Print this page

Mozilla - CA Program

Case Information

Subject	Include Renewed EDICOM root	**Link to Bugzilla Bug**	https://bugzilla.mozilla.org/show_bug.cgi?id=1239329
Case Number	00000077	**Case Record Type**	CA Root Inclusion Request
CA Owner/Certificate Name	EDICOM	**Request Status**	Information Verification In Process

General information about CA's associated organization

CA Email Alias 1	acedicom@edicomgroup.com	**CA Owner Information Verified?**	Data Verified
Company Website	http://acedicom.edicomgroup.com/en/index.htm		
Organizational Type	Commercial Organization		
Geographic Focus	Spain, European Union, Global		
Primary Market / Customer Base	Issues TLS client and server certificates, and electronic signature certificates to individuals and organizations worldwide.		
Recognized CAA Domains	edicomgroup.com		
Problem Reporting Mechanism	http://www.edicomgroup.com/auxiliar/contact.html		

Verification Policies and Practices

Policy Documentation	Documents are in Spanish and translated into English.	**CP/CPS Verified?**	Data Verified
CA Document Repository	https://acedicom.edicomgroup.com/eu/caedicom_en.xml		
Certificate Policy (Link)	https://acedicom.edicomgroup.com/eu/CAEDICOM01_CP_TLSCertificatesPolicy.pdf		
Certification Practice Statement (Link)	https://acedicom.edicomgroup.com/eu/CAEDICOM01_CPS_CertificationPracticeStatement.pdf		
Other Relevant Documents			

Auditor	AENOR INTERNACIONAL, S.A. (Unipersonal)	**Auditor Verified?**	Data Verified
Auditor Location	Spain		
Standard Audit Statement (Link)	https://bugzilla.mozilla.org/attachment.cgi?id=9003448	**Standard Audit Verified?**	Not Verified
Standard Audit Type	ETSI EN 319 411		
Standard Audit Statement Date	4/24/2018		
Standard Audit Period Start Date	6/19/2017		
Standard Audit Period End Date	4/24/2018		
Standard Audit Deviation	☑		
Standard Audit Comments			
Standard Audit ALV Comments	NEED: Audit statements must also be provided in English, per: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy#314-public-audit-information		
BR Audit Statement (Link)	https://bugzilla.mozilla.org/attachment.cgi?id=9003448	**BR Audit Verified?**	Not Verified
BR Audit Type	ETSI EN 319 411		
BR Audit Statement Date	4/24/2018		
BR Audit Period Start Date	6/19/2017		
BR Audit Period End Date	4/24/2018		
BR Audit Deviation	☑		
BR Audit Comments			
BR Audit ALV Comments	NEED: Audit statements must also be provided in English, per: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy#314-public-audit-information		
EV SSL Audit Statement (Link)		**EV SSL Audit Verified?**	Not Applicable
EV SSL Audit Type			
EV SSL Audit Statement Date			
EV SSL Audit Period Start Date			

EV SSL Audit Period End Date	
EV SSL Audit Deviation	
EV SSL Audit Comments	
EV SSL Audit ALV Comments	

Required and Recommended Practices

BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8910216		
Required Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Required Practices Verified?**	Not Verified

CA's Response to Required Practices

1. Publicly Available CP and CPS: CPS section 2.2
1.1 Revision Table, updated annually: CP/CPS page 2

1.2 CAA Domains listed in CP/CPS:
NEED Recognized CAA domains listed in CP or CPS, per
https://wiki.mozilla.org
/CA/Required_or_Recommended_Practices#CAA_Domains_listed_in_CP.2FCPS

1.3 BR Commitment to Comply statement in CP/CPS: CP sections 1.6, 2.2
1.4 CP/CPS Structured According to RFC 3647, No Stipulation requirements:
CPS section 1.1
2. Audit Criteria: CP section 8

2.1 Complete Audit History
NEED: Sequence of audit statements from creation of this root cert, per
https://wiki.mozilla.org
/CA/Required_or_Recommended_Practices#Complete_Audit_History
Also note:
https://www.mozilla.org/en-US/about/governance/policies/security-group/certs
/policy#313-audit-parameters
"Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps)."
This root has validFrom: 5/21/2014
https://bugzilla.mozilla.org/attachment.cgi?id=8707470 - audit period 10/31/2014-10/30/2015
WebTrust CA - https://bugzilla.mozilla.org/attachment.cgi?id=8816896
WebTrust BR - https://bugzilla.mozilla.org/attachment.cgi?id=8841805 - 10/31/2015-10/30/2016
ETSI EN 319 411 - https://bugzilla.mozilla.org/attachment.cgi?id=9003448 - 6/19/2017 - 4/24/2018

So it appears that we do not have audits for this root that cover the audit period 10/31/2016 - 6/18/2017.

3. Revocation of Compromised Certificates: CPS section 4.9.1
4. Verifying Domain Name Ownership: CP section 3.2.2
5. Verifying Email Address Control: CP section 3.2.2
6. DNS names go in SAN: CP section 7.1.2.8
7. OCSP: CPS section 7.4.6

- OCSP SHALL NOT respond "Good" for unissued certs: CPS section 7.4.7
8. Network Security Controls: CPS section 6.7

Forbidden and Potentially Problematic Practices

Forbidden Practices	https://wiki.mozilla.org /CA/Forbidden_or_Problematic_Practices	**Forbidden Practices Verified?**	Data Verified
CA's Response to Forbidden Practices	1. Long-lived Certificates: CP section 1.1 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CP section 3.2.2 3. Issuing End Entity Certificates Directly From Roots: CPS section 1.1 4. Distributing Generated Private Keys in PKCS#12 Files: CP sections 3.2.1, 6.2.3 5. Certificates Referencing Local Names or Private IP Addresses: CP section 3.2.2 6. Issuing SSL Certificates for .int Domains: CP section 3.2.2 7. OCSP Responses Signed by a Certificate Under a Different Root: CPS section 7.4.6 8. Issuance of SHA-1 Certificates: CP section 6.1.6 9. Delegation of Domain / Email Validation to Third Parties: CPS sections 1.3.1, 1.3.2		

Root Case Record # 1

Root Case Information

Root Certificate Name	CAEDICOM Root	**Root Case No**	R00000107
Request Status	Information Verification In Process	**Case Number**	00000077

Certificate Data

Subject	CN=CAEDICOM Root; OU=; O=EDICOM; C=ES
Issuer	
Valid From	2014 May 21
Valid To	2034 May 21
Certificate Serial Number	00FB712658AD99E5
SHA-1 Fingerprint	559BBA7B0FFE80D6D3829B1FD07AA4D322194790
SHA-256 Fingerprint	1501F89C5C4DCF36CF588A17C9FD7CFCEB9EE01E8729BE355E25DE80EB6284B4

Signature Hash Algorithm	SHA256WithRSA
Public Key Algorithm	RSA 4096 bits
SPKI SHA256	9962AB1699B0EB7C7E8A578BC79893042031C1158C633613199A90B9652A2A75
Subject + SPKI SHA256	CBE7775A6CBE4CF278AC73C19D89483BAA0B7AA5ABA1C413BA1F6B1159B2350B

Audits that apply to this Root Certificate

Standard Audit	☑	**Applicable Audits Verified?**	Data Verified
BR Audit	☑		
EV SSL Audit	☐		

Application Information

Explanation	Root renewal	**Application Information Verified?**	Data Verified
Role	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.		
Root Certificate Download URL	https://acedicom.edicomgroup.com/archivos/certificados/CAEDICOMRoot.cer		

Mozilla Fields

Mozilla Trust Bits	Email; Websites	**Mozilla Fields Verified?**	Data Verified
SSL Validation Type	OV		
Mozilla EV Policy OID(s)	Not EV		
Mozilla Applied Constraints	None		

CA Hierarchy Information

Cross-Signed by another Root Cert?	☐	**PKI Hierarchy Verified?**	Not Verified

Has Externally Operated SubCAs?	☐
CP/CPS allows Ext Operated SubCAs?	☐
Has External Registration Authorities?	☐
CP/CPS allows External RAs?	☐
Description of PKI Hierarchy	This root will only issue internally-operated subordinate CAs.
Constraints on External SubCAs & RAs	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.

Test Websites or Example Cert

Test Website - Valid	https://rootcertificateprograms.edicom.es/	**Test Websites Verified?**	Not Verified
Test Website - Expired	https://rootcertificateprogramsexpired.edicom.es/		
Test Website - Revoked	https://rootcertificateprogramsrevoked.edicom.es/		
Test Notes	NEED: Fix Revoked and Expired test websites. Currently they result in Error code: SSL_ERROR_BAD_CERT_DOMAIN The certificate is only valid for rootcertificateprograms.edicom.es.		

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	https://certificate.revocationcheck.com/rootcertificateprograms.edicom.es no errors	**Test Results Verified?**	Not Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=14975&opt=cablint,zlint,x509lint&minNotBefore=2014-05-21 NEED: Resolve Error ERROR: The Subject Alternate Name extension MUST contain only 'dnsName' and 'ipaddress' name types. https://crt.sh/?id=13492318&opt=zlint		
Test Website Lint Test	https://crt.sh/?caid=15530&opt=cablint,zlint,x509lint&minNotBefore=2014-05-21 NEED: Resolve Errors found by the		

	lint tests.
EV Tested	Not requesting EV treatment