.pdf<br>Certification Policies for Qualified certificates of signature for physical person with limited use: https://acedicom.edicomgroup.com/es/archivos/politicas_caedicom/1_0/CAEDICOM01%20-%20PoliticaCertificacionFirmaPersFisica.pdf<br>Certification Policies for Qualified certificates of signature for legal person with limited use: https://acedicom.edicomgroup.com/es/archivos/politicas_caedicom/1_0/CAEDICOM01%20-%20PoliticaCertificacionFirmaPersJuridica.pdf | **Verified?** | Verified |
| **CA Document Repository** | https://acedicom.edicomgroup.com/en/contenidos/practicasyPoliticas/practicasyPoliticas.htm | **Verified?** | Verified |
| **CP Doc Language** | English | | |
| **CP** | https://acedicom.edicomgroup.com/en/archivos/politicas_caedicom/1_0/CAEDICOM%20-%20TLS%20Certificates%20Policy.pdf | **Verified?** | Verified |
| **CP Doc Language** | English | | |
| **CPS** | https://acedicom.edicomgroup.com/en/archivos/politicas_caedicom/1_0/CAEDICOM01%20-%20CertificationPractices.pdf | **Verified?** | Verified |
| **Other Relevant Documents** | | **Verified?** | Not Applicable |
| **Auditor Name** | Auren | **Verified?** | Verified |
| **Auditor Website** | http://www.auren.com/ | **Verified?** | Verified |
| **Auditor Qualifications** | http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx | **Verified?** | Verified |

| | | | |
|---|---|---|---|
| **Standard Audit** | https://cert.webtrust.org/SealFile?seal=1958&file=pdf | **Verified?** | Verified |
| **Standard Audit Type** | WebTrust | **Verified?** | Verified |
| **Standard Audit Statement Date** | 11/3/2015 | **Verified?** | Verified |
| **BR Audit** | https://cert.webtrust.org/SealFile?seal=1958&file=pdf | **Verified?** | Verified |
| **BR Audit Type** | WebTrust | **Verified?** | Verified |
| **BR Audit Statement Date** | 11/3/2015 | **Verified?** | Verified |
| **EV Audit** | Not EV | **Verified?** | Not Applicable |
| **EV Audit Type** | | **Verified?** | Not Applicable |
| **EV Audit Statement Date** | | **Verified?** | Not Applicable |
| **BR Commitment to Comply** | TLS CP section 1.6 | **Verified?** | Verified |
| **SSL Verification Procedures** | TLS CP section 3.2.2: TLS server certificates: Checks will be made to ensure that the applicant person or organization controls the Internet domain indicated in the CN. Once the certificate application process is underway, the necessary instructions to continue will be provided through the contact route (e-mail, telephone or physical address) specified in the request and which must match the administrative contact listed in the Whois of the domain. | **Verified?** | Verified |
| **EV SSL Verification Procedures** | Not requesting EV treatment | **Verified?** | Not Applicable |
| **Organization Verification Procedures** | TLS CP sections 3.1 , 3.2 and 3.3. | **Verified?** | Verified |
| **Email Address Verification Procedures** | TLS CP section 3.2.2: TLS / e-mail client certificates: The e-mail address of the applicant is verified, so that once the certificate application process is initiated, the necessary instructions to continue with the same will be provided via the e-mail specified in the request and to be included in the certificate. ...<br>In the checking processes for ownership of an e-mail address, the e-mail from CAEDICOM will include a random, unique string, to form a challenge. The e-mail recipient will respond to the challenge following the instructions given in the mail. This challenge is unambiguously associated with the certificate issuance application. When the registry operator checks that the answer to the challenge is correct, ownership of the email address is demonstrated, and the certificate validation and issuance process may continue.<br>These e-mail address control or ownership validation processes are mandatory in every request for certificate issuance or renewal | **Verified?** | Verified |
| **Code Signing Subscriber Verification Pro** | Mozilla is no longer accepting requests to enable the Code Signing trust bit, because we plan to remove the Code Signing trust bit in the next version of Mozilla's CA Certificate Policy. | **Verified?** | Not Applicable |
| **Multi-Factor Authentication** | CPS section 5.2. | **Verified?** | Verified |
| **Network Security** | CPS section 6.7 | **Verified?** | Verified |

## Link to Publicly Disclosed and Audited subordinate CA Certificates

| | | | |
|---|---|---|---|
| **Publicly Disclosed & Audited subCAs** | https://acedicom.edicomgroup.com/en/contenidos/certificadosAcedicom/descargaCertificados.htm | **Verified?** | Verified |